NRC Digital System Research Plan
FY 2010-FY 2014

Digital Instrumentation and Controls Branch
Division of Engineering
Office of Nuclear Regulatory Research

February 2010

CONTENTS

Section **Page**

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

Table **Page**

EXECUTIVE SUMMARY

This document establishes research programs that support the U.S. Nuclear Regulatory Commission's (NRC's) mission and regulatory activities in the area of Digital Instrumentation and Controls (DI&C). The products from this research include, for example, the technical bases for rules, licensing guidance included in standard review plans, regulatory guides, NUREG/CR-series reports that provide additional information for NRC licensing and inspection staff, review procedures, proposals to influence relevant national and international standards, and organized knowledge transfer from other application sectors.

Following major market trends, nuclear facilities and byproduct licensees are expected to replace the traditional electromagnetic and analog elements in their safety systems and equipment with programmable DI&C systems and equipment. Major drivers are (1) migration of larger markets to DI&C, causing obsolescence and unavailability of older parts and skilled workers familiar with their application and maintenance; (2) ease of calibration and drift-compensation; (3) easier customization and greater flexibility, reconfigurability, and upgradeability through software; (4) elimination of degradation (wear and tear); (5) lower cost of implementation, maintenance, and change; (6) reduction of control cabinet size and space requirements; and (7) easier integration with highly integrated digital control rooms being proposed for new reactors as part of Design Certification (DC) and Combined Operating License (COL) applications.

The introduction of this technology into nuclear applications poses a variety of review challenges. These challenges include, for example, (1) failures from systemic causes; (2) failures resulting from increasing complexity, if not managed properly; (3) the need for commensurate competence; and (4) limited understanding of associated failure modes. In addition, because industry intends to exchange information between safety and nonsafety systems, NRC must develop expertise in evaluating complex digital communication systems.

A substantial increase in the use of digital systems in safety systems is expected for both new and operating reactors, as well as fuel cycles facilities. For this reason, a need exists for periodic review and update of the DI&C System Research Plan to improve the acceptance criteria and review procedures used to consistently assess the safety and security of digital systems. The "NRC DI&C System Research Plan FY 2010-FY 2014" is the third in a succession of DI&C research plans resulting from the recommendations provided by the 1997 National Research Council report titled, "Digital Instrumentation and Control Systems in Nuclear Power Plants" [1]. The format of this DI&C System Research Plan has evolved from the two previously issued DI&C Research Plans (FY 2000-FY 2004 and FY 2005-FY 2009) given that the new format more clearly articulates the Office of Nuclear Regulatory Research's strategic approach for DI&C activities and leverages anticipated resources.

The "NRC DI&C System Research Plan FY 2010-2014" describes the technical issues of ongoing and planned activities to support the regulation of digital technologies applied in the U.S. commercial nuclear industry. Projects and activities within projects are categorized into different complementary programs. The planning and direction of each research program and project will periodically be reviewed and revised as needed in the current environment of emerging technologies and state-of-the-art implementation of existing technologies.

ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
ADAMS	Agency-wide Documents Access and Management System
CFR	Code of Federal Regulations
CMMI-SAFE	Capability Maturity Model® Integration-Safety Engineering
COL	Combined Operating License
COMPSIS	Computer-Based Systems Important to Safety
DC	Design Certification
DI&C	Digital Instrumentation and Control
EM	Electromagnetic
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EPRI	Electric Power Research Institute, Inc.
FY	Fiscal Year
GIs	Generic Issues
HF	Human Factors
HRP	Halden Reactor Project
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISG	Interim Staff Guidance
ISO	International Organization for Standardization
LER	Licensee Event Report
LOOP	Loss of Offsite Power
NASA	National Aeronautics and Space Administration
NGNP	Next Generation Nuclear Plant
NMSS	Office of Nuclear Material Safety and Safeguards
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
NRO	Office of New Reactors
NRR	Office of Nuclear Reactor Regulation
NSIR	Office of Nuclear Security and Incident Response (see NRC)
OECD/NEA	Organization for Economic Cooperation and Development, Nuclear Energy Agency

PRA	Probabilistic Risk Assessment
PWDS	Plant-wide Data System
QSRM	Quantitative Software Reliability Method
R&D	Research and Development
RES	Office of Nuclear Regulatory Research
RIL	Research Information Letter
RIS	Regulatory Issue Summary
RF	Radiofrequency
RFI	Radiofrequency Interference
RG	Regulatory Guide
SPACE	Specification and Coding Environment (Teleperm XS)
SRM	Staff Requirements Memorandum
TRACE	TRACE/RELAP5 Advanced Computation Engine Project
V&V	Verification and Validation

1. INTRODUCTION

The U.S. Nuclear Regulatory Commission (NRC) is an independent government agency created by Congress in 1974 to regulate the civilian commercial, industrial, academic, and medical uses of nuclear materials to protect the public health and safety and to promote the common defense and security. NRC's Office of Nuclear Regulatory Research (RES) is a statutory office that furthers NRC's regulatory mission by providing technical advice, technical tools, and information for identifying and resolving safety issues; making regulatory decisions; and promulgating regulations and guidance. The RES Division of Engineering, Digital Instrumentation and Control (DI&C) Branch (RES/DE/DICB), develops and applies methods, data, tools, standards, and guidance used by licensing offices to assess the safety and security of DI&C systems. RES/DE/DICB also develops and implements a comprehensive research program to address digital system and software safety impacts and security aspects that can affect safety or security.

NRC generally developed the current nuclear power plant (NPP) DI&C review guidance in the 1990s. However, DI&C technology is evolving and changing rapidly , and NRC continues to refine its regulatory approach. Current control rooms are dominated by analog equipment such as electro-mechanical switches, annunciators, chart recorders, and panel-mounted meters. However, as NPPs upgrade their control rooms, analog equipment is being replaced with modern digital equipment including updated operator interfaces (i.e., displays) and soft controls. NRC expects an increase in the use of digital systems for both new reactors and retrofits in operating reactors as well as fuel cycle facilities. As a result, NRC continues to evaluate applicable licensing criteria and regulatory guidance to identify gaps and to perform research to fill the gaps.

The DI&C Research Plan defines a coherent set of research programs that support the regulatory needs of the NRC licensing offices. As a result, a need exists for periodic review and update of the DI&C Research Plan to ensure the research programs are supporting the NRC licensing offices in assessing the safety and security of digital systems. The DI&C Research Plan FY 2010-2014 is the third in a succession of DI&C research plans resulting from recommendations provided by the 1997 National Research Council report titled, "Digital Instrumentation and Control Systems in Nuclear Power Plants"[1]. RES provided the first plan (for FY 2000-2004) [2] to the Commission, as an attachment to a SECY Paper: NRC Research Plan for Digital Instrumentation and Control [3]. The second plan (for FY 2005-2009) [4] was published as an attachment to a Memorandum dated April 26, 2006 (ML061150040).

2. DI&C STRATEGIC APPROACH

2.1 Objectives

The Digital Instrumentation and Control (DI&C) Research Plan has the following objectives:

1. Ensure that NRC regulations and regulatory processes have sound technical bases and these bases are refined as new knowledge develops.

2. Prepare for anticipated changes in the nuclear industry that could have safety and security implications.

3. Develop improved methods to carry out NRC's regulatory responsibilities.

4. Maintain an infrastructure of expertise, facilities, analytical capabilities, and data to support regulatory decisions.

These objectives support the safety and security goals stated in NRC's FY 2008-2013 Strategic Plan [5] and were derived from the Advisory Committee on Reactor Safeguards (ACRS) 2008 report, "Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program" [6]. All programs, projects, and project deliverables in this plan support the agency strategic goals through the four research objectives identified above.

In general, DI&C regulatory research is driven by the needs of the licensing offices.

2.2 Research Planning Method and Application of Research Project Outputs

The planning process identified programs, projects, and deliverables that support the NRC DI&C research objectives through the following steps (also illustrated in Figure 2.1):

1. Identify the technical gaps impacting licensing work of the various NRC Licensing offices (i.e., the Offices of Nuclear Regulatory Regulation, New Reactors, Nuclear Material Safety and Safeguards, and Nuclear Security and Incident Response).
2. Derive the DI&C-specific NRC research program objectives (e.g., the technical bases needed).
3. Evaluate research opportunities in accordance with the selection and ranking criteria given in Section 2.3.

   Identify the work products to be delivered based on user office level of need or priority, for example:

   - Technical guidance.
   - Tools (and manuals as appropriate) to support the evaluation of licensee and vendor submittals under NRC review.
   - Review procedures (and optionally, inspection procedures) that guide the reviewer in using the technical guidance, acceptance criteria, and tools.
   - Knowledge transfer and learning resources.

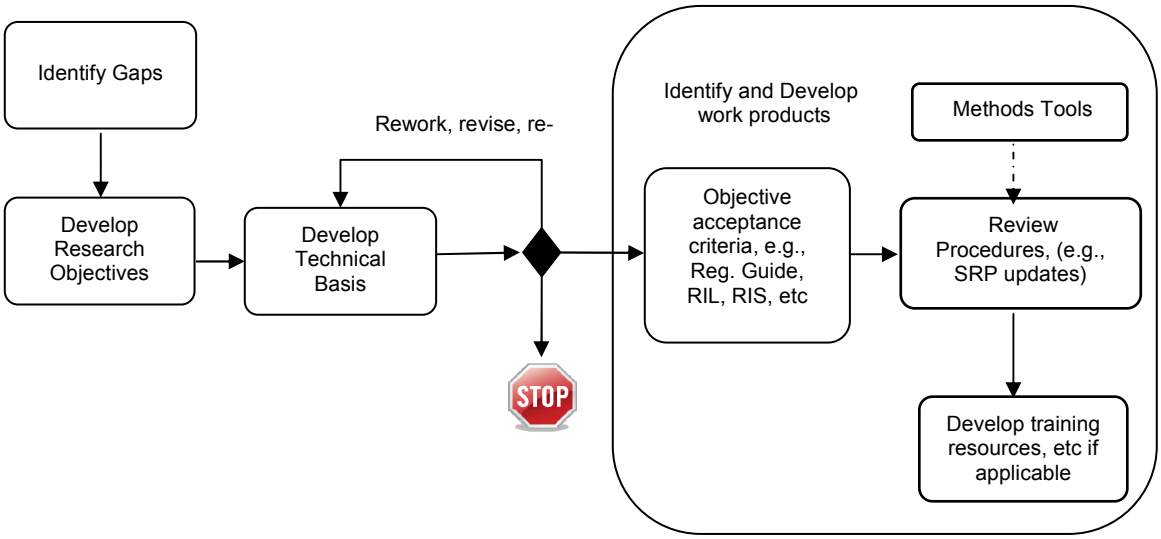

Figure 2.1 Method to Plan Research Programs, Projects, and Deliverables

4. Enable the plan to allow for internal and external (public) periodic revision, based on results from earlier-stage activities and other new information. For example, this will be facilitated by the new RES/DE/DICB internal website that will be used to communicate information about ongoing DI&C research plan projects including priorities, schedules and deliverables, DI&C regulatory guide (RG) updates and RES/DE/DICB contact information for those who have access to NRC internal websites.

   Project plans are not static, but include provisions to evolve, refine, and adapt later-stage activities based on stakeholder reviews of results from earlier-stage activities and other new information emerging in the interim period.

5. Tailor final deliverables to stakeholder needs as work products are completed. For each project, training can be requested by any stakeholder office. Training courses will be included as an optional task for each research project statement of work, as applicable.

Also, as part of the research planning process, RES/DE/DICB management developed a checklist of other considerations in the development of this plan, for example:

- Seek a broader, diverse set of inputs and perspectives.
- Determine industry issues, controversies, requests, complaints/protests where the root-cause analysis leads to a need for creating more knowledge and guidance.
- Develop criteria for rank-ordering and selection of projects. Define how these criteria are derived from the NRC research program objectives and other influencing factors.
- Seek other factors and considerations from NRC-internal customers.
- Promote continuation of projects identified in the FY05-FY09 research plan that are still desired/needed by the applicable regulatory office.

2.3 Selection and Priority-Ranking Approach

Unfinished projects carried over from the DI&C System Research Plan FY 2005-FY2009 [4], were the starting point for the DI&C System Research Plan FY 2010-FY 2014. The updated plan also includes project ideas from various NRC-internal stakeholders. Face-to-face meetings with NRC-internal stakeholders were held to address their user needs and to comment and provide information regarding the selection and priorities for the projects to be included in this plan.

Upon review with NRC-internal stakeholders, several communication tools were provided to allocate priorities and to identify the degree of strength of stakeholders' support. These communication tools identified the types of benefits contributed by the planned projects and identified the supporting stakeholders. The plan projects are prioritized from highest to lowest priority (please refer to Table 2 in Appendix 2) with respect to the completion 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.

2.4 Research Plan Schedule

This section addresses the expected baseline schedule (Figure 2.2) for the Digital System Research Plan FY 2010-FY 2014 programs and projects. The baseline schedule was based on the information gathered in Section 2.3. Because the projects are driven by the needs of the licensing offices and budgets, this expected schedule can evolve and adapt based on new information emerging over time.

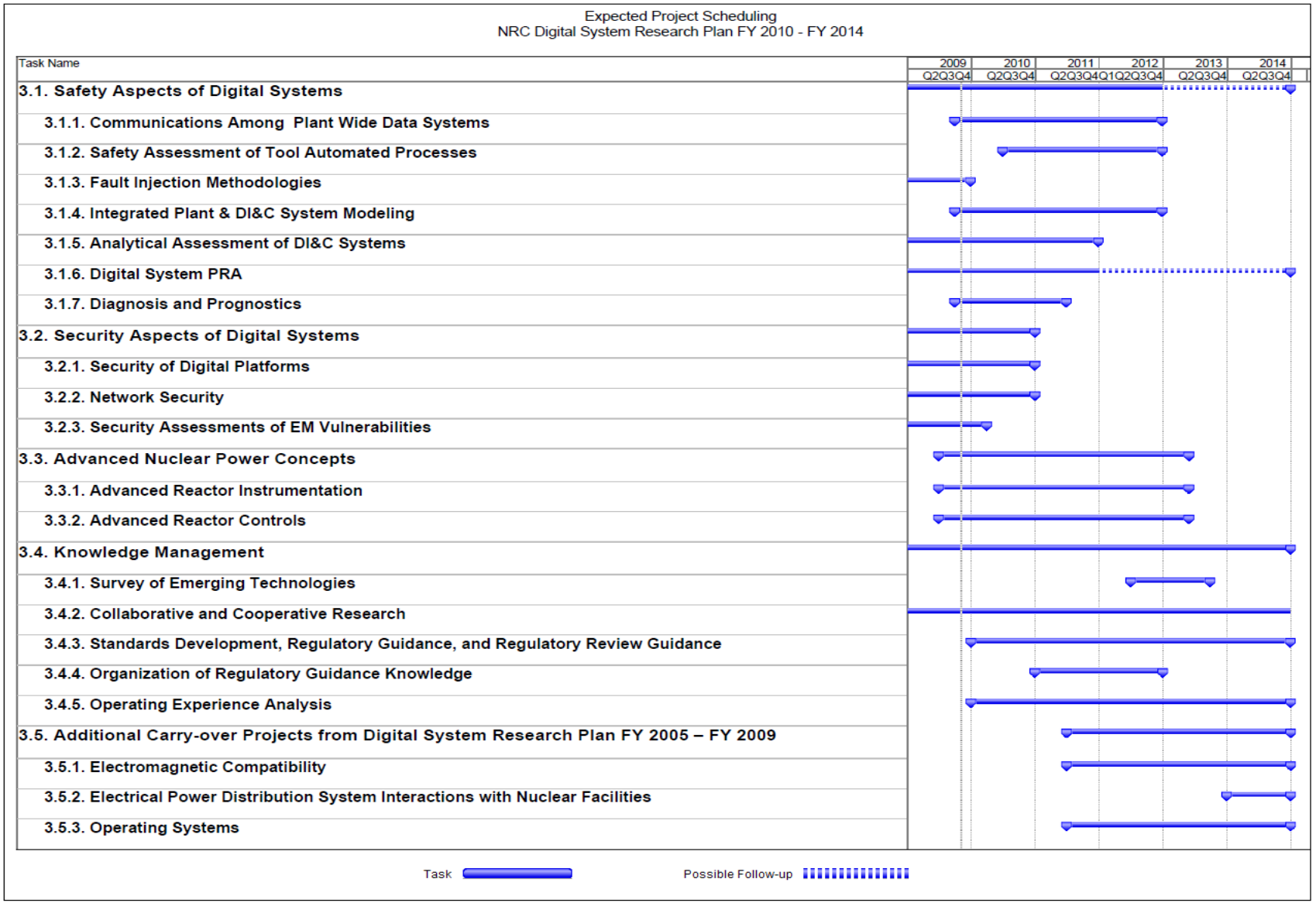

Figure 2.2 Expected Project Scheduling of the Digital System Research Plan FY 2010-FY 2014

2.5 Research Plan Organization

Research projects have been combined into five common topic areas called research programs, as shown in Figure 2.3. Each project contains sections titled, “Purpose,” “Project Basis,” “Safety Significance and Benefit,” “Technical Basis,” and “Deliverables.”

- “Purpose” seeks to communicate the goal and expected outcome of the project.
- “Project Basis” identifies the party responsible for requesting that the project be included in this research plan. It establishes the parties that will be present during periodic reviews of the project.
- “Safety Significance and Benefit” expresses why the work was requested and specifies the regulatory need.
- “Technical Basis” provides the technical context that has led to the formulation of the project.
- “Deliverables” lists the products which will communicate the outcomes of the project to the licensing offices.

<table>
<tr><th>3.1. Safety Aspects of Digital Systems</th><th>3.2. Security Aspects of Digital Systems</th><th>3.3. Advanced Nuclear Power Concepts</th></tr>
<tr><td rowspan="3">3.1.1. Communications among Plant-wide Systems

3.1.2. Safety Assessment of Tool Automated Processes

3.1.3.Fault Injection Methodologies

3.1.4. Integrated Plant & DI&C System Modeling

3.1.5. Analytical Assessment of DI&C Systems

3.1.6. Digital System PRA

3.1.7. Diagnostics and Prognosis</td><td>3.2.1. Security of Digital Platforms
3.2.2. Network Security

3.2.3. Security Assessments of EM/RF Vulnerabilities</td><td>3.3.1. Advanced Reactor Instrumentation

3.3.2. Advanced Reactor Controls</td></tr>
<tr><th>3.4. Knowledge Management</th><th>3.5. Additional Carry-over Projects from Digital System Research Plan FY 2005 – FY 2009</th></tr>
<tr><td>3.4.1. Survey of Emerging Technologies

3.4.2. Collaborative and Cooperative Research

3.4.3. Standards Development, Regulatory Guidance, and Regulatory Review Guidance

3.4.4. Organization of Regulatory Guidance Knowledge

3.4.5. Operating Experience Analysis</td><td>3.5.1. Electromagnetic Compatibility

3.5.2. Electrical Power Distribution System Interactions with Nuclear Facilities

3.5.3 Operating Systems</td></tr>
</table>

Figure 2.3 Digital System Research Plan FY 2010-FY 2014 Projects Organized by Programs

2.6 Interrelationships Across Disciplines, Projects, and Deliverables

Issues of regulatory importance often cross multiple disciplines including DI&C (e.g., Human Factors (HF) and Probabilistic Risk Assessment (PRA)). The aspects of these disciplines relating to DI&C are being addressed through deliverables spread throughout various research projects in this Research Plan. The dependency and relationships among these distributed deliverables can be captured through specific Strategic Roadmaps. Figure 2.4 shows an example of Strategic Roadmap for DI&C PRA.

Other issues that are best addressed through the Strategic Roadmap may arise through the course of technological advances. As part of periodic reviews, this Strategic Roadmap will be evaluated with provisions to evolve, refine, and adapt later-stage activities based on results obtained from delivered products and other new information emerging in the interim period. To ensure that deliverables relevant to the Strategic Roadmap are completed logically and in a timely manner, the NRC staff tracks deliverables through Roadmap task summaries and schedules.

In addition, to improve the efficiency and completeness of DI&C research efforts, a number of projects share information with other projects. These dependencies are indicated explicitly in the different projects (please refer to Table 1 of Appendix 1). Also, interrelationship dependencies exist with other branches (i.e., HF, PRA) and research plans as follows:

- Project 3.1.5, “Analytical Assessment of DI&C Systems,” provides the technical basis for reducing epistemic uncertainty. In addition, it provides information that can be used to assess the effects of degraded instrumentation and controls on operator's performance for a project that is managed by the NRC Office of Nuclear Regulatory Research, Division of Risk Analysis, Human Factors and Human Reliability Branch.

- Project 3.1.6, “Digital Systems PRA,” includes the "software reliability project" that is managed by the NRC Office of Nuclear Regulatory Research, Division of Risk Analysis, Probabilistic and Risk Analysis Branch.

- Project 3.4.2, “Collaborative and Cooperative Research,” acquires relevant knowledge from outside the NRC (e.g., Cooperative Nuclear Safety Research between NRC and the Electric Power Research Institute, Inc. (EPRI) for DI&C and HF [7]).

- Project 3.4.5, “Operating Experience Analysis,” uses Operating Experience data and information to the extent available.

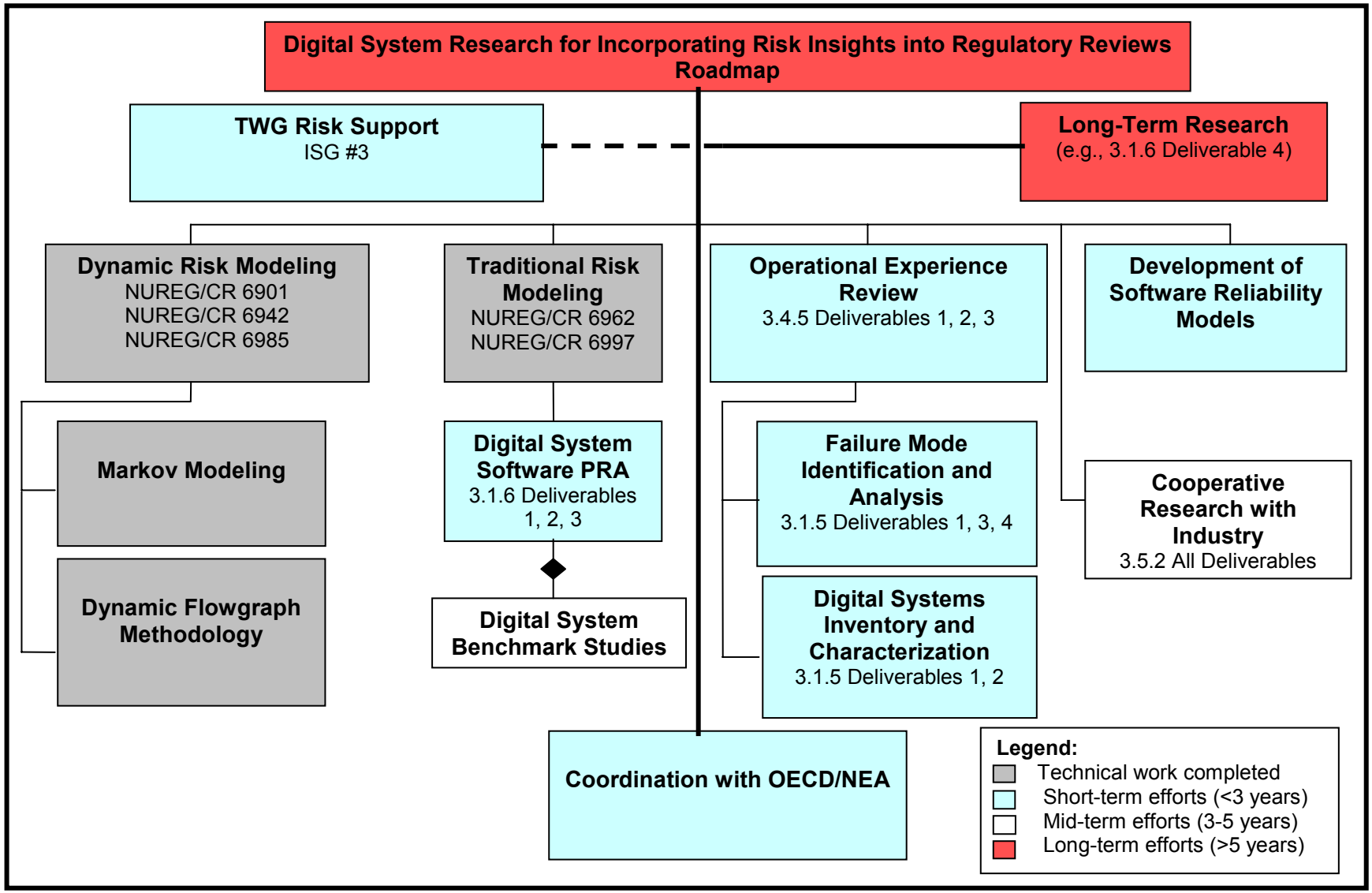

Figure 2.4 Digital System Research for Incorporating Risk Insights into Regulatory Reviews Roadmap

3. RESEARCH PROGRAMS

The "NRC Digital System Research Plan FY 2010-FY 2014" is organized hierarchically into the following five research programs:

1. 3.1 Safety Aspects of Digital Systems.
2. 3.2 Security Aspects of Digital Systems.
3. 3.3 Advanced Nuclear Power Concepts.
4. 3.4 Knowledge Management.
5. 3.5 Additional Carry-Over Projects from Digital System Research Plan FY 2005-FY 2009.

Each research program consists of research projects and associated specific research deliverables. In addition, this Research Plan describes activities that support the development of regulatory guidance, maintenance of NRC's research infrastructure and base of knowledge, and collaborative and cooperative development of supporting research deliverables.

3.1 Safety Aspects of Digital Systems

This research program will address aspects of digital technologies that can adversely affect safe operation of licensee facilities. The proposed deliverables will augment the NRC staff's capabilities to perform in-depth technical evaluations of digital safety system designs.

3.1.1 Communications Among Plant-wide Systems

Purpose

The purpose of this research project is to gain a better understanding of how plant-wide DI&C systems might be interconnected and what the implications of those interconnections might be.

Project Basis

This project stems from prior staff efforts, such as DI&C Interim Staff Guidance-4 (DI&C-ISG-04, ML072540138), that have focused on the reliability, redundancy, and independence requirements applicable to digital safety systems, including communication between safety and nonsafety systems. This project supports NRR and NRO.

Safety Significance and Benefit

This project intends to improve the quality, clarity, and consistency of regulatory guidance. Safety-significant questions of interest that this project intends to address include:

- How can DI&C systems share information without the communication links having a potential negative safety consequence?

- Where are the potential points of vulnerability to errors, malfunctions, carelessness, and malfeasance?

- What pathways are needed or appropriate among plant equipment, and between plant equipment and the outside world, and how should those be controlled and protected?

Technical Basis

The Plant-wide Data System (PWDS) refers to the network of systems whereby plant process information, status information, and actuation commands are distributed among diverse destinations. The PWDS may include the safety-related protection and control systems, all nonsafety control and monitoring systems, and all enterprise data systems, including on-site and off-site networking. Issues such as data isolation, interdivisional two-way communications, data density, and communication traffic levels appropriate for safety-related applications will be investigated by means of a high level architectural framework. This framework will identify characteristics that all applications should take into consideration and that are likely applicable to any NPP.

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

> 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.

Much NRC and industry effort has been focused on the isolation and independence requirements applicable to DI&C safety systems and on the influence of nonsafety control stations upon the safety systems. DI&C-ISG-04, for example, describes how controls and indications from all safety divisions can be combined into a single integrated workstation while maintaining reliability, redundancy, and independence (including adequate separation and isolation) among redundant channels (ML072540138). It will be beneficial to develop further regulatory guidance on communication processes that are appropriate for the exchange of information between plant sensors/actuators and the protection and control systems, and among safety channels.

Deliverables

This research project will produce the following:

1. A high level architectural framework of a plant-wide digital network that supports staff reviews of licensing requests relating to Highly Integrated Control Room communication protocols and systems for safety and nonsafety DI&C systems. The framework will identify characteristics that all applications should take into consideration and are applicable to any nuclear power plant.

2. A NUREG/CR on communication processes and review criteria for the exchange of information between plant sensors/actuators and the protection and control systems and among safety channels (such as for voting).

3. Regulatory guidance on DI&C network characteristics that provide adequate reliability, redundancy, and independence (including adequate separation and isolation) among redundant channels.

3.1.2 Safety Assessment of Tool Automated Processes

Purpose

To assess the use and limitations of software tools used in the automation of various DI&C lifecycle processes. Specifically, to develop a set of criteria for accepting the use of design and/or testing software tools for digital systems in licensing reviews. To do this, the NRC staff will also leverage experience, best practices, and standards from other industries, such as aviation and telecommunications.

Project Basis

This project is being established as new work to support NRR, NRO, and NMSS licensing reviews.

Safety Significance and Benefit

A lack of guidance exists which identifies clear acceptance criteria for the use of tool automated processes. Some of the tools are being used to develop operational codes to perform automated Verification and Validation (V&V) and requirements management. This project intends to improve the efficiency, effectiveness, and timeliness of regulatory reviews.

Technical Basis

Whereas tool-automated and tool-assisted engineering activities may result in fewer errors than manual engineering activities, the source of errors may shift from the primary engineering activities to the engineering activities for process design and tool automation. Whereas a mistake in the direct engineering activity affects only the object of that activity (one system), a mistake in process design or tool automation affects all systems designed with that process or tool.

- An error is further exacerbated when both the design process and the V&V process are semi-automated based on the same technological elements (e.g., a “graphical application programming language”).

- An error is further exacerbated by the lack of detectability of mistakes embedded in the engineering process infrastructure.

“Proven in use” claims by applications are not easily assessable. This issue is made more difficult when elements of the engineering process infrastructure are proprietary (e.g., a “graphical application programming language”, and tool-automated processes that depend on this language).

The NRC staff will find value in leveraging relevant experience, best practices, and standards outside the nuclear industry. An example of a collaborative and coordination forum that addresses automated tools is the Requirements and Technical Concepts for Aviation working group for DO-178-B

Deliverables

This research project will produce the following products:

1. A NUREG/CR containing a review of the processes, languages, and tools for developing NPP DI&C safety systems including assessments of the vulnerabilities associated with the use of the tools.

2. Regulatory guidance to provide acceptance criteria and adequacy of proof from industry operating experience (proven in use claims) regarding the use of tool-assisted or tool-automated engineering activities.

3.1.3 Fault Injection Methodologies

Purpose

The purpose of this research is to provide a process for evaluation and validation of digital systems using a fault injection process.

Project Basis

This project is an ongoing project conducted by University of Virginia and supported by NRR and NRO.

Safety Significance and Benefit

To gain an improve understanding of the ways in which the system can fail through testing and ways in which it is resistant to failure. In addition, to provide another means for obtaining "reasonable assurance" that a design is of high quality.

Technical Basis

High-quality design processes minimize the introduction of mistakes into the system design. Software quality assurance processes identify and remove faults introduced during the system development process and are the primary fault avoidance strategies addressed by this research project. 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 (e.g., design processes and V&V processes), faults can remain undetected in a system.

The purpose of system testing during the operation and maintenance life cycle phase is to detect faults that were not discovered during the system development process (e.g., improper handling of faults).

Deliverables

This research project will produce the following products:

1. A NUREG/CR which describes the methods for performing fault-injection of digital safety systems.

3.1.4 Integrated Plant & DI&C System Modeling

Purpose

The purpose of this research is to develop models of digital safety systems integrated with reactor accident analysis software tools.

Project Basis

This project is new work. Deliverables will be supplementary tools for NRC staff to independently review and evaluate the acceptability of licensing applications and proposed resolutions of safety issues and/or the development of technical bases for staff-proposed safety enhancements.

Safety Significance and Benefit

Integration of the plant model will enable better simulation of off-normal and transient conditions. This simulation capability allows NRC staff to better understand and assess the impacts on plant safety of DI&C system failures and errors. The ultimate use of this model can be failure mode and effects analysis on plant performance, input to PRA, HRA, DI&C system validation, etc. This project intends to improve the efficiency, effectiveness, and timeliness of regulatory reviews.

Technical Basis

Previous RES projects developed a method to couple third-party software to reactor accident analysis software tools, specifically the MATLAB-to-TRACE capability. A previous effort used the Oconee digital Integrated Control System as the case study. This research will build models of safety-related digital systems for use in support of reviews pertaining to DI&C and to assist in the characterization associated with the impact of DI&C system failure modes on reactor safety.

Deliverables

1. This research project will produce models of DI&C safety systems in reactor accident analysis software codes including associated documentation.

3.1.5 Analytical Assessment of DI&C Systems

Purpose

This research will develop an NRC capability for effective and efficient assessment of digital instrumentation and control (DI&C) systematic failures during the system lifecycle. The developed knowledge base will evolve iteratively. The goals of this project are:

- To improve the technical bases, knowledge, methods, tools, and data in support of relevant NRC regulatory guidance.
- To support further research in DI&C PRA.

Project Basis

This project is formulated in response to a Commission requirement [8] to identify and analyze DI&C failure modes and to discuss the feasibility of applying failure mode analysis to assess the safety impact of DI&C systems. It also supports the NRC Executive Director for Operations letter to the ACRS [9], by including the following goals:

- In identifying failure modes, focus on system failure paths (as opposed to just component-level failure mode identification).

- With respect to the issue of systematic failures, including those attributable to software, seek knowledge and information from other safety-critical, mission-critical application domains and relevant literature.

- Explore a more refined treatment of failures attributable to software and other systematic failures.

The research will also include exploration of system failures in the development process to the extent practicable.

The project also supports regulatory priorities transmitted through Staff Requirements Memorandum (SRM) M070607 dated June 22, 2007 (ML07173024), directing the staff to:

- Develop an inventory and classification (e.g., by function or other characteristics) of the various types of digital hardware and software systems that are being used and are likely to be used in nuclear power plants.

Safety Significance and Benefit

A lack of adequate understanding of hardware and software failure modes and associated contributing factors to these failures in DI&C systems exists, especially in those attributable to systematic causes. This lack of understanding limits NRC's capability to estimate the resulting impact on safety. In addition, prior NRC-sponsored research confirmed gaps in the technical bases, analytical foundation, methods, tools, and data [4]. This also limits NRC's ability to develop and quantify reliability models for digital systems.

The increasing rate of change of digital technology and its application environment further exacerbates the need for consistency in the assessment of safety by NRC reviewers and industry stakeholders of DI&C systems. This project intends to support the development of new regulatory guidance.

Technical Basis

Data from operational experience obtained and analyzed to date have been found to be inadequate to identify and analyze failure modes and causal factors, partly exacerbated by rapid technological changes as well as different application domains. Data from different systems are often not comparable, and meaningful aggregation is difficult (due to differences in the respective systems and their environments). Therefore, deliverable 1 (current inventory and classification) and deliverable 2 (its characterization) are planned to allow meaningful analysis

and conclusions from data about disparate systems and environments. It is likely that special techniques will be developed to extract meaningful information from data limited in quality and quantity.

Deliverables 2, 3, and 4 are planned to define boundaries within which a reasonable assessment of safety could be made and issues of concern identified.

Deliverable 3.1 is planned in response to a request from the Office of Nuclear Reactor Regulation (NRR) based on situations experienced in safety reviews, where the existing guidance is not sufficient (e.g., a distributed system with a network configured in redundant ring topology).

Deliverable 3.2 is planned in response to a request from NRR, based on emerging systems seen in safety reviews, where the existing guidance may not be sufficient for the complex systems resulting from industry's shift toward tightly integrated systems. For example, the existing Standard Review Plan (SRP) treats review of the Reactor Protection System separately from the review of data communication systems.

Deliverables 2-4 also support additional DI&C PRA and HRA research. Deliverables 2 and 3 bound the domain of DI&C systems. Deliverable 3 also provides a method for modeling the effects of software and hardware failures on digital systems, crews and the plant. Deliverable 4 bounds the domain of engineering process factors and characterizes the contributing factors and enables incorporating expert qualitative judgment in the estimation of risk.

Deliverables

1. Letter report inventorying and classifying the various types of DI&C systems and components that are being used or are likely to be used in NPPs.

2. Characterization of different kinds DI&C systems and the relationship to their environments, generalized in phases:

   2.1. Considering existing systems in NPPs

   2.2. Considering emerging systems in NPPs

   2.3. Considering knowledge gained from safety critical systems outside NPPs.

3. Identify credible failure modes typical of software-intensive DI&C systems (based on deliverable 2) and determine the interaction of these failure modes with the rest of the systems, operating crew, and the plant by developing fault/failure models, as follows:

   3.1. Analyze each NRC approved safety system platform (i.e., Common Q: AF100 & HSL; TXS: PROFIBUS & Ethernet; Triconex: Tricon) and identify all credible fault and failure modes. Include models to "roll up" or "up-integrate" effects of malfunctions in networked elements.

   3.2. Perform an analysis for systems with tightly coupled integration of traditionally decoupled or loosely coupled functions, applications (e.g., RTS, engineered safety features actuation system), signals, and infrastructural services, as exemplified in new licensing applications.

3.3. For each NRC-approved safety system platform (e.g., Common Q, TXS, Triconex) and each new type of module in it (e.g., Priority Logic Module), identify all credible fault and failure modes. Included are models to "roll up" or "up-integrate" effects of constituent or component malfunctions on the DI&C platform.

3.4. For each new type of component and technology (e.g., field-programmable gate array, programmable logic device, application specific integrated circuit, microprocessor) in each module (4.3), identify all credible fault and failure modes and known mechanisms.

4. Conduct a Process Failure Modes and Effects Analysis to identify engineering process factors and characterize their contribution to risk, and indentify preventive measures for the application domain.

A series of NUREG/CR reports will document the methodologies and results of the analysis performed in the above deliverables.

3.1.6 Digital System PRA

Purpose

The purpose of this research is to identify and develop methods, analytical tools, and regulatory guidance to support (1) including DI&C system models into NPP PRAs and (2) using information on the risks of DI&C systems in regulatory decisions for NPPs.

Project Basis

This project supports the development of PRA methods and tools for analyzing the reliability of digital systems to assist NRR and NRO in reviewing NPP licensing action submittals containing digital system risk information. It is ultimately intended to issue regulatory guidance, as appropriate, on risk-informed decision-making review methods applicable to DI&C systems.

Safety Significance and Benefit

The use of PRA aids the staff in focusing our regulatory attention in those areas of greatest relative safety significance. Also, incorporating DI&C system models into PRAs will support many of the NRC's risk informed programs as digital systems become more widely used in NPPs.

Technical Basis

The current licensing process for digital systems is based on deterministic engineering criteria. In its 1995 PRA policy statement, the Commission encouraged the use of PRA technology in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data. Although many activities have been completed in the area of risk-informed regulation, the risk-informed analysis process for digital systems has not yet been satisfactorily developed. Because, at present, no consensus methods exist for quantifying the reliability of digital systems, this project addresses risk assessment methods and data for digital systems.

Previous and current RES projects have identified a set of desirable characteristics for reliability models of digital systems and have applied various probabilistic reliability modeling methods to

an example digital system (i.e., a digital feedwater control system). The results of these "benchmark" studies have been compared to the set of desirable characteristics to identify areas where additional research might improve the capabilities of the methods. One specific area that is being pursued is the quantification of software reliability. Given the substantial differences in PRA modeling of software (versus conventional NPP components), a workshop involving experts with knowledge of software reliability and/or NPP PRA was convened in May 2009. At the workshop, the experts established a philosophical basis for modeling software failures in a reliability model. RES is now performing a review of quantitative software reliability methods (QSRMs), and plans to develop one or two technically sound approaches to modeling and quantifying software failures in terms of failure rates and probabilities. Assuming such approaches can be developed, they will then be applied to an example software-based protection system in a proof-of-concept study.

The results of the benchmark studies also have highlighted the following areas where enhancement in the state-of-the-art for PRA modeling of digital systems is needed:

- Approaches for defining and identifying failure modes of digital systems and determining the effects of their combinations on the system. Methods for determining the effects of the combinations of failure modes would reveal how modes propagate from their sources to the rest of the system and other systems of the plant.

- Methods and parameter data for modeling self-diagnostics, reconfiguration, and surveillance, including using other components to detect failures, such as watchdog timers and microprocessors. The data would encompass the fraction of failures that can be detected.

- Better data for hardware failures of digital components including addressing the potential issue of double-crediting fault-tolerant features such as self-diagnostics.

- Better data for the common-cause failures (CCFs) of digital components.

- Methods for modeling software CCF across system boundaries (e.g., due to common support software).

- Methods for addressing modeling uncertainties in modeling digital systems.

- Methods for human-reliability analysis associated with digital systems.

- Determining if and when a model of controlled processes is necessary in developing a reliability model of a digital system.

Input for resolving some of these issues will come from the work covered under Project 3.1.5, "Analytical Assessment of DI&C Systems" and Project 3.4.5, "Operating Experience Analysis." Work to resolve the remainder of these issues is anticipated to begin during the FY 2010-2014 period, as appropriate, based on technical and resource considerations. However, even if an acceptable method is established for modeling digital systems in a PRA, (1) the level of effort and expertise required to develop and quantify the models will need to be practical for vendors and licensees and (2) the level of uncertainty associated with the quantitative results will need to be sufficiently constrained so that the results are useful for regulatory applications.

Deliverables

This research project will produce the following products:

1. A letter report on the results of the workshop on the philosophical basis for modeling software failures in a reliability model.

2. A letter report on a comprehensive review of available QSRMs.

3. A NUREG/CR report that documents the selection of candidate QSRMs and how they will be applied to an example digital system.

4. Depending on the results of the above deliverables, additional deliverables may include a NUREG/CR report that documents the application of candidate QSRMs to an example digital system, and, ultimately, analytical tools and regulatory guidance to support (1) including DI&C system models into NPP PRAs and (2) using information on the risks of DI&C systems in regulatory decisions for NPPs.

3.1.7 Diagnostics and Prognostics

Purpose

The purpose of this research project is to investigate the integration of diagnostics and prognostics (D&P) systems into NPPs, and their impact on regulatory requirements (i.e., surveillance, calibration, and functional tests).

Project Basis

This research project supports the anticipatory Advanced Reactor Research Program that states RES should "Analyze advanced diagnostic and prognostic methods to support licensing of advanced reactors." In addition, this project will investigate uses of diagnostics and prognostics technologies in current and new reactors.

Safety Significance and Benefit

The proper use of digital diagnostics and prognostics to monitor the operation and condition of safety components may increase their reliability. However, the methods used to carry out the diagnostics and prognostics should not potentially compromise equipment operability. In addition, uncertainties in these systems should be thoroughly understood, and processes for managing these uncertainties should be developed. In addition, most D&P systems involve significant amounts of software; thus, software quality will be a focus of study.

Technical Basis

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.

The goal of these D&P techniques is to provide improved methods for detection and intervention of faults and impending failures to maintain the operability of 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.

Technical challenges associated with diagnostics and prognosis include determining what data to measure and how to measure it; data interrogation, communication, and integration; development of equipment life forecasting models; system integration and deployment; quantification of uncertainties; incorporation of smart components, and self-diagnostic systems.

Deliverables

This research project will produce the following products:

1. A NUREG/CR providing review procedures and acceptance criteria for D&P applications and self-testing features in digital systems in nuclear facilities.

2. Recommended regulatory guidance for applying D&P methods and self-testing features in digital systems in nuclear facilities, and procedures for reviewing D&P applications in nuclear facilities.

3.2 Security Aspects of Digital Systems

A source of potential failures in digital systems includes deliberate actions by a hostile individual or organization to maliciously manipulate the system during the development process or after the system has been installed. Three classes of security threats should be addressed:

1. Attempts to exploit vulnerabilities with the intent to disrupt system operations.
2. Unauthorized access to system networks.
3. Electromagnetic (EM) attacks to damage or disrupt digital equipment operations.

The common result of security threats can be safety system failure, or equipment or a human response at an inappropriate time due to an erroneous signal. The projects in this program investigate the appropriate elimination and/or mitigation of potential security hazards.

3.2.1 Security of Digital Platforms

Purpose

The purpose of this project is to identify potential cyber security vulnerabilities of NPP DI&C systems and to identify appropriate elimination and/or mitigation measures.

Project Basis

This project is an ongoing project conducted by Sandia National Laboratories and continues previously NRC-sponsored research [10].

Safety Significance and Benefit

A cyber attack on a NPP DI&C system, or malicious activity by an insider, may have safety significant consequences. This project intends to support development of regulatory positions to address cyber security. It will also provide the NRC staff with enhanced processes and tools for identifying and assessing security vulnerabilities.

Technical Basis

NRC staff report NUREG-0800, "Standard Review Plan," (SRP) Chapter 7, Revision 4, provides guidance to the staff for reviewing digital technology. The SRP, certain regulatory guidance documents (e.g., RG 1.152), and regulatory requirements (e.g., General Design Criteria in Appendix A to Part 50 of Title 10 of the Code of Federal Regulations) assert that safety-related systems be isolated to the degree that any credible failure in a nonsafety system shall not prevent any portion of a safety system from meeting its minimum performance requirements. In terms of data communication, the preferred approach to safety system isolation is to not allow communications in the direction from nonsafety systems to safety systems. The tenets of "one-way" communication contained in Chapter 7 of the SRP do not specifically take into account the deliberate and malicious attempts to disable a safety system that may occur as a result of a cyber attack. Several digital safety systems (e.g., Triconex Tricon, Areva-NP Teleperm XS, and Westinghouse Common Q) have been approved on a generic basis. This project will consider deliberate attempts to defeat isolation barriers of these systems.

Deliverables

1. This research project will expand staff knowledge and produce improved regulatory guidance in the area of cyber security and its potential impact on safety-related digital systems in nuclear facilities and applications.

3.2.2 Network Security

Purpose

The purpose of this project is to obtain network security information regarding potential cyber vulnerabilities in digital system architecture designs that could be used for safety applications. This effort will include the development of recommendations to evaluate wireless network security issues associated with deploying digital-based wireless communication systems in nuclear facilities.

Project Basis

This project is an ongoing project supported by NSIR. This research project supports regulatory priorities discussed with NSIR by identifying generic protection and mitigation measures appropriate to NPP environments. The project will support the review of DI&C system upgrades in currently operating nuclear plants and future plants [11]. This project also supports the Advanced Reactor Research Program.

Safety Significance and Benefit

This research project intends to support development of additional regulatory guidance on network security**.** The project will identify generic protection and mitigation measures appropriate to NPP environments. Deliverables from this project will provide the technical basis to evaluate architectures for compliance with NRC regulatory requirements. The data obtained from the laboratory and site assessments will also form the bases for regulatory guidance for licensing reviews and inspections.

Technical Basis - Wired Networks

Networking (both wireless and wired) is the interconnection of components (e.g., controllers, actuators, and sensors) with the objective of communicating among the associated subsystems. This networking of subsystems within a larger system framework 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 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 also will 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 preferred practices that prevent or mitigate insider cyber attack vectors, outsider cyber attack vectors, and developer cyber attack vectors.

Technical Basis - Wireless Networks

Because the installation of cabling is not required with wireless networks, reconfigurations of network assets may be performed more cost-efficiently, and associated cable penetrations through the containment may be eliminated.

Despite its potential there are safety issues with wireless networking that remain of concern because of its potential impact on safety (e.g., increased reliability concerns or misoperation of safety equipment resulting from cyber attacks). A significant security vulnerability concern with wireless networks is that wireless network transmissions are not confined to a conductive path that can be controlled.

Numerous security-related issues associated with implementing wireless systems have been identified and assessed, and regulatory issues associated with deployment have been identified (ML052200484) and need to be comprehensively addressed. Examples of the combinations of defensive measures to explore include password protection, encryption, administrative controls, network diversity and segmentation, firewalls, access point management (roaming), signal/noise/strength level monitoring, effects of wireless sensor usage, signal strength management, and even signal direction management. Future plans include validating tools and review procedures for assessing the security of wireless systems in nuclear facilities [12].

Deliverables

This research project will produce the following products:

1. A NUREG/CR detailing wireless and wired network security vulnerabilities and mitigation recommendations.

2. Regulatory guidance for identifying potential vulnerabilities and performing network security assessments.

3.2.3 Security Assessments of EM/RF Vulnerabilities

Purpose

The purpose of this project is to identify vulnerabilities of DI&C equipment used in NPPs due to attacks from electromagnetic (EM) and radio frequency (RF) weapons and to identify measures that may protect plant safety systems from such attacks.

Project Basis

This research is an ongoing project supported by NSIR. Although the Commission has not specifically identified EM- and RF-emitting technologies as credible threats to nuclear power facilities, some limited anticipatory research is considered to be prudent and warranted in this area.

Safety Significance and Benefit

This project intends to support a new regulatory position on EM and RF technologies. On September 6, 1983, SECY-83-367, "Staff Study of Electromagnetic Pulse Effects on Nuclear Power Plants and Discussion of Related Petitions for Rulemaking," was issued. In this paper, the staff recommended that the Commission direct the staff to take no further action on electromagnetic pulse (EMP). On November 15, 1983, the Commission issued a SRM approving the recommendation of no further action on EMP. Since that time, NPPs have replaced and are replacing numerous analog instrumentation and control systems with digital systems. Digital systems may have a higher vulnerability to EMP than analog systems. This project aims to quantify this potential problem.

Technical Basis

Sandia National Laboratories (SNL) evaluated this potential vulnerability in 1983. However, since the issuance of the Sandia report, the nature of EM weapons and the type of technologies used in nuclear facilities have changed. This project will evaluate the effects of these changes on the conclusions previously reached [10].

Deliverables

This research project will produce the following products:

1. A NUREG/CR which considers the effect of EMP/RF on DI&C safety systems and other equipment required to shutdown the plant and maintain adequate long-term core cooling. The NUREG/CR will include recommendations for potential mitigations where determined necessary.

2. Regulatory guidance relating to EM/RF vulnerabilities will be developed if appropriate and determined necessary.

3.3 Advanced Nuclear Power Concepts

The design and construction of new plants will make use of advances in I&C technology. NRC will utilize the results of the projects below to develop regulatory infrastructure for the review of new and advanced DI&C applications. Specifically, this research program is aimed at providing insights regarding the technology being developed for the Next Generation Nuclear Plant (NGNP).

3.3.1 Advanced Reactor Instrumentation

Purpose

The purpose of this research project is to provide technical information to the NRC staff in anticipation of the need to develop regulatory acceptance criteria for advanced reactor instrumentation.

Project Basis

This research project supports the anticipatory Advanced Reactor Research Program that states research is needed to:

- Analyze the requirements and potential safety issues involved with instrumentation to support licensing reviews of high-temperature gas-cooled reactors and liquid metal reactor design, construction, and operation.

- Analyze the requirements and potential issues involved with NGNP.

Safety Significance and Benefit

This project is included to facilitate regulatory assessment of state-of-the-art instrumentation technology and technology currently in the research and development (R&D) stage but with potential applications to the nuclear industry. This project intends to support the development of a new regulatory position.

Technical Basis

Advanced NPP designs will operate in conditions different from the current generation of NPPs. Consequently, it is expected that several new kinds of sensors will be developed and introduced to monitor these different conditions. For example, temperature, pressure, flow, and neutron detector instrumentation may be developed that will require changes in the methods for performing design and safety calculations (drift, calibration, response time, etc). This technology could offer advantages to licensees over instrumentation used in currently licensed

nuclear facilities (e.g., providing compensating measures for instrument error or control functionality at the sensor) but may create new challenges concerning regulatory assessments for acceptance.

Deliverables

This research project will produce the following products:

1. A NUREG/CR characterizing the capabilities and limitations of advanced instrumentation identified for use in advanced NPP safety systems.

2. Regulatory guidance for licensing advanced instrumentation identified for use in advanced NPP safety systems

3.3.2 Advanced Reactor Controls

Purpose

The purpose of this project is to enhance the NRC staff's understanding of how NPP control and safety systems will be designed for advanced reactor concepts including small light-water reactor (LWR) and non-LWR designs.

Project Basis

This research project supports the anticipatory Advanced Reactor Research Program that states RES will "Develop regulatory criteria used to review advanced control systems and algorithms that may be used in safety systems in advanced reactors."

Safety Significance and Benefit

This project is included to facilitate regulatory assessment of state-of-the-art controls technology and technology currently in the R&D stage but with potential applications to the nuclear industry. This project intends to support development of a new regulatory position.

Technical Basis

Advanced control approaches may be introduced in advanced nuclear reactor designs for operation with minimal supervision by plant operators for long periods of time. These highly automated NPPs could include nonlinear controllers, or even more advanced methods of control such as multivariable control. Advanced control design methods could support automated operations including startups, shutdowns, and changes of operating modes. How the control characteristics will affect the operational modes of nuclear facilities should be investigated.

Detailed control system 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. An opportunity may exist to collaborate in some of these research programs, particularly in the areas of advanced control algorithms and control of multiple NPP modules (ML061150050).

Deliverables

This research project will produce the following products:

- A NUREG/CR evaluating the capabilities and limitations of advanced controls proposed for use in advanced NPP safety systems.

- Regulatory guidance for licensing advanced controls proposed for advanced NPP safety systems.

3.4 Knowledge Management

In addition to research activities that are focused on specific issues and topics, NRC will actively communicate with the broader DI&C community to stay informed of technological developments that have potential use by the nuclear industry. This participation helps the NRC staff to develop and maintain capabilities to support identification and resolution of issues that develop as the nuclear industry employs state-of-the-art digital systems. As a result, NRC will be better prepared to make regulatory decisions when technological changes are introduced.

The projects listed below support:

- Maintaining expertise in safety assessment aspects of I&C engineering.

- Maintaining awareness of technological changes that may affect safety and regulatory guidance.

- Maintaining liaison with other Federal agencies, professional societies, international agencies, and other organizations [13].

- Coordinating NRC standards activities as these relate to Federal law and interaction writing organizations, including activities relating to the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) and OMB Circular A119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities" [13].

- Coordinating recommendations concerning risk-informed approaches to improve guidance for safety evaluation of new DI&C systems and changes to DI&C systems during the operational lifecycle.

3.4.1 Survey of Emerging Technologies

Purpose

The purpose of this project is the identification of key research areas on emerging (i.e., R&D stage), early adoption, and established technologies within the DI&C field that may become important in the future [14].

Project Basis

This research project is supported by RES, NRR, NRO, and NMSS. The project was established in response to a User Need Request from NRR to RES [15], requesting the following:

> Review emerging practices, design development and assessment methods and tools, and issues associated with evolving technology and new initiatives by the industry that could be included in license amendment applications or impact digital systems of nuclear plants. Identify the issues and provide augmented regulatory guidance and acceptance criteria. The RES research plan should be flexible. As issues are identified, they should be routinely provided to the supported offices. Once the item is considered applicable by a supported office, RES activities will proceed. The output will be letter reports on the issues, with review guidance to augment the staff guidance, and additional acceptance criteria.

Safety Significance and Benefit

This project is continued from the Digital System Research Plan FY 2005-FY 2009. Three NUREG/CRs have resulted from this ongoing effort [16, 17, 18]. These publications are helpful in reducing the time it takes to identify emerging technology that may require regulatory review in the digital area. This in effect can reduce the time it takes for emerging issues to reach a solution thus improving regulatory efficiency and effectiveness. This project intends to improve efficiency, effectiveness, and timeliness of regulatory reviews.

Technical Basis

It has been beneficial for NRC to develop a survey of the state-of-the-art technology areas within the I&C field. This is an ongoing task with periodic reports on specific technologies. The survey will identify present emerging capabilities that have potential applicability for safety-related systems in NPPs (e.g., wireless technology). Beyond a list of technologies, the survey also will provide high-level discussions of specific emerging capabilities and products in each technology area. This includes capabilities likely to migrate into safety-related applications at NPPs either through upgrades at existing plants or as design elements of advanced reactor concepts. NRC will use this effort as a starting point for understanding and then developing the technical basis for guidance for addressing safety-assessment issues associated with implementing new technologies with a focus at the R&D stage. A wide group of industry inputs will be sought, including plant owners groups, EPRI, and others in the nuclear industry. In addition, input will be sought from other industries such as the process industry and from research institutes such as universities and other Federal agencies including DOE and NASA.

Deliverables

This research project will produce the following products:

1. Periodic NUREG/CR reports and associated briefings to the NRC licensing offices on emerging capabilities that have potential applicability for safety systems in NPPs.

2. Workshops and resulting reports with subject matter experts from other application domains.

3.4.2 Collaborative and Cooperative Research

Purpose

The purpose of this project is to keep up with the rapidly changing DI&C technologies and to better understand the potential for systematic failures in DI&C systems especially attributable to software. To do this, the NRC staff will establish liaisons, participate in reviews, explore collaborative activities, leverage research activities and products from other agencies, and learn best practices.

Project Basis

The NRC staff should maintain liaison with other Federal agencies, professional societies, international agencies, and other organizations will provide valuable insights on DI&C issues.

Safety Significance and Benefit

Collaborative and cooperative research ensures that the agency maintains and improves its organizational capacity to do its work through the more effective use of resources by ensuring that NRC keeps pace with digital technology advances and standard practices. Participation in these collaborative and cooperative national and international research programs will provide benefits for NRC, the nuclear power industry (the Industry), and the public. This project intends to improve efficiency, effectiveness, and timeliness of regulatory reviews.

Technical Basis

As outlined in SECY-01-0155, 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. Therefore, the NRC staff will find value in tapping relevant expertise and experience outside NRC, outside the nuclear industry, and outside the United States. Examples of various collaborative and coordination forums and activities across these centers of expertise include:

- Requirements and Technical Concepts for Aviation working group for DO-178-C and D.
- Computer-based Systems Important to Safety (COMPSIS) Project.
- Electric Power Research Institute (EPRI).
- International Atomic Energy Agency (IAEA).
- Software Engineering Institute.
  - CMMI-SAFE PLUS team.
- Halden Reactor Project (HRP).
- National Science Foundation (relevant workshops, review panels).
- National Academy of Sciences (workshops, review panels on relevant studies).
- Department of Homeland Security, Office of Science and Technology (Research and Development)
- NASA mission-critical software development teams (e.g., Jet Propulsion Laboratory).
- Private industry outside the nuclear power generation industry, for example:
  - Defense & Aerospace
  - Automotive
  - Medical devices

In a Cooperative Agreement between NRC and EPRI for DI&C and Human Factors (HF) [7], the parties agreed to encourage cooperation in nuclear safety research, which provides benefits for NRC, the Industry, and the public. The objective of the ongoing collaboration R&D programs is the improvement of DI&C and HF methods, tools, data, and technical information useful to NRC and the industry. The specific objective of this cooperative program is to ensure the timely exchange of information (e.g., objectives, milestones, technical data, and results) on planned and ongoing research activities.
This cooperative program has the following specific objectives:

- Ensure the timely exchange of information (e.g., objectives, milestones) on planned and ongoing research activities.

- Ensure the sharing of technical data needed by the RES and EPRI R&D programs.

- Develop I&C analysis methods, tools, and/or data to support licensing of DI&C systems.

- Ensure the timely sharing of R&D results and tools.

- Assess the capabilities of current and advanced I&C technology, methods, and tools.

The Organization for Economic Cooperation and Development (OECD) HRP is a cooperatively funded international R&D project that operates under the auspices of the OECD's Nuclear Energy Agency with the sponsorship of 18 countries including the United States. Over the past 3 years, HRP has expanded its research efforts in the area of digital system safety. HRP's next 3-year research program focuses on dependability issues related to the engineering and architecture of digital safety systems. The staff has interacted with HRP on the development of the next 3-year program, particularly with regard to analysis of failure propagation. HRP also has established a software engineering laboratory—the Halden Reactor Project Software Engineering Laboratory —that provides the systems and resources needed to support research, development, assessment, consultancy, and training related to safety-oriented software engineering.

The staff believes the research products generated from the HRP research over the next few years will aid NRC in providing additional technical bases for decisions regarding current and new digital system designs and technologies for safety-related applications. The agency's continued cooperation with HRP will allow access to technical information on these systems as well as access to operating experience (OpE) from European reactor operators and vendors, thereby leveraging the agency's DI&C resources as it establishes a technical basis for reviewing advanced systems.

Deliverables

The exact nature of the deliverables depends on the specific activities and results from these cooperation and collaborations. The final deliverables will be targeted to specific objectives that have regulatory applicability. These deliverables will include:

1. Joint technical reports (e.g., failure modes identification and characterization).

2. Workshops and resulting reports.

3.4.3 Standards Development, Regulatory Guidance, and Regulatory Review Guidance

Purpose

To understand and evaluate national and international standards to improve the efficiency of the regulatory process and to gain knowledge from other application sectors and standards outside the nuclear industry.

Project Basis

These activities primarily are in support of NRO and NRR, as follows.

NRO, leading the Multinational Design Evaluation Program, has requested a review of the state of the art and comparative evaluation of relevant standardization and regulatory efforts outside the NRC, for example:

- International Electrotechnical Commission working groups for relevant standards: 61508, 61513, 60880, 60671, 61069, 61226, 62138, 9126, IEC 61478.

- IAEA working group for guide NS-G-1.3.

NRR has requested to continue to participate with the Institute of Electrical and Electronics Engineers (IEEE) in the review and development of standards. Some IEEE standards include:

- IEEE Std. 497-2002 is endorsed by RG 1.97, Revision 4
- IEEE Std. 603-991 is required by 10 CFR 50.55a(h).
- IEEE Std. 7-4.3.2-2003 is endorsed by RG 1.152, Revision 2.

Safety Significance and Benefit

This project intends to improve quality, clarity, and consistency of regulatory guidance.

Technical Basis

Other nations have deployed safety DI&C systems in NPPs. Foreign utilities and their DI&C technology suppliers are gaining approvals under their national regulations, often following international standards. Given the increasing globalization of nuclear power technology, it is important for the staff to understand the international standards applied in the DI&C area.

Deliverables

1. A NUREG/CR providing an evaluation of the similarities and differences of relevant standards and guidelines, as applicable to regulatory activities concerning safety systems in NPPs (e.g. certification, risk assessment, supporting aids and tools, and lifecycle processes for DI&C systems).

3.4.4 Organization of Regulatory Guidance Knowledge

Purpose

To improve the infrastructure to support regulatory decision-making (supporting Objective #4 of Section 2.1.) through knowledge management aids and tools.

Project Basis

NRR requested this project. The work products of this research will improve the effectiveness and efficiency of safety reviews, reduce the time required to conduct reviews, and reduce the time required to familiarize new reviewers with the regulatory framework.

Safety Significance and Benefit

This project intends to improve efficiency, effectiveness, and timeliness of regulatory reviews.

Technical Basis

There are a large number of NRC documents and industry standards with which NRC digital I&C reviewers must be knowledgeable to carry out technical reviews. The challenge is significant, particularly for newer NRC staff. This project will lessen the challenge.

Deliverables

1. Knowledge management aids and tools for search and navigation across NRC's framework of regulations and guidelines relevant to DI&C systems, for example:

    1.1. Subject-based summaries, including timelines, annotated bibliography, and list of precedents.

    1.2. Relationship mappings (bidirectional) across regulations, guidance, SRP acceptance criteria, required documents (work products), precedents, information notices, etc,

3.4.5 Operating Experience Analysis

Purpose

The purpose of this project is to analyze operating experience (OpE) of digital systems to identify credible failure modes and to use the knowledge derived from this analysis to improve the efficiency and effectiveness of regulatory reviews. This includes development of means for synthesizing the obtained knowledge and data (e.g., failure parameter database).

Project Basis

This research project in part responds to the ACRS letter to the Commission, dated May 18, 2007, that recommended the staff develop an inventory and classification structure (e.g., by function or other characteristics) for the various types of digital and software systems being

used and likely to be used in NPPs. In addition, the ACRS recommended that the staff should evaluate the OpE with digital systems in the nuclear industry and other industries to obtain insights regarding potential failure modes.

The project also supports regulatory priorities transmitted through SRM M070607 dated June 22, 2007 (ML07173024), directing the staff to:

- Evaluate the operating experience with digital systems in the nuclear and other industries (both safety and nonsafety) to obtain insights regarding potential failure modes

Safety Significance and Benefit

Data from OpE of digital systems obtained and analyzed to date has been found to be inadequate, lacking statistically significant quantity, detail, and pedigree, validity, or quality (e.g., lack of context conditions) to identify and analyze failure modes and causal factors adequately. This lack of adequate data is partly exacerbated by rapid technological changes as well as different application domains.

This project intends to improve efficiency, effectiveness, and timeliness of regulatory reviews.

Technical Basis

DI&C OpE in safety systems is limited and the quality and quantity of data available is inadequate. Often, the current root cause analysis is not deep enough to identify the true underlying cause and determine if the associated regulatory guidance should be improved. OpE alone will not identify all credible failure modes. Also, OpE data may not be statistically significant; therefore, analytical methods might have to be explored for establishing failure parameters (e.g., failure rates and distributions).

Some examples of the sparse, sketchy DI&C failure modes identified in different industries include:

- The failure modes typically reported in the PRAs for Gen III NPPs: “spurious operation” and “fails to function.” Consequently, the data provided in the PRAs for NPPs may only provide limited information on the failure modes or failure mechanisms of DI&C components and software.

- Failure modes reported in the petrochemical industry: short, erratic/high/low/no output, spurious operation, faulty signal, and control failure.

Sometimes applicants for a DC cite operational experience in non-safety applications in support of their safety-related analysis. However, the NRC staff has found the evidence to be inadequate.

Key questions to be answered include:

- What constitutes credible DI&C failure modes?

- What constitutes adequate OpE information that would support a finding that a DI&C system or component is acceptable?

- When the OpE information is not adequate, what information can be extracted from it that is meaningful and useful to the reviewers in some limited way?

In the course of answering these questions, RES intends to perform reviews of various sources of data including nonnuclear industry digital system failure data, and the COMPSIS project data, and periodically review nuclear digital OpE as these systems become more prevalent in the nuclear industry.

OpE information generated from this work will also support Projects 3.1.5 "Analytical Assessment of DI&C Systems and 3.1.6 "Digital System PRA."

Deliverables

1. Provide OpE based information to improve the review process.

2. Recommendations for an enhanced DI&C failure reporting framework for improved information content in reportable DI&C related incidents, and for supporting information required to substantiate "proven in use" claims.

3. A Digital component failure parameter database (i.e., failure data and failure modes of digital components of NPPs).

    a. Failure parameter database of hardware failures of digital system components, including digital design features such as watchdog timers and communication devices.

    b. Common cause failure parameters for digital components, if feasible.

    c. Failure mode distributions that break down component failure rates into their constituent failure modes.

    d. Failure parameter database of software failures of systems, if feasible.

    e. Failure parameter database for process-related digital system failures (for example, errors in configuration management of setpoints, parameters and software versions, or errors and omissions in requirements specifications).

3.5 Additional Carry-over Projects from Digital System Research Plan FY 2005 – FY 2009

The projects in this section are a continuation of projects identified in the Digital System Research Plan FY2005 – FY2009 which are still desired by the licensing offices. These projects were not started or completed during the FY2005 – FY 2009 timeframe, generally due to changes in priorities by the licensing offices.

3.5.1 Electromagnetic Compatibility

Purpose

The purpose of this research is to review the technical basis for operating limits in RG 1.180, Rev. 1, regarding conductive susceptibility tests, and update the guidance, if justified.

Project Basis

This research project supports regulatory priorities discussed with NRR. This research is an ongoing project with portions performed for NRC by Oak Ridge National Laboratory (ORNL) (NRC Job Code N6080, "Interactions with Industry on Standards").

Safety Significance and Benefit

This project intends to improve quality, clarity, and consistency of regulatory guidance.

Technical Basis

Electromagnetic and radiofrequency interference (EMI/RFI) are environmental stressors in which electric fields, magnetic fields, or radiofrequency (RF) waves interfere with the operation of an electrical or electronic device. The electric/magnetic fields and RF 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).

The NRC has developed regulatory guidance and acceptance criteria 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.

However, In July 2003, EPRI submitted a draft report describing its assessment of MIL-STD-461E (as endorsed by RG 1.180, rev. 1) 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). In addition, 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, because the original rationale for the high-frequency test limits was flawed, the corresponding operating limits described in the Safety Evaluation Report approving EPRI TR-102323, Rev. 0, also were 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.

Deliverables

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

3.5.2 Electrical Power Distribution System Interactions with Nuclear Facilities

Purpose

The purpose of this research project is to review existing standards and regulatory guidance to determine their applicability for addressing degraded power grid effects on digital components and to determine the effect of power fluctuations on DI&C systems.

Project Basis

This research project supports regulatory priorities discussed with NRR.

Safety Significance and Benefit

This project intends to improve quality, clarity, and consistency of regulatory guidance.

Technical Basis

In August 2003, the electrical power blackout in the northeastern United States caused nine NPPs to experience loss of offsite power (LOOP) abnormal operating occurrences. 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). This document 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 NPP 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 EDG. 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.

Data from operational experience of DI&C systems and their environments are limited. Therefore, a need exists to define boundaries within which a reasonable assessment of safety could be made and issues of concern could be identified.

Two examples of issues at the boundary of a DI&C system are identified below:

- The increasing use of power electronics in actuation systems (such as variable speed controllers and software-controlled power supplies) introduces risks that are not well understood. In addition to the hazards introduced internal to the power electronics, this technological change also increases the potential of detrimental EMI effects on logic-electronics in the DI&C systems.

- Dependencies of DI&C systems on power supplies are also not well understood (e.g., the control of power supplies across a distributed network of logic processing units, sensors, and actuators).

Deliverables

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

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

3. Regulatory guidance describing the models, tools, and review procedures for addressing the effects of power fluctuations on digital systems in NPPs.

4. Regulatory guidance addressing the effects of power fluctuations on digital equipment.

3.5.3 Operating Systems

Purpose

The purpose of this research project is to develop criteria that can be used to evaluate computer/microprocessor operating system characteristics and performance.

Project Basis

This research project supports regulatory priorities discussed with NRR. Specifically, the project was established in response to a request from NRR. The memo requested that RES:

Develop a set of guidelines (e.g., NUREG/CR that can be used as a branch technical position, attached as part of the SRP) which can be used to evaluate operating systems and internal diagnostics being used, or likely to be used in nuclear plant applications. Determine needed and unneeded features and evaluate their impact on real-time safety system applications. Develop review guidance and acceptance criteria, including criteria that can be used to evaluate acceptance testing, to augment the guidance in SRP Chapter 7 and issue the results in a NUREG/CR report [13].

Safety Significance and Benefit

Operating systems manage internal diagnostics, 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 and reliable manner. Because operating systems control all aspects of a computer's operation, operating system quality is critical to computer system quality. Therefore, NRC requires a technically sound method of confirming that the quality of an operating system is appropriate for the safety functions it supports.

Technical Basis

In the past, operating systems were small, simple, and custom-programmed for specific applications. Currently, any potential regulatory safety assessments of operating systems used in nuclear facilities and medical and industrial byproduct applications are becoming more difficult for three significant reasons. First, the increased computing capability of digital systems has led to the use of more complex operating systems. Second, many digital systems contain widely used 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.

In addition, 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. [4]

The research will involve (1) examining past performance of operating systems and identifying 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 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 [4]. Included in this project are efforts to determine 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.

Deliverables

This research project will produce the following products:

1. Regulatory guidance describing design aspects of digital operating systems (i.e., appropriate operating system selection criteria, best design practices, architectures, failure modes, and fault models).

2. Tools, review procedures, and acceptance criteria to support staff reviews of operating systems.

3. Technical guidance and acceptance criteria for evaluating self-testing features in digital systems.

GLOSSARY

The following are definitions of key terms with scope of application limited to this document to pre-existing definitions. These definitions are intended to promote usage of terms in meanings consistent with definitions in international standards. Where standards provide multiple meanings that are different or conflicting or inconsistent, the research plan uses the term only for the selected meaning, as given below.

Dependability –
a) A broad concept that incorporates various characteristics of digital equipment, including reliability, safety, availability, and maintainability. (NRC RIS 2002-22)

b) The collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance. (IEC 50-191)

Error – A discrepancy between a calculated, observed, or measured quantity and the true or theoretically correct value or condition. (IEEE)

Failure – The termination of the ability of an item to perform a required function. (IEEE)
Note: "Failure" is an event, as distinguished from "fault" which is a state. (IEC 50-191)

Fault – The state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.
Note 1: Item (or entity): Any part, component, device, subsystem, functional unit, equipment, or system that can be individually considered. Am item may consist of hardware, software, or both, and may also, in particular cases, include people.
Note 2: A fault is often the result of the failure of the item itself, but may exist without prior failure (as in the case of software).

Latent fault – an existing fault that has not yet been recognized (IEC 60050-191).

Mistake –
a) A human action that produces an unintended result (electronic computation, IEEE).
b) A human action that produces an incorrect result (software, IEEE).

Probabilistic risk analysis – A systematic method for addressing risk as it relates to the performance of a complex system to understand likely outcomes, sensitivities, areas of importance, system interactions, and areas of uncertainty.

Random hardware failure – A failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware. (IEC 61508-4, section 3.6.5)

Reliability – The ability of an item to perform a required function under stated conditions for a specified period of time. (IEEE)

Risk – Combination of the probability of occurrence of loss and the severity of that loss

[ISO/IEC Guide 51:1990]

Risk analysis – A procedure to develop probability estimates of occurrence of each specific hazard. (IEEE)

Risk assessment – The overall process of identifying all the hazards in a system (internal and external), estimating the risk from each hazard and the overall risk resulting from their combination. See also: Risk estimation.

Risk estimation – The process of assigning values to the severity of loss and the probability or likelihood of its occurrence. See also: Risk assessment.

Risk-Informed – An approach to decision-making in which risk insights are considered along with other factors such as engineering judgment, safety limits, and redundant and/or diverse safety systems. Such an approach is used to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to public health and safety. (NUREG 1614)

Safety – Adequate protection of public health and safety and the environment. (NUREG 1614 p. 4)

Note 1: Adequacy is determined with respect to the safety goals for a NPP defined in the Commission policy statement [19] in terms of a broadly defined acceptable level of radiological risk. This policy statement enables a mapping of the NRC definition of safety to that in ISO/IEC Guide 51:1999 and IEC 61508-4, viz. “freedom from unacceptable level of risk.”

Note 2 relevant to DI&C PRA: The NRC policy statement defines “acceptable level of risk” in terms of individual risk and societal risk (life and health) goals and quantitative targets. Guidelines relevant to NPP PRA map the policy level health goal into performance objectives such as “core damage frequency” from which the performance objective (“risk budget”; “risk responsibility”) can be derived and allocated for a reactor safety DI&C system.

Safety-related – In the regulatory arena, this term applies to systems, structures, components, procedures, and controls of a facility or process that are relied upon to remain functional during and following design-basis events. Their functionality ensures that the key regulatory criteria, such as levels of radioactivity released, are met. Examples of safety-related functions include shutting down a nuclear reactor and maintaining it in a safe shutdown condition.

Systematic failure – A failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design of the manufacturing process, operational procedures, documentation or other relevant factors. (Adapted from IEC 61508-4, Section 3.6.6)

Systemic cause – A cause related in a deterministic way to an effect or result.

Note: Related term & definition: Failure cause: The circumstances during engineering, manufacturing, installation, configuration, usage, or maintenance leading to a failure deterministically. (Adapted from IEC 60050-191)

REFERENCES

1. U.S. Nuclear Regulatory Commission, “Addendum to the Memorandum of Understanding between U.S. Nuclear Regulatory Commission and Electric Power Research Institute, INC. on Cooperative Nuclear Safety Research for Digital Instrumentation and Controls and Human Factors”, Addendum to the Memorandum of Understanding (ADAMS Accession Number ML090430387), 2009.

2. U.S. Nuclear Regulatory Commission, NRC Research Plan: Digital Instrumentation and Control (ML012080254).

3. U.S. Nuclear Regulatory Commission, “NRC Research Plan For Digital Instrumentation and Control” SECY Paper (ML011990569).

4. U.S. Nuclear Regulatory Commission, NRC Digital System Research Plan FY 2005 – FY 2009 (ML061150050).

5. U.S. Nuclear Regulatory Commission, “NRC Strategic Plan FY 2008-2013)” NUREG-1614, volume 4. URL: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1614/v4/index.html, [viewed 7/25/08]

6. U.S. Nuclear Regulatory Commission, “Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program”, ACRS, 2008.

7. U.S. Nuclear Regulatory Commission, “Addendum to the Memorandum of Understanding between U.S. Nuclear Regulatory Commission and Electric Power Research Institute, INC. on Cooperative Nuclear Safety Research for Digital Instrumentation and Controls and Human Factors”, Addendum to the Memorandum of Understanding (ML090430387), 2009.

8. U.S. Nuclear Regulatory Commission, “Staff Requirements Memorandum M080605B”, dated July 2008 (ML081780761).

9. U.S. Nuclear Regulatory Commission, “EDO letter to the ACRS dated May 28, 2008”, (ML081290195).

10. U.S. Nuclear Regulatory Commission, “Statement of Work for Job Code N6115”, (ML071790338).

11. U.S. Nuclear Regulatory Commission, “SPACE Engineering Work Station Statement of Work N6650", no ADAMS number yet.

12. U.S. Nuclear Regulatory Commission, “Digital System Dependability Performance”, Statement of Work (ML063560209).

13. Functional description of the Office of Nuclear Regulatory Research, Division of Engineering. URL: http://www.nrc.gov/about-nrc/organization/resfuncdesc.html#de, [viewed 7/25/08]

14. U.S. Nuclear Regulatory Commission, “Emerging Technologies Statement of Work”, page 1

(ML080770210).

15. User Need NRR-2002-017, Memo from S. Collins, NRR to A. Thadani, RES Re: Update of NRR Requests for Assistance (ML013530458)

16. NUREG/CR-6812, “Emerging Technologies in Instrumentation and Controls” (ML031920412)

17. NUREG/CR-6888, " Emerging Technologies in Instrumentation and Controls: An Update" (ML060870216)

18. NUREG/CR-6992, " Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update" (ML092950511)

19. U.S. Nuclear Regulatory Commission, “Safety goals for the operations of nuclear power plants; policy statement; republication” 51 FR 30028, PS-PR-{43-48}, effective 8/4/86.

Appendix I

Table 1: List of dependencies between projects and deliverables

Research Program	Project	Deliverables	Projects Supported	Dependency
3.1. Safety Aspects of Digital Systems	3.1.1. Communications Among Plant-wide Data Systems	Deliverable 1	N/A	N/A
		Deliverable 2		
		Deliverable 3		
	3.1.2. Safety Assessment of Tool Automated Processes	Deliverable 1	Project 3.4.1, and Project 3.4.3	Support survey of merging technologies and reviews of appropriate standards
		Deliverable 2	N/A	N/A
	3.1.3. Fault Injection Methodologies	Deliverable 1	N/A	N/A
		Deliverable 2		
		Deliverable 3		
	3.1.4. Integrated Plant & DI&C System Modeling	Deliverable 1	N/A	N/A
	3.1.5. Analytical Assessment of DI&C Systems	Deliverable 1	Project 3.4.2	Collaboration and sharing the results of classifying the various types of DI&C systems and components that are being used and are likely to be used in NPPs.
		Deliverable 2	1. Project 3.1.6, 2. Project 3.4.2	1. Results from this deliverable will provide Project 3.1.6 data to support development of PRA parameters. 2. Collaboration and sharing the results of a characterization of DI&C system domains for Project 3.4.2.
		Deliverable 3	Project 3.1.6, and Project 3.4.2	1. Results from this deliverable will provide Project 3.1.6 data to support development of PRA parameters. 2. Deliverable 4 will also support 3.4.2 by identifying credible failure modes typical of software-intensive DI&C systems.
		Deliverable 4	Project 3.1.6	Results from this deliverable will provide Project 3.1.6 data to support development of PRA parameters.

	3.1.6. Digital System PRA	Deliverable 1 Deliverable 2 Deliverable 3	N/A	N/A
	3.1.7. Diagnosis and Prognostics	Deliverable 1	Project 3.3.1	Project will provide advanced diagnostic and prognostic methods to support licensing of advanced reactors
		Deliverable 2	Project 3.3.1	Project will provide advanced diagnostic and prognostic methods to support licensing of advanced reactors
3.2. Security Aspects of Digital Systems	3.2.1. Security of Digital Platforms	Deliverable 1	N/A	N/A
	3.2.2. Network Security	Deliverable 1 Deliverable 2	N/A	N/A
	3.2.3. Security Assessments of EM Vulnerabilities	Deliverable 1 Deliverable 2	N/A	N/A
3.3. Advanced Nuclear Power Concepts	3.3.1. Advanced Reactor Instrumentation	Deliverable 1	Project 3.1.5, and Project 3.4.1,	Collaboration and sharing the results of characterizing the capabilities and limitations of advanced instrumentation identified for use in advanced NPP safety systems with Project 3.1.5 and Project 3.4.1.
		Deliverable 2	N/A	N/A
	3.3.2. Advanced Reactor Controls	Deliverable 1	Project 3.4.1	Collaboration and sharing the results of characterizing the capabilities and limitations of advanced controls identified for use in advanced NPP safety systems with Project 3.4.1
		Deliverable 2	N/A	N/A
3.4. Knowledge Management	3.4.1. Survey of Emerging Technologies	Deliverable 1	Project 3.1.5, Project 3.3.1, Project 3.3.2, and Project 3.4.2	1. Project will support research planned for Deliverable 5 in Project 3.1.5., focusing on the domains of DI&C systems, environments, and engineering processes characterized in Project 3.1.5.(Del 2). 2. Collaboration and sharing the results of emerging capabilities that have potential applicability for safety systems in NPPs for Project 3.3.1 and 3.3.2. 3. Collaboration and sharing the results for understanding and then developing the technical basis for guidance for addressing safety-

				assessment issues associated with implementing new technologies with a focus at the R&D stage.
		Deliverable 2	Project 3.1.5, Project 3.3.1, Project 3.4.2, and Project 3.4.2	1. Project will support research planned for Deliverable 5 in Project 3.1.5., focusing on the domains of DI&C systems, environments, and engineering processes characterized in Project 3.1.5.(Del 2). 2. Collaboration and sharing the results of emerging capabilities that have potential applicability for safety systems in NPPs for Project 3.3.1 and 3.3.2. 3. Collaboration and sharing the results for understanding and then developing the technical basis for guidance for addressing safety-assessment issues associated with implementing new technologies with a focus at the R&D stage.
	3.4.2. Collaborative and Cooperative Research	Deliverable 1	Project 3.1.5, Project 3.1.6, Project 3.4.1, Project 3.4.3, and Project 3.4.5	1. Results from this deliverable will feed Project 3.1.5. (Del 2.3 and 5) and 3.1.6. 2. Results from this deliverables will support Project 3.4.3 by providing knowledge from other application sectors and standards outside the nuclear industry, and evaluate and recommend its usage or leveraging. 3. Results from this deliverable particularly in regards to COMPSIS, will feed Project 3.4.5
		Deliverable 2	Project 3.1.5, Project 3.4.3, and Project 3.4.5	1. Results from this deliverable will feed Project 3.1.5. (Del 2.3 and 5). 2. Collaboration and sharing the results s will support Project 3.4.3 by providing knowledge from other application sectors and standards outside the nuclear industry, and evaluate and recommend its usage or leveraging. 3. Results from this deliverable particularly in regards to COMPSIS, will feed Project 3.4.5.

	3.4.3. Standards Development, Regulatory Guidance, and Regulatory Review Guidance	Deliverable 1	Project 3.1.5, Project 3.1.2, Project 3.4.1, and Project 3.4.2	1. Project supports research planned for Deliverable 5 in Project 3.1.5., focusing on the domains of DI&C systems, environments, and engineering processes characterized in Deliverable 2, Project 3.1.5. 2. Project supports research planned for Deliverable 1.1 in Section 3.1.2. 3. Project supports research planned in Section 3.4.1. 4. Collaboration and sharing the results s will support Project 3.4.2 by providing knowledge from other application sectors and standards outside the nuclear industry, and evaluate and recommend its usage or leveraging.
	3.4.4 Organization of Regulatory Guidance Knowledge	Deliverable 1	N/A	N/A
		Deliverable 2		
	3.4.5. Operating Experience Analysis	Deliverable 1	Project 3.1.5, and Project 3.4.2	Support Project 3.1.5 and 3.4.2 by providing an OpE-based analysis of failure modes in DI&C systems
		Deliverable 2	Project 3.1.2,	Provide a regulatory guidance that provides acceptance criteria, and adequacy of proof from industry operating experience
		Deliverable 3	Project 3.1.6	Results from this deliverable will provide Project 3.1.6 data to support development of PRA parameters
3.5 Additional Carry-Over Projects from Digital System Research Plan FY 2005 – FY 2009	3.5.1. Electromagnetic Compatibility	Deliverable 1	N/A	N/A
		Deliverable 2	N/A	N/A

	3.5.2. Electrical Power Distribution System Interactions with Nuclear Facilities	Deliverable 2	N/A	N/A
		Deliverable 3	N/A	N/A
		Deliverable 4	N/A	N/A
	3.5.3. Operating Systems	Deliverable 1	N/A	N/A
		Deliverable 2	N/A	N/A
		Deliverable 3	N/A	N/A

Appendix II

Digital System Research Plan FY2010 – FY2014 Project Priorities

The Research Plan projects are prioritized HIGH, MEDIUM, LOW with respect to the completion 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, as shown in Figure 5.

BASES FOR RESEARCH	COMPLETION DATE: <3 Years	3-5 Years	> 5 Years
Support development of a new regulatory position	HIGH	HIGH	HIGH
Improving quality, clarity, and consistency of regulatory guidance	HIGH	HIGH or MEDIUM	MEDIUM
Improving efficiency, effectiveness, and timeliness of regulatory reviews	MEDIUM	MEDIUM or LOW	LOW

Figure 5: Prioritization of Digital System Research Plan FY2010 – FY2014 Projects

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 project with a projected completion date exceeding 3 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 categorized 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 DI&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 categorized 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.

For more details on the associated priority of each project please refer to the following table:

Table 2: Digital System Research Plan FY2010 – FY2014 Projects Baseline Priorities

Research Program	Project	Originally Requested by	Priority
3.1. Safety Aspects of Digital Systems	3.1.1. Communications Among Plant-wide Data Systems	NRO, RES	MEDIUM
	3.1.2. Safety Assessment of Tool Automated Processes	NRR, NRO	MEDIUM
	3.1.3. Fault Injection Methodologies	NRR, NRO	HIGH
	3.1.4. Integrated Plant & DI&C System Modeling	NRR, RES	MEDIUM
	3.1.5. Analytical Assessment of DI&C Systems	Commission Directed	HIGH
	3.1.6. Digital System PRA	NRR, NRO	HIGH
	3.1.7. Diagnosis and Prognostics	NRR, NRO	HIGH
3.2. Security Aspects of Digital Systems	3.2.1. Security of Digital Platforms	NSIR	HIGH
	3.2.2. Network Security	NSIR, NRR	HIGH
	3.2.3. Security Assessments of EM Vulnerabilities	NSIR	HIGH
3.3. Advanced Nuclear Power Concepts	3.3.1. Advanced Reactor Instrumentation	NRR, NRO	MEDIUM
	3.3.2. Advanced Reactor Controls	NRR, RES	MEDIUM
3.4. Knowledge Management	3.4.1. Survey of Emerging Technologies	NRR, NRO, RES	LOW
	3.4.2. Collaborative and Cooperative Research	RES	MEDIUM
	3.4.3. Standards Development, Regulatory Guidance, and Regulatory Review Guidance	NRR, NRO	HIGH
	3.4.4 Organization of regulatory guidance knowledge	NRR, NRO	LOW
	3.4.5. Operating Experience Analysis	NRR	HIGH

3.5 Additional Carry-over Projects from Digital System Research Plan FY 2005 – FY 2009	3.5.1. Electromagnetic Compatibility	NRR, NRO	LOW
	3.5.2. Electrical Power Distribution System Interactions with Nuclear Facilities	NRR	LOW
	3.5.3. Operating Systems	NRR	LOW