Revision 06/2

NRC Digital System Research Plan
FY 2005 – FY 2009

Instrumentation and Electrical Engineering Branch
Division of Fuel, Engineering and Radiological Research
Office of Nuclear Regulatory Research

ABSTRACT

The NRC Digital System Research Plan for FY 2005 – FY 2009 defines a coherent set of research programs that support the regulatory needs of the U.S. Nuclear Regulatory Commission (NRC), Office of Nuclear Material Safety and Safeguards (NMSS), Office of Nuclear Reactor Regulation (NRR), and Office of Nuclear Security and Incident Response (NSIR). These program definitions describe the background and technical issues, as well as the research tasks and products that will create a combination of environmental qualification assessment processes, review procedures, reliability assessment capabilities, security assurance processes, and associated acceptance criteria. Additionally, the research programs will develop training curricula to enable the staff to use the research products consistently and efficiently. Together, these research products will complement existing risk-informed regulatory activities governing the safe and secure use of digital systems in U.S. nuclear facilities and applications.

CONTENTS

Tables

Figures

Revision 06/2

EXECUTIVE SUMMARY

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 U.S. Nuclear Regulatory Commission (NRC), Office of Nuclear Material Safety and Safeguards (NMSS), Office of Nuclear Reactor Regulation (NRR), and Office of Nuclear Security and Incident Response (NSIR). These program definitions describe the background and technical issues, as well as the research tasks and products that will create a combination of environmental qualification assessment processes, review procedures, reliability assessment capabilities, security assurance processes, and associated acceptance criteria. Additionally, the research programs will develop training curricula to enable the staff to use the research products consistently and efficiently. Together, these research products will complement existing risk-informed regulatory activities governing the safe and secure use of digital systems in U.S. nuclear facilities and applications.

Background

NRC regulations set forth in Title 10 of the *Code of Federal Regulations* (10 CFR), "Energy," require that safety systems in nuclear facilities and nuclear materials applications must be of sufficient quality to provide reasonable assurance that the facilities and materials applications will be used without undue risk to public health and safety, the environment, or the Nation's security. The mission of the NRC is to enforce these regulations and thereby protect public health and safety, the environment, and the Nations' security. Toward that end, the purpose of NRC research is to provide products that support the agency's regulatory activities. These products include, for example, technical bases for rules, licensing guidance included in standard review plans, regulatory guides, NUREG-series reports that provide additional guidance for NRC licensing and inspection staff, and review procedures.

In recent years, nuclear facility and byproduct licensees have begun replacing their analog instrumentation and control (I&C) safety systems and equipment with digital systems and equipment. These analog-to-digital upgrades are largely driven by the fact that (1) analog replacement parts are becoming increasingly difficult to obtain, and (2) digital systems offer better performance and additional features compared to analog systems.

While digital technology has the capability to improve operational performance, the introduction of this technology into nuclear facilities and applications poses a variety of challenges for the NRC and the nuclear industry. In particular, these challenges include (1) the increased complexity of digital technology compared to analog technology; (2) rapid changes in digital technology that require the NRC to update its knowledge of the state-of-the-practice in digital system design, testing, and application; (3) new failure modes associated with digital technology; and (4) the need to update the acceptance criteria and review procedures used in consistently assessing the safety and security of digital systems. Above all, it is important to recognize that the failure mechanisms associated with digital technology systems are different from those associated with analog technology systems. For example, protection logic provided by relay-based analog systems may be implemented in a digital system with software logic. Thus, in an analog system, a relay failure will affect only a single channel of the protection logic; however, in a digital system that emulates analog relay logic, a software fault could affect all channels of the protection system.

The Digital Safety System Research Plan

The NRC's 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, this Research Plan describes the background, technical issues, and ongoing and planned activities to meet the challenges of regulating the implementation of digital technologies in nuclear facilities.

Research activities supporting the regulation of digital technologies are classified as follows:

- Address system aspects of digital technology that can affect safety.
- Identify software quality assurance attributes that can affect safety.
- Evaluate digital system reliability to determine digital system contributions to risk.
- Address aspects of digital systems that can affect security, and thereby affect safety.
- Update regulatory practices in response to emerging technologies.
- Address issues arising from the use of new technologies in advanced reactor designs.
- Incorporate research results into NRC regulations, licensing, and inspection guidance.

In addition to supporting these regulatory activities for digital technologies, RES conducts the following activities to support the NRC staff's regulatory activities across a broad spectrum of disciplines and topics:

- Participate in developing and endorsing national and international standards as a means of providing regulatory guidance and acceptance criteria.
- Maintain research resources and manage the NRC's base of knowledge.
- Optimize the use of limited research resources through collaborative and cooperative research programs with other research organizations such as universities, industries, and other countries.

Research Plan Programs

This 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. Additionally, this Research Plan describes activities that support the development of regulatory guidance, maintenance of the NRC's research infrastructure and base of knowledge, and collaborative and cooperative development of supporting research products. The following discussion summarizes the research projects in each research program, as well as the generic research activities that are applicable to each area of research.

Revision 06/2

System Aspects of Digital Technology

System aspects of digital technology involve those internal and external factors that affect the performance of a digital system as a whole. This research program will address aspects of digital systems that can adversely affect safety, and will acquire or develop applicable technical information, guidance, tools, review procedures, and training to augment the NRC staff's capabilities to perform in-depth and realistic technical evaluations of digital safety system designs. The following research projects address the system aspects of digital technology:

- Environmental Stressors
- System Communications
- Commercial off-the-Shelf (COTS) Digital Systems
- Electrical Power Distribution Interactions with Nuclear Facilities
- Total Harmonic Distortion Effects on Digital Systems
- Operating Systems
- Diversity and Defense-in-Depth

Software Quality Assurance

Software quality assurance (SQA) is a planned and systematic pattern of actions necessary to provide confidence that a digital system conforms to established technical requirements. While the NRC currently has a set of digital system quality assurance guidelines, implementing these guidelines is resource-intensive for both the NRC and the industry. In addition, there is no set of regulatory guidance; acceptance criteria; and review tools, methodologies, and procedures that address self-testing features in digital systems. This could lead to inconsistencies in the amount of self-testing that is appropriate for use in safety-related digital systems. Further, additional effectiveness and consistency may be gained by augmenting the NRC's existing SQA processes with additional tools and review procedures. The following research projects will address the development of regulatory guidance; acceptance criteria; review tools, methodologies, and procedures; and associated training to enable the NRC to confirm that safety-related digital systems have an acceptable level of quality:

- Assessment of Software Quality
- Digital System Dependability
- Self-Testing Methods

Risk Assessment of Digital Systems

As discussed in the NRC's Policy Statement on Probabilistic Risk Assessment (PRA), the agency intends to increase its use of PRA methods in all regulatory matters to the extent supported by state-of-the-art PRA methods and data. Currently, I&C systems are not generally modeled in PRAs. As the NRC moves toward a more risk-informed regulatory environment, the staff will need data, methods, and tools related to the risk assessment of digital systems. The following research projects will address risk assessment of digital systems:

- Development and Analysis of Digital I&C Failure Data
- Development of Digital System Failure Assessment Methods
- Identification of Digital System Characteristics Important to Risk
- Development of Digital System Reliability Assessment Methods

Security Aspects of Digital Systems

Security of digital safety systems involves addressing potential security vulnerabilities as part of the system development process, and maintaining 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 should be performed on the systems (composed of COTS digital equipment) that have been developed using these platforms.

In addition to cyber-attack threats in existing digital systems (i.e., viruses, hackers, etc.), other threats to digital systems important to safety arise from the application of technologies that can introduce new system vulnerabilities. For example, electromagnetic (EM) attacks from high-energy radiofrequency devices (HERF attacks) might be used to physically damage digital equipment, while low-energy radiofrequency devices (LERF attacks) might be used to disrupt digital equipment operations by overwhelming the digital computers with concentrated EM energy. In either case, cyber or EM attacks may cause a safety system to fail or to operate at an inappropriate time, or cause an operator to respond inappropriately to erroneous signals or indications. As another example, the use of communications technologies and networks may provide unauthorized access to safety system networks and networks of systems that could cause a safety system to operate inappropriately or a nuclear facility operator to respond inappropriately to erroneous signals or indications.

The following research projects will address the security aspects of digital systems:

- Security Assessments of Cyber-Vulnerabilities
- Security Assessments of EM Vulnerabilities
- Network Security

Emerging Digital Technology and Applications

New innovations in digital technology (e.g., hybrid control rooms and smart transmitters) have the potential to improve both operating efficiency and safety in existing and advanced nuclear facility designs. The NRC's regulatory staff requires knowledge about emerging these technologies and applications to make timely decisions as they are introduced into the nuclear industry. Research addressing emerging digital technologies and applications will provide the staff with technical information and criteria for use in making appropriate regulatory decisions. This is particularly important because state-of-the-art implementations of existing technologies in new applications could introduce new challenges to safety and security that may not be addressed by other research activities. Additionally, new research projects will be created to address new safety concerns that may arise. The following research projects are planned for this research program:

- System Diagnosis, Prognosis, and Online Monitoring (SDPM)
- Radiation-Hardened Integrated Circuits
- Advanced Instrumentation and Controls
- Smart Transmitters
- Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs)
- Wireless Technology

Revision 06/2

Advanced Nuclear Power Plants (NPPs)

The new generation of advanced NPP designs is expected to have fully integrated digital control rooms and use a much higher degree of automation. The use of multiple modular NPPs also may require more complex control of both the primary I&C systems and all of the support systems, including the switch yard. Research programs will be developed to address issues as design information becomes available on advanced NPP designs. At this time, the following research projects are being developed to address advanced NPP reviews that are currently in progress:

- Advanced NPP Instrumentation
- Advanced NPP Controls and Highly Integrated Control Room Designs
- Advanced NPP Digital System Risk

Additional Research-Related Activities

The NRC conducts research-related activities to develop regulatory guidance on the basis of best practices described in national and international consensus standards, in addition to research activities that are focused on specific issues such as environmental stressors, software quality assurance, security, etc. To ensure that the agency's regulatory requirements are adequately represented in these standards, the NRC actively participates in the consensus standards development process.

In addition to developing standards-based regulatory guidance, the NRC maintains technical (human) resources capable of reviewing advances in emerging technologies that have potential for use by the nuclear industry. These technical resources are most effectively developed through continuing participation in national and international technical meetings, conferences, and training. Additionally, maintaining the research infrastructure and managing the NRC's base of knowledge through continuing research ensures that current capabilities are available and adaptable to support future needs as the nuclear industry continues to employ more advanced digital systems.

Given the breadth of research proposed in this Research Plan, the use of personnel, material, and financial resources must be optimized to obtain the maximum benefit from the research programs. The effective use of limited research resources is augmented by contributing NRC resources to collaborative and cooperative research projects that are funded in part by the NRC and by other organizations such as academic centers of excellence and international research groups.

Conclusion

The research programs described in this Research Plan are designed to develop a combination of quality assurance evaluation procedures, reliability assessment capabilities, environmental qualification processes, and security evaluation capabilities for digital systems to complement existing requirements regulating safety system designs, performance, and security. Additional research activities support development of regulatory guidance; maintenance of NRC research infrastructure; and collaborative and cooperative research programs. Much of the research described in this Research Plan is applicable to every area of regulation, regardless of the issue or technology being investigated.

This Research Plan is a living document, in that it will periodically be reviewed and revised, as needed, in the current environment of emerging technologies and state-of-the-art implementations of existing technologies. Participation in standards development activities and collaborative research programs will also ensure that the NRC keeps pace with digital technology advances and standard practices as new digital applications become viable alternatives to existing control systems in the U.S. nuclear industry.

The products of the research programs described in this Research Plan will augment the NRC's capabilities to regulate the use and management of radioactive materials and nuclear fuels for beneficial civilian purposes in a manner that protects the health and safety of the public and the environment; promotes the security of our Nation; and provides for regulatory actions that are open, effective, efficient, realistic, and timely.

ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
ANS	American National Standard
ANSI	American National Standards Institute
AOO	Abnormal Operating Occurrence
ASCAP	Axiomatic Safety-Critical Assessment Process
ASP	Accident Sequence Precursor
ASTM	American Society for Testing and Materials
ATWS	Anticipated Transient Without Scram
B&W	Babcock and Wilcox
BTP	Branch Technical Position
CCF	Common-Cause Failure
CFR	*Code of Federal Regulations*
CIA	Central Intelligence Agency
CMF	Common-Mode Failure
COTS	Commercial Off-the-Shelf
CPU	Central Processor Unit
CRSCE/SAL	Center of Railroad Safety-Critical Excellence, Safety Assessment Lab
CSCS	Center for Safety-Critical Systems (UVa)
CSNI	Committee on the Safety of Nuclear Installations
D3	Defense-in-Depth and Diversity
DBA	Design-Basis Accident
DCSS	Dry Cask Storage System
DNB	Departure from Nucleate Boiling
DoD	U.S. Department of Defense
DRAM	Dynamic Random Access Memory
DSSS	Direct Sequence Spread Spectrum
EDF	Électricité de France
EDG	Emergency Diesel Generator
EGDIC	Expert Group on Digital Instrumentation and Control
ELDR	Enhanced Low Dose Rate
EM	Electromagnetic
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPR	Evolutionary Power Reactor
EPRI	Electric Power Research Institute
FCF	Fuel Cycle Facility
FRA	Federal Railroad Administration
FY	Fiscal Year
GDC	General Design Criterion

HDD	Hard Disk Drive
HERF	High-Energy Radiofrequency
HRP	Halden Reactor Project
I&C	Instrumentation and Control
IC	Integrated Circuit
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INES	International Nuclear Event Scale
IP	Inspection Procedure
IPRACIT	International Partnership for Research on Advanced Control and Instrumentation Technologies
IROFS	Items Relied on for Safety
ISA	Instrument Society of America (or Integrated Safety Analysis)
ISFSI	Independent Spent Fuel Storage Installation
ISG	Interim Staff Guidance
IW	Intelligence Warfare
JCN	Job Control Number
LER	Licensee Event Report
LERF	Low-Energy Radiofrequency
LLNL	Lawrence Livermore National Laboratory
LOOP	Loss of Offsite Power
MRS	Monitored Retrievable Storage
MTTHE	Mean Time to Hazardous Event
NAS	National Academy of Sciences
NASA	National Aeronautics and Space Administration
NFPA	National Fire Protection Association
NMSS	Office of Nuclear Material Safety and Safeguards (NRC)
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
NRR	Office of Nuclear Reactor Regulation (NRC)
NSIR	Office of Nuclear Security and Incident Response (NRC)
OECD/NEA	Organization for Economic Cooperation and Development, Nuclear Energy Agency
ORNL	Oak Ridge National Laboratory
OSI	Open Systems Interconnect
OSU	Ohio State University
QA	Quality Assurance

PLC	Programmable Logic Controller
PPC	Plant Process Computer
PRA	Probabilistic Risk Assessment
PSU	Pennsylvania State University
RAM	Random Access Memory
RES	Office of Nuclear Regulatory Research (NRC)
RF	Radiofrequency
RFI	Radiofrequency Interference
RFID	Radiofrequency Identification
RG	Regulatory Guide
RHA	Radiation-Hardness Assurance
RPS	Reactor Protection System
RTD	Resistive Temperature Detector
SAR	Safety Analysis Report
SCADA	Supervisory Control and Data Acquisition
SDPM	System Diagnosis, Prognosis, Online Monitoring
SEE	Single-Event Effect
SELab	Halden Reactor Project Software Engineering Laboratory
SER	Safety Evaluation Report
SFDSF	Spent Fuel Dry Storage Facility
SFPO	Spent Fuel Project Office
SI	Safety Injection
SoC	System on a Chip
SPACE	Specification and Coding Environment (Teleperm XS)
SPDS	Safety Parameter Display System
SQA	Software Quality Assurance
SRP	Standard Review Plan
SRAM	Static Random Access Memory
THD	Total Harmonic Distortion
UMd	University of Maryland
UT	University of Tennessee
UVa	University of Virginia
V&V	Verification and Validation
VHDL	Very High-Speed Integrated Circuit Hardware Description Language

1 INTRODUCTION

The NRC Digital System Research Plan for FY 2005 – FY 2009 (the Research Plan) is an update to the "NRC Research Plan for Digital Instrumentation and Control" [see Accession #ML012080254 in the NRC's Agencywide Documents Access and Management System (ADAMS)], which the Office of Nuclear Regulatory Research (RES) provided to the Commission as an attachment to SECY-01-0155 (ML011990569), dated August 15, 2001, for Fiscal Year (FY) 2000 through FY 2004. The Research Plan defines the research programs, projects, and tasks that are planned for FY 2005 through FY 2009. In so doing, the Research Plan describes the technical issues and ongoing and planned activities to meet the challenges of implementing digital technologies in nuclear industry safety systems.

1.1 Background

In recent years, nuclear facility and byproduct licensees have begun replacing their analog instrumentation and control (I&C) safety systems and equipment with digital systems and equipment. These analog-to-digital upgrades are largely driven by the fact that (1) analog replacement parts are becoming increasingly difficult to obtain, and (2) digital systems offer better performance and additional features compared to analog systems.

While digital technology has the capability to improve operational performance, the introduction of this technology into nuclear facilities and applications poses a variety of challenges for the NRC and the nuclear industry. In particular, these challenges include (1) the increased complexity of digital technology compared to analog technology; (2) rapid changes in digital technology that require the NRC to update its knowledge of the state-of-the-practice in digital system design, testing, and application; (3) new failure modes associated with digital technology; and (4) the need to update the acceptance criteria and review procedures that are used in consistently assessing the safety and security of digital systems. Above all, it is important to recognize that the failure mechanisms associated with digital technology systems are different from those associated with analog technology systems. For example, protection logic provided by relay-based analog systems may be implemented in a digital system with software logic. Thus, in an analog system, a relay failure will affect only a single channel of the protection logic; however, in a digital system that emulates analog relay logic, a software fault could affect all channels of the protection system. Failure to adequately address these challenges in other industries (e.g., aviation, medical, and rail) has resulted in mishaps and near mishaps.

Moreover, some digital systems require significant effort by developers and independent assessors to gain assurance that use of the digital systems in safety systems will be in accordance with system and regulatory requirements. In the case of software quality assurance, the state-of-the-practice calls for many acceptance criteria to be confirmed during system development. Some of these acceptance criteria are subjective in nature, which could produce a sense of uncertainty in licensing arenas because the developers must depend more upon their own engineering judgment for determining when software is of sufficient quality, rather than using objective measures.

Recent advancements in software engineering hold promise for replacing or augmenting some subjective acceptance criteria with objective acceptance criteria. In so doing, developers could have more assurance that their software meets required acceptance criteria. Reducing uncertainty by using objective acceptance criteria reduces the burden of potentially over-proving a digital system. Reducing the burden of proof allows the system developer to devote more of their limited resources to other quality and security assurance activities, thereby potentially improving the reliability and safety of the digital system. By updating NRC requirements on the basis of state-of-the-art methods, the research programs described in this Research Plan can enable application of acceptance criteria to be more consistent and more technology neutral.

In the early 1990s, the NRC began developing guidance to support the review of digital systems in nuclear power plants (NPPs). Toward that end, the NRC commissioned the National Academy of Sciences (NAS), National Research Council, to review issues associated with the use of digital systems. In its report, entitled "Digital Instrumentation and Control Systems in Nuclear Power Plants," the National Research Council made several recommendations, including the need to develop a research plan that would balance short-term regulatory needs and long-term anticipatory research needs.

Additionally, the NRC's Advisory Committee on Reactor Safeguards (ACRS) has actively followed the ever-increasing use of digital systems and addressed the need for further research in the area of digital technology. In its 1998 report, entitled "Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program," the ACRS stated the following guidance:

> Although the basic framework for regulation and safety review of digital systems is established in the update to Chapter 7 of the SRP [Standard Review Plan] in July 1997, numerous issues remain. These issues must be addressed so that NRC can effectively regulate and review safety systems employing this rapidly evolving technology. Vulnerabilities of digital systems are different than analog systems. Failure probabilities and the failure characteristics of these systems are also different. Appropriate methods to include digital and software systems in PRAs [Probabilistic Risk Assessments] do not exist. Quality control and quality assurance expectations are not compatible with the use of commercial off-the-shelf hardware and software even though there may be excellent justification in terms of reliability for the use in commercial systems. There can be little doubt then that NRC line organizations will need substantial specialized engineering and research support to deal with the safety regulation of digital systems.

This guidance provided additional impetus from which NRC research addressing the unique features of digital systems has been conducted through FY 2004, as described in the NRC Research Plan for Digital Instrumentation and Control for FY 2000 – FY 2004.

1.2 Safety-Significant Considerations

While digital systems promise many potential benefits in terms of operational performance, reliability, and safety, the introduction of this technology into safety system applications poses a variety of challenges for the NRC and the nuclear industry. For example, rapid technological changes in the digital industry could adversely affect safety because digital technology applications are generally more complex than corresponding analog technology applications, and their operation and failure modes are more difficult to characterize.

These challenges require the NRC to maintain its knowledge of the state-of-the-practice in digital systems design, testing, application, and licensing and to develop more risk-informed performance-based regulatory guidance. The following four examples illustrate the broad range of failure mechanisms that have occurred as a result of inappropriately implementing digital safety systems:

(1) Some of the most serious computer-related accidents in the nuclear industry have involved medical radiation therapy misadministrations by a computer-controlled radiation therapy machine. Between June 1985 and January 1987, there were six events in the United States and Canada in which software architecture errors caused Therac-25 radiation therapy machines to overdose patients (Leveson, 1995). These accidents included the following causal factors:

- failure to perform a software safety analysis (i.e., incomplete requirements analysis) although almost full responsibility for safety relied on that analysis
- assuming the software was safe because it worked successfully in thousands of tests before overdosing a human (i.e., equating safety with reliability)
- failure to provide self-test, error detection, and error handling software features that could have indicated the existence of a problem well before the system operated catastrophically; this included failure to include defense-in-depth in the design (e.g., protection against faults in the software and hardware)

(2) The next example is a potentially serious event that occurred on November 3, 1994, at Turkey Point Station Unit 3 [NRC Licensee Event Report (LER) 94-005-02]. In that event, the Unit 3 emergency diesel generator (EDG) load sequencer failed to respond to a Unit 4 safety injection (SI) test signal that required a transfer of the Unit 3 SI pumps to the Unit 4 SI system. The failure was caused by a defect in the load sequencer software logic. That defect could prevent any or all of the four load sequencers from responding to input signals. The problem arose in trying to design the sequencers so that if a “real” emergency signal is received while the sequencer is being tested, the test signal would clear and the engineering safety features controlled by the sequencer would be activated.

As originally implemented, an SI signal received 15 seconds or later into particular self-test scenarios cleared the test signal but did not clear the inhibit signal latching logic that prevented actuation of selected equipment. The self-test signal initiated the latching logic, but an input signal incorrectly maintained the latching logic if the signal arrived prior to removal of the self-test signal. Thus, if a real signal arrived more than 15 seconds into the self-test scenario, the test signal cleared but the inhibit logic remained locked and prevented actuation of the SI signal. As a result of erroneous inhibit signals, any sequencer output could have been blocked. The specific outputs that could be blocked are determined by a combination of factors, including which self-test scenario was executing, the length of time the test was running, and which other inputs were received.

The designer and independent verifier of the load sequencer control logic both failed to recognize the interactions between the inhibit logic and the self-test logic. Additionally, an independent assessment team found that the software verification and validation (V&V) activity was not comprehensive enough to test certain aspects of the logic. In its review, the NRC staff indicated that the software V&V plan relied almost exclusively on testing, and lacked the analysis of both software requirements and software design that could have identified the design flaw.

(3) More recently, on January 21, 2002, cascading I&C failures at the Électricité de France (EDF) Flamanville-2 nuclear power plant contributed to an event that rated Level 2 on the International Nuclear Event Scale (INES) (*Nucleonics Week*, 2002). The INES event ratings range from 0 to 7, with 7 being the most severe. The sequence began following a maintenance error during replacement of obsolete components in inverters on the electrical panel that supplies the "A" train of the plant's I&C system. A qualification test revealed the error, but when operators tried to manually restart the inverters, the action caused spurious control system commands to isolate external power to the "A" train. Operators were unable to switch to backup power or start the "A" EDG. As a result, all redundant power supplies to the "A" train were lost. The Flamanville-2 event is an example of how an apparently small design or maintenance error in complex digital systems can lead to a common-cause failure (CCF) of redundant safety features.

(4) As a final example, on January 25, 2003, a computer network server on the plant network of the Davis-Besse Nuclear Power Station was infected with the SLAMMER MS-SQL server worm [USNRC Information Notice (IN) 2003-14]. Both the business network and the plant network were affected by the worm. As a consequence, large amounts of data were sent onto the plant site networks (a "denial of service" attack). The large amounts of data caused many of the plant site computers to cease communicating with other computers on the networks. The resulting slow network response was initially noticed around 9:00 a.m. on the business network. It was not until after 4:00 p.m. that degraded computer response time was noticed on the plant network. The Safety Parameter Display System (SPDS) became unavailable at 4:50 p.m., and the Plant Process Computer (PPC) became unavailable at 5:13 p.m. The unavailability of the SPDS and PPC placed additional burden on the reactor operators. The Davis-Besse event is an example of how a failure to adequately implement cyber security procedures can adversely affect nuclear facility operations and system reliability.

The above four events illustrate (1) the range of digital system failure mechanisms that can adversely affect nuclear facility and equipment operations, (2) the necessity for a broad-based approach to digital system reviews that addresses all aspects of digital system development, and (3) the need to develop risk-informed performance-based guidance that will be less susceptible to rapidly changing technologies.

1.3 Regulatory Bases Underlying the Scope of the Research Plan

The scope of the NRC Research Plan for Digital Instrumentation and Control for FY 2000 – FY 2004 was to support regulatory oversight of the nuclear power industry. Toward that end, the FY 2000 – FY 2004 Plan addressed development of criteria and methods for failure mode and reliability assessment of digital I&C systems in NPP safety systems.

With this updated Research Plan, the RES staff is expanding the scope beyond supporting NRR to include NMSS and NSIR. The justification for expanding the scope of the Research Plan is found in 10 CFR 1.11(b), "The Commission," which states that the Commission is responsible for licensing and regulating nuclear facilities and materials, and conducting research in support of licensing and regulatory processes. These responsibilities include regulating the following:

- NPP safety systems
- fuel fabrication facilities
- nuclear materials security systems
- independent spent fuel storage installations (ISFSIs)
- monitored retrievable storage (MRS) facilities
- high- and low-level waste disposal sites
- medical applications of radioactive sources
- industrial applications of radioactive sources

The NRC's regulations and review guidance provide qualitative acceptance criteria for review of digital I&C systems that are important to safety in fuel fabrication facilities, spent fuel and high-level waste storage installations, NPPs, and byproduct materials manufacturing and utilization facilities. Nonetheless, specific objective acceptance criteria are still being developed for digital systems. The rapid evolution of digital I&C system technologies requires the NRC to take a proactive role in formulating specific objective acceptance criteria to augment existing qualitative (but often subjective) criteria for approving digital systems used to monitor and control processes and activities that are important to safety in these nuclear facilities.

The following discussions summarize the regulatory bases underlying digital systems research that supports the NRC's regulatory activities throughout the nuclear industry.

1.3.1 Nuclear Power Plants

Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," of NUREG-0800, "Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants" (NPP SRP, ML033580677), describes the review process for NPP safety systems and systems important to safety. These review processes reference applicable sections of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants."

The NPP SRP provides guidance regarding reviews of digital systems. The scope of the guidance is extensive, addressing all aspects of digital system reviews. The guidance, however, could be augmented by incorporating specific procedures for reviewing digital systems, and by adding additional objective acceptance criteria for concluding that a digital system is acceptable for use in a safety system application.

1.3.2 Fuel Cycle Facilities

NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility" (FCF SRP, ML020930033), specifies that the description of the processes analyzed as part of the integrated safety analysis [ISA, 10 CFR 70.62(c)(1) (i–v)] is considered acceptable if it describes the features in sufficient detail to permit an understanding of the theory of operation, and to assess compliance with the performance requirements of 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," Subpart H, "Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material," §70.61, "Performance Requirements."]

The FCF SRP states that, for systems in general, a description at a systems level is acceptable, provided that it permits the NRC reviewer to adequately evaluate (1) the completeness of the hazard and accident identification tasks, and (2) the likelihood and consequences of the accidents identified. The FCF SRP does not distinguish between analog-based items relied on for safety (IROFS) and digital-based IROFS. Moreover, the FCF SRP does not objectively define the level of detail that is considered acceptable.

1.3.3 Dry Cask Storage Systems

NUREG-1536, "Standard Review Plan for Dry Cask Storage Systems" (DCSS SRP, ML010040297, et al.), provides regulatory guidance regarding quality controls and instrumentation for dry cask storage systems (DCSSs). The guidance provided in the DCSS SRP is general with regard to I&C systems reviews. The DCSS SRP references 10 CFR Part 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Class C Waste," Subpart G, "Quality Assurance," for the regulatory bases supporting quality assurance activities.

10 CFR Part 72, Subpart G, stipulates that quality assurance comprises all those planned and systematic activities necessary to provide adequate confidence that a structure, system, or component will perform satisfactorily in service. However, the DCSS SRP does not provide specific quantitative acceptance criteria for digital I&C systems important to safety. Since such systems are not excluded from the scope of 10 CFR Part 72, Subpart G, regulatory guidance and criteria must be developed to ensure that I&C systems important to safety are designed, purchased, fabricated, handled, shipped, stored, cleaned, assembled, inspected, tested, operated, maintained, repaired, modified, and decommissioned in accordance with the quality assurance requirements of 10 CFR Part 72, Subpart G.

1.3.4 Spent Fuel Dry Storage Facilities

NUREG-1567, "The Standard Review Plan for Spent Fuel Dry Storage Facilities" (SFDSF SRP, ML003686776), provides guidance for reviewing applications for license approval or renewal of commercial ISFSIs. 10 CFR 72.44(c) specifies the requirements to be included in technical specifications for ISFSIs and MRS installations. To guard against the uncontrolled release of radioactive materials, these requirements include functional and operating limits; monitoring instruments; limiting control settings; limiting conditions; surveillance requirements; design features; and administrative controls. The SFDSF SRP does not distinguish acceptance criteria for digital-based safety systems from those for analog-based safety systems.

Regulatory Guide (RG) 3.48, "Standard Format and Content for the Safety Analysis Report for an Independent Spent Fuel Storage Installation or Monitored Retrievable Storage Installation (Dry Storage)" (ML003739463), provides an outline and specific guidance regarding information to be included in an applicant's safety analysis report (SAR). RG 3.48 is intended to ensure the quality and uniformity of NRC staff reviews by establishing the review scope and requirements. However, RG 3.48 does not distinguish acceptance criteria for digital-based safety systems from those for analog-based safety systems.

The SFDSF SRP uses a basic outline defined by RG 3.48, with modifications based on staff experience with SAR reviews. The modified outline is used for the related safety evaluation report (SER) prepared by the NRC staff in response to the applicant's SAR. The SFDSF SRP includes regulatory requirements, staff positions, references to applicable national and other industry standards and codes, acceptance criteria, guidance on preparation of the SER, and other guidance.

In conjunction with the SFDSF SRP, the NMSS Spent Fuel Project Office (SFPO) developed several SFPO Director's interim staff guidance documents (ISGs) to address emerging issues. Although the SFDSF SRP was revised to incorporate most of these ISGs, additional ISGs will continue to be developed when required, and the SFDSF SRP will periodically be revised to reflect current staff guidance. Presently, there is no ISG that addresses digital safety systems.

1.3.5 Byproduct Materials

With regard to licenses for byproduct materials, 10 CFR 30.33, "General Requirements for Issuance of Specific Licenses," states that an application for a specific license will be approved if (in addition to other conditions) the applicant's proposed equipment and facilities are adequate to protect public health and minimize danger to life and property. There is no specific quantitative acceptance criteria for digital I&C systems that are used to protect public health and safety from the uses of byproduct materials in academic, medical, or industrial applications. Nonetheless, digital systems important to safety in byproduct instrumentation and devices must be of sufficient quality to protect public health and safety, public defense and security, and the environment. For example, 10 CFR Part 31, "General Domestic Licenses for Byproduct Material," §31.5, "Certain Detecting, Measuring, Gauging, or Controlling Devices and Certain Devices for Producing Light or an Ionized Atmosphere," requires that the on-off mechanism and indicator, if any, for devices must be tested for operability at regular intervals. In cases in which the on-off mechanism and indicator are implemented by a digital system, the quality of the mechanism and indicator must be such that the testing interval is adequate to protect public health and safety. The Therac-25 events, in which patients received lethal doses of radiation as a result of malfunctions in the digital on-off mechanism, highlight the necessity to develop a complete set of acceptance criteria for digital systems important to safety in byproduct material devices.

1.3.6 Safety System Security

The purpose of quality assurance (QA) activities (e.g., V&V) is to improve safety system reliability by detecting and then eliminating or mitigating faults that could cause system failures. Some digital system features may allow exploitation of, or access to, the system that the developers neither intended nor anticipated. Other security vulnerabilities may be deliberately incorporated into safety systems and designed to evade and thereby defeat QA processes. Confirmation of digital safety system quality, therefore, should address potential security vulnerabilities as part of the system QA process.

Three classes of security threats must be addressed. The most common class of security threats involves cyber attacks, in which individuals and undocumented organizations concentrate on incorporating or exploiting vulnerabilities in digital systems with the intent to disrupt system operations or illegally obtain information from the systems. A second class of security threats, although less common, is from electromagnetic (EM) attacks that can be used either to physically damage digital equipment or to disrupt digital equipment operations by overwhelming the digital computers with concentrated EM energy. A third class of security threats is from unauthorized access to safety system networks. In each of these cases (cyber attacks, EM attacks, and network access), QA goals are effectively compromised because safety systems could be caused to fail, operate at an inappropriate time, or cause a nuclear facility operator or byproduct material user to respond inappropriately to erroneous signals or indications.

1.4 The Necessity for Digital Technology Research

As described in Section 1.2, several technical issues associated with digital technology have the potential to adversely impact safety. These issues have arisen because of differences in the way analog and digital systems are designed, operated, and fail. The NRC regulations and regulatory guidance described in Section 1.3 were developed, in part, to address technical issues that have the potential to adversely impact safety; however, most of these regulations and regulatory guidance primarily provide qualitative acceptance criteria. The introduction of digital technologies into safety systems for nuclear facilities and nuclear material applications and the transition to a risk-informed regulatory environment have resulted in a need to determine the need for additional regulatory guidance and objective acceptance criteria for approving digital safety systems. A purpose of this Research Plan is to develop clearly defined regulatory guidance and acceptance criteria as regulatory needs are identified.

Industries and regulatory bodies (including the NRC) have implemented various processes to reduce the potential for digital system failures, but generally acknowledge that complete elimination of the potential for digital system failures is not realistic with current state-of-the-art techniques and processes. Given the complex nature of this issue, the NRC has been acquiring an understanding of the challenges of regulating the use of digital systems in safety applications.

Specific challenges regarding regulation of digital technologies fall into several areas. One area is the development of review procedures to identify digital system faults and their potential impact on digital system performance. The challenges in this area relate to addressing the unique failure modes and complexity associated with digital systems. For example, complete testing of digital systems is often impractical because of their complex design and operation; however, tools and review procedures for evaluating digital system development life cycle processes and products may complement testing strategies.

Digital equipment is different from analog equipment in its EM compatibility, and its susceptibility to environmental conditions. For example, digital equipment responds to electromagnetic interference (EMI) differently and affects the surrounding EM environment differently than analog equipment because the two technologies have significantly different EM frequency spectrums. Electromagnetic and environmental qualification techniques specifically designed for digital systems should be developed to complement existing environmental qualification processes.

NRC reviews of digital safety system development processes have primarily relied on qualitative acceptance criteria, partly because tools and review procedures for evaluating digital safety systems using quantitative acceptance criteria have not been readily available. The acquisition or development of tools and review procedures for quantitatively reviewing digital system life cycle processes will support the NRC's regulatory mission by making the staff's reviews more effective. The use of tools could augment existing review processes by providing supplementary review capabilities. This is especially important for reviewing highly complex digital systems. Additionally, the nuclear industry should be encouraged to accept the new tools and review procedures as integral components of NRC licensing processes to enable the agency to access the review materials in a format compatible with tool and review procedure requirements. In concert with the acquisition or development of tools and review procedures, the NRC must also develop sufficient expertise in the use of the tools and review procedures, as well as interpretation of the results.

The challenge of evaluating digital system reliability relates to the relatively undeveloped state-of-the-art methods for assessing digital system reliability. Quantitative measures of digital system reliability are available for digital system hardware, but review procedures for evaluating software reliability are not well-defined. However, comprehensive use of fault injection techniques for evaluating digital system dependability; metrics for quantitatively evaluating life cycle process and product quality; and methods for objectively determining that sufficient diversity and defense-in-depth features are incorporated into digital safety systems may reduce software reliability uncertainties.

Potential security vulnerabilities in digital safety systems may arise as a result of vulnerabilities that are either inadvertently or deliberately introduced into a digital system. The purpose of security assessment activities is to detect and then eliminate or mitigate vulnerabilities in the digital system that could be exploited either from the outside (e.g., a social miscreant or a hostile nation state) or from the inside (e.g., a disgruntled employee). The use of tools and procedures to detect digital safety system security vulnerabilities, and processes to implement security techniques in safety systems can help reduce the potential for system failures caused by cyber attacks.

In addition to determining the range of digital safety system failure mechanisms, the NRC must address the probability of adverse public health and safety consequences contributed by digital safety system failures. For example, an analysis of I&C contributions to nuclear reactor core damage probability examined 217 accident sequence precursor (ASP) events that occurred between 1984 and 1997 with conditional core damage probability greater than or equal to 1×10^{-5}. Thirty percent of these events were initiated by I&C system failures and at least one I&C failure contributed to the progression of an additional 10 percent of these events. Several of the identified ASP events involved the failure of digital controls that were embedded in larger plant systems (e.g., circuit breakers, transformers, and diesel generators). The analysis resulted in the following recommendations for I&C research:

- Develop methods and capabilities to identify the risk-importance of I&C systems.
- Identify risk-important I&C components in support and control systems (particularly power supply equipment).
- Identify risk-important I&C components in safety systems (particularly pumps, valves, and EDGs).
- Ensure that I&C safety research addresses component failures, design errors, and maintenance errors.

On the basis of the range and consequences of digital safety system failures, RES is conducting research to continually augment and supplement the NRC's capabilities for reviewing and assessing digital technology implementations in safety systems. The combination of QA evaluation review procedures, reliability assessment capabilities, security assessment capabilities, and environmental qualification processes specifically designed for digital systems will complement existing requirements regulating safety system design and performance.

1.5 Research Plan Organization

Section 2, "Objective and Scope," summarizes the purpose of this Research Plan and the approach followed to achieve that purpose. Section 3, "Research Programs," describes the research programs, projects, and tasks that will be used to fulfill the NRC's strategic mission. These programs, projects, and tasks are organized hierarchically into six research programs, which each contain three to six research projects, with each project consisting of two or more research tasks. This hierarchical structure is shown in Figure 1, "FY 2005 – FY 2009 Research Plan Programs 3.1, 3.2, and 3.3," and Figure 2, "FY 2005 – FY 2009 Research Plan Programs 3.4, 3.5, and 3.6." This section concludes with a description of research activities that generically support the research programs. Section 4, "Research Plan Task Summaries and Schedules," summarizes the Research Plan tasks and products and proposes schedules for each research project. Section 5, "References," provides references for the reports cited in the Research Plan. Appendix A, "Strategic Goals and Strategies," summarizes the NRC's strategic goals, outcomes, and corresponding strategies, as described in "U.S. Nuclear Regulatory Commission Strategic Plan for FY 2004 – FY 2009," NUREG-1614, Volume 3 (ML042230185).

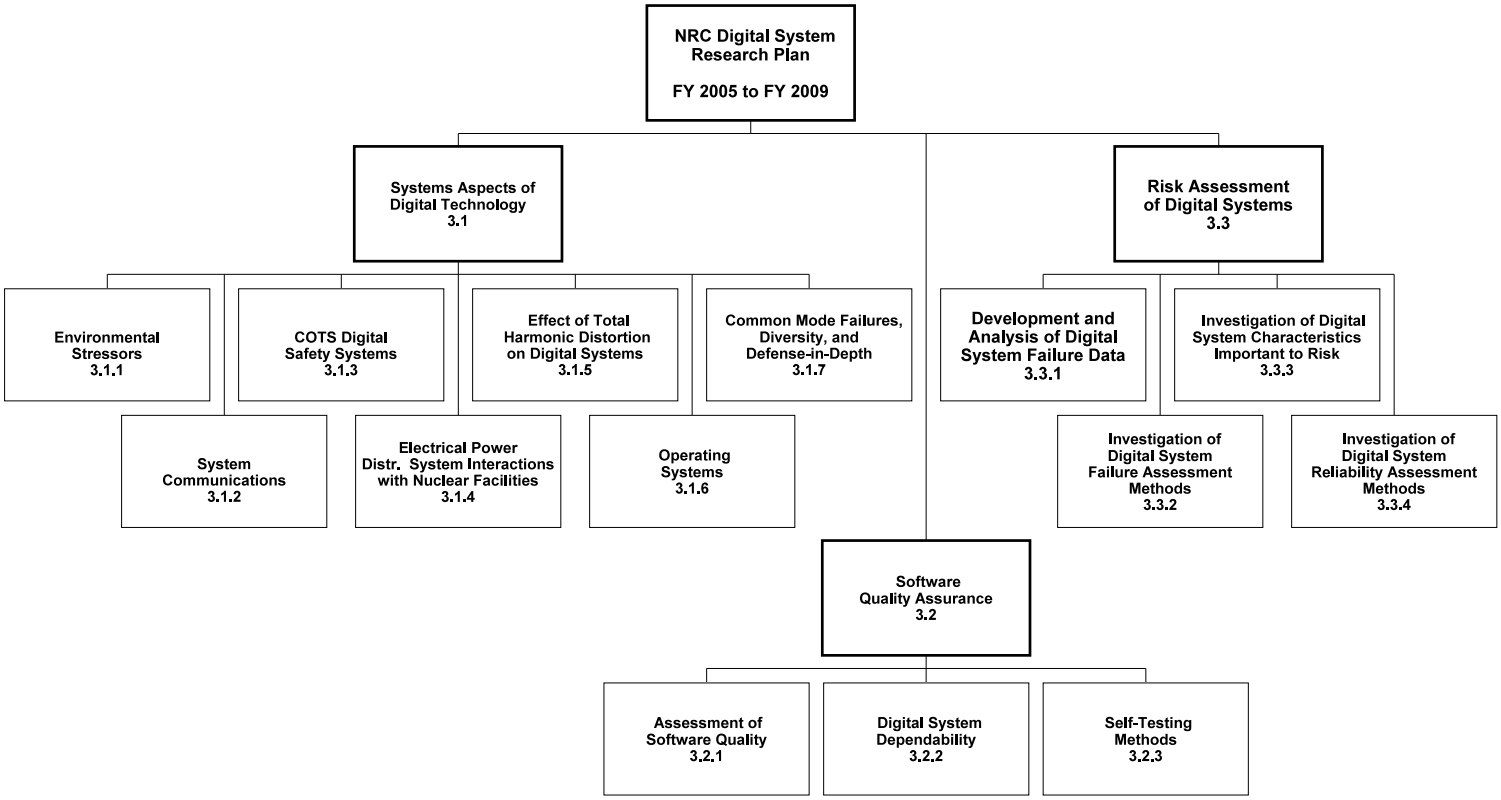

Figure 1. FY 2005 – FY 2009 Research Plan Programs 3.1, 3.2, and 3.3

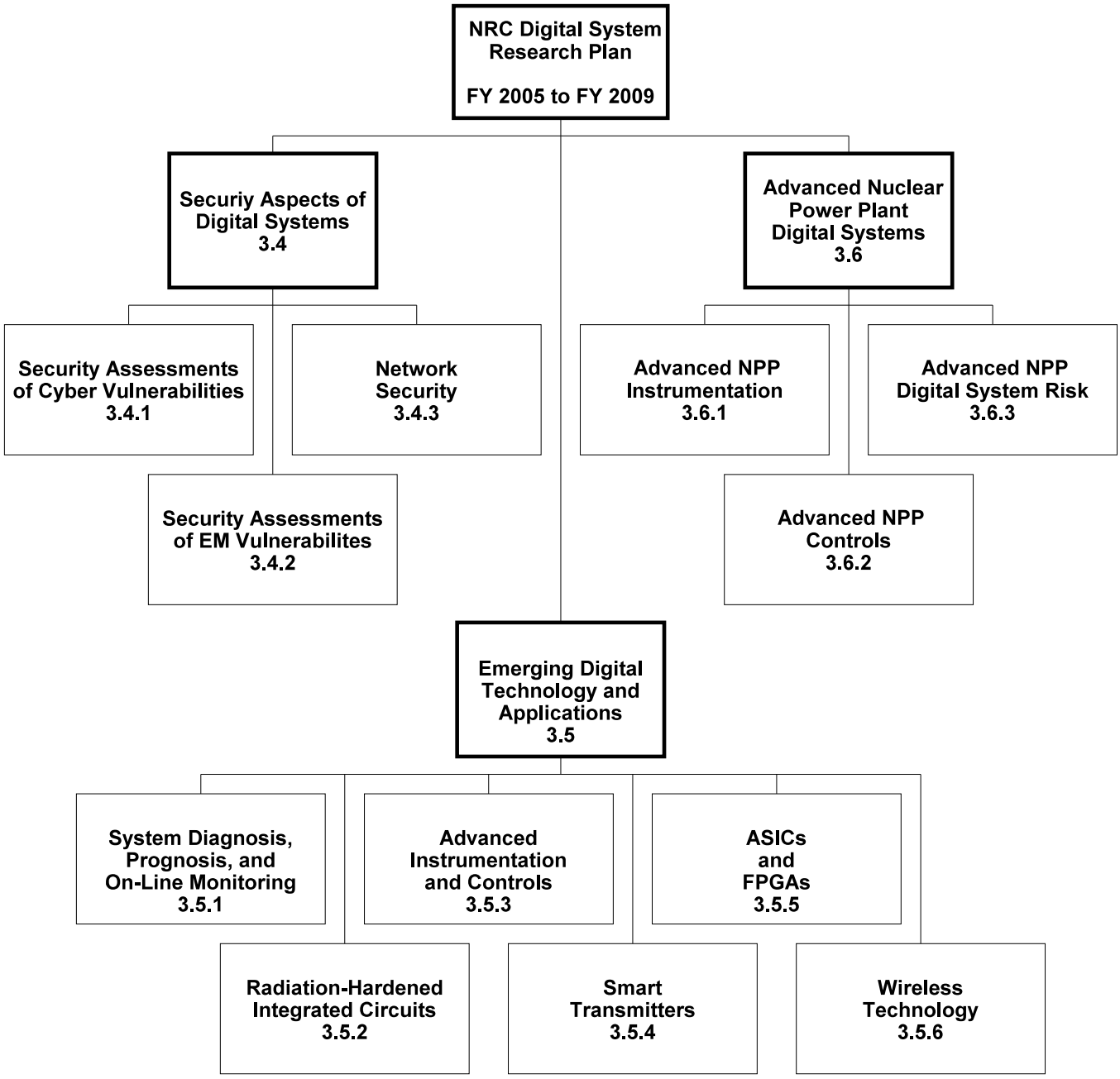

Figure 2. FY 2005 – FY 2009 Research Plan Programs 3.4, 3.5, and 3.6

2 OBJECTIVE AND SCOPE

A discussion of the Research Plan objective and scope requires a description of the relationship between the NRC's regulations, research programs, and strategic mission. The NRC's mission is to regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and to protect the environment. This mission applies to all uses of radioactive materials, regardless of the technology in which the materials are used (e.g., NPPs, fuel cycle facilities, waste storage processes and facilities, industrial manufacturing processes, medical uses, etc.), and regardless of the technology by which public health and safety, national security, and environmental protection are ensured (e.g., analog-based, digital-based, or passive safety systems, etc.). The NRC's mission is the basis for all of the agency's regulations and regulatory processes, guidance, and acceptance criteria.

The NRC's Strategic Plan identifies Safety, Security, Openness, Effectiveness, and Management as strategic goals for achieving the agency's mission. Additionally, the Strategic Plan describes strategies for achieving the strategic goals (e.g., six strategies for achieving the Safety goal). The means to support implementation of the strategies consist of programs and initiatives that are in place or must be established to ensure that the NRC realizes its strategic goals. The strategies for realizing the agency's strategic goals, and the outcomes to be expected from achieving those strategic goals, are described in NUREG-1614, Volume 3, and summarized in Appendix A, "Strategic Goals and Strategies."

The purpose of NRC regulations is to prescribe the processes by which the agency's licensees are to operate nuclear facilities and use radioactive materials to fulfill the agency's mission. Although prescriptive, these regulations do not provide sufficiently detailed information (in some areas) regarding the means by which licensees are to meet the regulatory criteria and the NRC staff is to assess licensee conformance to those criteria. Consequently, the agency provides additional guidance to NRC staff and licensees in the form of SRPs, Inspection Procedures (IPs), RGs, etc.

To ensure that the NRC continues to fulfill its mission, the staff continually reviews the agency's regulations and regulatory guidance to identify areas that require more detailed, objective acceptance criteria or revisions to account for changes in technologies. Research is the method the staff most commonly uses to develop this supplementary guidance and acceptance criteria. In the case of digital systems technology, almost all related research activities originate as research programs, projects, and tasks in the NRC's Research Plan.

To effectively regulate the nuclear industry, the NRC uses consensus standards as a basis for developing regulatory guidance. Consequently, the staff is actively involved in the process of developing consensus standards to ensure that those standards adequately represent the agency's regulatory positions. While much of this effort involves domestic standards organizations [e.g., Institute of Electrical and Electronics Engineers (IEEE) and Instrument Society of America (ISA)], domestic and international standards development organizations are beginning to harmonize their standards. Consequently, the NRC also coordinates its standards-related activities with standards development activities conducted by other countries.

The NRC maintains technical resources capable of reviewing advances in emerging technologies that have the potential for use by the nuclear industry in safety systems. These resources are most effectively developed through continued training and participation in national and international technical meetings and conferences. Additionally, maintaining infrastructure and knowledge management through continued research ensures that current capabilities are available and adaptable to support future needs as the nuclear industry continues to employ more advanced digital systems.

Given the breadth of research proposed by this Research Plan, the use of personnel, material, and financial resources must be optimized to yield the research products needed to support the agency's regulatory mission. The effective use of limited research resources may be augmented by contributing NRC resources to collaborative and cooperative research projects that are funded in part by the NRC and by other organizations such as academic centers of excellence and international research groups.

The objective of the above processes is to provide the means to achieve the agency's mission. How research activities support accomplishment of the agency's mission is illustrated in the following example and in Figure 3 using a specific Research Plan project. In this example, a review of regulatory guidance in SRPs, IPs, RGs, etc. indicated that acceptance criteria and guidance for EMI operating envelopes for fast transients for digital safety systems could be improved. This need for improvement was incorporated into the Research Plan in Research Program 3.1, "System Aspects of Digital Technology," as Task 3.1.1.A in Project 3.1.1, "Environmental Stressors." Task 3.1.1.A will develop improved regulatory guidance regarding the technical basis for EMI operating envelopes in nuclear facilities by using existing EM data from NPPs, characterizing transients in NPPs, and addressing nuclear industry concerns regarding existing EMI guidance. The RG developed in Task 3.1.1.A will provide more detailed guidance and acceptance criteria, which the staff will use to confirm that digital safety systems are appropriately qualified. Thus, this regulatory activity supports accomplishment of the agency's strategic mission.

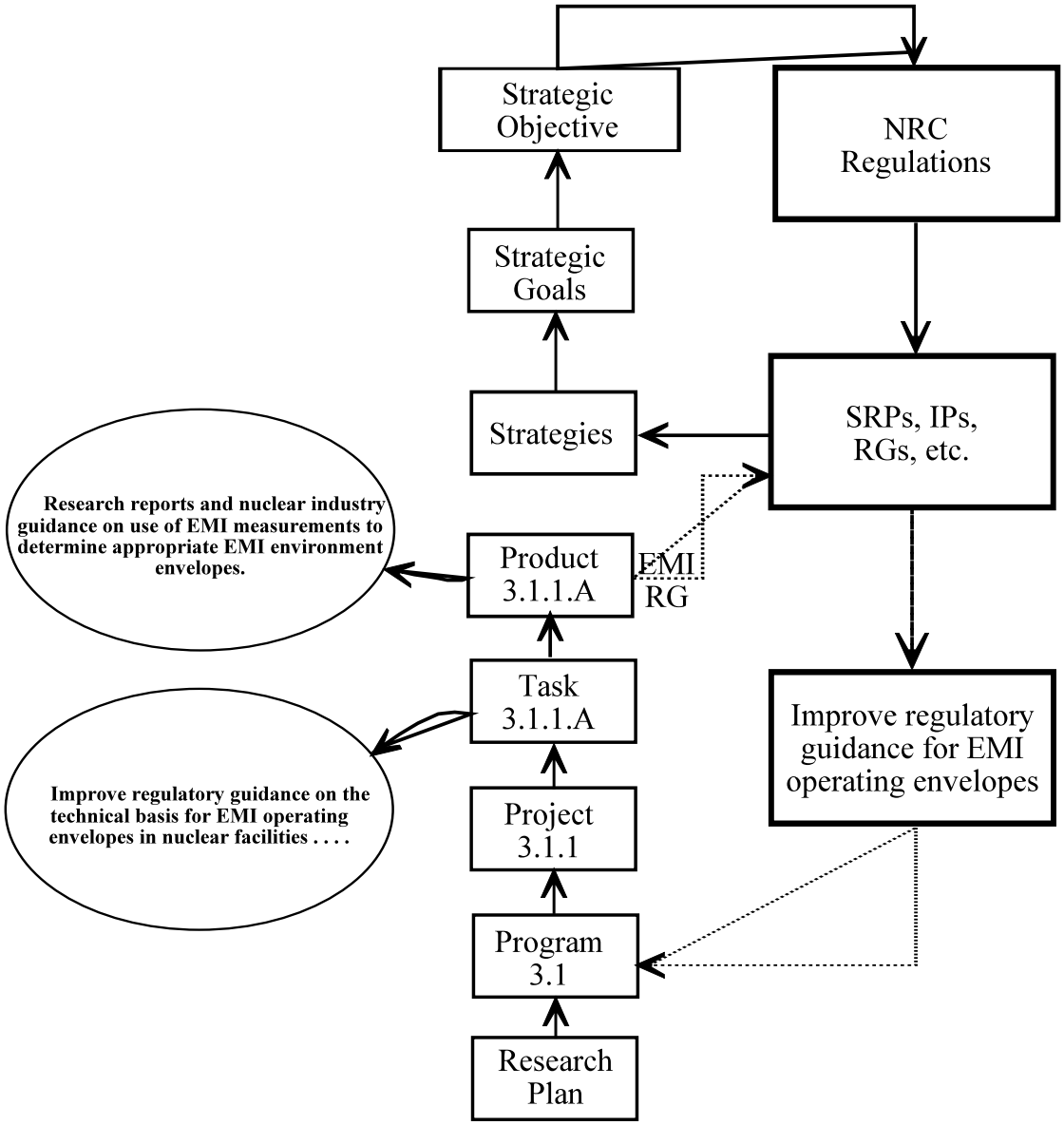

Figure 3. Relationship between the NRC's mission, strategic goals, implementing strategies, regulations, and Research Plan programs, projects, and tasks

2.1 Objective of this Research Plan

The objective of this Research Plan is to establish research programs and initiatives to gain a better understanding of digital I&C technologies, and (as appropriate) to acquire or develop tools, acceptance criteria, models, regulatory guidance, and review procedures to augment the NRC staff's capabilities to review and approve digital systems for safety applications in nuclear facilities and applications.

Specifically, this Research Plan will accomplish this objective through the following approaches:

- Characterize the challenges the staff must address to review and license digital safety systems.
- Specify research programs and schedules to address these challenges.
- Identify the products that must be developed from the research projects to meet the identified challenges.

In general, the research projects will produce the following products, as appropriate:

- technical guidance and conclusions
- acceptance criteria addressing the technical guidance
- tools (acquire as appropriate) to supplement evaluation of licensee and vendor products using the acceptance criteria
- review procedures (and optionally, inspection procedures) that guide the reviewer in using the tools, acceptance criteria, and technical guidance
- formal training modules to ensure that the research products are used appropriately and consistently

RES will work closely with the supported office(s) during the initial stage of defining each research project to identify the specific research products that must be developed. During the research project, RES will continue to communicate with the supported staff regarding the progress of the research to ensure that the supported staff can integrate the research products into projected schedules and licensing tasks on a timely basis. Additionally, the supported staff may be asked to provide assessments of product capabilities (e.g., beta testing) before the final products are delivered for use. This preliminary review and assessment will be conducted to ensure that the products meet the requirements and expectations of the supported staff. Channels of communication will be maintained between the RES staff and the supported office(s) following product delivery to provide support in using the products.

2.2 Scope of the Research Plan

The scope of this Research Plan has been established to support the needs of NMSS, NRR, and NSIR for effective regulation of digital safety systems in currently licensed and future nuclear facilities. Hence, the scope encompasses a set of research programs that address (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, and (6) Advanced Reactors.

This Research Plan includes additional research-related activities that (1) support development of regulatory guidance for the nuclear industry regarding the use of industry standards; (2) maintain the NRC's research capabilities and manage of the knowledge base supporting the agency's regulatory activities; and (3) promote collaborative and cooperative research on digital systems.

The following discussion summarizes the research programs and additional research-related activities.

2.2.1 System Aspects of Digital Technology

System aspects of digital technology involve those internal and external factors that impact the performance of a digital system as a whole. This area of research will develop a fundamental understanding of how digital technologies are used in systems important to safety, and will use that knowledge to acquire or develop applicable technical information, guidance, tools, review procedures, and training to augment the NRC staff's capabilities to perform in-depth and realistic technical evaluations of digital safety system designs.

2.2.2 Software Quality Assurance

Software quality assurance (SQA) is a planned and systematic pattern of actions necessary to provide confidence that a digital system conforms to established technical requirements. While the NRC currently has a set of digital system quality assurance guidelines, implementing these guidelines is resource-intensive for both the NRC and the industry. In addition, there is no set of regulatory guidance; acceptance criteria; and review tools, methodologies, and procedures that address self-testing features in digital systems. This could lead to inconsistencies in the amount of self-testing that is appropriate for use in safety-related digital systems. Further, additional effectiveness and consistency may be gained by augmenting the NRC's existing SQA processes with additional tools and review procedures.

2.2.3 Risk Assessment of Digital Systems

As discussed in the NRC's Policy Statement on Probabilistic Risk Assessment (PRA), the agency intends to increase its use of PRA methods in all regulatory matters to the extent supported by state-of-the-art PRA methods and data. Currently, I&C systems are not generally modeled in PRAs. As the NRC moves toward a more risk-informed regulatory environment, the staff will need data, methods, and tools related to the risk assessment of digital systems.

2.2.4 Security Aspects of Digital Systems

Security of digital safety systems involves addressing potential security vulnerabilities as part of the system development process, and maintaining security of the system after it is installed. In addition to cyber-attack threats in existing digital systems (i.e., viruses, hackers, etc.), the NRC must address other threats to digital systems arising from application of technologies that can introduce new system vulnerabilities. For example, EM attacks from high-energy radiofrequency devices (HERF attacks) might be used to physically damage digital equipment, while low-energy radiofrequency devices (LERF attacks) might be used to disrupt digital equipment operations by overwhelming the digital computers with concentrated EM energy. In either case, cyber or EM attacks may cause a safety system to fail or to operate at an inappropriate time, or cause an operator to respond inappropriately to erroneous signals or indications.

2.2.5 Emerging Digital Technology and Applications

New innovations in digital I&C technology (e.g., hybrid control rooms and smart transmitters) have the potential to improve both operating efficiency and safety in existing and advanced nuclear facility designs. The NRC's regulatory staff requires knowledge about emerging these technologies and applications to make timely decisions as they are introduced into the nuclear industry. Research addressing emerging digital technologies and applications will provide the staff with technical information and criteria for use in making appropriate regulatory decisions. This is particularly important because state-of-the-art implementations of existing technologies in new applications could introduce new challenges to safety and security that may not be addressed by other research activities. Additionally, new research projects will be created to address new safety concerns that may arise.

2.2.6 Advanced Nuclear Power Plants

The new generation of advanced NPP designs is expected to have fully integrated digital control rooms and use a much higher degree of automation. The use of multiple modular NPPs also may require more complex control of both the primary I&C systems and all of the support systems, including the switch yard. Research programs will be developed to address issues concerning the use of advanced instrumentation and controls, and development of risk modeling to understand the effect of digital systems proposed for use in advanced NPP designs within a risk-informed licensing framework. Additionally, this research may be useful for existing NPPs undergoing digital retrofits.

2.2.7 Additional Research-Related Activities

The NRC uses RGs to provide guidance to licensees and applicants on implementing relevant portions of Federal regulations pertaining to nuclear facilities. Many of these RGs endorse, with exceptions and clarifications, consensus standards published by national and international standards bodies. The NRC must be involved in the consensus standards development process to ensure that those standards adequately represent the agency's regulatory perspectives.

The also NRC requires a broad base of expertise to keep abreast of the wide variety of rapidly evolving issues involving implementation of digital technologies in nuclear facilities. The NRC most effectively maintains its base of expertise through continuing participation in national and international technical meetings and conferences. Another base of expertise resides in organizations outside the NRC, such as national laboratories, universities, and other industries. Maintenance of contractor and staff capabilities and facilities through continued research using existing resources will ensure that the infrastructure remains flexible and adaptable to changes in the nuclear industry.

To optimize available research resources, the NRC must also participate in cooperative research agreements with universities, other Federal agencies, industries, and other countries. Through participation in cooperative research programs, the NRC will acquire or develop cost-effective guidance, tools, review procedures, and acceptance criteria for reviewing digital systems, and thereby improve licensing and overview processes.

Section 4 of this Research Plan summarizes each research program and task described in Section 3, “Research Programs,” in a tabular format and correlates each research task to the NRC’s related strategies.

3 RESEARCH PROGRAMS

The NRC Digital System Research Plan for FY 2005 – FY 2009 is organized hierarchically into six research programs, consisting of related research projects and task. These six programs are described in Section 3.1, "System Aspects of Digital Technology;" Section 3.2, "Software Quality Assurance;" Section 3.3, "Risk Assessment of Digital Systems; Section 3.4, "Security Aspects of Digital Systems;" Section 3.5, Emerging Digital Technology and Applications," and Section 3.6, "Advanced Reactors." These research programs are designed to develop a combination of QA evaluation review procedures, reliability assessment capabilities, security assessment capabilities, and environmental qualification processes for digital systems to complement existing requirements regulating safety system designs, performance, and security. Additional activities described in Section 3.7, "Supporting Activities," support ongoing development of regulatory guidance, maintenance of the NRC's research infrastructure, and collaborative and cooperative research programs that supplement research projects and tasks in the six research programs. These additional activities are applicable to every area of research, regardless of the technology or issue being investigated.

The products of the research programs described Sections 3.1 – 3.6 will augment the NRC's current abilities to regulate the use and management of radioactive materials and nuclear fuels for beneficial civilian purposes in a manner that protects the health and safety of the public and the environment; promotes the security of our Nation; and provides for regulatory actions that are open, effective, efficient, realistic, and timely. The specific products may not include all of those listed as products in this section, as the NRC staff will identify appropriate products during the initial phase of each research project.

3.1 System Aspects of Digital Technology

This research program will address aspects of digital systems that can adversely affect safety, and will acquire or develop applicable technical information, guidance, tools, review procedures, and training to augment the NRC staff's capabilities to perform in-depth and realistic technical evaluations of digital safety system designs. The following research projects address the system aspects of digital technology:

- Environmental Stressors
- System Communications
- Commercial off-the-Shelf (COTS) Digital Systems
- Electrical Power Distribution Interactions with Nuclear Facilities
- Total Harmonic Distortion Effects on Digital Systems
- Operating Systems
- Diversity and Defense-in-Depth

The NRC Research Plan for Digital Instrumentation and Control for FY 2000 – FY 2004 (ML012080254) discussed various system aspects of digital technology. Tools and guidance were developed for environmental stressors, digital requirements specifications, diagnostics and fault tolerance, and operating systems. Technical reports, NUREG-series reports, and regulatory guides have been drafted in many of these areas (particularly environmental stressors). These reports are discussed in Section 3.1.1 of this Research Plan. New issues continue to arise which require the NRC to develop the tools needed to understand the system aspects of digital technology.

3.1.1 Environmental Stressors

Supported NRC Offices: NMSS and NRR

3.1.1.1 Background and Issues

Electromagnetic Compatibility Research

Electromagnetic and radiofrequency interference (EMI/RFI) are environmental stressors in which electric fields, magnetic fields, or radiofrequency waves interfere with the operation of an electrical or electronic device. The electric/magnetic fields and radiofrequency waves are generated from such sources as electric motors, relay switching, and mobile phones. EMI/RFI can produce "noise" on electric signals or cause digital equipment to perform in unexpected ways. Past events at NPPs have demonstrated how EMI/RFI can cause unexpected behavior in digital I&C systems (USNRC, 1994).

At one time, the NRC lacked a complete set of regulatory guides pertaining to EMI/RFI qualification for digital systems. To meet that need, RES developed RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Rev. 1 (ML032740277), to provide an acceptable process for EMI/RFI qualification. The updated RG 1.180, Rev. 1, addressed signal line test methods, as well as test methods consistent with International Electrotechnical Commission (IEC) 61000 and U.S. Military Standard (MIL-STD) 461E; extended the frequency range for radiated emissions and susceptibility testing to 10GHz; and relaxed surge withstand capability envelopes from 3kV to 2kV.

In NUREG/CR-5609, "Electromagnetic Compatibility Testing for Conducted Susceptibility Along Interconnecting Signal Lines" (ML032960137), RES provided the technical basis for guidance on electromagnetic compatibility testing to address conducted susceptibility along interconnecting signal lines for safety-related I&C systems. This contractor-prepared NUREG-series report includes findings from a confirmatory investigation of the comparability of the IEC and MIL-STD signal line susceptibility test methods using an EMI testing artifact, and presents recommendations for conducted susceptibility test methods and final operating envelopes that can be applied to signal lines.

In NUREG/CR-6782, "Comparison of U.S. Military and International Electromagnetic Compatibility Guidance" (ML033000345), RES described the applicability of the IEC electromagnetic compatibility (EMC) standards for the U.S. NPP environment. This contractor-prepared NUREG-series report presents the results of a review and assessment of commercial IEC 61000 standards, as well as a comparison with U.S. Military and IEEE guidance on test methods and the RG 1.180 guidance on operating envelopes. The report also included a review of MIL-STD-461E.

The combination of the regulations and criteria cited above provides the regulatory basis for the required confirmation (i.e., qualification) that safety-related I&C systems are compatible with the EM environment at nuclear facilities. This guidance is based on the condition that the EM environment at nuclear facilities has been adequately characterized and will be maintained.

Revision 06/2

In July 2003, the Electric Power Research Institute (EPRI) submitted a draft report describing its assessment of MIL-STD-461E test CS-114 for high-frequency conducted susceptibility test limits that EPRI had recommended in EPRI Technical Report (TR) 102323, Rev. 2. In that draft report, EPRI asserted that the CS-114 test limits in TR-102323 had proven to be overly conservative because the NPP emissions data upon which the test limits were based should not have included captured power transients (which are addressed by power surge susceptibility testing). Additionally, the test data were obtained using MIL-STD-461E procedures CE03 and CE102, which are not considered applicable for high-frequency conducted susceptibility testing per CS-114. EPRI concluded that, since the original rationale for the high-frequency test limits was flawed, the corresponding operating limits described in the SER approving EPRI TR-102323, Rev. 0, were also flawed.

Test results for all NPP equipment tested using the guidelines provided in EPRI TR-102323 had shown that the limits were too conservative for NPP environments. EPRI subsequently sought relief from the specific CS-114 testing limit criteria EPRI provided in EPRI TR-102323.

The purpose of this research is to review the technical basis for revising the CS-114 operating limits in RG 1.180, Rev. 1, and update the guidance in RG 1.180, Rev. 1, if the EPRI assertions are justified. This research is an ongoing project being performed for the NRC by Oak Ridge National Laboratory (ORNL) (NRC Job Code N6080, "Interactions with Industry on Standards").

Lightning Effects on Digital Safety Systems

Like other environmental stressors, lightning has the potential to cause failures in digital systems. Mitigating the potential impact of lightning-induced surge and the associated secondary EMI effects through lightning protection is an important element of maintaining the EM environment at a site within expected conditions. To protect against lightning, certain design measures can be taken to prevent or minimize its impact. Currently, Chapter 7 of the NPP SRP states that lightning protection should be addressed as part of the review of EMC. Also, the NPP SRP states that lightning protection features should conform to the guidance of National Fire Protection Association (NFPA) Std 78, "Lightning Protection Code," and IEEE Std 665, "Guide for Generation Station Grounding." This research will provide additional regulatory guidance (i.e., a regulatory guide) for licensees and applicants to follow to ensure that adequate lightning protection is implemented. In addition, this research will determine whether the guidance in the above standards should be enhanced to address protection of digital systems from lightning-induced effects because of the much lower operating voltages used by modern digital systems. This lightning research is an ongoing project being performed for the NRC by the ORNL (NRC Job Code W6851, "Guidance for Lightning").

Environmental Qualification of Digital Safety Systems

In draft NUREG/CR-6741, "Application of Microprocessor-Based Equipment in Nuclear Power Plants: Technical Basis for a Qualification Methodology" (ML012600340), RES provided an enhanced technical basis for environmental qualification guidance that addressed microprocessor-based safety-related I&C systems. In addition to providing final recommendations on qualification guidance, draft NUREG/CR-6741 presented a comparative analysis of IEEE Std 323 and IEC 60780 that provides the basis for endorsement of domestic and international qualification standards. This is an ongoing project that should be completed in FY 2006.

In Draft Regulatory Guide DG-1077, "Guidelines for Environmental Qualification of Microprocessor-Based Equipment Important to Safety" (ML0112710073), the NRC provided guidelines for environmental qualification of safety-related microprocessor-based equipment in NPPs. The draft guidance incorporated the technical basis for use of either IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," or IEC Std. 60780, "Nuclear Power Plants: Electrical Equipment of the Safety System Qualification," with clarifications, for application to digital systems. The guidance is organized in a manner suitable to facilitate the industry's implementation of these standards.

Regulatory guidance from the research activities described above will address safety concerns associated with environmental stressors, while improving licensing capabilities associated with qualifying digital systems.

3.1.1.2 Tasks

This research project has the following goals:

A. Review the technical basis for revising the CS-114 operating limits in RG 1.180, Rev. 1, and update the guidance in RG 1.180, Rev. 1, if EPRI conclusions regarding CS-114 operating limits are correct.

B. Develop regulatory guidance and acceptance criteria for establishing lightning protection and qualifying digital systems to withstand the electromagnetic effects resulting from lightning strikes.

C. Develop regulatory guidance to address environmental qualification of microprocessor-based equipment in mild environments.

3.1.1.3 Products

This research project is intended to yield the following products:

- possible revision of RG 1.180, Rev. 1
- regulatory guidance on consensus lightning protection practices to mitigate the impact of lightning on the EM environment at nuclear facilities
- regulatory guidance on environmental qualification of microprocessor-based equipment in mild environments

3.1.2 System Communications

Supported NRC Offices: NMSS and NRR

3.1.2.1 Background and Issues

For future communication system applications, the NRC has a need to acquire a set of tools and review procedures to support staff reviews of 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.

Revision 06/2

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

> 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.

As stated in GDC 24, NRC regulations 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; however, the NRC has not endorsed these provisions. 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,).

Additionally, digital safety system development platforms use vendor-specific communication protocols and, in some cases, dedicated microprocessors, to control data transfers between safety channels and within each safety channel.

Existing consensus standards describe acceptable design of the data communication systems, often referencing the Open Systems Interconnect (OSI) model. The OSI model is an abstract representation of data communication between two or more networked devices, which comprises seven logical layers with the physical connections at the lowest layer and the human-machine interaction functions (e.g., software graphical user interfaces) at the highest layer. The NRC should assess these consensus standards to determine their acceptability for safety system applications in NPPs.

The fundamental issues with data communication protocols overlap with those of COTS digital systems and the use of application-specific integrated circuits (ASICs) and field-programmable gate arrays (FPGAs). The reason for this overlap is that these protocols are generic rules for transferring data between two endpoints (perhaps even through intermediate devices, implying routing of messages) that are implemented in software running on hardware. The protocols are standardized (and reference the OSI model) for interoperability between devices. Additionally, existing devices can translate between protocols, adding further complexity.

Given the trend in safety systems toward highly networked architectures within safety system channels and applications, and the possibility for communications between safety and nonsafety systems, the NRC should develop failure analysis techniques and expertise in evaluating complex digital communication systems. As part of this development, the NRC will use case studies of current technologies to identify scenarios that could challenge a safety system, and identify mitigation measures to address those challenges.

Modeling tools and protocol analyzers can be used to verify protocol specifications and applications implemented in hardware and/or software. One challenge is the selection of the modulation protocol to be used for transmitting data. The features that could affect safety in each communication protocol proposed for use in safety systems should be identified to enable the NRC staff to evaluate proposed safety system communication protocol features to determine whether the communication protocol could adversely affect safety.

The NRC will acquire or develop tools (as appropriate) and review procedures to support the staff's safety evaluations of communication systems important to safety. The NRC will train its staff on the use of the tools and review procedures to augment the process for verifying the safety of communication systems. These training modules will be developed in tandem with tool acquisition or development to ensure that the tools and review procedures appropriately address the subject material.

3.1.2.2 Tasks

This research project has the following goals:

A. Identify communication protocols for data transfer within safety systems and for communications between safety and nonsafety systems.

B. Review consensus standards and other communication protocol specifications for potential endorsement in regulatory guides.

C. Identify communication system failure mechanisms and mitigation strategies.

D. Acquire or develop a set of tools and review procedures to support staff reviews of communication protocols and systems.

E. Develop curricula for training the staff on the use of the tools and review procedures for evaluating communication protocols and systems.

3.1.2.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance addressing findings on communication protocols within safety systems and applications, and for communications between safety and nonsafety systems
- regulatory guides endorsing communication protocol consensus standards and other specifications
- regulatory guidance addressing communication system failure mechanisms and mitigation strategies
- tools and review procedures to support staff reviews of communication protocols and systems
- training course(s) for the staff on the use of the tools and review procedures for evaluating communication protocols and systems

Revision 06/2

3.1.3 COTS Digital Systems

Supported NRC Offices: NMSS and NRR

3.1.3.1 Background and Issues

Nuclear power plants and industrial and medical users of byproduct materials use COTS components for safety-related applications. These COTS components include central processor units (CPUs) (e.g., Intel, AMD, and Motorola), microcontrollers, local area network (LAN) controllers, real-time operating systems, dual-port random access memory (RAM), analog-to-digital and digital-to-analog converters, etc. Generic acceptance of safety systems imposes new requirements on both NRC licensees and reviewers. Determining the acceptability of these COTS components requires assessing the hardware, software, interactions between hardware and software (i.e., the system), interactions between the safety system channels, interactions between safety and nonsafety systems, and human-machine interfaces.

Technological advances have made reviews of digital systems more challenging because of the high complexity of newer COTS digital systems. Consequently, EPRI, nuclear licensees, and other external stakeholders have presented to NRR risk-informed methods for performing safety assessments of digital systems. In addition, the RES staff has identified and evaluated new review methods during the past several years. For example, the Halden Reactor Project (HRP) is performing collaborative research with the NRC to evaluate the use of COTS operating experience in safety assessments (NRC Job Code Y6349, “Halden Environmentally Assisted Cracking”). The new methods identified by RES address Commission goals to risk-inform NRC regulations and processes while also providing assurance of adequate safety design. The NRC may be able to incorporate these methods into review procedures and activities that support existing licensing processes.

It is not clear whether the state-of-the-art in software engineering tools and review procedures for determining software quality has sufficiently matured to be useful in evaluating digital safety systems. Quantitative safety assessment methods exist for COTS equipment, but are not widely accepted. These quantitative methods are based on probabilistic analyses. Therefore, designs must be such that failure rates (or some other figure of merit used in a given method) must be sufficiently low to ensure adequate safety. Also, statistical uncertainties must be properly characterized to prevent overconfidence in system performance. Other issues include software reuse, hardware reuse (i.e., improper device selection), formal methods for assessing design requirements, model checking and state-space explosion (for complex systems), fault modeling and fault tolerant designs, safety system architecture issues, and determinism and timing. Various methods will be validated as appropriate to identify potential research objectives and products.

3.1.3.2 Tasks

This research project has the following goals:

A. Perform case studies of safety assessment methods for reviewing COTS-based digital systems.

B. Evaluate methods for performing risk-informed safety assessments of COTS-based digital systems.

C. Acquire or develop a set of tools (as appropriate), review procedures, and acceptance criteria to support existing methods for reviewing COTS-based digital systems and equipment.

D. Develop curricula for training the staff on the use of the tools and review procedures for performing safety evaluations of COTS-based digital systems and equipment.

3.1.3.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance describing assessment methods for reviewing COTS-based digital systems
- regulatory guidance for performing risk-informed safety assessments of COTS-based digital systems
- tools, review procedures, and acceptance criteria to support existing methods for reviewing COTS-based digital systems
- training course(s) for the staff on the use of the tools and review procedures for performing safety evaluations of COTS-based digital systems and equipment

3.1.4 Electrical Power Distribution System Interactions with Nuclear Facilities

Supported NRC Offices: NRR and RES

3.1.4.1 Background and Issues

The August 2003, the electrical power blackout in the northeastern United States caused nine NPPs to experience loss of offsite power (LOOP) abnormal operating occurrences (AOOs). This blackout demonstrated a need for improved understanding of the detrimental effects of multiple component and system interactions and the potential for common-mode failure involving the U.S. electric transmission and distribution systems. The interdependency between operating NPPs and the Nation's electric power grid was described in NUREG-1784, "Operating Experience Assessment: Effects of Grid Events on Nuclear Power Plant Performance" (ML033530400), which summarized the potential for power disturbances and LOOPs to impair the function of safety-related and electrical systems. The following three events describe electrical transmission system voltage fluctuations adversely affecting microprocessor-based NPP systems:

- LER 244/94-012, “Loss of 34.5-kV Offsite Power Circuit 751, Due to External Cause, Results in Automatic Start of B Emergency Diesel Generator,” states that, on September 29, 1994, while the R.E. Ginna Nuclear Power Plant was at 98 percent power, a private citizen operating heavy machinery accidentally knocked a tree into the 34.5-kV Offsite Power Circuit 751. The event resulted in a partial LOOP to safety buses 16 and 17 and the start and loading of one. Power was restored to safety buses 16 and 17 through Circuit 767 in 30 minutes. The LOOP resulted in a loss of program memory to a radiation monitor.
- LER 270/97-002, “Grid Disturbance Results in Reactor Trip Due To Manufacturing Deficiency,” states that, on July 6,1997, while at 100 percent power, the main generator voltage regulator on Oconee Nuclear Station, Unit 2, did not respond to a system grid disturbance created by the loss of two hydro units 15 miles from the Oconee plant site. The Oconee Unit 2 voltage could not be maintained within acceptable ranges as the main generator voltage regulator had been miscalibrated in 1994. The voltage decreased to 80 percent of nominal, tripping the reactor coolant pumps, which tripped the reactor. The voltage fluctuation also resulted in the loss of several nonsafety electrical loads in the turbine building and caused several programmable controllers on a control room vertical board to switch from automatic control to manual control.
- LER 293/97-007, “Safeguards Buses De-Energized and Losses of Offsite Power During Severe Storm While Shut Down,” states that, on April 1,1997, while at 0 percent power, a LOOP occurred at Pilgrim Nuclear Power Station Unit 1 during a severe storm. Severe undervoltage transients occurred on the 345-kV transmission system and resulted in automatic shutdown of safety-related 480/120v voltage-regulating transformers that were installed in 1992. Of interest was that these transformers contain programmable microprocessor control units that automatically shut down the transformer when the voltage drops to 384v (20 percent of nominal), in this case for 6 to 8 cycles.

Challenges in this area of research include modeling highly distributed, complex systems comprising digital, analog, discrete, high-voltage, high-current power components (including associated substations and interfaces with operating NPPs) to determine the effect of power fluctuations on NPP safety. This research will review existing standards and regulatory guidance to determine their applicability for addressing degraded power effects on digital components.

3.1.4.2 Tasks

This research project has the following goals:

A. Acquire or develop models, tools, and review procedures for identifying the effect of power fluctuations on digital systems in NPPs.

B. Review existing standards to determine their applicability for addressing effects of degraded power on digital components.

C. Develop curricula for training the staff on the use of the models, tools, review procedures, and regulatory guidance for addressing the effects of power fluctuations on digital systems.

3.1.4.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance describing the models, tools, and review procedures for addressing the effects of power fluctuations on digital systems in NPPs
- regulatory guidance addressing the effects of power fluctuations on digital equipment
- training course(s) on the use of the models, tools, review procedures, and regulatory guidance for addressing the effects of power fluctuations on digital systems

3.1.5 Effect of Total Harmonic Distortion in Digital Systems

Supported NRC Offices: NMSS and NRR

3.1.5.1 Background and Issues

IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," states that computers shall be designed to perform their safety functions when subjected to external or internal conditions that have significant potential to defeat a safety function (e.g., input and output processing failures, precision and roundoff problems, improper recovery actions, electrical voltage and frequency fluctuations, and maximum number of coincident signal changes). Power electronic equipment is susceptible to misoperation caused by harmonic distortion. This equipment is often dependent upon accurate determination of voltage zero crossings or other aspects of the voltage wave shape. Harmonic distortion can result in a shift of the voltage zero crossing or the point at which one phase-to-phase voltage becomes greater than another. These are both critical points for many types of electronic circuit controls, and misoperation can result from these zero crossing shifts.

IEEE Std 519-1992 (2nd printing in 2004), "IEEE Recommended Practices and Requirements for Harmonic Control in Electrical Power Systems," states that the type of equipment that is most susceptible to total harmonic distortion (THD) is equipment of which the design or constitution requires a (nearly) perfect sinusoidal fundamental input. This is frequently in the categories of communication or data processing equipment. Switching power supplies and some motor controllers in the electrical distribution system for safety systems can adversely affect safety system power quality. Other voltage and current disturbances are caused by devices that contribute non-linear loads to the voltage system. These power disturbances can adversely affect safety system operation.

One common non-linear load component in digital systems is the microprocessor, which is downstream from the high-quality power supplies that are designed to eliminate power disturbances. In smaller digital systems containing only a few microprocessors, the THD effect on the same or adjacent printed circuit boards may be negligible. However, in larger, more complex systems containing significantly more microprocessors and other non-linear load components, the THD effect may be significant. The degree to which this THD could affect the reliable operation of a safety system should be characterized.

Other types of electronic equipment can be affected by transmission of alternating current (ac) supply harmonics through the equipment power supply or by magnetic coupling of harmonics into equipment components. Computers and allied equipment such as programmable controllers frequently require ac sources that have no more than a 5% harmonic voltage distortion factor, with the largest single harmonic being no more than 3% of the fundamental voltage. Higher levels of harmonics result in erratic, sometimes subtle, malfunctions of the equipment that can, in some cases, have serious consequences. Instrumentation can be similarly affected, giving erroneous data or otherwise performing unpredictably.

Since most electronic equipment is located at a low voltage level of its associated power distribution system, it is frequently exposed to the effects of voltage notching. Voltage notches frequently introduce frequencies (both harmonic and nonharmonic) that are much higher than normally exhibited in 5-kV and higher voltage distribution systems. These frequencies can be in the radiofrequency (RF) range, and, as such, can introduce harmful effects associated with spurious RF. These effects usually are those of signal interference introduced into logic or communication circuits. Occasionally, the notching effect is of sufficient power to overload EMI filters and similar high-frequency sensitive capacitive circuits.

Existing NRC guidance for EMI/RFI equipment qualification does not address THD and voltage notching effects in digital systems. The NRC should produce guidance regarding the effect of THD on the performance and safety of digital systems and components. Additionally, the NRC may require tools to model the effect of THD-related effects on digital system components such as microprocessors, multiplexors, and digital instrumentation. Adding the capability to analyze the effect of THD-related effects in digital systems could lead to more accurate assessments of digital safety system performance in complex systems.

3.1.5.2 Tasks

This research project has the following goals:

A. Acquire or develop models, tools (as appropriate), and review procedures for evaluating THD-related effects in digital systems.

B. Review existing standards to determine their applicability for addressing THD-related effects in digital systems.

C. Develop curricula for training the staff on the use of the models, tools, and review procedures for evaluating THD-related effects in digital systems.

3.1.5.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance describing the models, tools, and review procedures for evaluating THD-related effects in digital systems
- regulatory guidance addressing THD-related effects in digital systems
- training course(s) on the use of the models, tools, and review procedures for evaluating THD-related effects in digital systems

3.1.6 Operating Systems

Supported NRC Offices: NMSS and NRR

3.1.6.1 Background and Issues

Operating systems manage memory, data, processing times, and interfaces between the application programs and the computer hardware. Operating systems also provide an environment that enables computer resources to be used in an efficient manner. Since operating systems control all aspects of a computer's operation, operating system quality is critical to computer system quality. Therefore, the NRC requires a technically sound method of confirming that the quality of an operating system is appropriate for the safety functions it supports.

In the past, the NRC was able to evaluate operating systems because they were small, simple, and custom-programmed for specific applications. Now, however, regulatory safety assessments of operating systems used in nuclear facilities and medical and industrial byproduct applications is becoming more difficult for three reasons. First, the increased computing capability of digital systems has led to the use of more complex operating systems. Second, many custom and COTS digital systems now contain COTS operating systems, rather than custom-made operating systems. Third, even with operating systems that are available for review, the NRC staff requires guidance regarding the features of operating systems that could minimize the potential for operating system errors, and failures that could adversely affect safety system operations. Additionally, the complexity in some operating systems is such that some features of an operating system may need to be excluded from safety system designs. Specific features that could adversely affect safety are not identified in current NRC guidance, and existing review processes do not provide operating system review acceptance criteria.

To investigate the fundamental issues in this technology area, this research project will further evaluate operating system characteristics and performance. The research will involve (1) examining past performance of operating systems and ranking the causes of computer failures attributable to operating system failures; (2) determining the potential risks of using operational history of an operating system as an indication of its quality; (3) performing tests on several of the most widely used COTS operating systems to determine their strengths and weaknesses; and (4) identifying operating system configurations, functions, and usage that would minimize the potential for operating system errors and failures.

3.1.6.2 Tasks

This research project has the following goals:

A. Evaluate design aspects of operating systems, appropriate operating system selection criteria, best design practices, architectures, failure modes, and fault models.

B. Acquire or develop a set of tools (as appropriate) and review procedures to support operating system safety assessments.

C. Develop curricula for training the staff on the use of the tools and review procedures for performing evaluations of operating systems used in safety-related applications.

Revision 06/2

3.1.6.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance describing design aspects of operating systems (i.e., appropriate operating system selection criteria, best design practices, architectures, failure modes, and fault models)
- tools, as appropriate, and review procedures for evaluating operating systems
- NRC staff training course(s) on the use of the tools and review procedures for performing evaluations of operating systems

3.1.7 Common-Mode Failures, Diversity, and Defense-in-Depth

Supported NRC Offices: NMSS and NRR

3.1.7.1 Background

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 10 CFR Part 50. In particular, GDC 21, "Protection System Reliability and Testability," requires in part that "…(1) no single failure results in the loss of the protection system…." Also, GDC 22, "Protection System Independence," requires that, "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 were written at a time when trip and mitigation systems were based on analog technology and incorporated diverse design features at the logic level to minimize the possibility of a common-mode failure (CMF) preventing the loss of a protection function or system. These analog-based NPP safety system designs rely on three design principles to compensate for failures that could degrade safety system reliability. Specifically, these design principles are (1) functional defense-in-depth, (2) functional diversity, and (3) system diversity. (Within the context of this discussion, safety functions comprise a safety system.) While these strategies should be applied for any safety system design, the process by which these principles are applied varies with the underlying technology used in the design. The following discussion provides an example of how a typical analog-based safety system design incorporates these three design principles into an integrated strategy for mitigating the consequences of functional failures and system failures.

Functional Defense-in-Depth

Analog-based NPP safety system designs employ functional defense-in-depth by incorporating three or more independent, separate channels of analog components to perform the same set of safety functions. The components comprising the same trip function in each channel are produced by the same manufacturer, have the same model numbers, are arranged in the same configuration, and are calibrated to the same tolerance requirements and trip setpoint.

For example, a typical Babcock and Wilcox (B&W) NPP reactor protection system (RPS) design comprises four separate and independent channels of identical safety functions. The set of safety functions consists of an overpower trip function, a high-temperature trip function, a high-pressure trip function, et al. Within a channel, each trip function is performed by an independent set of analog components consisting of a plant process measurement instrument, the wires leading from the measurement instrument to the RPS trip function analog components, the analog components that convert the measurement signal into a trip signal, and the connections between the RPS and the reactor trip breakers. A trip signal from each channel is combined with the trip signals from the other three identical channels of redundant equipment to cause the reactor to trip.

This use of functional redundancy (i.e., the same trip functions in redundant channels) in analog safety system designs provides defense-in-depth against random failures in a single component preventing a safety function from initiating a reactor trip or causing unnecessary reactor trips. For example, if an overpower trip function component in one B&W RPS channel fails, the overpower trip function in the other three channels could still trip the reactor on high power.

An acceptable level of hardware reliability is required for the functional defense-in-depth principle to be an effective design strategy to compensate for failures in a single channel. Ensuring that the analog hardware has an acceptable level of reliability is accomplished by selecting high-quality components, together with failure testing, environmental testing, and long-term proof-testing of the components assembled into a prototype of the protective function.

Functional Diversity

NPP safety system designs incorporate diverse (different) safety functions within each channel to ensure that the barriers against fission product release are protected if a CMF causes a loss of the same safety function in each channel. To illustrate the application of the functional diversity design principle in an NPP safety system, consider an example in which two RPS trip functions in a typical B&W-designed plant are the [reactor] overpower trip function and the [reactor coolant] high-temperature trip function.

The overpower trip function protects the fuel cladding fission product barrier by preventing the reactor from operating at a power level that could cause the fuel centerline temperature to increase and overheat the fuel cladding, thereby causing cladding failure. The high-temperature trip function prevents the reactor from being operated above a fixed coolant temperature at the reactor vessel outlet to ensure that the heat transfer rate from the fuel cladding to the reactor coolant does not decrease to the point at which film boiling could occur and thereby cause fuel cladding failures. These trip functions prevent different (diverse) plant states (i.e., high centerline fuel temperature and high cladding temperature) from degrading the fuel cladding fission product barrier.

In B&W-designed plants, the high-temperature trip function is not a primary protection function for any adverse reactor system event [although this function provides an upper limit for a departure from nucleate boiling (DNB) trip function]. However, the high-temperature trip function provides additional protection of the fuel cladding fission product barrier in the unlikely event that a CMF occurs in the four redundant overpower trip function channels. A system design in which two or more diverse trip functions (e.g., an overpower trip function and a high-temperature trip function) are used to accomplish the same protective action (i.e., protect the fuel cladding fission product barrier) is an example of using the functional diversity design principle to compensate for CMFs that could affect the same trip function in every channel.

The functional diversity design approach must include both the system functional logic and the plant condition(s) used as input by the diverse trip functions. An example illustrates the importance of this functional diversity requirement. Another B&W RPS trip function is the variable low RCS pressure trip function. This trip function protects the reactor fuel cladding fission product barrier by providing a margin to DNB. Reactor coolant system pressure and temperature are used by the variable low-pressure (DNB) trip function logic to define an envelope of pressure and temperature conditions within which the reactor must operate to remain above the DNB safety limit.

Since the DNB trip function monitors the approach to DNB, and the high-temperature trip function monitors reactor coolant temperature, from the perspective of trip setpoint value, the two trip functions are functionally diverse. However, in the B&W RPS design, the reactor coolant temperature sensor signals are shared by the DNB trip function and the high-temperature trip function. Consequently, a CMF of the temperature sensors or temperature signals in this design would cause a CMF of both the DNB trip function and the high-temperature trip function. Consequently, the DNB trip function and the high-temperature trip function are not an example of the functional diversity design principal because a CMF could defeat both trip functions. [However, if the DNB trip function temperature sensors were diverse from the high-temperature trip function temperature sensors such that a CMF of both sensors would not be likely to occur (e.g., resistance temperature detectors (RTDs) versus thermocouples), the two trip functions would be an example of the functional diversity design principle.]

For the functional diversity design principle to be an effective strategy for mitigating CMF of a protective function, the diverse trip function design (1) must be based upon a different plant condition (e.g., reactor coolant temperature and reactor power), or (2) must use diverse means of monitoring the same plant condition (e.g., reactor coolant temperature and DNB).

System Diversity

Functional defense-in-depth and functional diversity are design principles that mitigate failures of a single protective function in one channel and failures of the same protective function in every channel, respectively. Neither of these design strategies is effective against system-wide CMFs. For example, an RPS system-wide failure could prevent diverse trip functions (e.g., the overpower trip function and the high-temperature trip function in a B&W RPS) from protecting the barriers to fission product release. Consequently, a third design principle, known as system diversity, must be employed to prevent or mitigate CMFs of every protective function in every channel.

System-wide CMFs can be caused by either external or internal conditions or events. External conditions or events that could cause a system-wide CMF include a loss of instrumentation signals used by the system (e.g., a fire that destroys all instrumentation wires leading into the protection system); a failure of the system(s) actuated by the safety system (e.g., the reactor trip breakers); a failure of a common power source used by the system (e.g., a station blackout that affects the system power supplies); and environmental conditions that adversely affect the performance of the safety system (e.g., high temperature, humidity, radiation, etc.).

While a broad range of external conditions and events could cause a system-wide CMF, internal conditions that could cause a system-wide CMF generally relate to design and manufacturing defects in components used by every trip function (e.g., relay off-gassing that corrodes deenergize-to-actuate relays, chemical compounds in component packaging that degrade internal circuits, unanticipated aging-related failures, etc.).

The most common approach for providing system diversity is to install a backup system that has design features or functions sufficiently diverse from those of the safety system such that there is a low probability that a CMF or CCF could simultaneously affect both systems. An anticipated transient without scram (ATWS) system is an example of the system diversity design principle being used to compensate for CMFs that could cause the loss of an RPS capability to trip the reactor.

Diverse systems provide reasonable assurance that diverse safety functions will (1) be available to mitigate system-wide safety system failures, and (2) not cause the primary safety system to fail. For the system diversity design principle to be an effective strategy for ensuring that means are available to mitigate system-wide CMFs, system diversity features must be considered as part of an integrated plant design process that addresses system interactions and capabilities for performing safety functions using diverse systems not subject to the same CMFs.

The above three design principles have proven effective in minimizing CMF vulnerabilities in analog-based safety systems because of four underlying conditions. Specifically, (1) analog component failure mechanisms are well-understood; (2) failure frequencies are predictable on the basis of historical failure data; (3) testing can reliably identify all function and system failure states; and (4) QA methods are sufficiently reliable at eliminating manufacturing-related defects during the analog component manufacturing process. Common mode failures can arise in systems when the underlying conditions for applying the three design principles for addressing CMF vulnerabilities are overlooked.

The above three design principles are less effective for mitigating CMF vulnerabilities in digital systems because (1) software and system failure mechanisms are not well-understood; (2) failure frequencies cannot be reliably predicted on the basis of historical failure data; (3) testing processes for identifying function and system failure states are not well-defined, and (4) QA methods have not been shown to be sufficiently reliable at eliminating development-related defects during the software and system development and system maintenance process.

Digital system industry experience has shown that reliance upon QA processes alone to identify CMF vulnerabilities has not been completely effective at preventing CMFs in high-integrity digital systems. Consequently, other processes must be developed to augment existing QA processes such that the proper functional defense-in-depth, functional diversity, and system diversity features may be integrated into the design during the development process. Additionally, there should be a process for confirming that CMF vulnerabilities have not been introduced after a system has been modified.

The scope of this process development effort must address a broad spectrum encompassing software-, hardware-, and system-related CMF vulnerabilities. For example, CMF vulnerabilities can arise during conceptual development of a digital system when the potential for a CMF is not addressed in the description of the conceptual system. It is during this conceptual development phase that the diversity and defense-in-depth attributes of design diversity, equipment diversity, functional diversity, human diversity, signal diversity, and software diversity must be identified, as these diversity attributes cannot be overlooked by the system domain experts during subsequent development of the system requirements.

CMF vulnerabilities also can arise during the development of system, hardware, or software requirements as a result of specifying ambiguous requirements, specifying requirements without the benefit of domain expertise, or failing to specify requirements that address the diversity attributes identified in the conceptual design. Ambiguous requirements can lead to a design that cannot be adequately verified by inspection or sufficiently validated by testing. Additionally, unintended functionality is harder to detect during V&V activities when ambiguous requirements provide the baseline upon which the QA activities are defined. Specification of requirements without the benefit of domain expertise can also lead to unintended system states. Failing to specify diversity attributes in the system requirements can also lead to incorrect system states that could result in a CMF.

When addressing the potential for CMFs in digital systems, the initiating event for the CMF is typically assumed to be a software fault that occurs in every safety system channel. However, other types of CMF mechanisms have been identified in commercial digital systems. Three examples highlight the potential for hardware-based CMFs in digital systems. The first two examples involve the use of components fabricated by different manufacturers, but containing materials that share a CMF characteristic or property. The third example involves the effect of technology advances on the potential for CMFs.

In the first example, *IEEE Spectrum Online* reported that a faulty electrolyte in aluminum electrolytic capacitors used on printed circuit boards in the commercial digital equipment sector caused capacitors to begin failing in early 2002 (http://www.spectrum.ieee.org/WEBONLY/resource/feb03/ncap.html). The faulty electrolyte becomes unstable when charged, generating hydrogen gas, which ultimately causes the capacitors to burst, thereby leaking the electrolyte onto the printed circuit board. This causes numerous shorts and system failures on printed circuit boards and similar digital equipment, often requiring complete replacement of the faulted component.

The capacitors using the defective electrolyte were fabricated by many different manufacturers and then sold to manufacturers of digital components requiring capacitors to stabilize voltages in sensitive circuits. As reported in the article, some of the capacitor manufacturers have refused to admit using the faulty electrolyte in order to avoid expensive litigation and a loss of market advantage. Consequently, it is impossible to determine every application in which these faulty capacitors are being used.

The second example, reported in *Nikkei Electronics Asia* in February 2003, involves worldwide use of a faulty semiconductor encapsulation resin by various manufacturers for several years. In mid-2001, a hard disk drive (HDD) brand and model used in Toshiba personal computers was reported to be failing at an unusually high rate. The cause was determined to be a failure in the HDD controller caused by a short between pins within the integrated circuit (IC) package. Originally, the issue was thought to only affect HDDs, but then similar defects began appearing in a range of other equipment, including personal computer main boards, IC test systems, and industrial machinery. The issue developed into a major problem that rapidly involved a host of equipment and IC manufacturers.

As background, the flame retardant most commonly used in semiconductor encapsulation resins for many years is a combination of Bromine-based compounds with an antimony trichloride (Sb_2O_3) additive. This mixture was extremely effective, and an encapsulation resin with 2–3% content conformed to the Underwriters Laboratories, Inc. (UL) 94 standard for flame retarding performance, “The Standard for Flammability of Plastic Materials for Parts in Devices and Appliances.” However, Bromine-based compounds have been cited as potential sources of dioxins and other toxic gases when combusted, and this eventually led to restrictions on their use around 1990, primarily in Europe. These restrictions accelerated the trend toward developing halogen-free flame retardant materials, not only in encapsulation resins but in all types of applications. In response to these environmental concerns regarding the use of halogens in fire retardants, a manufacturer developed a fire retardant for semiconductor encapsulation resins that uses red phosphorous as the fire retardant chemical.

An investigation into the mechanism causing the semiconductor failures revealed that phosphoric acid ions were generated by a reaction between water vapor and the red phosphorous fire retardant material. In general, red phosphorous is protected by a covering of aluminum hydroxide [$Al(OH)_3$], but when this protective layer is compromised, the red phosphorous reacts with water vapor that is no longer blocked by the aluminum hydroxide barrier. The resulting phosphoric acid ions dissolve the semiconductor leadframes, made of copper (Cu) and other elements, causing ion migration and eventually leading to electrical shorts at the leadframe level.

The problem has not been found in all semiconductors using the red phosphorous-containing resin, apparently because of differences in the phosphoric acid concentration. A threshold level has been found to exist, below which the problem is unlikely to develop. The differences in concentration are a result of differences in red phosphorous content by encapsulating resin lot, degree of protective layer damage, and other incidental factors. During the investigation, no ion migration was found to have occurred where the protective layer was intact.

Revision 06/2

In the third example, which is described in greater detail in Section 3.5.2, “Radiation-Hardened Integrated Circuits,” advances in the technology for developing more powerful ICs by compressing adjacent circuits to add transistors has introduced a new failure mode into microprocessors, static random access memory (SRAM), and dynamic random access memory (DRAM) components, resulting from the effects of cosmic radiation. In older generation ICs with circuit spacings of 130nm to 250nm, cosmic radiation had minimal effect on ICs. However, as manufacturers have moved to 90nm and smaller circuit spacings, cosmic radiation has had an increasing effect on ICs, which has affected commercial applications such as network servers and routers. Since the technology for creating increasingly dense ICs is available to every manufacturer, a diversity strategy that relies on different manufacturers using different microprocessor designs is not supported by industry experience.

As these examples illustrate, many complex interactions may not be addressed using traditional diversity and defense-in-depth strategies, and may result in widespread system failures. Clearly, reliance on diversity and defense-in-depth as means of avoiding CMFs requires consideration not only of manufacturers, but of the raw materials and technological advances used by those manufacturers. This research project will address the effects of technology advances on the potential for CMFs in digital safety systems, and will provide ongoing guidance regarding industry experience. The research will also include case studies of various COTS digital system configurations that are currently approved for safety-related applications in NPPs to assess their susceptibility to CMFs. The results of this research will also be used to determine whether additional considerations of diversity or defense-in-depth should be integrated into NRC guidance, acceptance criteria, review methodologies, review procedures, and associated staff training.

Addressing the potential for CMFs in a digital system to identify the need for diverse systems is implicit in the review of digital system development processes. Regulatory guidance is provided in NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems” (ML9501180332), as well as Branch Technical Position (BTP) HICB-19, “Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems” [Chapter 7, “Instrumentation and Controls,” of NUREG-0800, “Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants” (ML033580677)]. The intention was to provide a means of assessing whether additional diversity would be required in a digital safety system on the basis of the attributes of the system.

NUREG/CR-6303 separated diversity attributes into the following six categories to facilitate assessments of adequate diversity in safety systems:

- design diversity
- equipment diversity
- functional diversity
- human diversity
- signal diversity
- software diversity

The staff guidance in NUREG/CR-6303 provides a set of recommended criteria for each diversity attribute, ranked in order of relative importance within each attribute. However, because of the number of criteria in each attribute, combined with the number of attributes, the number of possible combinations of criteria and attributes that could be used to assess adequate diversity makes it very difficult to use the guidance as a safety assessment tool. For example, using only one criteria from each category to assess adequate diversity would result in 3,456 different combinations of diversity criteria. Consequently, the deterministic approach described in NUREG/CR-6303 does not sufficiently address alternative coping strategies. This research project will develop optimum sets of diversity attributes and associated attribute criteria that can complement other design approaches as part of a comprehensive process for confirming that a design has appropriately addressed CMF vulnerabilities.

Several COTS-based platforms have been reviewed and approved for use in NPP safety systems. These platforms use libraries of functions that are assembled to create applications. However, the susceptibility of these applications to CMFs is not well-characterized. A process for reviewing these systems to identify potential CMF vulnerabilities could supplement the NRC's existing licensing processes. This research project will investigate the CMF susceptibility of various prequalified COTS NPP digital safety systems that have been or will be submitted to the NRC for review and approval. These digital systems will replace analog-based reactor trip systems and engineered safety features actuation systems in existing NPPs. The result of this research will be extended to address evaluations of digital safety systems in other types of nuclear facilities and applications.

Additionally, the fault injection tool and methodology developed in research project 3.2.2 will be used to inject faults into specific COTS digital system configurations to evaluate whether the staff can use the tool to identify CMF vulnerabilities caused by external faults and internal design errors in digital systems. Various system hardware and software configurations will be tested by inserting faults throughout redundant system components and then monitoring system responses to the injected faults.

The advantage of using a fault injection tool and methodology to evaluate CMF vulnerabilities in digital safety systems is that the tool may detect some CMFs caused by manufacturing and material defects that are not detected during the system development process. The purpose of this research task, therefore, is to (1) provide regulatory guidance on the use of the fault injection tool, and (2) evaluate whether a procedure can be developed for using the tool and methodology to identify specific digital safety system diversity and defense-in-depth requirements that compensate for CMF vulnerabilities detected by the tool.

3.1.7.2 Tasks

This research project has the following goals:

A. Test various CMF coping strategies described in NUREG/CR-6303 to develop optimum sets of coping strategies for achieving sufficiently diverse design features.

B. Perform case studies of various COTS digital system configurations that are currently approved for safety-related applications in NPPs to identify generic, configuration-specific CMF vulnerabilities, and validate the procedure developed in Task C (below) for using the tool and methodology developed in research project 3.2.2.

C. Provide regulatory guidance on use of the tool and methodology developed in research project 3.2.2, and evaluate whether a procedure can be developed for using the fault injection tool and methodology to identify specific digital safety system diversity and defense-in-depth requirements that compensate for CMF vulnerabilities detected by the tool.

D. Develop curricula for training the staff on the use of the coping strategies, fault injection tool, review procedures, and acceptance criteria for evaluating defense-in-depth and diversity requirements for digital systems.

3.1.7.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance documenting optimum NUREG/CR-6303 CMF coping strategies, review procedures, and acceptance criteria for defense-in-depth and diversity (D3) designs
- regulatory guidance describing a process by which the staff can conclude — on a deterministic basis — that an acceptable combination of diversity attributes has been addressed in various COTS digital system configurations
- regulatory guidance regarding use of the tool and methodology developed in research project 3.2.2 and a procedure for using the fault injection tool and methodology to identify specific digital safety system diversity requirements that compensate for CMF vulnerabilities detected by the tool
- NRC staff training on NUREG/CR-6303 CMFcoping strategies and review procedures, and use of the fault injection tool, methodology, and acceptance criteria for evaluating defense-in-depth and diversity requirements for digital systems

3.2 Software Quality Assurance

The research program described in Section 3.1, “System Aspects of Digital Technology,” focuses on the systems aspects, rather than component-specific aspects of software-intensive systems (i.e., digital systems). By contrast, this research program focuses on those aspects of digital systems related to software development in the system development life cycle.

To fully analyze a complex system, one must analyze the components comprising the system, as well as their integration as a system. Toward this end, one major division in analysis activities is between hardware and software. This division of activities is useful because the components of each have different capabilities and are subject to different constraints and limitations. The SQA research program focuses on assessing software (i.e., as a component of the system) that affects the system’s ability to fulfill its requirements.

GDC 21 states, "…The protection system shall be designed for high functional reliability…." Currently, the NRC does not have a standardized methodology for quantitatively assessing the reliability of a digital system. Rather, the current practice is to review the processes used to develop a safety system, with the presumption that a high-quality process will produce a system that satisfies regulatory requirements. However, additional details are required regarding the acceptance criteria by which the staff can determine the acceptability of both the software development process and the products resulting from that process.

A set of digital system QA evaluation attributes is provided in Chapter 7 of the NPP SRP. Corresponding guidance supporting other classes of nuclear facilities and byproduct applications is not as detailed. BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," identifies functional and development process characteristics that must be reviewed to ensure that the quality of a proposed digital system is sufficient for use in safety-related applications. Specifically, these include the following functional characteristics:

- Accuracy: The degree of freedom from error of sensor and operator input, the degree of exactness exhibited by an approximation or measurement, and the degree of freedom from error of actuator output.
- Functionality: The operations that must be performed. Functions generally transform input information into output information in order to affect reactor operation. Inputs may be obtained from sensors, operators, other equipment, or other software. Outputs may be directed to actuators, operators, other equipment, or other software.
- Reliability: The degree to which a system or component operates without failure. This definition does not consider the consequences of failure (only the potential for failure).
- Robustness: The ability of a system or component to function correctly in the presence of invalid inputs or stressful environmental conditions. This includes the ability to function correctly despite some violation of the assumptions in its specification.
- Safety: Those properties and characteristics that directly affect or interact with safety considerations. The other characteristics discussed in BTP HICB-14 are important contributors to the overall safety of a digital safety system, but are primarily concerned with the internal operation of the software. That is, the safety characteristic is primarily concerned with the effect of the software on system behavior and the measures taken to control system behavior.
- Security: The ability to prevent unauthorized, undesired, and unsafe intrusions. Security is a safety concern insofar as intrusions can affect safety-related functions.
- Timing: The ability of the system to achieve its timing objectives.

The development process characteristics are as follows:

- Completeness: Those attributes of the planning documents, implementation process documents, and design outputs that provide full implementation of required functions. The functions that digital safety system components are required to perform are derived from the general functional requirements of the safety system, and assignment of functional requirements to the components in the overall system design.

- Consistency: The degree of freedom from contradiction among the various documents and components of a safety system. There are two aspects of consistency. Internal consistency denotes consistency within the various parts of a component; for example, a software design is internally consistent if no set of design elements are mutually contradictory. External consistency denotes the consistency between one component and another; for example, software requirements and the resulting code are consistent with one another if there are no contradictions between the requirements and the code.
- Correctness: The degree to which a design output is free from faults in its specification, design, and implementation. There is considerable overlap between correctness properties and properties of other characteristics such as accuracy and completeness.
- Style: The form and structure of a planning document, implementation process document, or design output. Document style refers to the structure and form of a document. This has connotations of understandability, readability, and modifiability. Programming style refers to the programming language characteristics of the software and programming techniques which are mandated, encouraged, discouraged, or prohibited in a given implementation.
- Traceability: The degree to which each element of one life cycle product can be traced forward to one or more elements of a successor life cycle product, and can be traced backward to one or more elements of a predecessor life cycle product.
- Unambiguity: The degree to which each element of a product, and all elements taken together, have only one interpretation.
- Verifiability: The degree to which a system planning document, implementation process document, or design output is stated or provided in such a way as to facilitate establishment of verification criteria and performance of analyses, reviews, or tests to determine whether those criteria have been met.

While BTP HICB-14 provides generic guidance for conducting safety assessments of software quality, it does not provide specific activities to be performed by an NRC reviewer to confirm that a safety system has been developed with acceptable quality (both process and product). For example, while “verifiability” must be confirmed as part of a safety assessment, BTP HICB-14 and supporting references do not provide the process by which verifiability is evaluated or the criteria for concluding that the degree of verifiability is acceptable. Consequently, a conclusion of acceptability depends in part on the perspective of the specific reviewer performing the safety assessment. This ambiguity in acceptance criteria can lead to inconsistent safety assessment reviews of safety system quality by different staff members.

Software quality assurance may be defined in either of the following ways:

(1) a planned and systematic pattern of all actions necessary to provide adequate confidence that the software conforms to established technical requirements

(2) a set of activities designed to evaluate the process by which products are developed or manufactured (IEEE, 1991)

Currently, staff reviews of vendor/licensee software development activities to assess the safety of a proposed digital system are founded on the assumption that an assessment of system development processes is sufficient to conclude that a digital system is acceptable for use in a safety-related application. Compounding this constrained focus on process assessments, staff reviews have been limited in scope because the NRC does not have a comprehensive set of acceptance criteria and review tools, methodologies, and procedures for evaluating the development processes.

While a process-oriented assessment of development processes is a necessary component of a software-based digital system safety assessment, a corresponding assessment of products arising from the development processes is also required to ensure that not only has the system been developed in accordance with a set of acceptable processes, but that system requirements are correctly implemented. Because the review focus is on process in one area and product in the other, review guidance, acceptance criteria, review methodologies and tools for evaluating system development products must complement review guidance, acceptance criteria, review methodologies, and tools for evaluating system development processes.

Using a typical waterfall system development lifecycle as a framework for illustrating this point, Figure 4 shows the system development phase processes and products that should be evaluated in the safety assessment of a digital safety system. Verification-intensive safety assessment activities primarily focus on software and system development processes performed by the system developer starting in the Concepts development phase and proceeding through the Test and Integration phase. Safety assessments during these development phases are primarily process-oriented (e.g., whether the design addresses each of the requirements; whether each design element is implemented in the software code; whether test plans address each requirement; etc.).

Validation-intensive safety assessment activities primarily focus on software and system development products created by the system developer, starting in the Implementation phase and proceeding through the Installation and Checkout phase. Safety assessments during these development phases are primarily product-oriented (e.g., whether the system performs correctly; whether the system performs within its timing requirements; whether the system responds appropriately to boundary conditions and faulted signals; etc.).

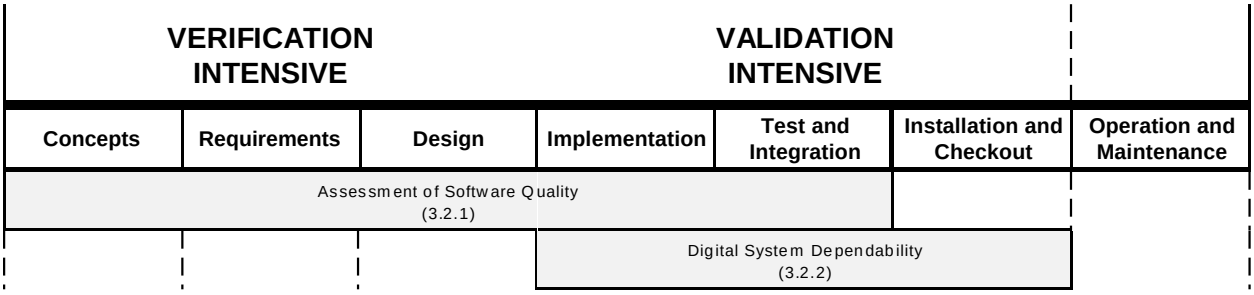

Figure 4. Scope of Software Development Evaluation Methodologies

Revision 06/2

The purpose of research project 3.2.1, "Assessment of Software Quality," is to provide the staff with capabilities for performing safety assessments of software development processes using verification-intensive procedures. The purpose of research project 3.2.2, "Digital System Dependability," is to provide the staff with capabilities for performing safety assessments of safety-related software development products using validation-intensive procedures. The verification-intensive safety assessment procedures and the validation-intensive safety assessment procedures overlap in the Implementation phase and the Test and Integration phase. This overlapping provides a necessary transition from the process safety assessment function to the product safety assessment function. Combining the process and product safety assessment capabilities into an integrated, comprehensive set of procedures will improve the consistency and quality of existing safety assessment activities.

In addition to the process-oriented and product-oriented safety assessment capabilities described above, research project 3.2.3, "Self-Testing Methods," will develop guidance for performing safety assessments of self-testing features in digital safety systems. This research will address (1) effectiveness of self-testing in determining system performance; (2) adverse effects of self-testing on safety system performance; (3) appropriate self-testing methods for safety systems; (4) the amount of self-testing that is sufficient for safety systems; (5) the additional complexity that self-testing features add to system reviews; and (6) methods for modeling the additional complexities in PRAs. The products of this research will provide guidance, acceptance criteria, review tools and methodologies, and associated training for the staff to perform safety assessments of self-testing features in digital safety systems.

3.2.1 Assessment of Software Quality

Supported NRC Offices: NMSS and NRR

3.2.1.1 Background and Issues

As the complexity of digital systems grows, vendors are increasingly utilizing development tools to design system architectures. The NRC has approved several generic platforms that can be used in a wide array of safety systems, such as the Teleperm XS specification and coding environment (SPACE), which uses a graphical user interface that hides the details of the lower-level system architecture from the user. Since the user is interacting with the development tool from a higher level, small design and implementation errors could go unnoticed. Consequently, the challenge is determining whether these development tools can be trusted to produce safe and reliable products.

A recent research project, "Digital System Software Requirements Guidelines," NUREG/CR-6734, Volumes 1 and 2 (ML0123301601, ML0123301841), identified 15 LERs in which digital system "failure[s] had safety significance" and "the proper definition and implementation of a software requirement would have mitigated or prevented the failure". This research suggests that additional assurances of software quality and reliability are desirable, particularly in identification and review of digital system safety significance.

Additionally, as microprocessor capabilities have become more extensive, system developers have been able to incorporate more complex applications in a single microprocessor system. For example, one proposed NPP safety system combines RPS functions and engineered safety features functions on the same microprocessor. An issue arises from this configuration, in that a software error that results in a single microprocessor failing to function could affect both the RPS functions and the engineered safety features system functions on the microprocessor channel. Thus, a CMF could potentially affect all safety-related functions in the plant.

Approving generic platforms benefits licensees and vendors by reducing the scope of review issues for specific systems developed using the platforms. This should result in an expedited review for specific implementations at nuclear facilities. An issue arises, however, when a specific system is implemented using the platform because the platform may not replicate the original platform that the NRC approved. Typically, the same components may be used but may be configured differently, or new component designs (e.g., different microprocessors and communication protocols) may be implemented in the platform in the years following the NRC's last review of the platform.

The use of metrics for evaluating development process quality is addressed in general terms by Regulatory Guide 1.152, which endorses the latest revision to IEEE Std 7-4.3.2 with some exceptions. Section 5.3.1.1 of IEEE Std 7-4.3.2-2003 requires that software quality metrics must be considered throughout the software life cycle to assess whether software quality requirements are met, and references IEEE Std 1061-1998, "IEEE Standard for a Software Quality Metrics Methodology." However, the NRC has not endorsed the use of specific software quality metrics.

In an effort to develop software system acceptance criteria to supplement existing regulatory guidance, the NRC sponsored research by Lawrence Livermore National Laboratory (LLNL) to survey current state-of-the-art practices in software reliability assessment. Through this research, LLNL identified and ranked measures that could potentially assist the NRC in evaluating the reliability of a software-intensive system.

Subsequently, the NRC sponsored a study by the University of Maryland (Umd), Center for Reliability Engineering, to validate the measures and associated ranking for assessing digital system reliability. The results of these two research projects showed that although the software development industry commonly uses approximately 80 engineering measures, a subset of metrics may be effective in evaluating software reliability. On that basis, UMd developed a method for using these measures in a reliability prediction system. (Implicit in the prediction of reliability using measures, is that reliability is one of the most important quality attributes). This research and the preliminary validation of the method were described in NUREG/GR-0019, "Software Engineering Measures for Predicting Software Reliability in Safety-Critical Digital Systems" (ML003775310), and NUREG/CR-6848, "Preliminary Validation of a Methodology for Assessing Software Quality" (ML042170285). Since the results of the preliminary validation were favorable, the development and large-scale validation of the research conducted by UMd and LLNL on the use of software engineering measures to assess software quality will be continued in this project (NRC Job Code Y6591, "Software Reliability Code Measurements").

This research project will also support improvements in augmented review processes, such as the NRC Audit Assistant, which is a database application used by NRC reviewers to organize digital system audits, record audit results, and provide weighted scores of audit results. Using a Yes/No question/answer format, the NRC Audit Assistant identifies specific topics that the NRC reviewer should consider over the life cycle of a digital safety system development process. While specific topics and associated questions are identified, the process by which an NRC reviewer can answer each question has not been incorporated into the tool. Additionally, a Bayesian decision process (for example) for evaluating an acceptable level of safety system quality may be a better approach than the rudimentary weighted scoring approach that is currently incorporated in the NRC Audit Assistant tool.

Additionally, the HRP is performing collaborative research with the NRC to determine software engineering practices and criteria that are effective in ensuring software quality (NRC Job Code N6290 “Halden Digital System Safety”).

3.2.1.2 Tasks

This research project will develop review procedures to augment the NRC’s existing processes for determining the quality and dependability of digital safety systems used by nuclear facilities and medical and industrial byproduct users. These review procedures will supplement SRP-guided safety assessments of digital safety systems.

Additionally, this research project will acquire, develop (if necessary), and improve existing tools for reviewing digital system development life cycle processes and products. The tools will augment the NRC’s processes and procedures for licensing digital safety systems used by nuclear facilities, applications, and byproduct material users.

These tools and review procedures will be validated using a large digital system model typical of those planned for use in the nuclear industry.

This research project has the following goals:

A. Acquire, develop (as necessary), and improve tools and review procedures for reviewing digital system development processes.

B. Develop acceptance criteria for the assessment tools and review procedures through cooperative interactions with the digital technology industry, the nuclear industry, and the public.

C. Prepare user documentation for each digital system development process assessment tool and review procedure.

D. Develop curricula for training the staff on the use of the tools and review procedures for reviewing digital system development processes.

3.2.1.3 Products

The results of this research project will be regulatory guidance that recommends acceptance criteria for each assessment tool and review procedure. Developing these acceptance criteria will augment regulatory assessments of digital system implementations. Additionally, this research activity will develop a curriculum for NRC staff to ensure that the tools and review procedures are used in a manner that is consistent with the agency's regulatory guidance. The NRC will encourage the nuclear industry to develop products that contain information appropriately formatted for use as input data for the tools and review procedures the staff will use to evaluate nuclear industry digital systems.

This research project is intended to produce the following products:

- tools and review procedures for reviewing digital system development life cycle processes
- acceptance criteria for the assessment tools and review procedures
- user documentation for each digital system development process assessment tool and review procedure
- NRC staff training courses on the use of the tools and review procedures for reviewing digital system development processes

3.2.2 Digital System Dependability

Supported NRC Offices: NMSS and NRR

3.2.21 Background and Issues

Basically, there are four approaches to dependability:

(1) Fault Avoidance: Preventing Errors from ever existing
(2) Fault Detection: Detecting Faults after they occur
(3) Fault Correction: Correcting errors or the effects of errors
(4) Fault Tolerance: Maintaining system functionality in the presence of faults

The objective of high-quality design processes is to minimize the introduction of errors into the system design. The objective of V&V processes is to identify and remove faults introduced during the system development process. Together, these two sets of processes (V&V) are the primary fault avoidance strategies addressed by the software quality assessment research program described above. However, the complexity of digital systems commonly is such that, regardless of the rigor of traditional quality assurance processes used during the development life cycle (i.e., design processes and V&V processes), errors can remain undetected in a system.

The purpose of system testing is to detect errors that were not discovered during the system development process (e.g., improper handling of faults). However, the process by which the system developer determines the set of tests that is sufficient to attain the desired level of assurance that the system quality is appropriate (i.e., the test coverage) is not well-defined.

Test coverage is defined as a measure of the proportion of a system exercised by a test suite (usually expressed as a percentage). Determining test coverage typically involves collecting information about which parts of a system are actually executed when conducting a series of tests in order to identify the branches, statements, or paths that have been tested. The most basic level of test coverage is branch coverage testing, and the most methodical level is path coverage testing. Some intermediate levels of test coverage exist, but are rarely used. Ideally, a test suite should test 100% of a system; however, 100% test coverage in complex systems may not always be attainable. One category of routines that is generally less well-tested than the functional routines is the fault-handling routines (i.e., Fault Detection, Handling & Tolerance), because, in the typical manufacturing environment, it is difficult to generate a complete set of hardware and software faults.

A good example of improper fault handling is described in two LERs concerning similar design-basis accident (DBA) sequencer malfunctions (see Accession No. ML9605070254). In both cases, the programmable logic controller (PLC) microprocessor unit was found to be failed in the field, and it was not possible to recreate the failure using troubleshooting processes. In these cases, it was not possible to identify the faults, or what should be changed to properly address the faults in the future. This experience suggests that the normal functional testing process should be augmented in the area of fault identification and handling.

One process for performing fault testing involves systematically inserting faults into a system, and then monitoring the system to determine its behavior in response to the faults. This process (fault injection) is performed using a combination of four techniques: (1) hardware-based, (2) software-based, (3) simulation-based, and (4) a hybrid approach. Hardware-based fault injection involves augmenting the system under analysis with specially designed test hardware to allow for the injection of faults into the system. Typically, these faults are injected at the IC pin level, although processors can sometimes be subjected to internal faults depending upon the test facilities built into the processor itself. Traditionally, software-based fault injection, on the other hand, involves modifying the software executing on the system under analysis in order to provide the capability to modify the system state (both processor registers and memory) according to the system developer's model view of the system.

Simulation-based fault injection involves constructing a simulation model of the system under analysis, including a detailed simulation model of the processor in use. The simulation models are developed using a hardware description language such as the Very High-Speed Integrated Circuit Hardware Description Language (VHDL).

A hybrid approach combines two or more of the other fault injection techniques to more fully exercise the system under analysis. For instance, performing hardware- and software-based fault injection experiments can yield significant benefit in terms of time to perform the fault injection experiments, reduced initial setup time before beginning the experiments, and so forth. However, given the significant gain in controllability and observability with a simulation-based approach, it might be useful to combine a simulation-based approach with one or more of the other approaches to more fully exercise the system under analysis.

In an effort to develop fault injection techniques to augment and supplement existing regulatory guidance and processes, the NRC sponsored research by the University of Virginia (UVa) to survey existing definitions and associated applications of CCFs and CMFs. This research determined that, because there is tight integration of hardware and software components in embedded digital systems, both must be analyzed in a unified manner [NUREG/GR-0020, "Embedded Digital System Reliability and Safety Analysis" (ML010570243)]. Fault injection was identified as a promising methodology for supporting this unified analysis.

The NRC, Électricité de France (EDF), the Federal Railroad Administration (FRA), Lockheed-Martin Inc., Maglev Inc., the New York City Transit Authority, and Union Switch & Signal Inc. are cosponsoring research on system-level risk assessment and numerical safety quantification of safety-critical systems at the UVa Center for Safety-Critical Systems (CSCS) and the Center of Railroad Safety-Critical Excellence (CRSCE) Safety Assessment Lab (SAL) (NRC Job Code K6079, "Digital System Dependability Performance"). System-level risk assessment is performed using the Axiomatic Safety-Critical Assessment Process (ASCAP), a simulation environment developed by the CRSCE. ASCAP uses a Monte-Carlo simulation approach to derive system-level risk metrics and to allocate numerical safety targets for safety-critical processor-based subsystems. These numerical safety targets are expressed in terms of the mean time to hazardous event (MTTHE) metric, which represents the average time to an unsafe failure of the system. The MTTHE metric can be expressed as a function of the system failure rate and fault coverage, which represent a measure of the system's ability to detect the presence of faults and react in a safe manner.

Typically, system failure rates can be estimated using common reliability analysis techniques. The challenge is estimating hardware and software design faults that may exist in the system. However, fault coverage is typically a difficult parameter to estimate and becomes the focus of the MTTHE compliance process. This process involves developing analytical, statistical, and fault/error models of the system, and creating a set of faults to be injected into the system. Fault injection can involve augmenting either the system hardware or software to support physical fault injection, or developing simulation models of the system hardware which can execute the actual system software and support fault injection. The results of fault injection experiments can then be used to develop a statistical estimate of the system fault coverage and the associated MTTHE.

(Note: In addition to the methodology described above for testing fault-handling routines, the Software Engineering Laboratory (SELab) of the Halden Reactor Project (HRP) is performing NRC-sponsored research to identify formal principles and adequate methods to systematically prove, on the basis of source code, the operational independence of functions; that is, analysis of fault tolerance. This research includes performing a case study and evaluating its results in order to demonstrate the feasibility of automating these principles and methods in a software tool. The testing methodology described above will be compared to the analytic tool developed by HRP.)

3.2.2.2 Task

This research project has the following goals:

A. Develop a state-of-the-art tool and methodology for determining the dependability of digital safety systems.

B. Establish dependability acceptance criteria for safety systems on the basis of the tool and methodology results.

C. Develop curricula for training the staff on the use of the tool, methodology, and acceptance criteria for evaluating the dependability of digital safety systems.

3.2.2.3 Products

This research project is intended to yield the following products:

- a state-of-the-art tool and methodology for determining the dependability of digital safety systems
- dependability acceptance criteria on the basis of the tool and methodology results
- NRC staff training course(s) on the use of the tool, methodology, and acceptance criteria for evaluating the dependability of digital safety systems

3.2.3 Self-Testing Methods

Supported NRC Offices: NMSS and NRR

3.2.3.1 Background and Issues

Systems may use self-testing methods to continuously test for hardware or software faults in digital systems. Because they are very similar to system diagnostics conducted by a technician or operator, self-testing methods can improve the availability of digital systems. The technical issues associated with self-testing methods concern the effect of self-testing on I&C systems that are currently installed in nuclear facilities and those being developed for future installation. This concern includes (1) effectiveness of self-testing in determining system performance, (2) the adverse effects of self-testing on safety system performance; (3) appropriate self-testing methods for safety systems, (4) the amount of self-testing that is sufficient for safety systems, (5) additional complexity that self-testing features add to system reviews, (6) added difficulty in maintaining a system after it is in operation, and (7) modeling the additional complexities in PRAs. In other words, the central question is whether the added complexity contributed by self-testing features is worth the added likelihood that a safety system could fail to operate as a result of a self-testing function fault.

An example of a self-testing defect that caused the Turkey Point Unit 3 EDG load sequencer to fail to respond to an SI test signal that required a transfer of the Unit 3 SI pumps to the Unit 4 SI system was reported to the NRC on November 15, 1994, in Information Notice 94289 (ML9411210123) and LER 94-005-02 (ML9508080294). The self-testing defect could have prevented the EDG load sequencers from responding to input signals requiring loading and starting of the SI pumps. The problem arose in designing the sequencers such that if a "real" emergency signal was received while the sequencer was in self-test mode, the test signal would clear and the engineering safety features controlled by the sequencer would be activated. The self-testing feature was not properly implemented and, consequently, would have prevented the SI pumps from being started.

Another example of a self-testing defect that caused problems in an NPP safety system was reported to the NRC on June 29, 1999, in Information Notice LD-99-036 (ML9907070151). A self-testing feature in the oscillation power range monitor (OPRM) used by 12 boiling-water reactor NPPs could have caused one or more OPRM trip channels to be out of service for a short period of time. Specifically, the self-testing defect concerned the slave OPRM module randomly resetting, potentially causing the OPRM trip channel to be out of service for a short period of time (typically less than 1 minute). The defect could have led to a failure to detect and suppress unstable thermal-hydraulic-induced core power oscillations. The defect was traced to a priority baton error on the microprocessor used in this OPRM design, and was such that, had a slave OPRM not been used to check the operability of the master OPRM, the error would not have occurred.

Currently, because of limited NRC staff time and resources, safety evaluations of digital systems generally focus on the safety functions performed by the digital system. Usually, only minimal focus is placed on the interaction of self-testing features with safety functions, except for scheduling aspects of performing self-testing between cyclic calculations of trip function states. This research project will augment existing guidance in the NPP SRP with guidance regarding the types of self-testing that could potentially adversely affect safety, and the appropriate amount and type of self-testing features that should be implemented in digital safety systems.

3.2.3.2 Tasks

This research project has the following goals:

A. Develop technical guidance and review procedures for evaluating self-testing features in digital systems.

B. Develop curricula for training the staff on the use of the guidance and review procedures for performing safety assessments of self-testing features in digital systems.

3.2.3.3 Products

This research project is intended to yield the following products, as appropriate:

- technical guidance and acceptance criteria for evaluating self-testing features in digital systems
- NRC staff training course(s) on the use of the technical guidance and review procedures for performing evaluations of self-testing features in digital systems

3.3 Risk Assessment of Digital Systems

As discussed in the NRC's Policy Statement on Probabilistic Risk Assessment (PRA), the agency intends to increase its use of PRA methods in all regulatory matters to the extent supported by state-of-the-art PRA methods and data. Since digital systems will play an important role in NPP safety, the need for risk assessment methods for digital systems becomes more evident. An ASP database study 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 its prevalence and potential impact on plant safety, future risk-informed regulatory decisions are likely to require risk assessment of digital systems.

The NRC Research Plan for Digital Instrumentation and Control for FY 2000 – FY 2004 (ML012080254) identified the need for the NRC to use tools and methods to perform quantitative risk assessments of NPP digital systems. It is important that nuclear facility and application licensees evaluate digital system implementations to ensure that new systems do not result in more than a minimal increase in the frequency of occurrence of an accident or the likelihood of occurrence of a malfunction of a structure, system, or component important to safety. Determining the frequency or likelihood of such events involving digital modifications, in any but a purely qualitative way, requires digital system performance and reliability evaluation capabilities.

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. Toward that end, this research program will investigate the use of methods, tools, and criteria to meet these three digital risk assessment objectives. Thus, the research will assess the types and causes of failures that can occur in digital systems, characterize the risk-importance of I&C systems (impact of digital failures on safety), develop digital reliability assessment methods (frequency of failures), and collect and analyze the data needed to support this work. The staff also recognizes that this research may reveal that it is not practical to integrate digital systems (including software) into PRAs, and that a PRA may not be an efficient or accurate tool for digital system review. Nonetheless, this conclusion cannot be reached without the necessary supporting research.

3.3.1 Development and Analysis of Digital System Failure Data

Supported NRC Offices: NMSS and NRR

3.3.1.1 Background and Issues

This research project is a continuation of the research initiated by the NRC Research Plan for Digital Instrumentation and Control for FY 2000 – FY 2004 (ML012080254) . The NRC has already begun work on this project through a cooperative agreement with the Organization for Economic Cooperation and Development, Nuclear Energy Agency (OECD/NEA) (NRC Job Code N6010, "COMPSIS").

By analyzing digital system failure data, the NRC seeks to determine which digital failures would have the largest impact on safety, and then focus risk assessment activities and review efforts accordingly. Additionally, analysis of digital system failure data could provide feedback on the effectiveness of the NRC's regulatory programs. Implicit in these objectives is the need to have sufficient digital failure data available for these analyses. However, there are several issues related to analysis of the data.

The first issue regarding analysis of digital system failure data is not the lack of data, but the inability to collect the data. For example, LERs provide some digital system failure data, but it is often difficult to determine the cause of the failure from the content of the reports. The ability to identify the root cause of failures, their effects, and how the failures could have been prevented is the type of analysis needed to support the regulatory review and risk analysis of digital systems. Most licensees maintain a record of I&C failures that provides some of this information; however, the low number of safety-related digital systems results in a low number of failure reports. Nonetheless, access to this information would support this research project.

Another issue is the ability to apply the collected data to similar systems that are currently in use. A research task will develop an inventory of digital systems currently in use in the nuclear industry, including the particular applications for which each is used. The digital system data will then be categorized by plant system, product line, or product type. It will then be possible to quantify failure rates across product lines by associating the product lines with known failures from LERs or plant maintenance databases. Furthermore, licensees could use this inventory for reference in future plant upgrades. Digital system data sources could include industry organizations such as EPRI, and may require input from licensees to ensure data accuracy.

Process industries use COTS digital equipment similar to that used in the nuclear industry. In addition to data from other industries, other potential sources of COTS digital equipment failure data include the U.S. Department of Defense (DoD) and the National Aeronautics and Space Administration (NASA). Both the defense and aerospace industries have made a strong effort to implement COTS equipment in their high-integrity systems. Some of the same COTS equipment problems found in defense and aerospace systems may translate to nuclear industry digital systems important to safety. Using the experience of other industries would help the NRC to address potential digital I&C problems before they occur. However, when a digital component fails, many users replace the component without documenting the root cause of the failure because the documentation process is not cost-effective compared to the cost of simply installing a relatively inexpensive replacement component. Consequently, only the most serious failures are formally addressed and documented (i.e., failures that have significant consequences relative to cost or loss of life).

3.3.1.2 Tasks

The purpose of this research project is to populate a database of digital system failure data from existing sources; analyze the data systematically to identify the frequency, severity, cause, and possible prevention of each digital I&C failure; and then train NRC staff on the use of the data and analysis techniques.

This research project has the following goals:

A. Collect and assess digital system failure data from domestic and foreign nuclear facilities and industries that use digital systems critical to safety. Particular attention will be paid to COTS digital system equipment.

B. Evaluate digital system failure assessment methods used by defense, aerospace, and other industries to determine their contributions to overall safety.

C. Develop a process for analyzing the digital system failure data to identify the frequency, severity, cause, and possible prevention of digital system failures.

D. Develop curricula for training the staff on the use of the digital system failure database and database assessment process.

3.3.1.3 Products

This research project is intended to yield the following products:

- regulatory guidance documenting the results and conclusions from the assessment of digital system failure data
- regulatory guidance reports documenting digital system failure assessment methods used by defense, aerospace, and other industries to determine their impact on overall safety
- tools and review procedures for performing reliability assessments of digital systems
- NRC staff training course(s) on the use of the digital system failure database, the database assessment process, and the tools and review procedures for performing reliability assessments of digital systems

3.3.2 Development of Digital System Failure Assessment Methods

Supported NRC Offices: NMSS and NRR

3.3.2.1 Background and Issues

Identifying failure modes in digital systems (e.g., software faults, system faults, external events, environmental conditions, or security events) and then determining their effect on safety are the first steps in evaluating digital system contributions to risk at a nuclear facility or in industrial or medical applications of byproduct materials. Because of the complex design and operation of digital systems, such systems can have a large number of failure modes; however, not all of these failure modes may result in safety-significant system failures. Therefore, those failure modes that can affect the safety function are of greatest interest when determining digital system contributions to the total risk assessment of a nuclear facility. For example, an NPP digital RPS may not be able to correctly time stamp an event (an internal fault), but if the RPS is still capable of initiating a reactor trip within the required response time, the fault would not result in a safety-significant digital RPS failure. Consequently, the fault would not contribute to the total NPP risk.

With regard to the nuclear power industry, NPP licensees are required to prove by analyses that their NPPs remain in a safe state during selected design-basis events that are postulated to occur coincident with a single failure of the safety system function that would be required to mitigate the event. This is the "single failure criterion" licensing-basis condition. With digital systems, it is difficult to prove that a safety system meets the single failure criterion because it is difficult to prove the absence of faults that could adversely affect redundant identical safety channels and trains. Similar challenges may exist for industrial and medical users of byproduct materials.

Using a D3 analysis, it is often assumed that, in lieu of identifying specific failure modes, the redundant channels in the digital safety system have failed, and an analysis is performed to show that the facility or application will continue to operate safely. Consequently, D3 analyses using this approach do not provide the information required for risk assessment of digital systems because these analyses do not identify specific failure modes within the system, or how those failure modes might affect other systems.

When including a digital system as a "black-box" in PRAs, the primary concern is determining the probability that the digital system will perform on demand, complete its safety function, not prevent the function from happening, not perform unintended functions, and not initiate its safety functions until they are required (i.e., the system performs its function despite the potential presence of faults). Potential digital system failure modes can be identified either through data analysis or by analytical means. By analyzing data, potential digital failures may be recognized if those failures have occurred in other systems. While some failures may not be applicable to the digital system under analysis, those identified through data analysis could provide a baseline in the identification process.

Digital system failures may also be identified through various analytical methods that identify digital failure modes and their impact on safety. Some common methods include hazard analysis, failure modes and effects analysis, fault tree analysis, and operability analysis. At this time, guidance and criteria are not well-defined with regard to the use of these methods (i.e., depth of analysis, scope, etc.) and how such methods might be used to support risk assessments of digital systems. The objective of this research project is to develop a process by which digital system failure modes can be identified and characterized by their impact on required safety functions. The NRC has already begun work on this project through a cooperative agreement with OECD/NEA (NRC Job Code N6010, "COMPSIS").

3.3.2.2 Tasks

This research project has the following goals:

A. Survey the analytical methods for identifying digital system failure modes and their impact on safety. Describe the advantages and disadvantages of each method; and provide recommendations for digital system failure assessment techniques and the criteria for using the techniques for risk assessments of digital systems.

B. Conduct case studies of digital safety systems using the recommended digital system failure assessment techniques to determine (1) the amount of effort associated with the proposed criteria and methods, (2) the effectiveness of the criteria, and (3) suitability of the criteria and methods for nuclear facility and byproduct material applications.

Revision 06/2

C. Develop curricula for training the staff on the use of the analytical techniques and the criteria for using each technique.

3.3.2.3 Products

This research project is intended to yield the following products:

- regulatory guidance documenting the results and conclusions from the survey of analytical methods for identifying digital system failure modes and their impact on safety
- regulatory guidance documenting the case studies and the conclusions derived from studies regarding the effectiveness of the digital system failure assessment techniques
- NRC staff training course(s) on the use of the analytical techniques and the criteria for using each technique

3.3.3 Identification of Digital System Characteristics Important to Risk

Supported NRC Offices: NMSS and NRR

3.3.3.1 Background and Issues

A large number of digital systems may be used in nuclear facilities and industrial and medical byproduct applications, but only a portion may be important in terms of risk. It is necessary to determine the risk-importance of these systems for two reasons. First, risk-importance could be used to determine the required level of regulatory review. In situations where the digital system is not risk-important, less review may be required. It could also help focus research efforts on the aspects of those digital systems having a significant impact on safety. Second, risk-importance evaluations could help identify those digital systems that are significant in terms of risk, but may be overlooked during safety evaluations and PRAs. This situation is particularly true of embedded digital systems, such as in circuit breakers, diesel generator systems, and other important systems and components.

The risk-importance of digital systems has been investigated in general risk studies (e.g., individual plant examinations and NPP RPS studies). While the studies sufficiently identified the risk associated with some major safety systems, they did not address systems throughout the subject facilities (including those embedded in larger NPP systems). Therefore, this research issue involves developing digital system models (where models do not exist) and calculating the risk-importance of the digital systems, including those that are embedded in larger risk-important systems. The NRC has already begun this research through a cooperative agreement with Ohio State University (OSU), Pennsylvania State University (PSU) and the University of Tennessee (UT) (NRC Job Code K6472, “Risk Importance of Digital Systems”).

Identification of digital systems for developing risk models for PRAs may be performed through the analysis of piping and instrumentation diagrams and other technical information describing facility systems. One avenue that could help identify embedded digital systems would be to use systems identified as part of the assessments that were conducted at nuclear facilities in preparation for the Year 2000 transition. Since the design and layout of these facilities vary, one possibility is to calculate risk-importance on a generic basis by using a group of reference facilities, and then utilize a complete PRA of several facilities as a baseline.

If an identified digital system does not exist in a facility PRA model, the study could establish and document necessary assumptions and acceptance guidelines in order to incorporate the digital system into the PRA. For small or simple systems, risk models may need to be developed only to the point where the digital system is considered a “black box.” By treating the small or simple digital systems as a black box, the change in risk could be estimated for cases in which the simple digital system black box fails.

For large or complex systems, it may be necessary to develop risk models beyond the black box level to address specific risk-significant components. This “gray box” or “white box” approach may be necessary to ensure that components of larger digital systems that could be significant risk contributors are identified and appropriately addressed in the PRA model. The process by which these risk-significant components of large or complex digital systems are identified should be standardized, with corresponding acceptance guidelines, to ensure that the process is performed consistently for each system.

3.3.3.2 Tasks

This research project has the following goals:

A. Identify and develop generic risk models of digital systems and components of systems in nuclear facilities.

B. Calculate the risk-importance of the generic digital systems.

C. Develop risk models beyond the “black box” level for large or complex risk-important digital systems.

D. Develop a process for identifying sub-components of digital systems that may warrant special regulatory and/or research attention.

E. Develop curricula for training the staff on the risk-importance of digital systems.

3.3.3.3 Products

The results of the risk-importance study will be documented in a technical report. This report will be used by NRC staff involved in both digital system and PRA reviews, and this could help the NRC make its activities and decisions more effective, efficient, and realistic. For example, as licensees conduct more digital modifications of safety systems, the NRC staff may be able to adjust the depth of its reviews and better allocate resources to those digital modifications having the highest risk-importance. From a PRA perspective, knowing the risk-importance of digital systems will help the NRC determine the level of detail required to accurately model digital systems. In addition to providing guidance on the risk-importance of digital systems and components, acceptance guidelines should be developed to ensure that the systems are appropriately modeled. The results will support future research efforts by identifying risk-important areas, issues, and acceptance criteria.

This research project is intended to yield the following products:

- regulatory guidance documenting the results and conclusions from the development of the nuclear facility digital system risk models
- regulatory guidance describing the calculation of risk importance of the nuclear facility digital system risk models
- regulatory guidance describing the risk models beyond the “black box” level for large or complex high-risk-important digital systems
- regulatory guidance describing a process for identifying sub-components of digital systems that may warrant special regulatory and/or research attention
- NRC staff training course(s) on the risk-importance of digital systems

3.3.4 Development of Digital System Reliability Assessment Methods

Supported NRC Offices: NMSS and NRR

3.3.4.1 Background and Issues

An important aspect of risk analysis of digital systems is determining the likelihood of a digital system failure. Since digital systems play a key role in the operation of safety systems (and therefore affect risk), occasions will arise in which the reliability of digital systems should be evaluated. Data for analog systems is not necessarily applicable to digital systems and, therefore, those data cannot be used to estimate the reliability of digital systems. The reliability of digital components may be better than analog components; however, digital equipment is more complex in design, and offers a greater potential for design errors.

A second reason for evaluating the reliability of digital systems involves reducing uncertainty in PRAs. For example, RG 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis” (ML023240437), mentions two types of uncertainty, namely aleatory and epistemic uncertainty. Aleatory uncertainty involves the randomness of events, while epistemic uncertainty (to a degree) involves a lack of knowledge about the model and its parameters. Therefore, epistemic uncertainty can be reduced by gaining knowledge about the model and its parameters. Current NPP PRAs, for example, do not model the majority of digital systems, but include these systems within other NPP systems. To reduce the epistemic uncertainty associated with PRAs, it will become necessary to model and estimate the likelihood of digital system failures.

Estimating the likelihood of analog system failures is straightforward since operational history exists for these systems and the estimation process is well-developed. However, estimating the likelihood of digital system failures is more complicated. First, because digital systems are more complex from a design and operational standpoint, they requrie more time and effort in the modeling process. The complexity also expands the number of potential faults to a very large number. Second, many digital systems provide self-tests and fault recovery routines. Therefore, a digital system fault may or may not result in a failure, depending upon the success of fault detection and recovery. Third, system design errors may not lead to a failure unless certain inputs and conditions are reached. Therefore, digital systems may successfully pass a large number of tests, and yet fail because an unexpected input or condition occurred and triggered the latent error. Unfortunately, it is very difficult to relate those unexpected inputs and conditions into the reliability estimates.

Industry and academia have worked to develop digital system reliability estimation methods. Some of the basic methods estimate digital hardware reliability using available data and then estimate software reliability according to software test results. The hardware and software reliability are then combined to generate a digital system reliability. Other methods consider both the hardware and software as an integrated system to account for their interactions and dependencies.

At present, the NRC does not have standard methods for determining the failure probability of digital systems. If an acceptable method was available, the evaluation of new technology would be simplified and the review of digital systems could be generalized to a greater extent. The challenge for the NRC is to identify digital system reliability assessment methods that (1) provide adequate model completeness, (2) do not require an excessive amount of effort, and (3) can be applied to digital equipment in safety systems, including COTS equipment. The challenge in this area of research is identifying methods for determining the likelihood of failure for complete digital systems (hardware and software). The acceptance criteria for using those methods must also be identified.

The incorporation of analog system architectures and characteristics into the research could provide a necessary probabilistic baseline that could be used to compare the effect of implementing a digital system relative to an analog system. This comparison could provide valuable insights into the comparative effect of digital systems on PRAs.

Since digital system reliability assessment is state-of-the-art, this project is expected to span several years. The NRC has begun work on these tasks through a cooperative agreement with OSU, PSU, and UT (NRC Job Code K6472, “Risk Importance of Digital Systems”). By participating in the cooperative agreement, the NRC is able to better manage its resources to achieve the desired outputs, and it is able to tap into the experience and knowledge gained by academia, other Government agencies, and industry. Additionally, the NRC is performing collaborative research with HRP to test digital reliability assessment methods (NRC Job Code Y6349, “Halden Environmentally Assisted Cracking”). The results of this research will be integrated with the results of the OSU, PSU and UT research.

Revision 06/2

3.3.4.2 Tasks

The first task will identify digital system reliability assessment methods and analyze their benefits and shortcomings (i.e., assessed according to effectiveness in estimating digital system reliability and effort required for assessment). During this phase, there may arise a need to further develop some of the promising reliability assessment methods to a state that would be suitable for NRC use. In particular, reliability assessment methods should be developed to the state where they also can address COTS equipment. Case studies involving nuclear applications should be used to identify the suitability and required modifications to the identified reliability assessment methods.

The second task will recommend a digital system reliability assessment method suitable for NPPs, and possibly extend the results to industrial and medical uses of byproduct materials. Along with this recommendation, this task will provide guidelines and acceptance criteria for using the identified method. Before the second phase is executed, results of the first phase will be assessed to determine the probable success of using the identified method. A pilot project using the recommended digital system reliability assessment method will be used to determine the applicability of the reliability assessment method to nuclear systems, its effectiveness for determining reliability, and its ease of use.

This research project has the following goals:

A. Identify digital system reliability assessment methods and determine the advantages and disadvantages of each method.

B. Recommend digital system reliability assessment method(s) suitable for nuclear facility and application licensing activities.

C. Develop curricula for training the staff on the use of the recommended digital system reliability assessment method.

3.3.4.3 Products

The results of these tasks will be a series of technical reports describing digital system reliability assessment methods and their acceptable use. The guidance and acceptance criteria for digital system reliability assessment methods will be included in regulatory guidance that describes an acceptable method for digital system risk assessment. The results of these tasks will prepare the NRC for risk-informed regulatory activities and decisions by (1) supporting review of digital system risk assessments, (2) facilitating the calculation of risk change associated with digital system upgrades, and (3) providing the capability to reduce PRA uncertainty where digital systems play a significant role in safety.

This research project is intended to yield the following products:

- regulatory guidance describing the advantages and disadvantages of the digital system reliability assessment methods identified in Task A
- regulatory guidance recommending digital system reliability assessment method(s) suitable for nuclear facility and application licensing activities
- NRC staff training course(s) on use of the recommended digital system reliability assessment method(s)

3.4 Security Aspects of Digital Systems

Digital systems provide many advantages that are not as readily available in analog systems; for example, system parameters may be reviewed and changed while the system is operating, and new versions of the system may be installed from remote locations. However, these features can be disadvantages from a security standpoint.

As stated in Section 3.1.7, "Common Mode Failures, Diversity, and Defense-in-Depth," when identical or nearly identical digital systems are used in multiple channels of a process system as a means of achieving functional redundancy, a failure in two or more channels arising from a fault in the digital system is classified as a CMF. The purpose of quality assurance activities is to detect and eliminate or mitigate faults as early in the digital system life cycle as possible to prevent digital system failures. Another source of CMF failures that can occur in digital systems involves failures caused by deliberate actions on the part of a hostile individual or organization, either by accessing the digital system after it is installed, or providing unauthorized access during the system development process.

Lapses in security can be more difficult to detect than lapses in quality assurance, in that security vulnerabilities may be deliberately incorporated into digital systems with the intent to evade traditional fault detection measures, or system vulnerabilities may not be considered when specifying system requirements. Unless specifically addressed, these vulnerabilities can adversely affect quality assurance strategies designed to enhance system reliability. A research effort to acquire or develop processes and tools for detecting security vulnerabilities could enhance digital system reliability by remedying or mitigating security vulnerabilities that could result in system failures.

Security of digital systems important to safety involves addressing potential security vulnerabilities as part of the system development process, and maintaining the security of the system after installation. Several digital system development platforms anticipated for use in safety applications in the nuclear industry have been reviewed and approved by the staff. Therefore, security assessments should be performed on digital systems developed using these platforms, as well as systems composed of COTS digital equipment.

General security guidance is provided in NRR BTP HICB-14 and is restated as a regulatory position in RG 1.152, Rev. 2. Review processes for confirming that the security guidelines in BTP HICB-14 and RG 1.152, Rev. 2, have been appropriately implemented may require supplemental information. Additional guidance also is provided in NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants."

Three classes of security threats must be addressed. The most common class of security threats involves cyber attacks, in which individuals and undocumented organizations concentrate on incorporating or exploiting vulnerabilities in digital systems with the intent to disrupt system operations or illegally obtain information from the systems. A second class of security threats, although less common, is from electromagnetic (EM) attacks that can be used either to physically damage digital equipment or to disrupt digital equipment operations by overwhelming the digital computers with concentrated EM energy. A third class of security threats is from unauthorized access to safety system networks. In each of these cases (cyber attacks,

EM attacks, and network access), QA goals are effectively compromised because safety systems could be caused to fail, operate at an inappropriate time, or cause a nuclear facility operator or byproduct material user to respond inappropriately to erroneous signals or indications.

Security aspects of digital systems is a new program in the NRC Digital System Research Plan for FY 2005 – FY 2009. The NRC Research Plan for Digital Instrumentation and Control for FY 2000 – FY 2004 (ML012080254) did not specifically address security, but rather implied security-related research in program areas such as wireless communications and firewalls.

3.4.1 Security Assessments of Cyber-Vulnerabilities

Supported NRC Offices: NSIR

3.4.1.1 Background and Issues

The purpose of cyber security assessments is to detect and eliminate or mitigate vulnerabilities in the digital system that could be exploited either from outside the digital system protected area (e.g., a social miscreant or hostile nation-state) or from inside the digital system protected area (e.g., a disgruntled employee). The process of defending against this class of failures is made more challenging by the rapidly evolving "industry" that is developing new attack methods on a daily basis. For example, as of the middle of September 2004, one company providing antivirus software for Microsoft Windows™ operating systems reported cataloguing 68,125 viruses in its database. While the Windows™ operating system is not used in safety-related operating systems of nuclear facilities, this example indicates the aggressive nature of the cyber community in developing new methods of attacking computer-based systems. It is reasonable and prudent to expect a similar aggressiveness toward other operating systems and computer-based applications, including those used in the nuclear industry. In addition to developers of viruses, worms, and associated computer programs, there is an industry of 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.

The basis for emphasizing digital system cyber security measures against outside threats is supported by several Federal agencies. In a report on "Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination (Testimony, 07/26/2000, GAO/T-AIMD-00-268)," dated July 26, 2000, the General Accounting Office (GAO) stated, "The National Security Agency has determined that potential adversaries are developing a body of knowledge about U.S. systems and about methods to attack these systems." In "Joint Vision 2020," DoD stated, "The United States itself and the U.S. forces around the world are subject to information attacks on a continuous and regular basis regardless of the level and degree of engagement in other domains of operation." On February 23, 2000, in a Statement for the Record before the Congressional Joint Economic Committee, "Cyber Threats and the U.S. Economy," John A. Serabian, Jr., the Information Operations Issue Manager at the Central Intelligence Agency (CIA) stated that the CIA is detecting doctrine and offensive cyber warfare programs in other countries; that foreign nations have begun to include intelligence warfare (IW) in military doctrine and teachings regarding defensive and offensive applications; and that foreign nations are now aware of the need to disrupt the flow of information that traverses civilian infrastructures that support military strategies. Executive Order 13010, "Critical Infrastructure Protection," dated July 15, 1996, identified as

U.S. critical infrastructure telecommunications, electrical power systems, gas/oil storage and transport, banking and finance, transportation, water supply systems, emergency services, and continuity of Government. As an example of an infrastructure attack (whether by an individual or hostile nation state is irrelevant), on January 25, 2003, the SQL Slammer Worm infected 90% of vulnerable computers worldwide within 10 minutes of release, and doubled in size every 8.5 seconds, with a full scanning rate of 55 million scans per second.

The basis for emphasizing digital system cyber security measures against threats from a person inside the digital system protected area is supported by several factors. A person with authorized access to the digital system understands the system; knows what data and systems are critical and available; knows the location of the data and systems; can access the data and systems at opportune times; and can thereby use those access opportunities to introduce malicious programs that could disrupt systems operations.

A common perception is that system security is assured by allowing only "trusted" individuals to have access to critical systems. These trusted individuals can be either employees or contractors/temporary hired help. The basis for this perception appears sound; however, an article by M.T. Reed, which appeared in *Federal Computer Week* on August 2, 2004, reported that, in 2003 (i.e., a single year), the Federal Inspectors General (IGs) (1) realized potential savings of $18B in investigations of fraud, waste, and abuse, (2) initiated 6,500 successful prosecutions, and (3) suspended or disbarred from government contracting more than 7,600 individuals and businesses. It is highly likely that one or more of the 6,500 people prosecuted and one or more of the 7,600 individuals or businesses that were disbarred from government contracting were considered, at one time, to be trusted persons or businesses. Clearly, experience does not support the perception that allowing only trusted persons or businesses access to critical systems will ensure the systems are secure.

Two security-related NRC orders issued in the wake of the terrorist attacks on September 11, 2001, mandated, in part, that NPP licensees take certain actions to enhance cyber security of their digital systems. In response, through a contract with Pacific Northwest National Laboratory (PNNL) and in cooperation with the Nuclear Energy Institute (NEI) Cyber Security Task Force, the NRC developed NUREG/CR-6847, "Cyber Security Self-Assessment Method for 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 NUREG/CR-6847 as a foundation, the Task Force prepared NEI-04-04, "Cyber Security Program for Power Reactors," to provide NPP licensees with comprehensive guidance for developing and managing an effective cyber security program. NEI-04-04, currently in draft form, is expected to be implemented voluntarily by the nuclear power industry.

As part of the agency's ongoing effort to respond to the two security-related NRC orders issued in the wake of the terrorist attacks on September 11, 2001, the Commission will codify the mandated cyber security enhancement requirements in new regulations in 10 CFR Part 73. Additionally, the staff will develop regulatory guidance that relies heavily on the work to develop NUREG/CR-6847, which the industry used in its NEI-04-04 program management guideline. In so doing, 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/CR-6847.

Revision 06/2

In a memorandum on "Status of Cyber Security Activities at Nuclear Power Plants," dated October 5, 2004 (ML0422230386), the staff informed the Commission of the activities described above, and stated that the Commission would be advised of needed regulatory actions based on the results of NRC licensee implementations of NEI 04-04. In the meanwhile, the staff is developing a comprehensive cyber security plan to guide the large number of activities in this growing area of concern. The NSIR staff may consult with RES, NRR, and the Office of Information Services (OIS) as this plan is developed.

The NRC is planning to engage other Federal agencies, most notably the Department of Homeland Security and the Federal Energy Regulatory Commission, as well as the North American Electric Reliability Council, in an effort to leverage related work these agencies have completed or are conducting. The NRC also is participating in a project sponsored by the inter-governmental Technical Support Working Group (TSWG) to develop a software-based tool that will facilitate the implementation of NUREG/CR-6847, and to develop a device that will provide secure communications for Supervisory Control and Data Acquisition (SCADA) systems. The tool is expected to use a question/answer format to guide security audits of installed networks and digital systems through the NUREG/CR-6847 topic areas. The product of this research may be integrated into the NRC's cyber security review processes.

3.4.1.2 Tasks

This research project will study cyber security aspects of digital systems and components approved for safety applications in nuclear facilities and applications and acquire or develop a regulatory policy, set of tools, review procedures, and guidelines to support cyber security assessments and development of cyber security guidelines for nuclear facilities and applications. This research will include the following tasks:

A. Evaluate cyber security aspects of digital systems in nuclear facilities and applications.

B. Develop regulatory policy, and acquire or develop tools (as appropriate), review procedures, acceptance criteria, and guidelines to support cyber security assessments of digital systems in nuclear facilities and applications.

C. Develop curricula for training the staff on the use of the regulatory policy, tools, and review procedures for performing cyber security assessments of digital systems in nuclear facilities and applications.

3.4.1.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory policy and guidance and describing the cyber security aspects of digital systems in nuclear facilities and applications
- tools, review procedures, and guidelines to support cyber security assessments of digital systems in nuclear facilities and applications
- NRC staff training course(s) on the use of the regulatory policy, tools, and review procedures for performing cyber security assessments of digital systems in nuclear facilities and applications

3.4.2 Security Assessments of EM Vulnerabilities

Supported NRC Offices: NSIR

3.4.2.1 Background and Issues

Aside from physical destruction of computers, attacks on computers can be classified as attacks through legitimate computer gateways, such as the modem and the keyboard (cyber attacks), and attacks through other-than-legitimate gateways (backdoor attacks). Vulnerability of computers to cyber attacks is addressed by the research project described in Section 3.4.1, "Security Assessments of Cyber Vulnerabilities."

At the current technological level, backdoor attacks can be carried out mainly by utilizing RF technology and, thus, can be classified as EM attacks. (These attacks should not be confused with passive surveillance of emanated signals by unauthorized personnel). Furthermore, as opposed to simple computer failures, levels of redundancy in a digital system may not address vulnerabilities to an EM attack. The purpose of EM security assessments is to detect and then eliminate or mitigate vulnerabilities in the digital system that could be exploited by an EM attack.

One premise underlying many special applications of RF technology is based on the principal that any wire or electronic component is, in fact, an unintended antenna, both transmitting and receiving. Importantly, every such unintended antenna is particularly responsive to its specific resonance frequency and, to some extent, several related frequencies, although it is not responsive to other frequencies under normal conditions. If the objective of an attack is to influence the device's functioning, then appropriate RF signals could be transmitted to the targeted device. That RF signal, being received by pertinent components of the device, would generate a corresponding signal within the device. Producing and transmitting a signal which would effectively control the targeted device through an EM attack is an extremely difficult task that requires technology and expertise that is not readily available. However, producing and transmitting a signal to disrupt the normal functioning of the target devise is a much simpler technological task. This type of attack can be classified as a jamming RF attack.

Jamming RF attacks can utilize either HERF or LERF EM attack technology. HERF EM attack technology is very advanced, and its practical applications are still being developed and tightly controlled by the appropriate Federal agencies. HERF attacks are based on concentrating large amounts of HERF EM energy within a small space, narrow frequency range, and a very short period of time. The result of such concentration is an overpowering non-nuclear EM pulse, capable of causing substantial damage to electronic components. If the HERF EM pulse is strong enough, it can damage electronic components, regardless of their specific resonance frequencies.

By contrast, LERF EM attack technology utilizes relatively lower energy, and is spread over a wide frequency spectrum. It can, however, be effective in disrupting normal functioning of computers because its wide RF spectrum may contain frequencies matching the resonance frequencies of critical components. Generally, the LERF EM attack approach does not require time compression, and does not utilize high-tech components. The technology and expertise for this type of attack are widely available, inexpensive to build, and requires components that may be purchased at most electronics supply sources. One serious aspect of an LERF EM attack on a digital system is that an unprotected microprocessor in the digital system could produce

random unpredictable outputs. The induced malfunction could result in a single, easily correctable processing error, a total loss of system functionality, or generation of unsafe commands to a subsystem controlled by the computer. Because the affected computer may be a component in a larger system network, the failure of the computer might trigger a snow-balling effect with second, third, and following chain failures. The full effect of such an event is difficult to predict or neutralize, unless the digital systems are reliably protected against EM attacks.

Although the research proposed in this section does not directly support the NRC's plans described in Section 3.4.1 above, it is prudent to conduct research to better understand how proposed safety-related digital systems respond to deliberate (and perhaps malevolent) use of EM energy fields. Digital systems can be tested by certified EM testing laboratories to ensure that they will operate properly when subjected to expected EMI (from any source). The challenge is identifying the appropriate EM levels at which digital systems must be tested to address potential EM threats. Once these levels are identified, the laboratories can generate testing signals similar to those of expected EM weapons. Although the Commission has not considered EM weapons as a credible threat to nuclear power facilities, some limited anticipatory research in this area is warranted.

3.4.2.2 Tasks

This research project has the following goals:

A. Identify and evaluate the EM security aspects of digital systems in nuclear facilities and applications.

B. Acquire or develop a set of tools (as appropriate), review procedures, and acceptance criteria to support EM security assessments of digital systems in nuclear facilities and applications.

C. Develop curricula for training the staff on the use of the tools and review procedures for performing EM security assessments of digital systems in nuclear facilities and applications.

3.4.2.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance describing the EM security aspects of secure digital systems in nuclear facilities and applications
- tools and review procedures to support EM security assessments of digital systems in nuclear facilities and applications
- NRC staff training course(s) on the use of the tools and review procedures for performing EM security assessments of digital systems in nuclear facilities and applications

3.4.3 Network Security

Supported NRC Offices: NSIR

3.4.3.1 Background and Issues

Networking is the interconnection of subsystems (e.g., controllers, actuators, and sensors) with the objective of communicating among the subsystems. This networking of subsystems within a larger system can present security vulnerabilities in the system as a result of weaknesses in the network design that could be exploited via a cyber attack propagated through a vulnerable subsystem. These vulnerabilities could be inherent in the system features or could be incorporated into the system features during system development or prior to system installation.

The research described in Section 3.4.1, "Security Assessments of Cyber Vulnerabilities," will develop processes for assessing the cyber security of networks currently installed in NPPs. The network security research project described in this section will address secure network design techniques for networks yet to be installed in nuclear facilities. This research will obtain from digital industry security experts information regarding cyber vulnerability mitigation strategies that can be built into or added onto digital system architecture designs during the network design and development phase. The research will also identify strengths and weaknesses of various network architecture designs, including built-in and added-on cyber vulnerability mitigation strategies. The areas to be addressed will include design features that prevent or mitigate insider cyber attack vectors, outsider cyber attack vectors, and developer cyber attack vectors.

Network security research will be conducted to develop the following assets:

- guidance on appropriate mitigation measures
- regulatory acceptance criteria complementing existing NRC security assessment processes for confirming implementation of security mitigation measures
- recommendations regarding acquisition of T&M for evaluating secure network designs using the acceptance criteria
- assistance in developing review procedures and inspection procedures
- corresponding training curricula for the NRC staff

In the event technical guidance cannot be correlated to existing regulatory requirements, this research project will recommend the scope of new regulatory requirements or interpretation of existing regulations that could be correlated to the recommended acceptance criteria.

Unlike wired networks, wireless networks use the electromagnetic frequency spectrum (typically operating in the Gigahertz frequency range) as the primary communication medium. The advantage of using wireless network technology in harsh environments such as NPPs and high-level waste storage facilities is that the same capabilities of a wired network can be achieved with a wireless network while reducing the time workers are exposed to the harsh environment during the installation of the network resources. Additionally, since the installation of additional cabling is not required with wireless networks, reconfigurations of network assets may be performed more cost-efficiently.

Wireless technologies that have had a significant impact on the non-nuclear industry already include the following:

- wireless LANs, in which several computers are interconnected by wireless devices
- radiofrequency identification (RFID) tagging, in which small RFID devices can be used for numerous applications, including inventory control and access management
- radiofrequency sensor technology

Despite its benefits for use in harsh environments, such as in containment buildings at NPPs and high-level waste storage facilities, there are issues with wireless networking that remain of concern because of its potential impact on safety resulting from cyber attacks (e.g., increased likelihood of failure or mis-operation of safety equipment). The significant security vulnerability difference with wireless networks is that wireless networks transmissions are not confined to a conductive path that can be easily controlled. For example, while wired communications can be intercepted and corrupted by unauthorized persons, it is typically easier to control access to these signals than signals that are transmitted wirelessly.

In general, there must be a layered defense approach to wireless network security because no single security measure can ensure a wireless network is impenetrable. Combinations of the following measures should be employed where possible: (1) password protection, (2) encryption, (3) administrative controls, (4) network diversity and segmentation, (5) firewalls, (6) access point management (roaming), and (7) signal strength management.

Thus far, a number of security-related issues associated with implementing wireless systems have been identified and assessed, and regulatory issues associated with deployment have been investigated. Future plans include validating tools and review procedures for assessing the security of wireless systems in the nuclear facilities.

Wireless network security research will be conducted to identify wireless technologies appropriate for safety systems in nuclear facilities, and to develop the following assets:

- guidance for administrative controls, engineering designs, network diversity, and segmentation strategies for protecting wireless systems from cyber attacks
- regulatory acceptance criteria complementing existing NRC security assessment processes for confirming implementation of security mitigation measures
- recommendations regarding acquisition of tools and methodologies for evaluating secure wireless network designs using the acceptance criteria
- assistance in developing review procedures and inspection procedures
- corresponding training curricula for the NRC staff

Communication pathways outside nuclear facilities via modems and computer networks are provided to key personnel such as the facility manager. While these computer systems are not part of nuclear facility safety system architectures, many of these systems are relied upon by facility operators to determine the status of important processes. The use of firewalls provides the primary method for restricting access to these nuclear facility networks. However, firewalls are effective only when they are correctly implemented and maintained.

Recent cyber attacks that prevented access to computer system network resources by overloading commercial sites, and penetrated secure DoD computers illustrate the potential for social miscreants and others to circumvent firewalls and corrupt data stored in computers. This ability to penetrate firewalls poses a potential threat to nuclear facility safety and security. For example, safety systems might be caused to operate by causing a nonsafety-related feedwater system in an NPP to fail, which could result in a reactor trip and initiation of engineered safety features systems to maintain the plant in a safe state.

The purpose of firewall research is to develop regulatory guidance for reviewing the installation, maintenance, and operation of firewall applications in nuclear facilities.

Firewall research will be conducted to develop the following assets:

- classification and characteristics of firewalls
- general guidance on security policies for firewalls
- guidance on installing and maintaining firewalls
- expanded review guidance of NUREG/CR 6847 to assist reviewers in evaluating the security risk of firewalls
- NRC training course(s) on the use of the regulatory guidance and the review procedures for firewall applications in nuclear facilities

3.4.3.2 Tasks

This research project has the following goals:

A. Identify network features appropriate for nuclear facilities and applications and formulate guidance for administrative controls, engineering designs, network diversity, and segmentation strategies for protecting networks from cyber attacks.

B. Acquire or develop security tools and review procedures for safety-related network applications.

C. Investigate on-going worldwide efforts to develop regulatory guidance for installing and maintaining firewall applications in safety-related applications.

D. Develop review procedures for identifying potential vulnerabilities in safety-related firewall applications.

E. Develop curricula for training the staff on the technical guidance and use of the security tools and review procedures for safety-related network applications.

3.4.3.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance on network features appropriate for nuclear facilities and applications for administrative controls, engineering designs, network diversity, and segmentation strategies for protecting networks from cyber attacks
- security tools and review procedures for network applications in nuclear facilities
- regulatory guidance for installing and maintaining safety-related firewall applications

- review procedures for identifying potential vulnerabilities in safety-related firewall applications
- NRC staff training course(s) on the technical guidance and security tools and review procedures for evaluating safety-related network applications

3.5 Emerging Digital Technology and Applications

When economic incentives sufficiently outweigh the costs, vendors, licensees, owners groups, and nuclear industry representatives (e.g., NEI and EPRI) usually propose the introduction of new technologies into systems important to safety in nuclear facilities. These new technologies may be in the form of systems to be implemented in existing nuclear facilities, or may involve advanced nuclear facility designs. By becoming informed of the operation, design, and reliability of emerging I&C technologies and applications, the NRC is better prepared to make future regulatory decisions in these areas. Knowledge about and the capability to assess these new, emerging technologies are critical to assisting NMSS, NRR, and NSIR staff in reviewing these systems.

This research will include developing additional information on these technologies, acquiring or developing assessment tools and review procedures (if applicable), and (as appropriate) revising regulatory guidance to support unique features of each new technology. Many of the research projects described in this program are ongoing projects being performed for the NRC by ORNL (NRC Job Code Y6962, “Emerging Technologies”).

This research plan will address the following areas of research regarding new technologies:

- System Diagnosis, Prognosis and Online Monitoring
- Radiation Hardened Integrated Circuits and Components
- Advanced Instrumentation
- Smart Transmitters
- ASICS and FPGAs
- Wireless Technology

The areas of research regarding system diagnosis, prognosis, and online monitoring; advanced instrumentation; smart transmitters; and wireless technology were introduced in the NRC Research Plan for Digital Instrumentation and Control for FY 2000 – FY 2004 (ML012080254). The NRC Digital System Research Plan for FY 2005 – FY 2009 builds on that foundation by elaborating on these technological advances with the addition of radiation-hardened ICs and components, as well as ASICs and FPGAs.

3.5.1 System Diagnosis, Prognosis, Online Monitoring (SDPM)

Supported NRC Offices: NMSS and NRR

3.5.1.1 Background and Issues

The goal of SDPM techniques is to provide improved, online methods of identifying, monitoring, and mitigating errors and impending failures to maintain the operability of the equipment. Another application of this technology may be in the area of virtual instrumentation and parameter estimation, such that performance and applications of existing instrumentation can be enhanced. These enhancements could result in improved plant performance and additional economic benefit; however, additional safety concerns could arise as a result of estimating plant conditions on the basis of virtual instrumentation.

Advances in microelectronics, smart sensor technology, and artificial intelligence are making it possible to advance the state-of-the-art in SDPM. For example, smart sensor technology is being used for on-board intelligent signal processing, reasoning, and data fusion for identification of impending failures in centrifugal charging pump gearboxes. Online monitoring technology is being integrated with wireless communication technology to implement condition-based monitoring programs in situations where it can be very costly to maintain the physical cable connections between equipment monitoring devices. Software-based systems are being developed to assist operators with detection of anomalies in dynamic systems, identification of the faulty components responsible for the anomalies, and optimization of the response to the upset conditions.

As with other rapidly advancing technologies, the NRC must continue to be proactive and monitor the technology trends in SDPM, with a view to addressing any new regulatory challenges. The technical issues that will need to be addressed include methods adopted in performing online monitoring and diagnostics that do not compromise equipment operability or availability. Additionally, most SDPM systems involve significant amount of software; thus, software quality becomes an issue of concern. Also, uncertainties in the analysis of these systems must be thoroughly understood.

For several years, the nuclear power industry has been applying online diagnostic methods because of restricted accessibility to vital mechanical components and the safety implications associated with their failure. A significant number of available diagnostic systems provide online information and monitoring of loose parts, vibration, leakage, dynamic fatigue, reactor core status, and so forth. Rapid development of microprocessors is promoting increased application of embedded microprocessors, computers, and display systems to provide higher-level information on equipment and process behavior, and scenario prediction for development of countermeasures. Many of these online diagnostic systems use embedded software, and some include fuzzy logic and neural networks. The question of the impact of software and hardware on digital system quality assurance remains a significant challenge.

Many SDPM systems are classified as process diagnostic systems related to plant operability, although they do have an impact on safety through their effect on operator actions or maintenance scheduling. The NRC has already begun work on this research through a cooperative agreement with OSU, PSU, and UT (NRC Job Code K6472, "Risk Importance of Digital Systems"). This research project will investigate issues arising from the integration of these systems into the main control room, their impact on operator performance and control room practice, and approaches to digital system quality assurance.

3.5.1.2 Tasks

This research project has the following goals:

A. Survey the use of SDPM methods in nuclear facilities, review state-of-the-art SDPM methods, and evaluate the effectiveness and uncertainties of SDPM methods.

B. Develop review procedures for SDPM applications in nuclear facilities.

C. Develop curricula for training the staff on the use of the review procedures for SDPM applications.

3.5.1.3 Products

This research project is intended to yield the following products:

- revised guidelines for applying SDPM methods in nuclear facilities (e.g., RG 1.118, "Periodic Testing of Electric Power and Protection Systems"), and procedures for reviewing SDPM applications in nuclear facilities
- review procedures for SDPM applications in nuclear facilities
- NRC staff training course(s) on the guidance and review procedures for evaluating SDPM applications

3.5.2 Radiation-Hardened Integrated Circuits

Supported NRC Offices: NMSS and NRR

3.5.2.1 Background and Issues

Ionizing radiation from alpha particles in packaging materials, beta particles, protons, neutrons, pions, and muons can have adverse effects on integrated circuits. The two most important effects are (1) displacement damage, in which the radiation causes physical damage to the crystal lattice (mainly the SiO_2 used to isolate neighboring transistors, gate isolation, and surface passivation in ICs); and (2) ionizing effects, in which the radiation literally knocks off orbital electrons from an atom. Most ionization effects in microelectronics can be related to either the total amount of radiation that is absorbed (total dose) or the rate at which radiation is absorbed (dose rate). Radiation-hardened integrated circuits (rad hard ICs) are electronic circuit components that have been specially designed to withstand the damaging effects of ionizing radiation. Approaches such as minimizing gate oxide thickness during IC manufacture and using GaAs or silicon-on-sapphire components are two methods of mitigating the adverse effects of ionizing radiation.

Variability in the radiation response of COTS devices is currently a significant radiation-hardness assurance (RHA) issue. However, emerging approaches such as rad-hard technologies and improved manufacturing processes may resolve this impediment. These improvements are most likely to be seen first in space applications. Therefore, it is warranted to monitor special-purpose applications while confirming the radiation tolerant characteristics of commercial ICs. This should help guide the formulation of a framework for using IC-based digital equipment for safety-related applications in harsh environments in nuclear facilities.

Application of COTS components and emerging IC technologies for nonsafety digital systems in nuclear facilities and applications is beginning, and the migration of such technologies into safety applications appears to be inevitable. A number of issues should be evaluated, including enhanced low dose rate (ELDR) effects and single-event effects (SEEs) phenomena.

The ELDR effect in linear bipolar integrated circuits is an example of an effect that cannot be dealt with using traditional RHA methods. The basic problem is that certain types of bipolar devices degrade far more severely at low dose rates (.001 to .005 kGy(Si)/s) than at the higher dose rates used in most older testing methodologies. An issue resulting from this behavior is that different failure modes can occur under low dose rate conditions than at high dose rate conditions, which makes it impossible to fully bound the problem by testing only at high dose rates. Another issue is that nearly all manufacturers of linear ICs produce some products with dose rate sensitivity, but there are pronounced differences in the response of different devices and processing lines to the same radiation environment.

A SEE results from a single, energetic particle causing an IC to malfunction. Single-event phenomena can be classified into three effects (in order of permanency):

- single event upset (soft error)
- single event latchup (soft or hard error)
- single event burnout (hard failure)

A single event upset (SEU) is defined by NASA as “radiation-induced errors in microelectronic circuits caused when charged particles (usually from the radiation belts or from cosmic rays) lose energy by ionizing the medium through which they pass, leaving behind a wake of electron-hole pairs.” SEUs are transient, nondestructive soft errors. A reset or rewriting of the device results in normal device behavior thereafter. An SEU may occur in analog, digital, or optical components, or may have effects in surrounding interface circuitry. SEUs typically appear as transient pulses in logic or support circuitry, or as bit flips in memory cells or registers. Also possible is a multiple-bit SEU, in which a single ion affects two or more bits and causes simultaneous errors. Multiple-bit SEUs are a problem for single-bit error detection and correction where it is impossible to assign bits within a word to different locations, such as in dynamic random access memory (DRAM) components and certain static random access memory (SRAM) components. A severe SEU is the single-event functional interrupt (SEFI) in which an SEU in the device’s control circuitry places the device into a test mode, halt, or undefined state. The SEFI halts normal operations, and requires a power reset to recover.

Single event latchup (SEL) is a condition that causes loss of device functionality as a result of a single-event-induced current state. SELs are hard errors, and are potentially destructive (i.e., may cause permanent damage). The SEL results in a high operating current above device specifications. The latched condition can destroy the device, adversely decrease the bus voltage, or damage the power supply. Originally, the concern was latchup caused by heavy ions; however, latchup can be caused by protons in very sensitive devices. An SEL is cleared by a power off-on reset or power strobing of the device. If power is not removed quickly, catastrophic failure may occur as a result of excessive heating, or metallization or bond wire failure. SEL is strongly temperature-dependent; the threshold for latchup decreases at high temperature.

Single event burnout (SEB) is a condition that can cause device destruction as a result of a high current state in a power transistor. SEBs cause the device to fail permanently. SEBs include burnout of power metal-oxide-semiconductor field-effect transistors (MOSFETs), gate ruptures, frozen bits, and noise in charge-coupled devices (CCDs). An SEB can be triggered in a power MOSFET biased in the OFF state (i.e., blocking a high drain-source voltage) when a heavy ion deposits enough charge to turn the device on. SEB susceptibility has been shown to decrease with increasing temperature.

A power MOSFET may undergo single-event gate rupture (SEGR), which is the formation of a conducting path (i.e., localized dielectric breakdown) in the gate oxide, resulting in a destructive burnout. SEB can also occur in bipolar junction transistor single-event dielectric rupture (SEDRs). SEDR (also referred to as micro-damage) occurs in the complementary metal-oxide semiconductor (CMOS) and is similar to SEGR observed in power MOSFETs.

Manufacturers measure SEEs in failures in time (FITs); one FIT equals one failure in 10^9 device hours. Typical hard failures, such as electromigration, have a FIT of 1 to 50, and the aggregate failure rate is approximately 200 FITs. However, unchecked soft errors can have FITs of 50,000 per IC.

SEEs were first observed in orbiting satellites in the mid-1970s and have since been observed as a growing problem at lower altitudes in lockstep with IC-process-geometry reductions, lower voltages, and increasing clock speeds. Since the early 1980s, SEEs have occurred in commercial electronics, and are now becoming a dominant reliability-failure mechanism in modern CMOS technologies, memory ICs, FPGAs, and devices using combinatorial logic.

An example of SEEs affecting commercial equipment was reported in an article, entitled "Sun Screen," by Daniel Lyons, which appeared in *Forbes Magazine* on November 13, 2000. According to that article, Sun Microsystems, Inc., recalled workstations in the late 1990s as a result of "…an odd problem involving stray cosmic rays and memory chips in the flagship Enterprise server line, whose models are priced at $50,000 to more than $1 million." The article went on to state, "The problem involves 'cache' memory chips, which store the most frequently needed code for instant access. In May [2000], after months of struggling to identify the cause, Sun found it had been shipping servers whose cache modules contained faulty SRAM (static random access memory) chips from a supplier it won't name. The faulty chips are easily disrupted by stray radiation, alpha particles, or cosmic rays. The trouble occurs at the bit level — a one turns into a zero, or vice versa. When the computer detects an error in memory, it shuts down and reboots itself. High altitude, high temperatures, and other factors can contribute to the problem."

A field notice on a Web site sponsored by Cisco Systems, Inc., entitled, "Cisco 12000 Single Event Upset Failures Overview and Work Around Summary" (http://www.cisco.com/en/US/products/hw/routers/ps167/products_field_notice09186a00801b3df8.shtml), reports another example of SEEs affecting commercial equipment. According to that field notice, Cisco 12000 line cards may reset after single event upset (SEU) failures. This field notice highlights some of those failures, why they occur, and what workarounds are available.

SEEs may become more commonplace as microprocessors and digital components progress from the older 2.5µm (250 nm) – 1.3µm (130 nm) lithography technologies into the 90nm, 65nm, 45nm, and smaller lithography technologies. Also, SEE problems could become more complex as the IC industry moves to system-on-chip designs because no one design team typically owns all of the areas [on-chip memory, logic, intellectual property (IP), and software) that SEEs can affect.

Manufacturers use accelerated testing to test most devices that are subject to time-to-market constraints. In accelerated testing, protons are directed into a tungsten-irradiating target product. For example, the testing spectrum can match the atmospheric spectrum caused by cosmic rays, but can be approximately one million times more intense than environmental rates. Tests have produced a wide span of results — from devices that fail almost immediately to devices that are resistant to SEEs. Such testing has allowed the development of tools and underlying models that allow users to simulate radiation strikes, taking into account both the strength of a strike and all possible angles of that strike on a part of a device.

NASA has developed a methodology for designing reliable space systems that addresses these RHA issues. The methodology includes hazard definition, hazard evaluation, requirements definition, evaluation of device usage, and application of radiation engineering techniques with the active involvement of designers. It may be possible to adopt this methodology, with some revision, for nuclear industry applications.

Technology advances and obsolescence of traditional analog equipment are leading to the use of IC-based electronics in the nuclear industry for nonsafety applications, followed by safety applications. The capability of current and emerging digital technologies to withstand ELDR-related events and SEEs over an extended period should be evaluated, and the radiation tolerant characteristics afforded by various implementation approaches should be determined. Such confirmatory research will support development of technical bases for guidance on effective design and implementation practices. As a result, the transition to IC technologies in the nuclear industry can be managed to avoid potential safety issues and licensing uncertainties.

3.5.2.2 Tasks

This research project has the following goals:

A. Determine radiation-hardened IC technologies appropriate for safety systems in nuclear facilities and applications.

B. Develop review procedures and guidance for qualifying radiation-hardened IC devices for use in safety systems for nuclear facilities and applications.

C. Develop curricula for training the staff on the use of the review procedures for licensing radiation-hardened ICs in safety systems for nuclear facilities and applications.

Revision 06/2

3.5.2.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance on radiation-hardened IC technologies appropriate for safety systems in nuclear facilities and applications
- review procedures and guidance for qualifying radiation-hardened IC devices for use in safety systems for nuclear facilities and applications
- NRC staff training course(s) on the guidance and review procedures for licensing radiation-hardened ICs in safety systems for nuclear facilities and applications

3.5.3 Advanced Instrumentation and Controls

Supported NRC Offices: NMSS and NRR

3.5.3.1 Background and Issues

Improvements in plant efficiency and safety through the use of advanced instrumentation (e.g., flow, temperature, pressure, and neutron flux) and controls (e.g., non-linear controllers, neural-fuzzy controllers, etc.) have encouraged nuclear facility licensees to retrofit existing instrumentation or implement advanced instrumentation for measuring processes important for safety (e.g., ultrasonic feedwater flow meters in support of measurement uncertainty recovery power uprates in NPPs).

Highly automated control rooms in other industries use modern control theory controllers to increase plant availability and decrease operator workloads. These advanced control approaches may be introduced in hybrid control rooms at existing NPPs and in advanced nuclear facility control room designs. These highly automated control rooms could include simple feed-forward controllers, non-linear controllers, neural-fuzzy controllers or even more advanced methods of control. How these control algorithms will affect the operational modes of nuclear facilities should be investigated.

To make timely and informed regulatory decisions regarding advanced instrumentation and controls, research in this area is focused on providing technical information to the NRC staff in a timely manner. Also, the NRC has been coordinating this research with the international community and will use the results of this collaborative research (NRC Job Code Y6873, “International Cooperative Research Program on Digital I&C”).

3.5.3.2 Tasks

This research project has the following goal:

A. Identify advanced I&C technologies appropriate for safety systems.

3.5.3.3 Products

This research project is intended to yield the following product:

- regulatory guidance identifying advanced instrumentation technologies appropriate for safety systems.

3.5.4 Smart Transmitters

Supported NRC Offices: NMSS and NRR

3.5.4.1 Background and Issues

Smart transmitters offer digital communication of data from the sensor to the control system. Some smart transmitters are also capable of providing compensating measures for instrument error or control functionality at the sensor. This technology could offer several advantages over instrumentation now used in nuclear facilities (e.g., digital communication of data from the sensor to the control system, and providing compensating measures for instrument error or control functionality at the sensor). Research in this area focuses on providing technical information to the NRC staff and developing regulatory acceptance criteria for this technology.

3.5.4.2 Tasks

This research project has the following goals:

A. Identify smart transmitter technologies and characteristics appropriate for safety systems in nuclear facilities and applications.

B. Develop review procedures for licensing nuclear facility and application safety systems that use smart transmitters.

C. Develop curricula for training the staff on the use of the guidance and review procedures for licensing nuclear facility and application safety systems that use smart transmitters.

3.5.4.3 Products

This research project is intended to yield the following products:

- regulatory guidance identifying smart transmitter characteristics appropriate for safety systems in nuclear facilities and applications
- review procedures for licensing nuclear facility and application safety systems that use smart transmitters
- NRC staff training course(s) on the use of the guidance and review procedures for licensing nuclear facility and application safety systems that use smart transmitters.

Revision 06/2

3.5.5 ASICs and FPGAs

Supported NRC Offices: NMSS and NRR

3.5.5.1 Background and Issues

Application-specific integrated circuits (ASICs) and field-programmable gate arrays (FPGAs) are not new to safety-related systems. The NRC approved a Westinghouse ASIC-based system for use in the nuclear industry, and Toshiba Corporation has stated that future Toshiba-based safety-related applications in the nuclear industry will be based on FPGA technology. While neither of these platforms has been used extensively in safety-related nuclear applications, there is a possibility that these emerging technologies will be submitted for NRC review in the foreseeable future.

ASIC and FPGA design processes are similar, but ASIC components have advantages over FPGA components in terms of cost (in large numbers), performance, and reliability. By contrast, as the name implies, FPGAs can be reconfigured after a control system has been installed, which is advantageous in terms of time-to-market and field maintenance. For this reason, experience in other safety-related industries shows that the design process for FPGA technology is less-stringent than for ASIC design projects because FPGAs are perceived as easy to modify and correct late in the development process. This perception has led to design methods that might not be acceptable for safety-critical systems because this places a disproportionate burden on validation (testing) activities.

Recent advances enable integration of intellectual property (IP) into ASIC and FPGA platforms in the form of CPU cores running proprietary software operating systems, digital signal processing (DSP) cores, and, in the case of ASICs, mixed-signal (i.e., digital and analog) SoCs. The capability to integrate IP into ASIC and FPGA platforms (CPU and DSP cores, mixed-signal SOCs, etc.) leads to very complex functionality on a single IC chip. The situation can be further exacerbated either by lack of adequate design documentation or diligence in reviewing the documentation when it is made available by the vendor. Even without such IP, the ASIC and FPGA platforms can contain hundreds of thousands of transistor gates, which allows extremely complex functionality on a single chip.

Another common and potentially serious misunderstanding about ASIC and FPGA technologies is that they are “less complex” than microprocessor-based systems. ASIC and FPGA devices are fundamentally complex “software designs implemented by hardware engineers.” As more functions are moved onto single IC chips, greater attention must be given to the system development process. Experience shows, however, that ASIC and FPGA disciplined design methodologies have not progressed at the same rate as the capability to add functionality to ASICs and FPGAs, implying that project managers may not fully appreciate the risk to safety. There could also be a perception that the process is improved by using automated software design tools. In fact, there may be an over-reliance on these design tools, as indicated by several projects in which problems were linked to improper use of the tools.

From a safety perspective, it is difficult to assess the correctness of ASIC and FPGA devices without extensive documentation, tools, and review procedures. Therefore, several aspects of these technologies should be addressed during safety reviews. First, reviewers need vendor information about ASIC and FPGA design processes , including software design tools and development methodologies (similar to that used for current software reviews). Second, reviewers must consider specific device design information (over and above the system-level documentation) for the system under review, such as requirements and design specifications, data sheets, user manuals, programmer's manuals, and so forth. Third, reviewers need device failure mode information, including mitigating fault tolerant designs (e.g., triple modular redundancy, concurrent error detection) and workaround design changes resulting from faults found too late in the design process to correct without extensive cost (a potential issue with third-party ASIC/FPGA devices). Fourth, to ensure consistent reviews of ASIC and FPGA safety systems, the NRC must acquire or develop tools and review procedures (as well as corresponding training) to support staff evaluations of safety functions implemented in ASICs and FPGAs.

Because NMSS, NRR, and NSIR are ultimately responsible for revising their standard review plans and interim staff guidance documents, outputs from this research will comprise NUREG-series reports, letter reports, and research reports for NRC staff. These reports will emphasize the importance of a proactive approach to safety assessments of ASIC and FPGA devices when incorporated into safety-related systems.

Also, several industry standards are available or under development regarding ASIC and FPGA design. The RES staff will review these industry standards and issue related regulatory guides as appropriate. Such regulatory guides will benefit both NRC staff and licensees replacing older analog and digital systems with modern digital systems incorporating ASIC and/or FPGA devices.

3.5.5.2 Tasks

This research project has the following goals:

A. Identify ASIC and FPGA components, design synthesis tools, best design techniques and practices, and failure modes and fault models used in safety-related systems in nuclear, aerospace, aeronautical, transportation, and process control industries.

B. Acquire or develop (as appropriate) safety assessment techniques (e.g., fault injection techniques, and quantitative analysis techniques), and associated review procedures for licensing ASIC and FPGA safety system applications in nuclear facilities and applications.

C. Develop curricula for training the staff on the use of the safety assessment techniques for licensing ASIC and FPGA safety system applications in nuclear facilities and applications.

Revision 06/2

3.5.5.3 Products

This research project is intended to yield the following products:

- regulatory guidance identifying ASIC and FPGA devices and design techniques appropriate for use in safety systems for nuclear facilities and applications
- safety assessment techniques and associated review procedures for licensing ASIC and FPGA safety system applications in nuclear facilities and applications
- NRC staff training course(s) on the use of the safety assessment techniques for licensing ASIC and FPGA safety system applications in nuclear facilities and applications

3.5.6 Wireless Technology

Supported NRC Offices: NMSS and NRR

3.5.6.1 Background and Issues

Wireless networking is the interconnection of subsystems (e.g., controllers, actuators, and sensors) without a physical medium such as copper wires, with the objective of communicating among the subsystems. Wireless networking uses the EM frequency spectrum as the primary communication medium, and typically operates in the Gigahertz frequency range.

Benefitting from the advances of the telecommunications industry, wireless technology is increasingly finding its way into the nuclear industry. The following wireless technologies have already had a significant impact on non-nuclear industries:

- wireless LANs, in which several computers are interconnected by wireless devices
- RFID tagging
- RF sensor technology

Application of wireless technology in the nuclear industry is likely to increase. The NRC, therefore, must continue to be proactive and monitor wireless technology trends, with a view toward addressing new regulatory challenges.

In addition to the modulation protocol issues briefly described in Section 3.1.2, “System Communications,” understanding communication protocol issues is important in addressing the application of wireless technology in nuclear safety environments. Despite the benefits of using wireless technology in harsh environments, such as in containment buildings at NPPs and high-level waste storage facilities, there are issues with wireless technology that remain of concern because of the potential impact on safety (e.g., increased likelihood of failure of the safety equipment) and security.

The NRC is studying wireless technology and its migration into nuclear facility balance-of-plant and business applications (NRC Job Code Y6475, “Wireless Technology”). The objective is to acquire an understanding of wireless technology and then develop the technical basis for guidance to address safety-related issues associated with the implementation of wireless systems in the nuclear industry.

Thus far, a number of safety-related issues associated with implementing wireless systems have been identified and assessed, and regulatory issues associated with deployment have been investigated. Confirmatory research is underway to simulate the operation of wireless systems in a NPP environment. A propagation model of the NPP environment is being developed and coupled with models of wireless systems. Future plans include validating the propagation model and conducting realistic simulations to assess the performance of wireless systems in the NPP environment.

The expected product is a set of computer models that can be used as an auxiliary resource to simulate the actual operation of wireless systems in nuclear facilities and confirm potential deployment issues. The results of the assessments, investigations, and simulations will be summarized to form the technical basis for guidance to address the safety-related issues and deployment considerations associated with implementing wireless systems in the nuclear industry. Additionally, where necessary, acceptance criteria will be developed to address the use of wireless technologies in the nuclear industry.

3.5.6.2 Tasks

This research project has the following goals:

A. Identify wireless technologies appropriate for safety systems in nuclear facilities;

B. Address safety-related issues and deployment considerations associated with implementing wireless systems in nuclear facilities.

C. Develop review procedures and acceptance criteria for licensing wireless technology applications in nuclear facility safety systems.

D. Develop curricula for training the staff on the use of the guidance and review procedures for licensing wireless technology applications in nuclear facility safety systems.

3.5.6.3 Products

This research project is intended to yield the following products:

- regulatory guidance identifying wireless technologies appropriate for safety systems in nuclear facilities
- regulatory guidance addressing safety-related issues and deployment considerations associated with implementing wireless systems in nuclear facilities
- review procedures and acceptance criteria for licensing wireless technology applications in nuclear facility safety systems
- NRC staff training course(s) on use of the guidance and review procedures for licensing wireless technology applications in nuclear facility safety systems

Revision 06/2

3.6 Advanced Nuclear Power Plant Digital Systems

The review process for next-generation reactor designs involves certifying standard reactor designs through a rulemaking process (Subpart B of 10 CFR Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants"). This design certification process requires applicants to provide the technical information necessary to demonstrate compliance with the safety standards set forth in NRC regulations (10 CFR Parts 20, 50, 73, and 100). Applicants for design certification must also provide information related to resolution of unresolved and generic safety issues; issues that arose after the accident at Three Mile Island; a detailed analysis of the design's vulnerability to certain accidents or events; and inspections, tests, analyses, and acceptance criteria. Prior to requesting a design certification review, vendors must provide preliminary design descriptions to the NRC in a pre-application submittal. The NRC reviews the pre-application submittal to identify issues that the vendor must address in its final application.

The NRC has received preliminary descriptions of the following advanced NPP designs:

- Atomic Energy of Canada Ltd Technologies, Inc., Advanced CANDU Reactor™ 700 (ACR-700)
- General Electric Company, Economic and Simplified Boiling-Water Reactor (ESBWR)
- Evolutionary Power Reactor (EPR)
- PBMR Pty., Pebble Bed Modular Reactor (PBMR)

Each of these designs incorporates unique design features that do not exist in the current generation of U.S. NPPs. The ACR-700, for example, will perform online refueling operations using robotic equipment. The NRC has not developed acceptance criteria for the review of robotic controls. These review requirements present challenges to the NRC staff that must be addressed before the design certification process can be completed.

One major area of research outlined on the Department of Energy (DOE) Long-Term Nuclear Technology Research and Development Plan involves instrumentation and controls. Several research topics proposed in this plan are of particular interest to advanced NPPs. In particular, these include robust communications and wireless sensors, smart instrumentation, and plant condition monitoring. Also of interest is research into distributed computing, advanced control algorithms, and online monitoring. Cooperative research funding has been allocated to INL to model advanced NPP instrumentation and control designs (NRC Job Code Y6946, "Modeling of Advanced Reactor I&C"). Additionally, in implementing its long-term research plan, DOE has developed six related Nuclear Energy Research Initiative programs. These include research in the areas of automatic generation of control architectures, self-diagnostic monitoring systems, smart sensors, and advanced instrumentation.

The national and international research community has also been involved in research and development of advanced control and monitoring systems for NPPs for many years (NRC Job Code Y6873, "International Cooperative Research Program for Digital I&C"). Compared to the United States, the international community (particularly in Europe, Japan, and Korea) has developed integrated advanced control rooms and performed more research in the areas of automated NPP operations and advanced NPP monitoring and diagnosis. Consequently, the NRC is working proactively with vendors, licensees, and international research organizations to stay abreast of developments and research results pertaining to advanced reactor designs and technologies. This effort includes participating in international conferences for exchange of information; participating in national and international standards committees and working groups (e.g., the OECD Expert Group on Digital Instrumentation and Control and the IAEA Online Monitoring Working Group); and collaborating with international research organizations (e.g., the Halden Reactor Project) on several research initiatives associated with advanced reactor designs. Additionally, this research may be useful for existing NPPs undergoing digital retrofits.

3.6.1 Advanced NPP Instrumentation

Supported NRC Offices: NRR and RES

3.6.1.1 Background and Issues

Some systems in advanced NPP designs will operate in conditions different from the current generation of NPPs. Consequently, it is expected that several new kinds of sensors may be developed to monitor these different conditions. For example, there may be temperature, pressure, flow, and neutron detector instrumentation that will require changes in the methods for performing design and safety calculations (drift, calibration, response time, etc). Current regulatory guidance and tools may need to be reviewed and enhanced to support the review of these systems.

Because of longer fuel cycles and much longer times between maintenance outages, the advanced NPPs may require more extensive use of online monitoring, diagnostics, and predictive maintenance. Instrumentation will be needed to support this increased automated surveillance. Additionally, the process by which these systems integrate with the control systems needs be understood.

3.6.1.2 Tasks

This research project has the following goals:

A. Characterize the capabilities and limitations of advanced instrumentation identified for use in advanced NPP safety systems.

B. Acquire or develop tools, review procedures, and acceptance criteria for licensing advanced instrumentation identified for use in advanced NPP safety systems.

C. Develop curricula for training the staff on the use of the tools and review procedures for licensing advanced instrumentation identified for use in advanced NPP safety systems.

Revision 06/2

3.6.1.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance characterizing the capabilities and limitations of advanced instrumentation identified for use in advanced NPP safety systems
- tools, review procedures, and acceptance criteria for licensing advanced instrumentation identified for use in advanced NPP safety systems
- NRC staff training course(s) on use of the tools and review procedures for licensing advanced instrumentation identified for use in advanced NPP safety systems

3.6.2 Advanced NPP Controls and Highly Integrated Control Room Designs

Supported NRC Offices: NRR and RES

3.6.2.1 Background and Issues

Advanced NPP designs may propose the use of relatively low-power (~100 MW) modular NPP units combined onto a single site. The use of multiple modular NPPs may require more complex control of both the primary instrumentation and control systems and the support systems. These complex controls could include simple feed-forward controllers, non-linear controllers, neural-fuzzy controllers, or even more advanced methods that the NRC has not reviewed. Advanced NPP designs may combine discrete safety control and trip capabilities within the same controller. How these control algorithms will effect the operational modes of modular NPPs should be investigated. Additionally, review guidance and tools may need to be acquired or developed to analyze these advanced control methods.

Advanced NPPs will be designed for operation with minimal supervision by plant operators for long periods of time. This may include automated startups, shutdowns, and changes of operating modes. For example, to be effective, modular NPPs must be operated like a single larger plant, with perhaps as few as 3 operators for 10 NPP modules at a site. NPP operations with a minimum of supervision will require more highly automated control systems for normal and off-normal conditions. The NRC needs to enhance its understanding of how NPP control and safety systems will be designed to cope with partial failures of interconnected systems, particularly at the switchyard and control room.

Advanced NPPs may be designed for operation with highly integrated “cockpit-style” control room designs. This design approach will require human-machine interface designs that rely extensively on digital software-based controls and possibly use of touch-screen and voice-actuated control technologies. Some designs apply strategies for co-mingling safety-related and nonsafety-related controls within the same controller device. Designs using touch-screens have been proposed and licensed in the United States; therefore, the NRC must enhance its understanding of how these control room design strategies comply with industry standards and regulatory requirements. With this enhanced understanding, the NRC can develop acceptance criteria, review methodologies, and review procedures for licensing advanced control room designs.

Detailed control systems design studies using plant simulators to help optimize advanced NPP control system designs are being performed by the vendors and through joint efforts with other organizations, such as universities and U.S. national laboratories, including ORNL and INL. There may be an opportunity to collaborate in some of these research programs, particularly in the areas of advanced control algorithms and control of multiple NPP modules.

3.6.2.2 Tasks

This research project has the following goals:

A. Characterize the capabilities and limitations of advanced controls identified for use in advanced NPP safety systems.

B. Acquire or develop tools (as appropriate), review procedures, and acceptance criteria for licensing advanced controls proposed for advanced NPP safety systems.

C. Develop curricula for training the staff on the use of the tools and review procedures for licensing advanced controls proposed for advanced NPP safety systems.

3.6.2.3 Products

This research project is intended to yield the following products, as appropriate:

- regulatory guidance for evaluating the capabilities and limitations of advanced controls proposed for use in advanced NPP safety systems
- tools, review procedures, and acceptance criteria for licensing advanced controls proposed for advanced NPP safety systems
- NRC staff training course(s) on use of the tools and review procedures for licensing advanced controls proposed for advanced NPP safety systems

3.6.3 Advanced NPP Digital System Risk

Supported NRC Offices: NRR and RES

3.6.3.1 Background and Issues

Additional risk modeling may be needed to understand the effect of the digital systems proposed for use in advanced NPP designs within a risk-informed licensing framework. Modeling will also be needed to support reviews of operator and control interfaces. Given the lack of models and data to support this risk analysis, the uncertainties in this area are relatively high. Much of this research will be performed in Research Project 3.3.4, "Investigation of Digital System Reliability Assessment Methods." The NRC has already begun work on this research through a cooperative agreement with OSU, PSU and UT (NRC Job Code K6472, "Risk Importance of Digital Systems"). The results of that research will be applied to support this research project.

Revision 06/2

3.6.3.2 Tasks

The first task will use the results of research project 3.3.4 to identify the suitability and required modifications of the identified reliability assessment methods for modeling risk contributions from digital systems proposed for use in specific advanced NPP designs (e.g., ACR-700, ESBWR, and EPR). The second task will recommend a digital system reliability assessment method suitable for each advanced NPP design. Along with the recommendation, this task will provide guidelines and acceptance criteria for using the identified method.

This research project has the following goals:

A. Identify digital system reliability assessment methods suitable for specific advanced NPP designs and determine the advantages and disadvantages of each reliability assessment method.

B. Recommend digital system reliability assessment methods and review procedures for licensing safety systems in each advanced NPP.

C. Develop curricula for training the staff on the use of the recommended digital system reliability assessment methods and review procedures for licensing the safety systems in each advanced NPP design.

3.6.3.3 Products

The results of these tasks will be a series of technical reports describing digital system reliability assessment methods and their acceptable use for each advanced NPP design submitted to the NRC for review. The acceptance criteria for digital system reliability assessment methods will be included in regulatory guidance. The results of these tasks will prepare the NRC for risk-informed regulatory activities and decisions by supporting the review of digital system risk assessments for advanced NPP designs.

This research project is intended to yield the following products:

- regulatory guidance describing digital system reliability assessment methods and their acceptable use for each advanced NPP design submitted to the NRC for review
- acceptance criteria for the digital system reliability assessment methods
- NRC staff training course(s) on use of the recommended digital system reliability assessment methods

3.7 Additional Research-Related Activities

In addition to research activities that are focused on specific issues such as environmental stressors, software quality assurance, security, etc., the NRC conducts research-related activities to develop regulatory guidance on the basis of best practices described in national and international consensus standards. To ensure that NRC regulatory requirements are adequately represented in the consensus standards, the NRC actively participates in the consensus standards development process.

In addition to developing standards-based regulatory guidance, the NRC maintains technical resources capable of reviewing advances in emerging technologies that have the potential for use by the nuclear industry. These technical resources are most effectively developed through continuing participation in national and international technical meetings and conferences. Additionally, maintaining the research infrastructure and managing the NRC's base of knowledge through continuing research ensures that current capabilities are available and adaptable to support future needs as the industry continues to employ more advanced digital systems.

Given the breadth of research proposed by the Research Plan, the use of personnel, material, and financial resources must be optimized to obtain the maximum benefit from the research programs. The effective use of limited research resources is augmented by contributing NRC resources to collaborative and cooperative research projects that are funded in part by the NRC and by other organizations such as academic centers of excellence and international research groups. These additional research-related activities are described more fully in the following three sections.

3.7.1 Standards Development and Regulatory Guidance

Supported NRC Offices: NMSS, NRR and NSIR

The NRC uses regulatory guides to provide guidance to agency licensees and applicants on implementing relevant portions of Federal regulations pertaining to nuclear facilities. Typically, the RGs endorse, with exceptions and clarifications, standards published by recognized standards bodies such as the IEEE, ISA, American Society for Testing and Materials (ASTM), and American National Standards Institute (ANSI). Evolving technologies, new findings, and improved methods necessitate that these standards continue to be revised on a regular basis. For example, the IEEE requires each of its standards to be reviewed every 5 years to determine whether the standard should be reaffirmed, rewritten, stabilized, or rescinded. This IEEE chose this 5-year period to ensure that its standards are maintained current with applicable technology. This standards revision frequency, in turn, requires the NRC to continue participating in standards bodies to ensure that regulatory requirements remain consistent with the latest version of the consensus standards. The following activities illustrate the breadth of subjects the NRC addresses in supporting development of standards and regulatory guidance.

Regulatory Guide 1.97, Rev. 4, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants" (currently draft guide DG-1128) will endorse IEEE Standard 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Generating Stations" with some exceptions and clarifications. The method for selecting accident monitoring instrumentation, as described in the IEEE standard and endorsed in the regulatory guide, is less-prescriptive than the current guidance and is technology-neutral. The current guidance, Regulatory Guide 1.97, Rev. 3, endorses ANSI/ANS Standard 4.5-1980, "Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors," with exceptions and clarifications. Rev. 4 of Regulatory Guide 1.97 is intended for new NPPs. In developing this revised guide, the NRC convened a task group of staff members to resolve technical issues associated with the endorsed standard. The issues discussed by the task group included which plants (new or current) could use the proposed revision and how, as well as exceptions and clarifications to the standard to be included as regulatory positions in the guide.

Revision 06/2

Regulatory Guide 1.105, Rev. 4, “Setpoints for Safety-Related Instrumentation” (currently draft guide DG-1141) may endorse a new draft of ISA Std 67.04.01, “Setpoints for Nuclear Safety-Related Instrumentation,” and its associated recommended practice ISA-RP67.04.02-2000, “Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation.” The revision will address issues related to setpoint methodology and the application of technical specification-related values in meeting the requirements of 10 CFR 50.36, “Technical Specifications.” NRC staff first identified a need for better guidance on these issues in 2003 during a regulatory review of a license amendment request. The NRC staff subsequently held several meetings with NEI to discuss and resolve these concerns. The NRC plans to issue a related generic communication, and a revision to the standard technical specifications is in progress. The regulatory guide will complement the generic communication and standard technical specifications.

Regulatory Guide 1.152, Rev. 2, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” endorses IEEE Std 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations” with additional guidance regarding potential security vulnerabilities. Through endorsement of the IEEE standard, this revised guide provides licensees with updated guidance on the use of computers in safety systems. The staff issued the updated regulatory guidance in January 2006.

As illustrated in the above examples, maintaining regulatory guidance that is consistent with industry consensus standards requires the NRC to take the following actions:

- Support participation in consensus standards development activities for digital technologies and develop regulatory guidance for NRC staff and the nuclear industry regarding the use of the consensus standards.
- Develop curricula for training the staff on the use of the consensus standards and associated regulatory guidance.

These activities will result in the NRC developing the following assets:

- revised and new RGs endorsing revised versions of consensus standards for digital technologies
- NRC staff training course(s) on use of the consensus standards and associated regulatory guidance

The NRC maintains a schedule of regulatory guide revisions so that, as industry standards are revised, the associated regulatory guidance will be updated accordingly.

3.7.2 Maintenance of Resources and Knowledge Management

Supported NRC Offices: NMSS, NRR and NSIR

The NRC requires a broad base of expertise to remain abreast of the wide variety of issues involving implementation of digital technologies in nuclear facilities. Part of this broad base of expertise resides in the NRC staff. The other significant part of this expertise resource resides in supporting organizations outside the NRC, such as the national laboratories and universities. Maintenance of resources and knowledge management is a twofold effort in that (1) the NRC must maintain resources to respond appropriately and in a timely manner to evolving technologies, new findings, and improved methods, and to address existing safety challenges arising from the use of digital technologies, and (2) the existing knowledge and skill sets within the NRC research organization must be maintained in light of staff turnover.

Maintaining agency resources and managing the agency's base of knowledge will require the NRC to take the following actions:

- Stay abreast of new technologies (see section 3.5) as these technologies become available and compile practical knowledge of their application in the nuclear industry.
- Acquire or develop evaluation tools and review procedures, with associated training, for those new technologies the nuclear industry proposes for use in safety and security systems.
- Periodically assess the technical capabilities and qualifications of the NRC research organization in light of current and new technologies being used by the nuclear industry in safety and security systems.
- Continue to participate in national and international standards committees and working groups.

These activities will result in the following benefits:

- technically competent research staff capable of providing research products that support NRC responsibilities for regulating safe and secure applications of new and emerging digital systems in the nuclear industry
- maintaining a knowledge base of digital technologies within the NRC in an effective and consistent manner

3.7.3 Collaborative and Cooperative Research

Supported NRC Offices: NMSS, NRR and NSIR

As recommended in the NAS review of the NRC's I&C research program, and as outlined in SECY-01-0155, the NRC has been working to establish an active collaborative and cooperative role in developing tools and methods to evaluate the safety and risk-significance of nuclear facility applications employing advanced digital technologies. The NRC is participating in cooperative research in the area of advanced digital technologies for NPPs (which can include human-system interactions and human factors engineering).

Revision 06/2

Three international collaborative research initiatives that are being developed or are in place include (1) the International Partnership for Research on Advanced Control and Instrumentation Technologies (IPRACIT) (NRC Job Code Y6873, "International Cooperative Research Program for Digital I&C"), (2) the Expert Group on Digital Instrumentation and Control (EGDIC) sponsored by the OECD/NEA Committee on the Safety of Nuclear Installations (CSNI) (NRC Job Code Y6873, "International Cooperative Research Program for Digital I&C"), and (3) the HRP (NRC Job Code Y6349, "Halden Environmentally Assisted Cracking"). The objective of these activities is to coordinate resources and advance the capabilities of all member organizations to evaluate the safety and risk significance of advanced digital systems used in current and next-generation NPPs. This will be accomplished by defining and executing consensus research plans that establish the safety basis for application of advanced technologies and promotes acquisition or development and implementation of new evaluation methods and tools.

The staff has collaborated with HRP on I&C research initiatives for many years, and is currently collaborating with HRP in using of COTS equipment operating experience in safety assessments (supports 3.1.3); ranking software engineering practices and criteria (supports 3.2.1); and testing digital reliability assessment methods (supports 3.3.4). Participation in these collaborative international research programs will ensure that the NRC keeps pace with digital technology advances and standard practices.

Further, the staff participates in domestic collaborative and cooperative research activities primarily through involvement with research conducted by universities, the national laboratories, and industry. For example, as described in Section 3.2.2, the NRC, FRA, Lockheed-Martin Inc., Maglev Inc., New York City Transit Authority, and Union Switch & Signal, Inc. (and EDF), are cosponsoring research on system-level risk assessment and numerical safety quantification of safety-critical systems at the UVa CSCS and the CRSCE/SAL. In addition, UMd is performing collaborative research with the NRC and LLNL to develop a methodology for predicting software quality using software engineering measures (supports 3.2.1 and 3.3.4). OSU, PSU and UT are also performing cooperative research for the NRC (NRC Job Code K6472, "Risk Importance of Digital Systems") to develop policies and methods for including currently available reliability models in NPP PRAs (supports 3.3.1 – 3.3.4, 3.5.1, and 3.5.3).

Collaborative and cooperative research activities are expected to yield the following benefits:

- technical findings, coordinated research activities, and establishment of direct collaboration, as warranted
- consensus on needed research activities to avoid technical omissions, minimize duplication, and identify complementary activities that can be performed by international partners
- an integrated research program with shared collaborative and cooperative funding and staff exchanges

4 RESEARCH PLAN TASK SUMMARIES AND SCHEDULES

This section summarizes the tasks, products, priorities, schedule, and corresponding supported strategies from the NRC's Strategic Plan for research that will need to be done to accomplish the goals of the research program. These summaries are provided in tabular format to enable better correlation of research program projects with tasks and strategies for achieving the NRC's strategic goals.

The Research Plan task summaries in this section include a qualitative assessment (priority) of the relative importance of each research task with respect to the time frame in which research products must be delivered to the supported offices (i.e., completion date), and the bases for developing the research products. The research projects are prioritized from highest to lowest priority with respect to the completion time frame and bases for the research, as shown in Figure 5.

BASES FOR RESEARCH	COMPLETION DATE: 2 Years	5 Years	> 5 Years
Existing Ongoing Research Projects	HIGH	HIGH	HIGH
Supported-Office Research Requests	HIGH	HIGH or MEDIUM	MEDIUM
Issues Identified by Consensus Meetings	MEDIUM	MEDIUM or LOW	LOW

Figure 5. Prioritization of Research Project Tasks

Ongoing research projects include (1) ongoing high-priority projects in the process of developing a product for a supported office, (2) ongoing projects for which the NRC has contractually obligated budget and resources; or (3) ongoing projects requiring long-term research to develop a product for a supported office.

A supported-office research task with a projected completion date exceeding 2 years but less than 5 years could be prioritized as either HIGH or MEDIUM to reflect the importance of one research project task relative to other supported-office research tasks in the same completion timeframe, given the assumption that resource constraints will affect which supported-office research project or task completion date should be delayed. Research projects initiated by a supported-Office for which funding sources have been identified are prioritized as HIGH priorities.

Similarly, the MEDIUM or LOW priorities for research projects to address issues identified by RES and the supported offices reflect the effect that digital I&C research budget and schedule constraints could have on the number of additional research projects that may be planned after the research resources have been allocated to higher priority projects. Consequently, research projects to address emerging issues for which funding sources have been identified are prioritized as MEDIUM priority projects. Supported-office research tasks and consensus research tasks with projected completion dates exceeding 5 years and are not currently funded are prioritized as MEDIUM and LOW, respectively, to reflect the uncertainties associated with estimating research needs, budget, and resource priorities more than 5 years in the future.

The research project task identifiers A, B, C, D, and E in the following summaries correspond to the task identifiers assigned to the project tasks described in Section 3.

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1)

Environmental Stressors (3.1.1)				
Task A:	Review the technical basis for revising the CS-114 operating limits in RG 1.180, Rev. 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," and update the guidance in RG 1.180, Rev. 1 if EPRI conclusions regarding CS-114 operating limits are correct.			
Product(s):	Possible revision of RG 1.180			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High(NRR user need (2002-17))		**JCN:** N6080	
Start Date: 1Q FY05	**Completion Date**: 2Q FY08		**Current Activity**: Yes	
Task B:	Develop regulatory guidance and acceptance criteria for establishing lightning protection and qualifying digital systems to withstand the electromagnetic effects resulting from lightning strikes.			
Product(s):	Regulatory guidance on consensus lightning protection practices to mitigate the impact of lightning on the electromagnetic environment at nuclear facilities.			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High (NRR user need (2002-17))		**JCN:** W6851	
Start Date: 1Q FY05	**Completion Date**: 4Q FY05		**Current Activity**: Complete	
Task C:	Develop regulatory guidance to address environmental qualification of microprocessor-based equipment in mild environments.			
Product(s):	Regulatory guidance on environmental qualification of microprocessor-based equipment in mild environments.			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High (NRR user need (2002-17))		**JCN:** N6080	
Start Date: 1Q FY05	**Completion Date**: 2Q FY07		**Current Activity**: Yes	

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

Environmental Stressors (3.1.1) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

System Communications (3.1.2)				
Task A:	Identify communication protocols for data transfer within safety systems and communications between safety and nonsafety systems.			
Product(s):	Regulatory guidance addressing findings on communication protocols within safety systems and applications, and for communications between safety and nonsafety systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN:** N6118	
Start Date: 1Q FY07	**Completion Date**: 2Q FY08		**Current Activity**: No	
Task B:	Review consensus standards and other communication protocol specifications for potential endorsement in regulatory guides.			
Product(s):	Regulatory guides endorsing communication protocol consensus standards and other specifications			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN**: N6118	
Start Date: 1Q FY07	**Completion Date**: 2Q FY08		**Current Activity**: No	
Task C:	Identify communication system failure mechanisms and mitigation strategies.			
Product(s):	Regulatory guidance addressing communication system failure mechanisms and mitigation strategies			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN**: N6118	
Start Date: 1Q FY07	**Completion Date**: 2Q FY08		**Current Activity**: No	

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

System Communications (3.1.2) (continued)

Task D: Acquire or develop a set of tools and review procedures to support staff reviews of communication protocols and communication systems.

Product(s): Tools and review procedures to support staff reviews of communication protocols and communication systems

Supported Strategies:	**SAFETY**	**SECURITY**	**OPENNESS**	**EFFECTIVENESS**
	1, 2, 4			1, 2, 3, 4, 7, 9

Priority: Medium (Consensus agreement) **JCN:** N6118

Start Date: 1Q FY07 **Completion Date**: 2Q FY08 **Current Activity**: No

Task E: Develop curricula for training the staff on the use of the tools and review procedures for evaluating communication protocols and communication system applications.

Product(s): Training course(s) on the use of the tools and review procedures for evaluating communication protocols and communication systems.

Supported Strategies:	**SAFETY**	**SECURITY**	**OPENNESS**	**EFFECTIVENESS**
	1, 2, 4, 6			1, 9

Priority: Medium (Consensus agreement) **JCN:** N6118

Start Date: 2Q FY08 **Completion Date**: 3Q FY08 **Current Activity**: No

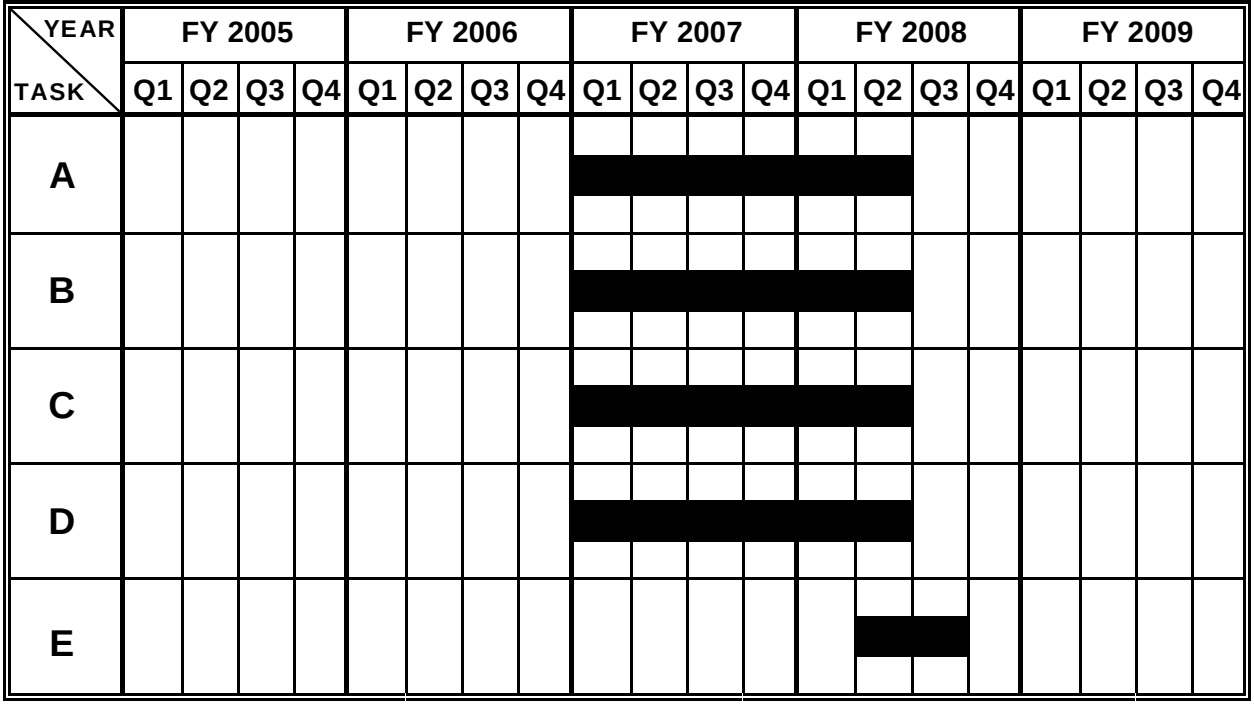

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

COTS Digital Systems (3.1.3)				
Task A:	Perform case studies of safety assessment methods for reviewing COTS-based digital systems.			
Product(s):	Regulatory guidance describing assessment methods for reviewing COTS-based digital systems			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	Medium (NRR user need (2002-17.9))		**JCN:** None	
Start Date: 1Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task B:	Evaluate methods for performing risk-informed safety assessments of COTS-based digital systems.			
Product(s):	Regulatory guidance for performing risk-informed safety assessments of COTS-based digital systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	Medium (NRR user need (2002-17.9))		**JCN:** None	
Start Date: 1Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task C:	Acquire or develop a set of tools (as appropriate), review procedures, and acceptance criteria to support existing methods for reviewing COTS-based digital systems and equipment.			
Product(s):	Tools, review procedures, and acceptance criteria to support existing methods for reviewing COTS-based digital systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	Medium (NRR user need (2002-17.9))		**JCN:** None	
Start Date: 1Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

COTS Digital Systems (3.1.3) (continued)				
Task D:	Develop curricula for training the staff on the use of the tools and review procedures for performing safety evaluations of COTS-based digital systems and equipment.			
Product(s):	Training course(s) for the staff on the use of the tools and review procedures for performing safety evaluations of COTS-based digital systems and equipment			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 4, 6
Priority:	Low (Consensus agreement)		**JCN:** None	
Start Date: 3Q FY09	**Completion Date**: 1Q FY10		**Current Activity**: No	

YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																	■	■	■	■
B																	■	■	■	■
C																	■	■	■	■
D																				■

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

Electrical Power Distribution System Interactions with Nuclear Facilities (3.1.4)				
Task A:	Acquire or develop models, tools, and review procedures for identifying the effect of power fluctuations on digital systems in NPPs.			
Product(s):	Regulatory guidance describing the models, tools, and review procedures for addressing the effects of power fluctuations on digital systems in NPPs			
Supported Strategies:	**SAFETY**	**SECURITY**	**OPENNESS**	**EFFECTIVENESS**
	1, 2, 4		1, 2, 6	1, 2, 3, 4, 7, 9
Priority:	Low (Consensus agreement)		**JCN:** None	
Start Date: 1Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task B:	Review existing standards to determine their applicability for addressing the effects of degraded power on digital components.			
Product(s):	Regulatory guidance on addressing the effects of power fluctuations on digital equipment			
Supported Strategies:	**SAFETY**	**SECURITY**	**OPENNESS**	**EFFECTIVENESS**
	1, 2, 4, 6		1, 2, 6	1, 2, 3, 4, 7, 9
Priority:	Low (Consensus agreement)		**JCN:** None	
Start Date: 1Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the models, tools, and review procedures, and regulatory guidance for addressing the effects of power fluctuations on digital systems.			
Product(s):	NRC staff training course(s) on the use of the models, tools, review procedures, and regulatory guidance for addressing the effects of power fluctuations on digital systems			
Supported Strategies:	**SAFETY**	**SECURITY**	**OPENNESS**	**EFFECTIVENESS**
	1, 2, 4, 6			1, 9
Priority:	Low (Consensus agreement)		**JCN:** None	
Start Date: 3Q FY09	**Completion Date**: 1Q FY10		**Current Activity**: No	

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

Electrical Power Distribution System Interactions with Nuclear Facilities (3.1.4 continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

Effect of Total Harmonic Distortion in Digital Systems (3.1.5)				
Task A:	Acquire or develop models, tools (as appropriate), and review procedures for evaluating THD-related effects in digital systems.			
Product(s):	Regulatory guidance describing the models, tools, and review procedures for evaluating THD-related effects in digital systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Low (Consensus agreement)		**JCN:** None	
Start Date: 2Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task B:	Review existing standards to determine their applicability for addressing THD-related effects in digital systems.			
Product(s):	Regulatory guidance addressing THD-related effects in digital systems			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Low (Consensus agreement)		**JCN:** None	
Start Date: 1Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the models, tools, and review procedures for evaluating THD-related effects in digital systems.			
Product(s):	NRC staff training course(s) on the use of the models, tools, and review procedures for evaluating THD-related effects in digital systems			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Low (Consensus agreement)		**JCN:** None	
Start Date: 3Q FY09	**Completion Date**: 1Q FY10		**Current Activity**: No	

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

Effect of Total Harmonic Distortion in Digital Systems (3.1.5 continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

Operating Systems (3.1.6)				
Task A:	Evaluate design aspects of operating systems (i.e., appropriate operating system selection criteria, best design practices, architectures, failure modes, and fault models).			
Product(s):	Regulatory guidance describing design aspects of operating systems (i.e., appropriate operating system selection criteria, best design practices, architectures, failure modes, and fault models)			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	Low (Consensus agreement)		**JCN:** None	
Start Date: 1Q FY08	**Completion Date**: 3Q FY09		**Current Activity**: No	
Task B:	Acquire or develop a set of tools (as appropriate) and review procedures to support operating system safety assessments.			
Product(s):	Tools and review procedures for evaluating operating systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	Low (Consensus agreement)		**JCN:** None	
Start Date: 1Q FY09	**Completion Date**: 3Q FY09		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the tools and review procedures for performing evaluations of operating systems used in safety-related applications.			
Product(s):	NRC staff training course(s) on the use of the tools and review procedures for performing evaluations of operating systems.			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Low (Consensus agreement)		**JCN:** None	
Start Date: 2Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

Operating Systems (3.1.6) (continued)																			
YEAR	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
TASK	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

Common-Mode Failures, Diversity, and Defense-in-Depth (3.1.7)				
Task A:	Test various CMF coping strategies described in NUREG/CR-6303 to develop optimum sets of coping strategies for achieving sufficiently diverse design features.			
Product(s):	Regulatory guidance documenting optimum NUREG/CR-6303 CMF coping strategies, review procedures, and acceptance criteria for D3 designs			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN:** N6176	
Start Date: 1Q FY06	**Completion Date**: 4Q FY08		**Current Activity**: No	
Task B:	Perform case studies of various COTS digital system configurations that are currently approved for safety-related applications in NPPs to identify generic, configuration-specific CMF vulnerabilities; and validate the procedure developed in Task C below for using the tool and methodology developed in research project 3.2.2.			
Product(s):	Regulatory guidance describing a process by which the staff can conclude (on a deterministic basis) that an acceptable combination of diversity attributes have been addressed in various COTS digital system configurations			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN:** N6176	
Start Date: 1Q FY06	**Completion Date**: 4Q FY08		**Current Activity**: No	
Task C:	Provide regulatory guidance on the use of the tool and methodology developed in research project 3.2.2 and evaluate whether a procedure can be developed for using the fault injection tool and methodology to identify specific digital safety system diversity and defense-in-depth requirements that compensate for CMF vulnerabilities detected by the tool.			
Product(s):	Regulatory guidance on the use of the tool and methodology developed in research project 3.2.2 tool and a procedure for using the fault injection tool and methodology to identify specific digital safety system diversity requirements that compensate for CMF vulnerabilities detected by the tool			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN:** N6176	
Start Date: 4Q FY07	**Completion Date**: 4Q FY08		**Current Activity**: No	

Table 4.1 Task Summaries: System Aspects of Digital Technology (3.1) (continued)

Diversity and Defense-in-Depth (3.1.7) (continued)

Task D: Develop curricula for training the staff on the use of the coping strategies, fault injection tool, review procedures, and acceptance criteria for digital systems

Product(s): NRC staff training on NUREG/CR-6303 CMFcoping strategies and review procedures, and use of the fault injection tool methodology and acceptance criteria for evaluating defense-in-depth and diversity requirements for digital systems

Supported Strategies:	**SAFETY**	**SECURITY**	**OPENNESS**	**EFFECTIVENESS**
	1, 2, 4, 6			1, 9

Priority: Medium (Consensus agreement) **JCN:** N6176

Start Date: 3Q FY07 **Completion Date**: 1Q FY09 **Current Activity**: No

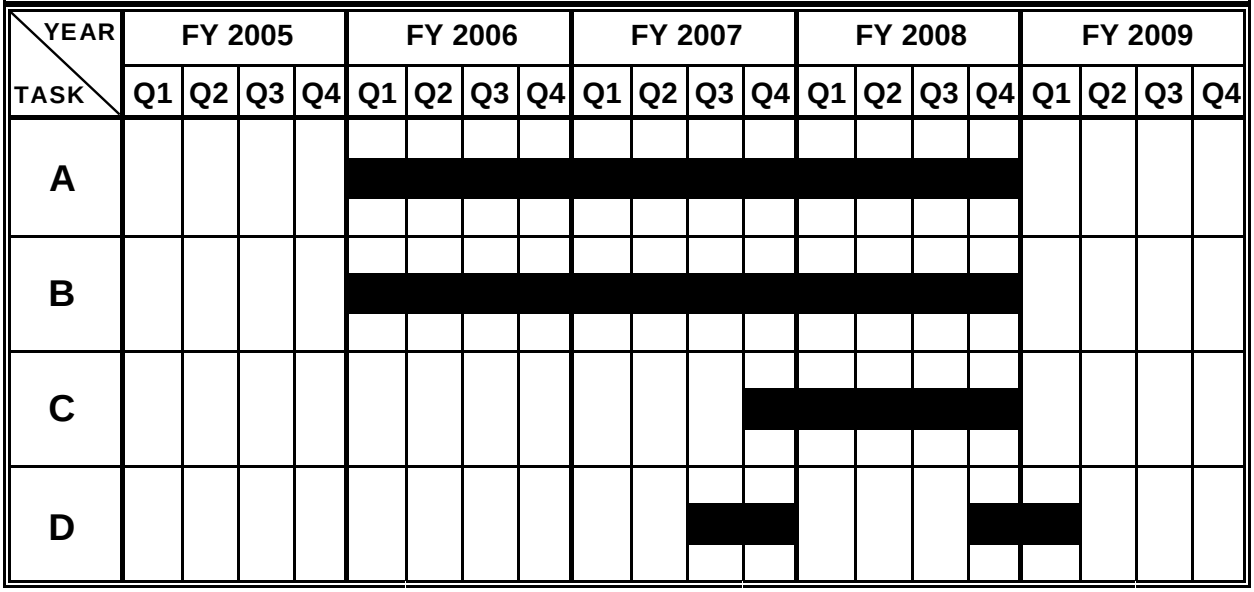

Table 4.2 Task Summaries: Software Quality Assurance (3.2)

Assessment of Software Quality (3.2.1)				
Task A:	Acquire, develop (as necessary), and improve tools and review procedures for reviewing digital system development processes.			
Product(s):	Tools and review procedures for reviewing digital system development life cycle processes			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN:** Y6591	
Start Date: 1Q FY05	**Completion Date**: 4Q FY06		**Current Activity**: Yes	
Task B:	Develop acceptance criteria for the assessment tools and review procedures through cooperative interactions with the digital technology industry, the nuclear industry, and the public.			
Product(s):	Acceptance criteria for the assessment tools and review procedures			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN:** Y6591	
Start Date: 4Q FY06	**Completion Date**: 4Q FY07		**Current Activity**: No	
Task C:	Prepare user documentation for each digital system development process assessment tool and review procedure.			
Product(s):	User documentation for each digital system development process assessment tool and review procedure			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN:** Y6591	
Start Date: 4Q FY06	**Completion Date**: 4Q FY07		**Current Activity**: No	

Table 4.2 Task Summaries: Software Quality Assurance (3.2) (continued)

Assessment of Software Quality (3.2.1) (continued)				
Task D:	Develop curricula for training the staff on the use of the tools and review procedures for reviewing digital system development processes.			
Product(s):	NRC staff training courses on the use of the tools and review procedures for reviewing digital system development processes			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN:** Y6591	
Start Date: 4Q FY07	**Completion Date**: 1Q FY08		**Current Activity**: No	

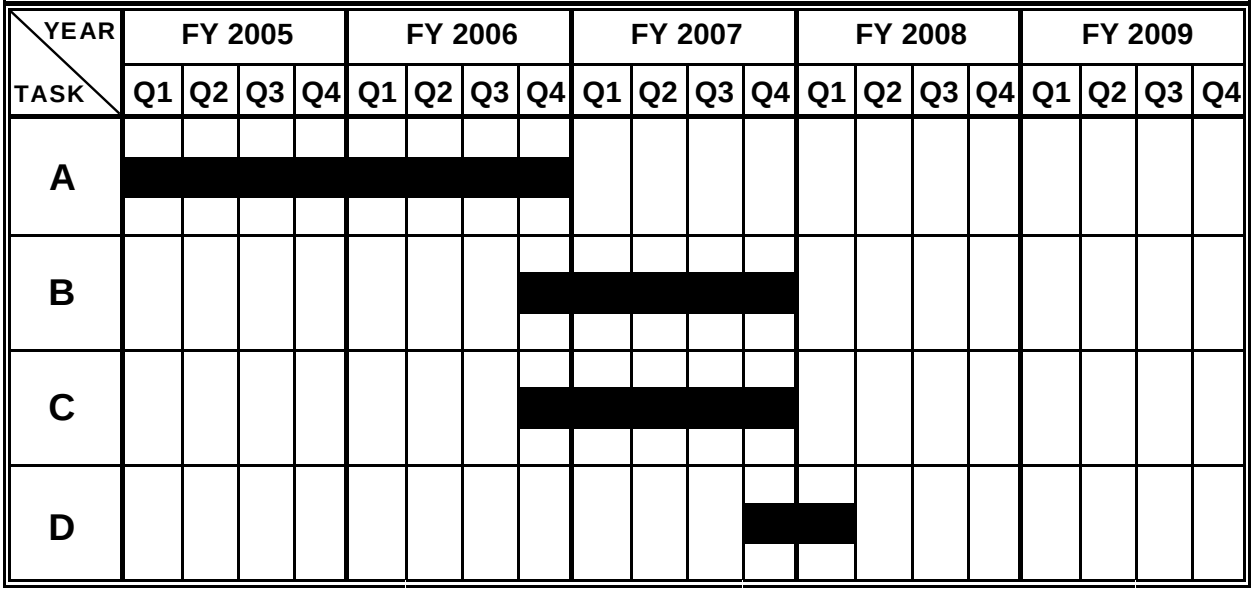

Table 4.2 Task Summaries: Software Quality Assurance (3.2) (continued)

Digital System Dependability (3.2.2)				
Task A:	Develop a tool and methodology for determining the dependability of digital safety systems.			
Product(s):	A tool and methodology for determining the dependability of digital safety systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	Medium (Consensus agreement)		**JCN:** N6124	
Start Date: 1Q FY06	**Completion Date**: 4Q FY07		**Current Activity**: No	
Task B:	Establish dependability acceptance criteria for safety systems on the basis of the tool and methodology results.			
Product(s):	Dependability acceptance criteria on the basis of the tool and methodology results			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	Medium (Consensus agreement)		**JCN:** N6124	
Start Date: 3Q FY07	**Completion Date**: 2Q FY08		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the tool, methodology, and acceptance criteria for evaluating the dependability of digital safety systems.			
Product(s):	NRC staff training course(s) on the use of the tool, methodology, and acceptance criteria for evaluating the dependability of digital safety systems			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN:** N6124	
Start Date: 1Q FY08	**Completion Date**: 2Q FY08		**Current Activity**: No	

Table 4.2 Task Summaries: Software Quality Assurance (3.2) (continued)

Digital System Dependability (3.2.2) (continued)																				
YEAR	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
TASK	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.2 Task Summaries: Software Quality Assurance (3.2) (continued)

Self-Testing Methods (3.2.3)

Task A: Develop technical guidance and review procedures for evaluating self-testing features in digital systems.

Product(s): Technical guidance and acceptance criteria for evaluating self-testing features in digital systems

Supported Strategies:	**SAFETY**	**SECURITY**	**OPENNESS**	**EFFECTIVENESS**
	1, 2, 4		1, 2, 6	1, 2, 3, 4, 7, 9

Priority: Low (Consensus agreement) **JCN:** None

Start Date: 1Q FY09 **Completion Date**: 4Q FY09 **Current Activity**: No

Task B: Develop curricula for training the staff on the use of the guidance and review procedures for performing safety assessments of self-testing features in digital systems.

Product(s): NRC staff training course(s) on the use of the technical guidance and review procedures for performing evaluations of self-testing features in digital systems

Supported Strategies:	**SAFETY**	**SECURITY**	**OPENNESS**	**EFFECTIVENESS**
	1, 2, 4, 6			1, 9

Priority: Low (Consensus agreement) **JCN:** None

Start Date: 4Q FY09 **Completion Date**: 1Q FY10 **Current Activity**: No

YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																	■	■	■	■
B																				■

Table 4.3 Task Summaries: Risk Assessment of Digital Systems (3.3)

Development and Analysis of Digital System Failure Data (3.3.1)				
Task A:	Collect and assess digital system failure data from domestic and foreign nuclear facilities and industries that use digital systems critical to safety. Particular attention will be paid to COTS digital system equipment.			
Product(s):	Regulatory guidance documenting the results and conclusions from the assessment of digital system failure data			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN:** N6010	
Start Date: 1Q FY05	**Completion Date**: 4Q FY09		**Current Activity**: Yes	
Task B:	Evaluate digital system failure assessment methods used by defense, aerospace, and other industries to determine their contributions to overall safety.			
Product(s):	Regulatory guidance documenting digital system failure assessment methods used by defense, aerospace, and other industries to determine their impact on overall safety			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN:** N6010	
Start Date: 1Q FY05	**Completion Date**: 4Q FY09		**Current Activity**: Yes	
Task C:	Develop a process for analyzing the digital system failure data to identify the frequency, severity, cause, and possible prevention of digital system failures.			
Product(s):	Tools and review procedures for performing reliability assessments of digital systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 6, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN:** N6010	
Start Date: 1Q FY05	**Completion Date**: 4Q FY09		**Current Activity**: Yes	

Table 4.3 Task Summaries: Risk Assessment of Digital Systems (3.3) (continued)

Development and Analysis of Digital System Failure Data (3.3.1) (continued)				
Task D:	Develop curricula for training the staff on the use of the digital system failure database, the database assessment process, and the tools and review procedures for performing reliability assessments of digital systems.			
Product(s):	NRC staff training course(s) on the use of the digital system failure database, the database assessment process, and the tools and review procedures for performing reliability assessments of digital systems			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	High (NRR user need (2002-17))		**JCN:** N6010	
Start Date: 3Q FY07	**Completion Date**: 4Q FY09		**Current Activity**: No	

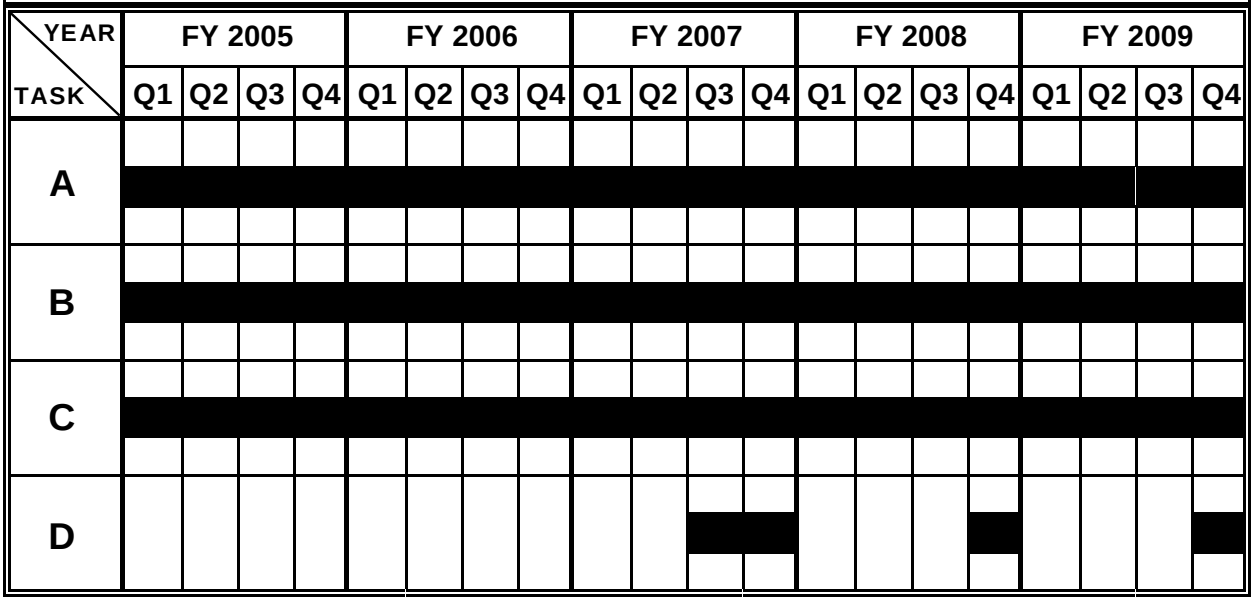

Table 4.3 Task Summaries: Risk Assessment of Digital Systems (3.3) (continued)

Development of Digital System Failure Assessment Methods (3.3.2)				
Task A:	Survey the analytical methods for identifying digital system fault modes and their impact on safety. Describe the advantages and disadvantages of each method; and provide recommendations for digital system failure assessment techniques, and the criteria for using the technique(s) for risk assessments of digital systems.			
Product(s):	Regulatory guidance documenting the results and conclusions from the survey of the analytical methods for identifying digital system failure modes and their impact on safety			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	Medium (NRR user need (2002-17.9))		**JCN:** None	
Start Date: 1Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task B:	Conduct case studies of digital safety systems using the recommended digital system failure assessment technique(s) to determine (1) the amount of effort associated with the proposed criteria and methods, (2) the effectiveness of the criteria, and (3) the suitability of the criteria and methods for nuclear facility applications.			
Product(s):	Regulatory guidance documenting the case studies and the conclusions derived from the studies regarding the effectiveness of the digital system failure assessment techniques			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	Medium (NRR user need (2002-17.9))		**JCN:** None	
Start Date: 1Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the analytical techniques and the criteria for using each technique.			
Product(s):	NRC staff training course(s) on the use of the analytical techniques and the criteria for using each technique			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN:** None	
Start Date: 4Q FY09	**Completion Date**: 1Q FY10		**Current Activity**: No	

Table 4.3 Task Summaries: Risk Assessment of Digital Systems (3.3) (continued)

Development of Digital System Failure Assessment Methods (3.3.2) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																	■	■	■	■
B																	■	■	■	■
C																				■

Table 4.3 Task Summaries: Risk Assessment of Digital Systems (3.3) (continued)

Identification of Digital System Characteristics Important to Risk (3.3.3)				
Task A:	Identify and develop generic risk models of digital systems in nuclear facilities.			
Product(s):	Regulatory guidance documenting the results and conclusions from the development of the nuclear facility digital system risk models			
Supported Strategies:	**SAFETY** 1, 2, 3, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN:** K6472	
Start Date: 1Q FY05	**Completion Date**: 4Q FY08		**Current Activity**: Yes	
Task B:	Calculate the risk importance of the generic digital systems.			
Product(s):	Regulatory guidance describing the calculation of risk importance of the nuclear facility digital system risk models			
Supported Strategies:	**SAFETY** 1, 2, 3, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN:** K6472	
Start Date: 3Q FY05	**Completion Date**: 3Q FY09		**Current Activity**: Yes	
Task C:	Develop risk models beyond the “black box” level for large or complex high risk-important digital systems;			
Product(s):	Regulatory guidance describing the risk models beyond the “black box” level for large or complex high risk-important digital systems			
Supported Strategies:	**SAFETY** 1, 2, 3, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN:** K6472	
Start Date: 4Q FY05	**Completion Date**: 3Q FY09		**Current Activity**: Yes	

Table 4.3 Task Summaries: Risk Assessment of Digital Systems (3.3) (continued)

Identification of Digital System Characteristics Important to Risk (3.3.3) (continued)				
Task D:	Develop a process for identifying sub-components of digital systems that may warrant special regulatory and/or research attention.			
Product(s):	Regulatory guidance describing a process for identifying sub-components of digital systems that may warrant special regulatory and/or research attention			
Supported Strategies:	**SAFETY** 1, 2, 3, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN:** K6472	
Start Date: 1Q FY06	**Completion Date**: 3Q FY08		**Current Activity**: Yes	
Task E:	Develop curricula for training the staff on the risk-importance of digital systems.			
Product(s):	NRC staff training course(s) on the risk-importance of digital systems			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN:** K6472	
Start Date: 3Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	

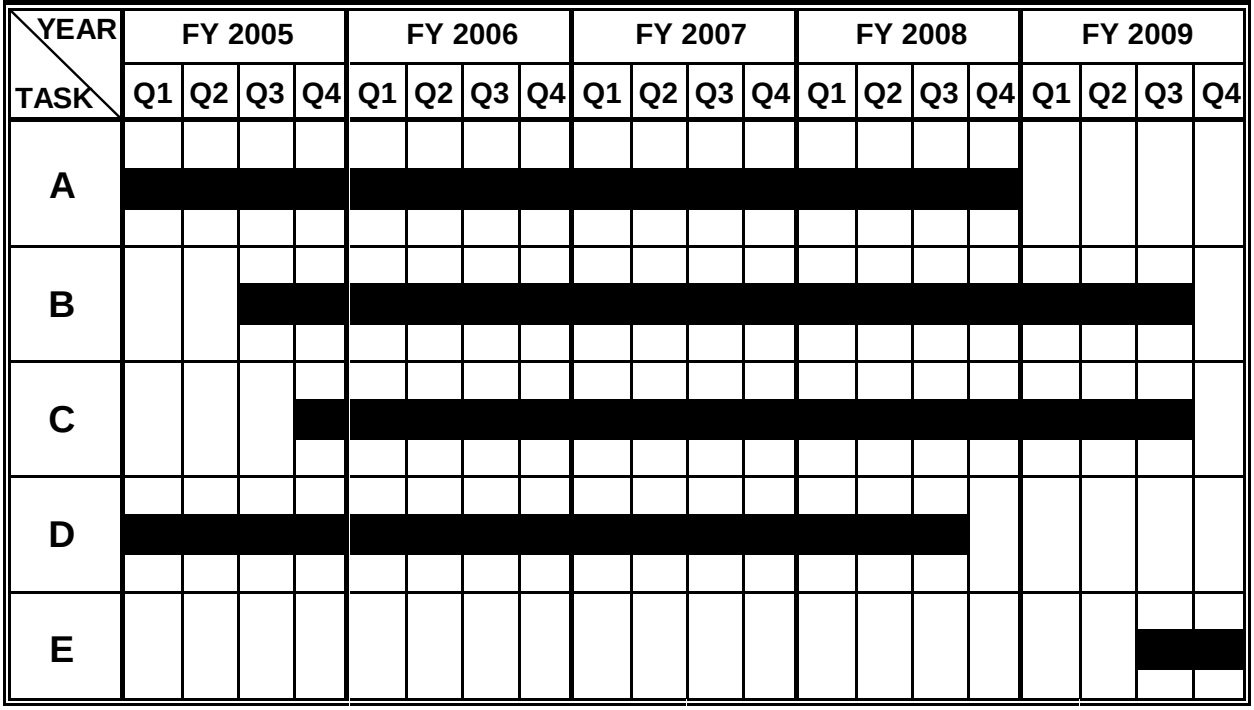

Table 4.3 Task Summaries: Risk Assessment of Digital Systems (3.3) (continued)

Development of Digital System Reliability Assessment Methods (3.3.4)				
Task A:	Identify digital system reliability assessment methods and determine the advantages and disadvantages of each method.			
Product(s):	Regulatory guidance describing the advantages and disadvantages of the digital system reliability assessment methods identified in Task A			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN**: K6079	
Start Date: 1Q FY06	**Completion Date**: 4Q FY08		**Current Activity**: Yes	
Task B:	Recommend digital system reliability assessment method(s) suitable for nuclear facility and application licensing activities.			
Product(s):	Regulatory guidance recommending digital system reliability assessment method(s) suitable for nuclear facility and application licensing activities			
Supported Strategies:	**SAFETY** 1, 2, 3, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN**: K6079	
Start Date: 3Q FY08	**Completion Date**: 3Q FY09		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the recommended digital system reliability assessment method.			
Product(s):	NRC staff training course(s) on use of the recommended digital system reliability assessment method(s)			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN**: K6079	
Start Date: 3Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	

Table 4.3 Task Summaries: Risk Assessment of Digital Systems (3.3) (continued)

Development of Digital System Reliability Assessment Methods (3.3.4) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.4 Task Summaries: Security Aspects of Digital Systems (3.4)

Security Assessments of Cyber-Vulnerabilities (3.4.1)				
Task A:	Evaluate cyber security aspects of digital systems in nuclear facilities and applications.			
Product(s):	Regulatory policy and guidance and describing the cyber security aspects of digital systems in nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 3, 4, 5	**SECURITY** 1, 4	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NSIR support)		**JCN**: N6304	
Start Date: 1Q FY06	**Completion Date**: 3Q FY09		**Current Activity**: Yes	
Task B:	Develop regulatory policy, and acquire or develop tools (as appropriate), review procedures, acceptance criteria, and guidelines to support cyber security assessments of digital systems in nuclear facilities and applications.			
Product(s):	Tools, review procedures, and guidelines to support cyber security assessments of digital systems in nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY** 1, 4, 5	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NSIR support)		**JCN**: N6304	
Start Date: 3Q FY06	**Completion Date**: 3Q FY09		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the regulatory policy, tools, and review procedures for performing cyber security assessments of digital systems in nuclear facilities and applications.			
Product(s):	NRC staff training course(s) on the use of the regulatory policy, tools, and review procedures for performing cyber security assessments of digital systems in nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY** 2, 4, 5	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN**: N6304	
Start Date: 3Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	

Table 4.4 Task Summaries: Security Aspects of Digital Systems (3.4) (continued)

Security Assessments of Cyber-Vulnerabilities (3.4.1) (continued)																				
YEAR	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
TASK	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A					■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
B								■	■	■	■	■	■	■	■	■	■	■	■	
C																			■	■

Table 4.4 Task Summaries: Security Aspects of Digital Systems (3.4) (continued)

Security Assessments of EM Vulnerabilities (3.4.2)				
Task A:	Identify and evaluate the EM security aspects of digital systems in nuclear facilities and applications.			
Product(s):	Regulatory guidance describing the EM security aspects of secure digital systems in nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 3, 4, 5	**SECURITY** 1, 4	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NSIR support)		**JCN**: N6119	
Start Date: 1Q FY07	**Completion Date:** 3Q FY08		**Current Activity:** No	
Task B:	Acquire or develop a set of tools (as appropriate), review procedures, and acceptance criteria to support EM security assessments of digital systems in nuclear facilities and applications.			
Product(s):	Tools and review procedures to support EM security assessments of digital systems in nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY** 1, 4**, 5**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NSIR support)		**JCN**: N6119	
Start Date: 1Q FY07	**Completion Date:** 3Q FY08		**Current Activity:** No	
Task C:	Develop curricula for training the staff on the use of the tools and review procedures for performing EM security assessments of digital systems in nuclear facilities and applications.			
Product(s):	NRC staff training course(s) on the use of the tools and review procedures for performing EM security assessments of digital systems in nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY** 2, 4, 5	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN**: N6119	
Start Date: 3Q FY08	**Completion Date:** 4Q FY08		**Current Activity:** No	

Table 4.4 Task Summaries: Security Aspects of Digital Systems (3.4) (continued)

Security Assessments of EM Vulnerabilities (3.4.2) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.4 Task Summaries: Security Aspects of Digital Systems (3.4) (continued)

Network Security (3.4.3)				
Task A:	Identify network features appropriate for nuclear facilities and applications and formulate guidance for administrative controls, engineering designs, network diversity, and segmentation strategies for protecting networks from cyber attacks.			
Product(s):	Regulatory guidance on network features appropriate for nuclear facilities and applications for administrative controls, engineering designs, network diversity, and segmentation strategies for protecting networks from cyber attacks			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY** 1, 4	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High (NSIR support)		**JCN**: N6115, N6116	
Start Date: 1Q FY06	**Completion Date**: 3Q FY09		**Current Activity**: Yes	
Task B:	Acquire or develop security tools and review procedures for safety-related network applications.			
Product(s):	Security tools and review procedures for network applications in nuclear facilities			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY** 1, 4, 5	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High (NSIR support)		**JCN**: N6115	
Start Date: 1Q FY07	**Completion Date**: 3Q FY09		**Current Activity**: No	
Task C:	Investigate on-going worldwide efforts to develop regulatory guidance for installing and maintaining firewall applications in safety-related applications.			
Product(s):	Regulatory guidance for installing and maintaining safety-related firewall applications			
Supported Strategies:	**SAFETY** 1, 2, 3, 4, 5	**SECURITY** 1, 4	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High (NRR user need (2000-6))		**JCN**: N6115	
Start Date: 1Q FY07	**Completion Date**: 3Q FY09		**Current Activity**: No	

Network Security (3.4.3) (continued)

Task D: Develop review procedures for identifying potential vulnerabilities in safety-related firewall applications.

Product(s): Review procedures for identifying potential vulnerabilities in safety-related firewall applications

Supported Strategies:	**SAFETY**	**SECURITY**	**OPENNESS**	**EFFECTIVENESS**
	1, 2, 3, 4, 5	1, 4	1, 2, 6	1, 2, 3, 4, 7, 9

Priority: High (NRR user need (2000-6)) **JCN**: N6115

Start Date: 1Q FY08 **Completion Date**: 3Q FY09 **Current Activity**: No

Task E: Develop curricula for training the staff on the technical guidance and use of the security tools and review procedures for safety-related network applications.

Product(s): NRC staff training course(s) on the technical guidance and security tools and review procedures for evaluating safety-related network applications

Supported Strategies:	**SAFETY**	**SECURITY**	**OPENNESS**	**EFFECTIVENESS**
	1, 2, 4, 6	2, 4, 5		1, 9

Priority: Medium (Consensus agreement) **JCN**: N6115, N6116

Start Date: 3Q FY09 **Completion Date**: 4Q FY09 **Current Activity**: No

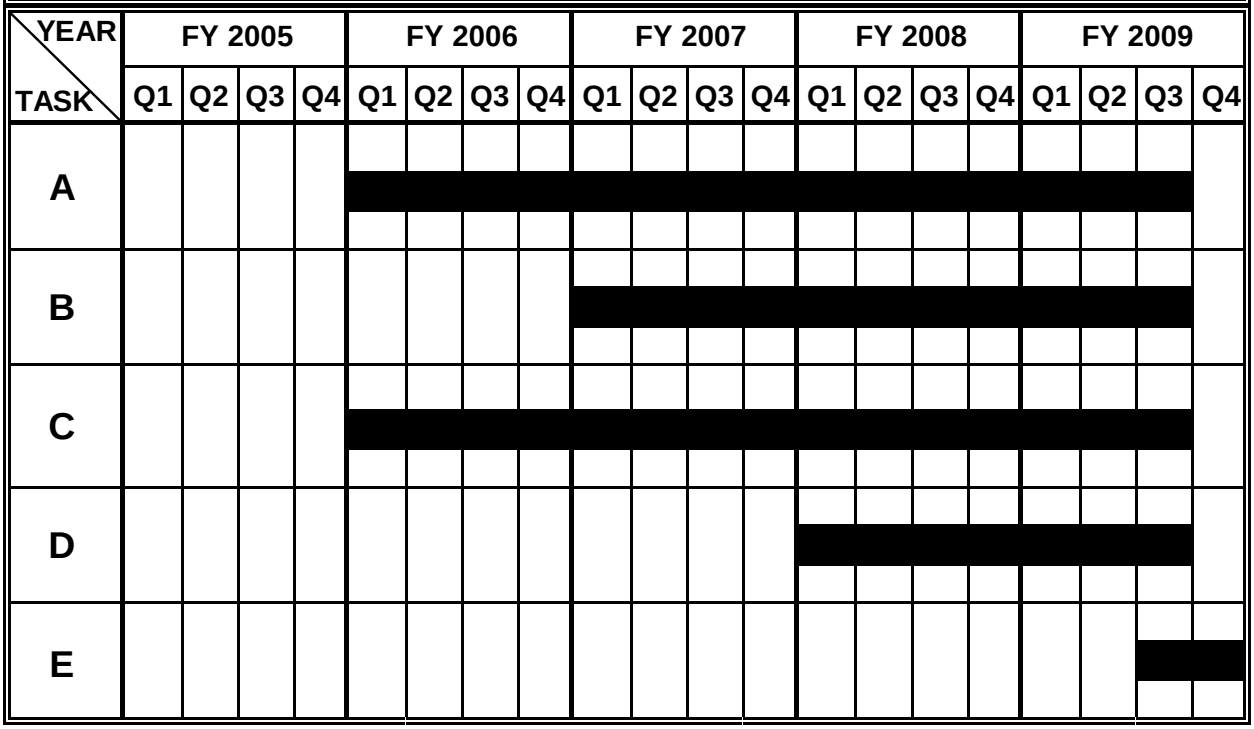

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5)

System Diagnosis, Prognosis, Online Monitoring (3.5.1)				
Task A:	Survey the use of SDPM methods in nuclear facilities, review state-of-the-art SDPM methods, and evaluate the effectiveness and uncertainties of SDPM methods.			
Product(s):	Revised guidelines for applying SDPM methods in nuclear facilities (e.g., RG 1.118, "Periodic Testing of Electric Power and Protection Systems"), and review procedures for reviewing SDPM applications in nuclear facilities			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN**: Y6473	
Start Date: 1Q FY05	**Completion Date:** 3Q FY07		**Current Activity**: Yes	
Task B:	Develop review procedures for SDPM applications in nuclear facilities.			
Product(s):	Review procedures for SDPM applications in nuclear facilities			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN**: Y6473	
Start Date: 4Q FY06	**Completion Date:** 3Q FY07		**Current Activity**: Yes	
Task C:	Develop curricula for training the staff on the use of the review procedures for SDPM applications.			
Product(s):	NRC staff training course(s) on the guidance and review procedures for evaluating SDPM applications			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement))		**JCN**: Y6473	
Start Date: 3Q FY07	**Completion Date:** 4Q FY07		**Current Activity**: No	

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5) (continued)

System Diagnosis, Prognosis, Online Monitoring (3.5.1) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5) (continued)

Radiation-Hardened Integrated Circuits (3.5.2)				
Task A:	Determine radiation-hardened IC technologies appropriate for safety systems in nuclear facilities and applications.			
Product(s):	Regulatory guidance on radiation-hardened IC technologies appropriate for safety systems in nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (NRR user need (2002-17.9))		**JCN**: None	
Start Date: 1Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task B:	Develop review procedures and guidance for qualifying radiation-hardened IC devices for use in safety systems for nuclear facilities and applications.			
Product(s):	Review procedures and guidance for qualifying radiation-hardened IC devices for use in safety systems for nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (NRR user need (2002-17.9))		**JCN**: None	
Start Date: 3Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the review procedures for licensing radiation-hardened ICs in safety systems for nuclear facilities and applications.			
Product(s):	NRC staff training course(s) on the guidance and review procedures for licensing radiation-hardened ICs in safety systems for nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Low (Consensus agreement)		**JCN**: None	
Start Date: FY10+	**Completion Date**: FY10+		**Current Activity**: No	

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5) (continued)

Radiation-Hardened Integrated Circuits (3.5.2) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5) (continued)

Advanced Instrumentation and Controls (3.5.3)				
Task A:	Identify advanced I&C technologies appropriate for safety systems.			
Product(s):	Regulatory guidance identifying advanced instrumentation technologies appropriate for safety systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High (NRR user need (2002-17.9))		**JCN**: Y6476, Y6962	
Start Date: 1Q FY05	**Completion Date**: 4Q FY09		**Current Activity**: Yes	

YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5) (continued)

Smart Transmitters (3.5.4)				
Task A:	Identify smart transmitter technologies and characteristics appropriate for safety systems in nuclear facilities and applications.			
Product(s):	Regulatory guidance identifying smart transmitter characteristics appropriate for safety systems in nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	High(NRR user need (2002-17.9))		**JCN**: Y6474	
Start Date: 1Q FY07	**Completion Date**: 3Q FY08		**Current Activity**: No	
Task B:	Develop review procedures for licensing nuclear facility and application safety systems that use smart transmitters.			
Product(s):	Review procedures for licensing nuclear facility and application safety systems that use smart transmitters			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN**: Y6474	
Start Date: 1Q FY08	**Completion Date**: 3Q FY08		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the guidance and review procedures for licensing nuclear facility and application safety systems that use smart transmitters.			
Product(s):	NRC staff training course(s) on the use of the guidance and review procedures for licensing nuclear facility and application safety systems that use smart transmitters			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN**: Y6474	
Start Date: 3Q FY08	**Completion Date**: 4Q FY08		**Current Activity**: No	

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5) (continued)

Smart Transmitters (3.5.4) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A									■	■	■	■	■	■	■					
B													■	■	■					
C															■	■				

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5) (continued)

ASICs and FPGAs (3.5.5)				
Task A:	Identify ASIC and FPGA components, design synthesis tools, best design techniques and practices, and failure modes and fault models used in safety-related systems in nuclear, aerospace, aeronautical, transportation, and process control industries.			
Product(s):	Regulatory guidance identifying ASIC and FPGA devices and design techniques appropriate for use in safety systems for nuclear facilities and applicationss			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	Low (Consensus agreement)		**JCN**: None	
Start Date: 1Q FY08	**Completion Date**: 2Q FY09		**Current Activity**: No	
Task B:	Acquire or develop (as appropriate) safety assessment techniques (e.g., fault injection techniques, and quantitative analysis techniques), and associated review procedures for licensing ASIC and FPGA safety system applications in nuclear facilities and applications.			
Product(s):	Safety assessment techniques and associated review procedures for licensing ASIC and FPGA safety system applications in nuclear facilities and applications			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Low (Consensus agreement)		**JCN**: None	
Start Date: 1Q FY09	**Completion Date**: 3Q FY09		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the safety assessment techniques for licensing ASIC and FPGA safety system applications in nuclear facilities and applications.			
Product(s):	NRC staff training course(s) on the use of the safety assessment techniques for licensing ASIC and FPGA safety system applications in nuclear facilities and application			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Low (Consensus agreement)		**JCN**: None	
Start Date: 3Q FY09	**Completion Date**: 4Q FY09		**Current Activity**: No	

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5) (continued)

ASICs and FPGAs (3.5.5) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5) (continued)

Wireless Technology (3.5.6)				
Task A:	Identify wireless technologies appropriate for safety systems in nuclear facilities.			
Product(s):	Regulatory guidance identifying wireless technologies appropriate for safety systems in nuclear facilities			
Supported Strategies:	**SAFETY** 1, 2, 4, 5	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN**: Y6475	
Start Date: 2Q FY06	**Completion Date:** 3Q FY07		**Current Activity**: No	
Task B:	Address safety-related issues and deployment considerations associated with implementing wireless systems in nuclear facilities.			
Product(s):	Regulatory guidance addressing safety-related issues and deployment considerations associated with implementing wireless systems in nuclear facilities			
Supported Strategies:	**SAFETY** 1, 2, 3, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN**: Y6475	
Start Date: 2Q FY06	**Completion Date:** 3Q FY07		**Current Activity**: No	
Task C:	Develop review procedures and acceptance criteria for licensing wireless technology applications in nuclear facility safety systems.			
Product(s):	Review procedures and acceptance criteria for licensing wireless technology applications in nuclear facility safety systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (Consensus agreement)		**JCN**: Y6475	
Start Date: 1Q FY07	**Completion Date:** 3Q FY07		**Current Activity**: No	

Table 4.5 Task Summaries: Emerging Digital Technology and Applications (3.5) (continued)

Wireless Technology (3.5.6) (continued)				
Task D:	Develop curricula for training the staff on the use of the guidance and review procedures for licensing wireless technology applications in nuclear facility safety systems.			
Product(s):	NRC staff training course(s) on use of the guidance and review procedures for licensing wireless technology applications in nuclear facility safety systems			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN**: Y6475	
Start Date: 3Q FY07	**Completion Date:** 4Q FY07		**Current Activity**: No	

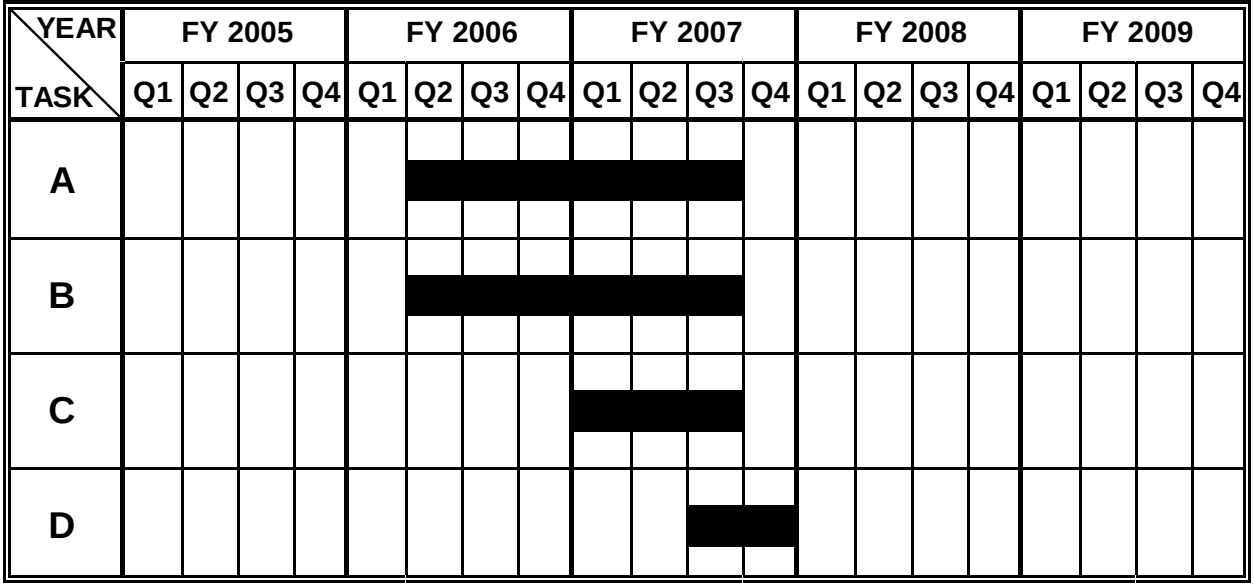

Table 4.6 Task Summaries: Advanced Nuclear Power Plant Digital Systems (3.6)

Advanced NPP Instrumentation (3.6.1)				
Task A:	Characterize the capabilities and limitations of advanced instrumentation identified for use in advanced NPP safety systems.			
Product(s):	Regulatory guidance characterizing the capabilities and limitations of advanced instrumentation identified for use in advanced NPP safety systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NRR initiative)		**JCN**: N6191	
Start Date: 3Q FY05	**Completion Date:** 4Q FY09		**Current Activity: Yes**	
Task B:	Acquire or develop tools, review procedures, and acceptance criteria for licensing advanced instrumentation identified for use in advanced NPP safety systems.			
Product(s):	Tools, review procedures, and acceptance criteria for licensing advanced instrumentation identified for use in advanced NPP safety systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 5, 7, 9
Priority:	High (NRR initiative)		**JCN**: N6191	
Start Date: 1Q FY07	**Completion Date:** 4Q FY09		**Current Activity: No**	
Task C:	Develop curricula for training the staff on the use of the tools and review procedures for licensing advanced instrumentation identified for use in advanced NPP safety systems.			
Product(s):	NRC staff training course(s) on use of the tools and review procedures for licensing advanced instrumentation identified for use in advanced NPP safety systems			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY** 2, 4, 5	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN**: N6191	
Start Date: 4Q FY07	**Completion Date:** 4Q FY09		**Current Activity:** No	

Table 4.6 Task Summaries: Advanced Nuclear Power Plant Digital Systems (3.6) (continued)

Advanced NPP Instrumentation (3.6.1) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.6 Task Summaries: Advanced Nuclear Power Plant Digital Systems (3.6) (continued)

Advanced NPP Controls (3.6.2)				
Task A:	Characterize the capabilities and limitations of advanced controls identified for use in advanced NPP safety systems.			
Product(s):	Regulatory guidance for evaluating the capabilities and limitations of advanced controls proposed for use in advanced NPP safety systems			
Supported Strategies:	**SAFETY** 1, 2, 3, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 8, 9
Priority:	High (NRR initiative)		**JCN**: N6190	
Start Date: 3Q FY05	**Completion Date**: 4Q FY09		**Current Activity**: Yes	
Task B:	Acquire or develop tools (as appropriate), review procedures, and acceptance criteria for licensing advanced controls proposed for advanced NPP safety systems.			
Product(s):	Tools, review procedures, and acceptance criteria for licensing advanced controls proposed for advanced NPP safety systems			
Supported Strategies:	**SAFETY** 1, 2, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 7, 8, 9
Priority:	High (NRR initiative)		**JCN**: N6190	
Start Date: 1Q FY07	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the tools and review procedures for licensing advanced controls proposed for advanced NPP safety systems.			
Product(s):	NRC staff training course(s) on use of the tools and review procedures for licensing advanced controls proposed for advanced NPP safety systems			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Medium (Consensus agreement)		**JCN**: N6190	
Start Date: 4Q FY07	**Completion Date**: 4Q FY09		**Current Activity**: No	

Table 4.6 Task Summaries: Advanced Nuclear Power Plant Digital Systems (3.6) (continued)

Advanced NPP Controls (3.6.2) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

Table 4.6 Task Summaries: Advanced Nuclear Power Plant Digital Systems (3.6) (continued)

Advanced NPP Digital System Risk (3.6.3)				
Task A:	Identify digital system reliability assessment methods suitable for specific advanced NPP designs and determine the advantages and disadvantages of each reliability assessment method.			
Product(s):	Regulatory guidance describing digital system reliability assessment methods and their acceptable use for each advanced NPP design submitted to the NRC for review			
Supported Strategies:	**SAFETY** 1, 2, 3, 4	**SECURITY**	**OPENNESS** 1, 2, 6	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (NRR user need (2000-6))		**JCN**: None	
Start Date: 1Q FY07	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task B:	Recommend digital system reliability assessment methods and review procedures for licensing safety systems in each advanced NPP.			
Product(s):	Acceptance criteria for the digital system reliability assessment methods			
Supported Strategies:	**SAFETY** 1, 2, 3, 4	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 2, 3, 4, 7, 9
Priority:	Medium (NRR user need (2002-17.9))		**JCN**: None	
Start Date: 1Q FY08	**Completion Date**: 4Q FY09		**Current Activity**: No	
Task C:	Develop curricula for training the staff on the use of the recommended digital system reliability assessment methods and review procedures for licensing the safety systems in each advanced NPP design.			
Product(s):	NRC staff training course(s) on use of the recommended digital system reliability assessment methods			
Supported Strategies:	**SAFETY** 1, 2, 4, 6	**SECURITY**	**OPENNESS**	**EFFECTIVENESS** 1, 9
Priority:	Low (Consensus agreement)		**JCN**: None	
Start Date: 4Q FY08	**Completion Date**: 4Q FY09		**Current Activity**: No	

Table 4.6 Task Summaries: Advanced Nuclear Power Plant Digital Systems (3.6) (continued)

Advanced NPP Digital System Risk (3.6.3) (continued)																				
YEAR / TASK	FY 2005				FY 2006				FY 2007				FY 2008				FY 2009			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
A																				
B																				
C																				

5 REFERENCES

ANSI/ANS — "Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors," ANSI/ANS 4.5-1980.

CIA — "Cyber Threats and the U.S. Economy," Statement for the Record before the Congress Joint Economic Committee, February 23, 2000, John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, Washington, DC.

GAO — "Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination (Testimony, 07/26/2000, GAO/T-AIMD-00-268)," General Accounting Office, Washington, DC, July 26, 2000.

IEEE — "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Generating Stations," IEEE Standard 497-2002.

IEEE — "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Std 7-4.3.2-2003.

IEEE — "IEEE Recommended Practices and Requirements for Harmonic Control in Electrical Power Systems," IEEE Std 519-1992 (2nd printing in 2004).

IEEE — "IEEE Standard for a Software Quality Metrics Methodology," IEEE Std 1061-1998.

IEEE — "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations," IEEE Std 665-1995.

ISA — "Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation," ISA-RP67.04.02-2000.

ISA — "Setpoints for Nuclear Safety-Related Instrumentation," ISA Std 67.04.01.

Leveson — Leveson, Nancy G., and Clark S. Turner, "An Investigation of the Therac-25 Accidents", *IEEE Computer*, Vol. 25, No. 7, pp. 18–41, July 1993.

NAS — "Digital Instrumentation and Control Systems in Nuclear Power Plants," National Research Council, National Academy of Science Press, Washington, DC, 1997.

NEI — "Cyber Security Program for Power Reactors," NEI-04-04. (This document is withheld from public disclosure in accordance with 10 CFR 2.390.)

Nucleonics Week — "Cascade of Failures Earns INES Level 2 at Flamanville-2," *Nucleonics Week*, Vol. 43, No. 6, February 7, 2002.

The President "Critical Infrastructure Protection," Executive Order 13010, July 15, 1996.

USDOD "Joint Vision 2020," Department of Defense, Washington, DC, May 30, 2000.

USNRC "Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants," NUREG/CR-6842 (ML04230687).

USNRC "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Regulatory Guide 1.174 (ML023240437).

USNRC "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants." Regulatory Guide 1.97, Rev. 4 (currently draft guide DG-1128, ML052150210).

USNRC "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152, Rev. 2 (ML053070150).

USNRC "Guidelines for Environmental Qualification of Microprocessor-Based Equipment Important to Safety," Draft Regulatory Guide DG-1077 (ML0112710073).

USNRC "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," NUREG/CR-6847 (ML043200191). (This document is withheld from public disclosure in accordance with 10 CFR 2.390.)

USNRC "Design Defect in Safeguards Bus Sequencer Test Logic Places Both Units Outside the Design Basis," LER 94-005-02 (Accession # 9508080294).

USNRC "Loss of 34.5 kV Offsite Power Circuit 751, Due to External Cause, Results in Automatic Start of B Emergency Diesel Generator," LER 244/94-012.

USNRC "Grid Disturbance Results in Reactor Trip Due To Manufacturing Deficiency," LER 270/97-002.

USNRC "Safeguards Buses De-Energized and Losses of Offsite Power During Severe Storm While Shut Down," LER 293/97-007.

USNRC "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Regulatory Guide 1.180, Rev. 1 (ML032740277).

USNRC "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," NUREG/CR-6303 (9501180332).

USNRC "NRC Research Plan for Digital Instrumentation and Control" SECY-01-0155 (ML011990569 and ML012080254).

USNRC "Operating Experience Assessment: Effects of Grid Events on Nuclear Power Plant Performance," NUREG-1784 (ML033530400).

USNRC "Potential Vulnerability of Plant Computer Network to Worm Infection," NRC Information Notice 2003-14, August 29, 2003 (ML032410430).

USNRC "Setpoints for Safety-Related Instrumentation," Regulatory Guide 1.105, Rev. 4 (planned draft guide DG-1141).

USNRC "Standard Format and Content for the Safety Analysis Report for an Independent Spent Fuel Storage Installation or Monitored Retrievable Storage Installation (Dry Storage)," Regulatory Guide 3.48 (ML003739463).

USNRC "Standard Review Plan for Dry Cask Storage Systems," NUREG-1536 (ML010040297, et al.).

USNRC "Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-0800 (ML033580677).

USNRC "The Standard Review Plan for Spent Fuel Dry Storage Facilities" NUREG-1567 (ML003686776).

USNRC "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility," NUREG-1520 (ML020930033).

USNRC "U.S. Nuclear Regulatory Commission Strategic Plan," NUREG-1614, Volume 3 (ML042230185).

USNRC "Digital System Software Requirements Guidelines," NUREG/CR-6734, Volumes 1 and 2 (ML0123301601, ML0123301841).

USNRC "Application of Microprocessor-Based Equipment in Nuclear Power Plants: Technical Basis for a Qualification Methodology," NUREG/CR-6741 (ML012600340).

USNRC "Embedded Digital System Reliability and Safety Analysis," NUREG/GR-0020 (ML010570243)

USNRC "Comparison of U.S. Military and International Electromagnetic Compatibility Guidance," NUREG/CR-6782 (ML033000345).

USNRC "Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems," NUREG/GR-0019 (ML003775310)

USNRC "Preliminary Validation of a Methodology for Assessing Software Quality," NUREG/CR-6848 (ML042170285)

USNRC "Electromagnetic Compatibility Testing for Conducted Susceptibility Along Interconnecting Signal Lines," NUREG/CR-5609 (ML032960137).

Revision 06/2

APPENDIX A
STRATEGIC GOALS AND STRATEGIES

A.1 The NRC Strategic Plan

The NRC Strategic Plan is described in NUREG-1614, Volume 3, "U.S. Nuclear Regulatory Commission Strategic Plan for FY 2005 – FY 2009" (ML042230185). Its objective is to enable the NRC to fulfill its mission to regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment. This mission applies to all uses of radioactive materials, regardless of the technology in which the materials are used (e.g., NPPs, fuel cycle facilities, waste storage processes and facilities, industrial manufacturing processes, medical uses, etc.), and regardless of the technology by which public health and safety, national security, and environmental protection are ensured (e.g., analog-based, digital-based, or passive safety systems, etc.). The NRC's mission is the basis for all of the agency's regulations and regulatory processes, guidance, and acceptance criteria.

Fulfillment of the NRC's mission is ensured when the following specific outcomes are achieved and maintained:

- no nuclear reactor accidents
- no inadvertent criticality events
- no acute radiation exposures resulting in fatalities
- no releases of radioactive materials that result in significant radiation exposures
- no releases of radioactive materials that cause significant adverse environmental impacts
- no instances where licensed radioactive materials are used domestically in a manner hostile to the security of the United States
- no significant licensing or regulatory impediments to the safe and beneficial uses of radioactive materials
- stakeholders are informed and involved in NRC processes as appropriate

The Strategic Plan identifies Safety, Security, Openness, Effectiveness, and Management as strategic goals and correlates these goals with the above outcomes. Additionally, the Strategic Plan describes strategies for achieving the strategic goals and provides numerous examples of means to support implementation of the strategies. The means to support the strategies consist of programs and initiatives that are in place or must be established to ensure that the NRC realizes its strategic goals.

The Strategic plan addresses the following five goals and related strategic outcomes:

I. Safety: Ensure protection of public health and safety and the environment.
- no nuclear reactor accidents
- no inadvertent criticality events
- no acute radiation exposures resulting in fatalities
- no releases of radioactive materials that result in significant radiation exposures
- no releases of radioactive materials that cause significant adverse environmental impacts

II. Security: Ensure the secure use and management of radioactive materials.
- no instances where licensed radioactive materials are used domestically in a manner hostile to the security of the United States

III. Openness: Ensure openness in NRC regulatory processes.
- stakeholders are informed and involved in NRC processes as appropriate

IV. Effectiveness: Ensure that NRC actions are effective, efficient, realistic, and timely.
- no significant licensing or regulatory impediments to the safe and beneficial uses of radioactive materials

V. Management: Ensure excellence in agency management to carry out the NRC's strategic objective.
- continuous improvement in NRC's leadership and management effectiveness in delivering the mission
- a diverse, skilled workforce and an infrastructure that fully support the agency's mission and goals.

The first four goals are directly applicable to the research plan programs; consequently, this appendix only summarizes the strategies for achieving the first four Strategic Plan goals. Correlations between the supporting strategies for Goals I through IV of the Strategic Plan and the Research Plan tasks and products are provided in Section 4 of the Research Plan, "Research Plan Task Summaries and Schedules."

A.1.1 Goal I: Safety

The NRC will employ the following strategies to ensure protection of public health and safety and the environment:

1. Develop, maintain, and implement licensing and regulatory programs for reactors, fuel facilities, materials users, spent fuel management, decommissioning sites, and waste-related activities to protect public health, safety, and the environment.
2. Develop systematic improvements in NRC regulatory programs to ensure the safe use and management of radioactive materials.
3. Use sound science and state-of-the-art methods to establish risk-informed and, where appropriate, performance-based regulations.
4. Utilize regulatory programs and applied research effectively to anticipate and resolve safety issues.

5. Evaluate and utilize domestic and international operational experience and events to enhance decision-making.

6. Conduct NRC safety oversight programs, including inspections and enforcement activities, to monitor licensee performance.

A.1.2 Goal II: Security

The NRC will employ the following strategies to ensure the secure use and management of radioactive materials:

1. Use relevant intelligence information and vulnerability analyses to determine realistic and practical security requirements and mitigation measures.

2. Conduct effective oversight activities and exercises to evaluate licensee security performance.

3. Enhance the handling and storage of sensitive security and other pertinent information and the communication of such information to licensees and Federal, State, and local partners.

4. Support interagency efforts to develop an integrated approach to the security of nuclear facilities and radioactive materials that supplements licensee efforts with appropriate Federal, State, and local government assets.

5. Use a risk-informed, graded approach to establish appropriate regulatory controls for possession, handling, import, export, and transhipment of radioactive materials.

6. Coordinate with Federal and international counterparts to provide appropriate security and control to prevent the proliferation of special nuclear materials and nuclear technology and to reduce the potential for harmful use of high-risk radioactive material.

A.1.3 Goal III: Openness

The NRC will employ the following strategies to ensure openness in its regulatory processes:

1. Provide accurate and timely information to the public about the uses of and risks associated with radioactive materials.

2. Enhance the awareness of the NRC's independent role in protecting public health and safety and the environment.

3. Provide accurate and timely information about the safety performance of the licensees regulated by the NRC.

4. Provide a fair and timely process to allow public involvement in NRC decision-making in matters not involving sensitive unclassified, safeguards, classified, or proprietary information.

5. Provide a fair and timely process to allow authorized (appropriately cleared with a need to know) stakeholders involvement in NRC decision-making in matters involving sensitive unclassified, safeguards, classified, or proprietary information.

6. Obtain early public involvement on issues most likely to generate substantial interest and promote two-way communication to enhance public confidence in the NRC's regulatory processes.

A.1.4 Goal IV: Effectiveness

The NRC will employ the following strategies to ensure that its actions are effective, efficient, realistic, and timely:

1. Use state-of-the-art methods and risk insights to improve the effectiveness and realism of NRC actions.
2. Improve NRC regulation by adding needed requirements and eliminating unnecessary requirements.
3. Use performance-based regulation to minimize unnecessarily prescriptive requirements.
4. Use realistically conservative, safety-focused research programs to resolve safety-related issues.
5. Enhance cooperation with Federal, State, and Tribal governments and international counterparts.
6. Minimize unnecessary regulatory or jurisdictional overlap.
7. Anticipate challenges and respond quickly to changes in the regulatory and technical environment.
8. Make timely regulatory decisions.
9. Foster innovation at the NRC to improve systematically the NRC's regulatory programs.