POICY ISSUE
(Information)

August 15, 2001 SECY-01-0155

FOR: The Commissioners

FROM: William D. Travers
Executive Director for Operations

SUBJECT: NRC RESEARCH PLAN FOR DIGITAL INSTRUMENTATION AND CONTROL

PURPOSE:

The purpose of this paper is to inform the Commission of the Research Plan (Plan) for Digital Instrumentation and Control (I&C) for fiscal years 2001-2004.

BACKGROUND:

Over the past decade, obsolescence of many of the analog I&C system components and equipment and advances in technology have led to an increasing use of digital I&C systems in U.S. nuclear power plants. Advanced reactor designs make significant use of digital I&C systems. These systems can provide many benefits in operational performance and safety to the nuclear industry. However, the introduction of digital technology into nuclear power plants also presents challenges. These include rapid technology changes, significant complexity, operational issues, and failure modes that are different from analog technology. In recognition of these issues, the staff, under the direction of the Commission, updated Chapter 7, Instrumentation and Controls, of NUREG-0800, “Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants,” (SRP) and issued Revision 4 of SRP Chapter 7 in June 1997.

The SRP provides guidance to the staff in performing safety reviews of applications to construct and operate nuclear facilities. It establishes criteria and guidelines for both operating plants (modifications) and proposed future advanced reactor designs, which the staff uses in evaluating whether an applicant/licensee of a nuclear power plant meets the Commission's regulations. The guidance in Chapter 7 is currently used for the review of advanced reactors, plant-specific digital retrofits and topical reports on digital equipment, and is presently considered adequate. It is also used as the basic reference review document by the regulatory agencies of several foreign countries in the review of advanced reactor I&C system designs.

CONTACT: S. Arndt, RES
(301) 415-6502

However, in view of the rapidly evolving digital technology and related standards and the need for quantitative assessment of digital I&C system reliability and risk, the staff has developed this Plan. The Plan provides a flexible guide for both short-term and long-term research activities. The results of this research will (1) enhance technical reviews, (2) provide better insights and guidance into the risks and reliability of digital systems and (3) maintain an informational database on evolving technology and new industry initiatives, including new tools, techniques, and practices relevant to the design and evaluation of future applications for nuclear power plant digital I&C systems.

In preparing the Plan, the staff has consulted the following sources:

- NUREG/CP-0136, documenting a workshop on Digital Systems Reliability and Nuclear Safety (September 1993)

- the National Academies of Science/National Research Council (NAS/NRC) study "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues" (1997)

- the Advisory Committee on Reactor Safeguards (ACRS) Report, “Review and Evaluation of the Nuclear Regulatory Commission’s Safety Research Program” (1998)

- an expert panel convened by RES to assess the state-of-the-art in digital systems research (September 1999).

The staff has also benefitted from ACRS review of the Plan. The staff has incorporated the ACRS comments on the draft Plan into the current version. The ACRS reviewed the revisions to the Plan and provided a strong endorsement of it in NUREG-1635 Vol. 4, “Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program,” (May 2001).

DISCUSSION:

The Plan addresses the need for the digital I&C research program, discusses technical issues and challenges, and establishes actions and schedules. The research has been targeted to support current regulatory activities, and potentially to support future regulatory requirements, including advanced reactor reviews and use of probabilistic risk assessment (PRA) methods in the I&C area.

The short-term research needs are focused on (i) improving efficiency of the technical review process, (ii) addressing reliability and risk considerations, (iii) reflecting evolving technology aspects, and (iv) keeping current with industry standards and practices. The long-term needs are geared toward understanding emerging I&C technologies, developing tools to evaluate their application to existing and advanced reactors, and developing appropriate methods to incorporate digital systems’ reliability information into plant PRAs. To meet the needs discussed above, the staff plans to engage in research tasks in four general areas:

(1) Systems Aspects of Digital Technology

Activities in this area will address both internal interactions and external factors that affect digital system performance, such as, electromagnetic interference and lightning. Guidance will be developed to ensure specifications are provided for environmental qualification of digital systems. Operating systems and computer diagnostics also fall into this research area.

(2) Software Quality Assurance

Software quality assurance is a planned and systematic process for controlling actions necessary to provide adequate confidence that an item, or product, conforms to established technical requirements. Existing guidance relies on subjective measures. The staff will investigate various objective criteria and software engineering techniques to identify opportunities to improve the effectiveness, efficiency and realism of staff review of digital systems.

(3) Risk Assessment of Digital I&C Systems

The NRC is increasing the use of PRA technology in regulatory matters to the extent supported by the state-of-the-art in PRA methods and data. Currently, I&C systems are not generally modeled, in detail, in plant PRAs; however, a recent Accident Sequence Precursor database study (summarized in Appendix A of the Plan) demonstrates the importance of I&C systems on plant safety. As the NRC moves toward a risk-informed regulatory environment, the staff will need the data, methods, and tools to permit accurate and effective risk assessment of digital I&C systems. The staff will analyze U.S. and foreign digital I&C failure data, investigate digital failure and reliability assessment methods, and quantify the risk importance of digital systems.

(4) Emerging I&C Technology and Applications

Innovations in digital I&C technology have the potential to improve the safety of nuclear power plants. The staff requires knowledge of emerging technology and applications in order to make timely and accurate decisions. Research tasks in this area will provide the technical information and criteria for effective regulatory decisions. These tasks are focused on emerging technology and applications known to be pertinent to the nuclear community. Examples include predictive maintenance and online monitoring systems, advanced instrumentation, smart transmitters, wireless communication, and computer security.

As part of its development, the staff has had several discussions with the ACRS and presented the Plan in several public forums, including the 2000 Water Reactor Safety Meeting and the 3rd American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation and Control and Man-Machine Interface Technologies. These interactions with the technical community have provided insights that have been factored into the final version of the Plan. The draft Plan was used as an input to the FY 2002 and FY 2003 budget development and has guided the development and implementation of digital I&C research programs throughout FY 2001. Furthermore, the Plan is responsive to the agency's needs in developing a regulatory framework to address new reactor concepts that would allow effective implementation of new technologies.

The Emerging I&C Technology and Applications section of the Plan provides for the annual development of an emerging technology report that will be used to understand how cutting edge technologies and advancements in current technologies might affect the digital I&C program in the coming years. In this way, both changes in digital systems technologies, such as the increase in the use of wireless communications, and changes in the nuclear industry, such as the development of new I&C in support of advanced reactors will be incorporated into the Plan.

As the results of these projects become available, the staff will (1) provide products that could enhance technical reviews and (2) revise and update the research program by increasing emphasis on areas that can provide improvement to the regulatory process as appropriate. Further, an internal Technical Advisory Group composed of RES, NRR and NMSS staff, will be formed to facilitate technical information exchange among the staff in the various offices, address progress, and identify changes to the Plan as technology and needs change. Although, research in this area in support of regulation of nuclear materials has been limited in the past, it is anticipated that future updates to the research program will include NMSS program areas.

RESOURCES:

The resources for the effort outlined in the Plan were addressed in the FY 2003 budget proposal through the Planning, Budget and Performance Management process.

To achieve the stated goals, the staff will continue to explore the possibility of leveraging its resources by participating in cooperative research with other Federal Government agencies and international organizations.

COORDINATION:

The Office of Nuclear Reactor Regulation has concurred in this paper. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections. The Office of the General Counsel has no legal objection to this paper.

/RA/

William D. Travers
Executive Director
for Operations

Attachment: NRC Research Plan - Digital Instrumentation and Control

Attachment

NRC Research Plan
Digital Instrumentation and Control

Engineering Research Applications Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The purpose of this document is to describe the Research Plan for Digital Instrumentation and Control (I&C) (Plan) in terms of its background, challenges and technical issues, on-going and planned activities, schedule, and resources. The Plan describes research activities for FY 2001-2004.

Background and Challenges

Nuclear power plant licensees are replacing, and will continue to replace, analog I&C equipment with digital equipment. Two main reasons for analog-to-digital upgrades are (1) analog replacement parts are becoming more difficult to obtain and (2) digital I&C systems offer better performance and additional features compared to analog systems. While digital technology has the capability to improve operational performance, there are challenges to the introduction of this technology into nuclear power plants. These challenges include (1) rapid changes in digital technology that requires the NRC to update its knowledge of the state-of-the-practice in digital system's design, testing and application, (2) the increased complexity of digital technology compared to analog technology, and (3) unique failure modes associated with digital technology. Failure to adequately address these challenges in other industries (e.g., aviation, medical, and rail) has resulted in mishaps and near mishaps.

RES Digital I&C Research Program

The NRC Office of Nuclear Regulatory Research (RES) is performing research to better understand digital technology and to update the tools used in assessing the safety of digital I&C applications in US nuclear power plants. The following list identifies ways that the digital I&C research program supports NRC's strategic performance goals.

Maintain Safety

As mentioned above, digital I&C systems have unique failure mechanisms when compared to analog technology. For example, the same protection logic provided by analog relay systems may be implemented using a digital programmable logic device. In the analog system, inputs and safety functions are processed in parallel, whereas in the digital device, the input and safety functions are processed in a sequential fashion. Because of the sequential nature of digital devices, developers must pay particular attention to timing and scheduling of algorithms or the device may fail to perform its required function. The research program contains tasks to understand digital failure mechanisms and provide regulatory tools that address them.

Reduce Unnecessary Regulatory Burden

Digital systems can be complex devices requiring large amounts of effort from developers and independent assessors to gain assurance for their use in safety systems. In the case of software quality assurance, the state-of-the-practice calls for many subjective criteria to be met by software. Numerous subjective criteria produce a sense of uncertainty in licensing arenas because the developers must depend more upon their own engineering

judgment for determining when software is of sufficient quality. To prevent delays in the licensing process, developers may over-prove a software system. Recent advancements in software engineering holds the promise of replacing some, but not all, subjective criteria. In doing so, developers have more surety that their software does meet the stated criteria. By reducing uncertainty through objective criteria, the unnecessary burden from potentially over-proving a digital system is lifted from licensees. This research plan contains activities that will seek objective criteria that can be used as an alternate method to evaluate the acceptability of digital I&C systems.

Improve Regulatory Effectiveness, Efficiency, and Realism

Because of digital system complexity, it is important that NRC's regulatory activities be effective and efficient in order to ensure the safe implementation of digital technology in nuclear power plants. The research program proposes several tasks in the area of risk assessment of digital systems that will provide the NRC with the technical bases, tools, and methods for effective, efficient, and realistic licensing of digital systems. For example, not all digital failures will have the same impact upon plant safety. By having the tools to identify those digital failures that have the most impact on plant safety, the NRC is better able to efficiently assess the safety of a digital system. Also, as digital upgrades are performed on safety systems, it is important to identify realistic failure probabilities (and its associated uncertainty) for inclusion into plant probabilistic risk assessments (PRAs).

Increase Public Confidence

Public confidence is supported by supplying appropriate technical information and criteria to the regulatory process in a timely manner. For example, as emerging technology and applications enter nuclear power plants, the NRC will be faced with regulatory decisions based on such innovations. It is important to develop adequate information on emerging technologies, such as, advanced instruments, automated and intelligent maintenance systems, and programmable controls/protection systems, so that it can make timely decisions based on the most available and accurate information.

As a short term goal, and as requested by the Office of Nuclear Reactor Regulation (NRR), the digital I&C research program will develop methods and tools needed to support improvements in the review of digital systems, while maintaining or improving the predictability of the review process. Although, research in digital I&C in support of regulation of nuclear materials has been limited in the past and is not specifically discussed in the Plan, the research in support of these short term goals will also support the review of digital systems that is starting to be more common in the materials area (for example the review of Mixed Oxide Fuel (MOX) facility construction permit). In the long term, digital failure characteristics and probabilities must be modeled sufficiently well so that digital systems can be effectively added to risked-based regulatory programs. Another long term goal is to develop new regulatory guidance for the review of emerging I&C technology in the digital area.

Tasks Within the Research Program

In order to meet the goals discussed above, RES will engage in a series of tasks, grouped into the following four areas: (1) System Aspects of Digital Technology, (2) Software Quality

Assurance, (3) Risk Assessment of Digital I&C Systems, and (4) Emerging I&C Technology and Applications. The following is a discussion of the tasks within each area.

Systems Aspects of Digital Technology

Systems aspects of digital I&C systems involve those factors, both internal and external, that impact the performance of the system. This plan discusses four types of system aspects that have the potential to impact plant safety and future regulatory decisions.

- *Environmental Stressors* include electromagnetic interference/radio-frequency interference (EMI/RFI), temperature, humidity, smoke, and lightning. Research efforts will provide appropriate acceptance criteria for the qualification of digital equipment against these stressors.

- *Digital Requirement Specifications* describe the functions expected from the digital I&C system, and they state how the digital system interfaces with other plant systems and components. Research efforts will review current tools that are used in other industries to provide the staff with methods and tools for the review of requirements specification.

- *Diagnostics and Fault-Tolerance* are special features with many digital I&C systems that enable the system to detect internal problems and either avoid or handle the problem, or alert the operator to the problem. While these features could improve reliability, research efforts will investigate both positive and negative safety impacts.

- *Operating Systems* control basic functions of a digital I&C system, including its communication functions, memory management, and processor scheduling. These systems are becoming larger and more complex, making the review of such systems difficult. Research efforts will identify the aspects of operating systems that may adversely impact safety.

Software Quality Assurance

Software quality assurance is a planned and systematic pattern of all actions necessary to provide adequate confidence that an item, or product, conforms to established technical requirements. While the NRC currently has a set of software quality assurance activities, these activities are resource-intensive for both the NRC and the industry. In addition, current software testing activities do not specify how they should be performed or how much testing should be conducted. This leads to an inconsistency in the amount of testing and testing methods for similar digital I&C systems. The digital I&C research tasks will address these issues in the following ways:

- *Objective software engineering criteria* provide a measurable acceptance level for software quality. Because software engineering is a young discipline, methods for evaluating software quality have relied on subjective judgment. However, research results from academia and other industries show potential software measures that could be used to establish minimum software quality acceptance levels. Research efforts will investigate the potential of using such measures for NRC regulatory purposes.

- *Criteria for software testing* are important to software quality assessments. Software test criteria should dictate the types of tests and the number/type of test cases. Research efforts will support software quality assessments by supplying software test criteria.

Risk Assessment of Digital I&C Systems

The NRC intends to increase the use of probabilistic risk assessment (PRA) technology in regulatory matters to the extent supported by the state-of-the-art in PRA methods and data. Currently, I&C systems are not, generally modeled in plant PRAs, however, a recent Accident Sequence Precursor database study demonstrates the prevalence and improtance of I&C systems on plant safety (see Appendix A). As the NRC moves toward a risk-informed regulatory environment, the NRC will need the data, methods, and tools related to the risk assessment of digital I&C systems. The following tasks describe how the research program will address these needs.

- *Performing analysis on digital I&C failure data* provides several benefits to the NRC, including: (1) the ability to determine which digital failures have the largest impact on plant safety, (2) feedback on the effectiveness of NRC regulatory programs, and (3) support for the risk assessment of digital I&C systems. Research efforts will gather and assess digital failure data from domestic/foreign nuclear power plants and other industries having digital systems that are critical to safety. Particular attention will be paid to commercial off-the-shelf digital I&C equipment.

- *Digital failure assessment methods* are used by defense and aerospace industries to determine types of failures and their impact on overall safety. Understanding this information is particularly important as the NRC moves toward a risk-informed environment. To assist digital system failure assessments, research efforts will provide criteria outlining the proper use of failure assessment methods.

- *Identifying the risk-importance of digital I&C systems* will help the NRC determine the required level of regulatory review for digital upgrades and focus research efforts on those aspects of digital I&C systems having a significant impact on plant safety.

- *Digital reliability assessment methods* estimate the likelihood of a digital I&C failure that would adversely affect plant safety. Due to the complex nature of digital systems and the uniqueness of software failures, estimating the likelihood of digital failures is difficult. Several reliability assessment methods have been used by other industries and show potential for use in the nuclear industry. Research efforts will identify digital reliability assessment methods that are applicable to the nuclear industry and provide criteria for their proper use.

Emerging I&C Technology and Applications

New innovations in the area of digital I&C technology have the potential to help nuclear power plants in both operating efficiency and safety. NRC regulatory programs require knowledge about emerging technology and applications in order to make timely decisions. Research tasks associated with this area will provide the technical information and criteria for regulatory

decisions. The following are the emerging technologies and applications addressed by the research program; not including those that may appear in a few years.

- *Predictive maintenance and on-line monitoring systems* provide the automatic capability to determine system/component failure or the need for maintenance. Such systems will motivate changes to surveillance and maintenance practices at nuclear power plants that result in operational cost reductions. Research efforts will analyze the safety impacts of this technology.

- *Advanced instrumentation* for measuring flow, temperature, pressure, neutron flux, and other plant variables hold the potential to improve upon plant efficiency, safety, or both. To make timely and informed regulatory decisions involving advanced instrumentation (e.g., power uprates), the NRC needs the technical bases surrounding this emerging technology.

- *Smart transmitters* offer digital communication of data from the sensor to the control system. Some smart transmitters are also capable of providing compensating measures for instrument error or control functionality at the sensor. Research efforts will provide technical information to the NRC regulatory programs on this technology.

- *Wireless communication* is the transmission of plant data over radio-frequency networks. While this technology would eliminate some of the problems associated with cables, it also has its own inherent problems which will be identified by the digital I&C research program.

- *Firewalls* prevent the unauthorized access and corruption/degradation of the performance of computer systems. Research will be conducted to assess the potential for such corruption/degradation of computers in nuclear power plants. These efforts will identify what measures should be taken to prevent unauthorized access.

The digital I&C research program will meet the needs of NRC regulatory programs, as they relate to digital technology. The digital I&C research program will also include a task to monitor the state-of-the-art in this area and develop new research projects to address any new safety concerns that may arise due to the implementation of emerging technologies. Digital I&C systems offer several benefits to NRC licensees, including increased operational efficiency and improved reliability. However, digital technology is complex and possesses failure modes not present in analog devices. In the short term, the digital I&C research program will provide methods and tools which support the introduction of digital technology without allowing new failure mechanisms into nuclear power plants. In the long term, the research program will provide timely information on emerging technologies and applications, and it will support the incorporation of digital systems into plant PRAs.

1 INTRODUCTION

The purpose of the Research Plan for Digital Instrumentation and Control (I&C) is to describe the proposed digital I&C research program in terms of its background, challenges and technical issues, planned activities to meet the challenges, schedule, and resources. The plan will provide the basis for the research in this area for fiscal years 2001-2004.

I&C systems (whether analog and digital) play an important role in the safe operation of nuclear power plants. Digital I&C systems promise many potential benefits to the nuclear industry in terms of operational and safety performance. For example, digital systems are essentially free of the drifts associated with analog systems, have higher data handling and storage capabilities, and provide improved performance in terms of accuracy and computational capabilities. However, there are challenges to the introduction of digital technology into nuclear power plants, including the rapid changes to the technology. In addition to the rapid change, digital technology is more complex than analog technology, and its operation and failure modes are different. This requires the NRC to update its knowledge of the state-of-the-practice in digital systems design, testing and application. Failure to adequately address these challenges, could result in significant risks to the health and safety of the public (Leveson, 1995). Faults in digital systems have been implicated in mishaps and near mishaps in communications systems, air-traffic control systems, and electric power systems.

As an example of the crucial role that software plays in the aircraft industry today, consider the July 2, 1994, crash of a large, commercial aircraft attempting to land at Charlotte, North Carolina. As a result of the investigation of that crash, the Federal Aviation Administration (FAA) determined that a software design feature in the wind-shear detection system delayed the detection of wind shear when the wing flaps of the aircraft were in transition. The FAA issued an Airworthiness Directive which called for the replacement of the software in that wind-shear detection system on over 1600 aircraft. The directive to change the software applies to a large number and variety of commercial transport aircraft.

These mishaps and incidents have also occurred in the nuclear industry. Perhaps the most serious computer related events were the medical mis-administrations with a computer-controlled radiation therapy machine, which massively overdosed six people (leading in some cases to their death). Between June 1985 and January 1987 there were six events in which the Therac-25 radiation therapy machine overdosed six patients due to a software error, in Canada and the United States (Leveson 1995). The causal factors in these incidents included:

- failure to perform a safety analysis on the software (i.e., an incomplete requirements analysis) although near full responsibility for safety rested on it;

- assuming the software was safe because it worked successfully in thousands of tests before overdosing a human (i.e., equating safety to reliability) and;

- failure to provide self-test, error-detection, and error handling features in the software that could have indicated the existence of a problem well before failing catastrophically. This also includes failure to include defense-in-depth in the design; for example, protection against software bugs could have been built into the software and the hardware.

Another less serious, nuclear industry example was the November 3, 1994 Turkey Point Unit 3 emergency diesel generator (EDG) load sequencer failure to respond to a unit 4 safety injection (SI) signal because of a defect in the sequencer software logic. The problem arose when an error occurred in a portion of logic, which is supposed to actuate the sequencer if an SI actuation signal arrives while the sequencer is in an automatic self-test mode. The design of the control unit that failed was such that, if a real SI signal arrived 15 or more seconds into particular test scenarios, the test signal was properly cleared, but not the inhibit logic. SI actuation is prevented if the inhibit logic is not cleared. The root cause of the event was that the designer and the independent verifier of the control unit both failed to recognize the interactions between the inhibit and self-test logic. An independent assessment team found that the software verification and validation (V&V) activity was not comprehensive enough to test certain aspects of the logic. In its review, the NRC staff indicated that the software V&V plan was weak in that it relied almost exclusively on testing, and lacked the analysis of both software requirements and software design that could have identified the design flaw.

Because challenges to digital I&C systems are so complex, the analysis, audit, and inspection of digital I&C systems is a difficult task. In response to the challenges, the NRC Office of Nuclear Regulatory Research (RES) is performing research to better understand this technology and to update the tools used to assess the safety of digital I&C applications in U.S. nuclear power plants. The purpose of the current digital I&C research program presented in this plan is to address these issues and develop new technical information needed to assist the NRC in improving the efficiency and effectiveness of its regulatory programs. This initiative will:

- develop guidance, tools, and methods in reviewing digital I&C areas;
- provide objective criteria for acceptance of new technology;
- provide review criteria for new technology;
- provide information on new systems to assure new failure modes are not introduced;
- reduce the expenditure of effort needed to review topical reports and plant specific applications in this area;
- suggest improvements to current review guidance in order to reduce the time it takes for the review of digital systems;
- improve realism by developing an understanding of the new technology in advance of its application in plants.

The NRC is already pursuing many of the initiatives mentioned above. For example, the NRC participates in a cooperative agreement with other federal agencies and industries at the University of Virginia (UVa). The purpose of the cooperative agreement is to investigate and develop methods and tools for digital system reliability assessment. One benefit of participating in the cooperative agreement is the ability to gain technical information and lessons-learned from academia and other industries concerned with safety. Another benefit is the ability to combine resources with others to meet a common research objective. Through participation in the cooperative research program, the NRC hopes to gain (1) guidance, tools, and methods for

reviewing digital system reliability assessment, (2) provide objective criteria regarding digital reliability assessment, and (3) propose an efficient, yet effective method for digital reliability assessment. section 3.4.4 provides more detail on the UVa cooperative agreement.

The recent Y2K experiences enhanced the public's awareness of the issues concerning digital systems in nuclear power plants. An aggressive pursuit of research in this area, as described in this Plan, will support the public confidence performance goal, as well as the other strategic performance goals, by assuring the public that the staff has adequate information on current and emerging technologies to support decisions based on best available information.

1.1 Background

The NRC recognizes the improvements that digital technology can offer nuclear power plants in terms of operational performance, reliability, and safety. However, it also recognizes several technical issues associated with digital I&C systems that have the potential to impact plant safety. The NRC's experience in licensing analog I&C systems is being used to address digital I&C technical issues. However, many new issues have arisen because of the differences in the way digital and analog I&C systems are designed, operated, and fail. As the nuclear industry moves into a deregulated environment, and licences are extended from 40 to 60 years, many plants will look to digital I&C systems as a way to reduce operating costs and improve safety.

In the early 1990's the NRC began developing guidance to support the review of digital systems in nuclear power plants. RES commissioned the National Academy of Sciences' National Research Council to review the issue associated with the use of digital I&C systems. The National Research Council issued its report and made several recommendations including a recommendation to develop a research plan that would balance short-term regulatory needs and long-term research needs (NAS, 1997). In 1999 RES convened an expert panel to assess the state-of the art in digital systems research. The panel provided input on the most important on-going research issues in the digital systems area (USNRC, 1999a).

In 1997, the NRC completed an update to Chapter 7, Instrumentation and Control, of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants." This update to the Standard Review Plan (SRP) addressed many of the regulatory review issues associated with digital technology. In support of the SRP update, the NRC also developed six regulatory guides (RG) addressing software quality assurance (RG 1.168 "Verification, Validation, Reviews and Audits for Digital Computer Used in Safety Systems of Nuclear Power Plants," RG 1.169 "Software Configuration Managements for Digital Computer Used in Safety Systems of Nuclear Power Plants," RG 1.170 "Software Test Documentation for Digital Computer Used in Safety Systems of Nuclear Power Plants," RG 1.171 "Software Unit Testing for Digital Computer Used in Safety Systems of Nuclear Power Plants," RG 1.172 Software requirements Specification for Digital Computer Used in Safety Systems of Nuclear Power Plants," and RG 1.173 Software Life Cycle Processes for Digital Computer Used in Safety Systems of Nuclear Power Plants"). These regulatory guides endorsed eight IEEE standards with exceptions (IEEE Standards 603, 7-4.3.2, 828, 830, 1008, 1012, 1028, 1042 and 1074). Other work contributing to the updated regulatory framework included technical reports on specific topics such as defense-in-depth analysis for digital I&C systems and review guidance for computer data communications and programable logic controllers. For some

technical issues, the SRP endorses industry guidelines. One example is the EPRI guidelines for dedication of commercial off-the-shelf digital I&C equipment.

Since the update of the SRP, RES has been supporting the digital I&C regulatory framework by providing review guidelines and technical information on specific I&C issues. Examples of such support include review guidance on software languages, sample rate and computer wordlength selection, and environmental qualification of digital I&C systems.

Recognizing the need for further research in the area of digital I&C technology, the ACRS made the following comment in their 1998 report, “Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program."

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

1.2 Opportunities and Challenges Associated With Digital I&C Systems

Since their construction, nuclear power plants depended upon analog I&C systems to provide monitoring, control, and protection. These analog I&C systems, many of which are still in operation, have proven to be effective. However, the general direction of the nuclear industry is to replace their analog I&C equipment with digital equipment for the following reasons:

- Analog I&C systems are experiencing typical aging behavior (e.g., mechanical failures and environmental degradation) and qualified replacement parts are becoming increasingly difficult to obtain because of waning vendor support.

- Digital I&C systems offer new, or improved, system performance in terms of accuracy and computational capability. Examples of new computational capability include the on-line ability to perform self-tests and detect failed sensors in safety systems.

- Digital I&C systems have higher data handling and storage capacities, so operating conditions can be more fully measured and displayed.

- Digital systems are capable of nearly drift free operation and can be designed to tolerate faults.

For these reasons nuclear utilities are replacing and upgrading I&C and electrical systems with systems that include digital technology at an ever increasing rate. These replacements will be in every part of the plant, including the Reactor Protection System (RPS), Engineered Safety Feature Actuation System (ESFAS), monitoring systems, balance-of-plant (BOP) control systems, and electrical systems. The Office of Nuclear Reactor Regulation (NRR) has reviewed two topical reports in this area and is expecting additional topical reports and plant specific reviews. There are unique issues associated with digital systems that make the review of these systems both difficult and resource intensive (a person year or more is not uncommon for each topical). Some of the challenges facing the NRC in regulating these systems include:

- Changing technology and analog system obsolescence make the transition to digital systems a requirement for most if not all systems, especially for plants that will be extending their licence.

- Uncertainty associated with the introduction of any new technology leads to issues on how to provide the appropriate level of realism and conservatism. Software engineering is not yet a mature discipline and changes rapidly with changing technology, making programmatic reviews difficult.

- Limited methods for assessing digital system reliability and safety make detailed analysis of the digital systems difficult and resource intensive. Presently it is not possible to adequately quantify software reliability because high levels of complexity inherent in these systems leads to difficulty in testing.

- The mismatch between the time frames associated with digital systems development and development of regulatory tools makes timely and efficient review of emerging technologies difficult.

- The balance between the need for robust, standard components and the opportunities to improve performance by utilizing rapidly advancing, state-of-the-art devices and methods creates a situation where the use of new technology may be less than desirable. For example use of commercial software tools, operating systems, and testing software diagnostics, provides economic advantages, but can add to system complexity.

- Digital equipment is sensitive to environmental challenges (temperature, humidity, EMI/RFI, power quality, surges, grounding, smoke, etc).

While digital I&C systems offer many potential benefits, the regulatory concern is their correct operation and reliability. As mentioned above, I&C systems play an important role in nuclear power plant safety. This aspect is demonstrated in a recent study of the Accident Sequence Precursor (ASP) database (see Appendix A). In this study, failure of I&C components contributed to 40% of all ASP events having a conditional core damage probability greater than or equal to 1×10^{-5}. Of these events, 30% were initiated by I&C-related failures. The ASP study shows the importance of ensuring that certain I&C systems (whether digital or analog) operate correctly and with high reliability. Assessing the safe and reliable operation of analog I&C systems is relatively straightforward and well-understood. Assessing the safe and reliable operation of digital I&C systems presents certain challenges.

Specific challenges underlying the difficulty of regulating this technology will be addressed by this Plan. These challenges fall into several areas, one of which is to develop methods and standards for identifying faults and their potential impact in digital I&C systems. The challenges in this area lie with the complexity and unique failure modes associated with these systems. For example, experts have known for some time that testing of all possible states of digital I&C systems is not possible due to their complex design and operation. Furthermore, it is the unexpected inputs and conditions that typically cause digital I&C systems to fail. Additionally, digital system reliability assessment methods are not yet well defined. In light of these facts, industries and regulatory bodies (including the NRC) have implemented various activities to reduce the potential for digital failures, but acknowledge that complete knowledge of digital failure potential is not a realistic task in most situations at the present time. The NRC needs effective and efficient methods for understanding the challenges to digital systems. Through research, methods and tools will be developed to support the effective regulation of these technologies.

1.3 Short and Long Term Goals for Digital I&C Systems in Nuclear Power Plant Application

As recommended in the National Research Council study (NAS, 1997), this research plan for digital I&C has been developed to address both the short term goal of supporting the effective and efficient regulation of these new systems, balanced with long-term research needs. The current review guidelines provide methods for review and approval of the digital systems that have been submitted. But, for the NRC to efficiently regulate and review systems employing this rapidly evolving technology, improvements in the review guidance is needed. Quality control and quality assurance expectations for digital systems are not compatible with other components. Current software and digital system quality assurance and testing methods are not as efficient as other guidelines in more mature fields. The short term goal of this digital I&C research plan is to develop the methods and tools needed to support improvements in the review of digital systems. This goal will be met by providing tools and methods that reduce the time it takes to review digital I&C system packages, while maintaining or improving the predictability of the review process. Accomplishing this goal will allow NRC to more effectively review digital systems upgrades while maintaining safety, reducing unnecessary regulatory burden, and improving the efficiency, effectiveness, and realism of NRC oversight.

In the longer term, the failure probabilities and the failure characteristics of digital systems need to be modeled sufficiently well so that digital systems can be effectively added to risked-based regulatory programs. One long term goal is to develop methods to include digital and software systems in the risk-based regulatory structure. Another long term goal of the plan is to reduce the time it takes to develop new regulatory guidance for the review of emerging technology in the digital areas. This long term goal will be carried out by keeping informed of emerging technologies, understanding their safety concerns related to emerging digital I&C systems, and enabling the early development of regulatory guidance as new technology is applied in the nuclear power industry.

In implementing its research plan to achieve the above goals, the staff intends to continue to tap the resources of other federal government agencies, industry, academia and internal agencies to the extent possible in order to leverage its research dollars. Indeed, with the introduction of its Information Technology for the Twenty-First Century initiative, the executive

branch of the federal government has proposed a dramatic new commitment to research in information technology [NSTC, 1999]. This is a multi-agency information technology research initiative that increases federal investment in a number of areas including the development of reliable software for high confidence and safety-critical applications, security of software systems, human-computer interaction, and fundamental research on emerging technologies.

1.4 Plan Organization

The digital I&C program goals and scope are discussed in section 2. The major areas associated with digital I&C technology and the programs to address them are discussed in section 3 “Issue and Task Descriptions”, including background and tasks to address the issues. Section 4, "Interactions With Relevant Digital I&C Activities," describes the possible collaborations between the NRC digital I&C research program and other programs within the NRC, nuclear industry, federal government, and international organizations. Section 5, "Schedule and Resources," provides a schedule for the research that will be done to accomplish the goals of the Plan. In addition section 5 provides the resource estimates for the various parts of the Plan.

2 PROGRAM GOALS AND SCOPE

2.1 Program Goals

RES is performing research to better understand digital technology and to update the tools used in assessing the safety of digital I&C applications in US nuclear power plants. The following list identifies ways that the digital I&C research program supports NRC's strategic performance goals.

Maintain Safety

As mentioned above, digital I&C systems have unique failure mechanisms when compared to analog technology. For example, the same protection logic provided by analog relay systems may be implemented using a digital programmable logic device. In the analog system, inputs and safety functions are processed in parallel, whereas in the digital device, the input and safety functions are processed in a sequential fashion. Because of the sequential nature of digital devices, developers must pay particular attention to timing and scheduling of algorithms or the device may fail to perform its required function. The research program contains tasks to understand digital failure mechanisms and provide regulatory tools that address them.

Reduce Unnecessary Regulatory Burden

Digital systems can be complex devices requiring large amounts of effort from developers and independent assessors to gain assurance for their use in safety systems. In the case of software quality assurance, the state-of-the-practice calls for many subjective criteria to be met by software. Numerous subjective criteria produce a sense of uncertainty in licensing arenas because the developers must depend more upon their own engineering judgment for determining when software is of sufficient quality. To prevent delays in the licensing process, developers may over-prove a software system. Recent advancements in software engineering holds the promise of replacing some, but not all, subjective criteria. In doing so, developers have more surety that their software does meet the stated criteria. By reducing uncertainty through objective criteria, the unnecessary burden from potentially over-proving a digital system is lifted from licensees. This research plan contains activities that will seek objective criteria that can be used as an alternate method to evaluate the acceptability of digital I&C systems.

Improve Regulatory Effectiveness, Efficiency, and Realism

Because of digital system complexity, it is important that NRC's regulatory activities be effective and efficient in order to ensure the safe implementation of digital technology in nuclear power plants. The research program proposes several tasks in the area of risk assessment of digital systems that will provide the NRC with the technical bases, tools, and methods for effective, efficient, and realistic licensing of digital systems. For example, not all digital failures will have the same impact upon plant safety. By having the tools to identify those digital failures that have the most impact on plant safety, the NRC is better able to efficiently assess the safety of a digital system. Also, as digital upgrades are

performed on safety systems, it is important to identify realistic failure probabilities (and its associated uncertainty) for inclusion into plant probabilistic risk assessments (PRAs).

Increase Public Confidence

Public confidence is supported by supplying appropriate technical information and criteria to the regulatory process in a timely manner. For example, as emerging technology and applications enter nuclear power plants, the NRC will be faced with regulatory decisions based on such innovations. It is important to develop adequate information on emerging technologies, such as, advanced instruments, automated and intelligent maintenance systems, and programmable controls/protection systems, so that it can make timely decisions based on the most available and accurate information.

To meet the short and long term goals of the Plan, research programs have been developed based on the four agency performance goals of maintaining safety, increasing public confidence, reducing unnecessary regulatory burden, and making NRC activities and decisions more effective, efficient, and realistic.

The short term goal of the Plan is to improve the effectiveness of the review program, thereby making NRC activities and decisions more effective and efficient. The program objectives supporting that goal will provide the technical bases, methods, and tools in response to user needs identified by the NRR. These research products will reduce the effort needed to evaluate current applications of digital technology while maintaining safety. Although, research in digital I&C in support of regulation of nuclear materials has been limited in the past and is not specifically discussed in the Plan, the research in support of these short term goals will also support the review of digital systems that is starting to be more common in the materials area (for example the review of Mixed Oxide Fuel (MOX) facility construction permit). The long term goals of the program include the development of technical bases related to the inclusion of digital I&C into risk based regulation. The long term goals also include the timely development of regulatory guidance to support the review of emerging digital I&C technology. These goals will prevent the introduction of digital-related flaws that pose a significant and negative impact on plant safety, without becoming an impediment to the advantages of using digital I&C technology.

2.2 Program Scope

The digital I&C research program activities are grouped into four areas. The first two areas, Systems Aspects of Digital Technology, and Software Quality Assurance have been developed to meet the short term goal of improving the review of digital systems by providing tools and methods for the current review process. The third area, Risk Assessment of Digital I&C Systems, has been developed to meet the long term goal of including digital systems in risked based regulatory programs. The fourth area, Emerging I&C Technology and Applications, has been developed to meet the long term goal of reducing the time it takes for the NRC to become ready to review the application of new technology to nuclear power plants. The following is a summary of the four areas.

Systems Aspects of Digital I&C Systems. This work will provide the technical bases for environmental qualification of digital I&C systems, effects of requirements specifications on system quality, operating systems, and computer diagnostics.

Software Quality Assurance. Data and information on software engineering practices, software measures, and software testing will provide a significant reduction in the amount of resources needed by both the NRC and licensees to assess software quality, by providing methods and metrics that are acceptable to the staff.

Risk Assessment and Digital I&C Systems. Criteria directing the review of digital I&C risk assessments will be developed. These activities include the analysis of data in the nuclear industry and other industries, investigations of digital system reliability assessment methods, and integration of digital system model into PRA's.

Emerging I&C Technology and Applications. Introduction of advanced instrumentation, automatic surveillance systems, and digital system diagnostics may lead licensees to make changes to their plants to take advantage of these systems. In such cases, the NRC staff needs the technical bases to evaluate the acceptance of emerging I&C technology and applications. The NRC needs to be pro-active in (1) identifying the areas that will need additional review, and (2) developing research to meet these needs.

2.3 Program Interaction within the NRC

The staff recognizes the need to conduct research in the area of digital I&C in a manner that complements or is complimented by other related NRC programs. To this end, the staff has identified interfaces with research programs in the areas of human performance and probabilistic risk assessment including, fire risk, and human reliability analysis, and interfaces with program offices that will utilize the products of research. In regard to the research on human performance, digital I&C research will be integrated as needed with the Emerging Issues program area as described in the Agency-Wide Program Plan on Human Performance in Nuclear Power Plant Safety.

In regard to systems, structures, and components (SSCs) that rely on digital devices to achieve or support functionality, an important goal of the NRC research program is to ensure that technical bases exist for regulating these SSCs using a risk-informed performance-based approach that is consistent with the approach being used for SSCs that do not rely on digital devices. To achieve this goal, there must exist means by which the incremental risk associated with replacing existing SSCs with ones using digital devices can be assessed. Determining incremental risk requires a systems analysis of the digital I&C SSC followed by a broader probabilistic risk analysis to determine the contribution to risk from operation with the digital SSC. Developing methods for doing these analyses will be the focus of a coordinated research effort between the Division of Risk Analysis and Applications (DRAA) and the Division of Engineering Technology (DET). As discussed in other parts of this Plan, DET will focus its efforts in this area on (1) evaluating digital safety assessment methods; and (2) investigating methods for estimating the reliability digital devices with emphasis on software reliability analysis. DRAA will focus its efforts toward (1) developing an approach for screening systems receiving digital upgrades based on risk importance; and (2) modeling SSCs with digital devices

in a PRA or a qualitative risk assessment[1] using input from digital safety assessments and reliability analyses.

A Technical Advisory Group, comprised of RES, NRR and NMSS staff, will be formed to facilitate technical information exchange, address progress and identify changes to the Research Plan as technology and needs change.

[1]RG 1.174 discusses the use of qualitative analyses to support plant changes that have been proposed in the risk-informed regulatory arena.

3 ISSUE AND TASK DESCRIPTIONS

The digital I&C research program consists of issues categorized into four broad areas: systems aspects of digital technology, software quality assurance, risk assessment of digital I&C systems, and emerging I&C technology. These areas were previously identified in digital I&C expert panel reports (NAS, 1997; USNRC, 1999a). They consist of specific tasks to address specific research issues. The purpose of this chapter is to identify those issues (including relevant background) and describe the general approach (tasks) to address them.

The following sections describe the program outcome, specific issues and tasks by area. The schedule for the development of the research products along with the resource estimates are presented in section 5 of the plan.

3.1 Program Outcome

There are three program outcomes supported by the short and long-term goals of the digital I&C research plan. The outcomes are:

1) An improved regulatory review process that will ensure that the current level of safety is maintained, while improving the scrutability and efficiency of reviews, and reducing the time it takes NRR to review digital I&C system packages.

2) A reduction in the time it takes to develop new regulatory guidance for the review of emerging technology in the digital area, thereby reducing the time it takes for licensees to get new systems into the field, reducing unnecessary regulatory burden, and improving efficiency, effectiveness, and realism.

3) New capabilities to address digital I&C systems in PRA, and thereby supporting risk informed applications involving digital I&C systems.

The digital I&C research program is designed to facilitate the introduction of digital I&C technology into nuclear power plants while ensuring adequate safety is maintained. The research products to be provided under the tasks in sections 3.2, “Systems Aspects of Digital Technology and Improvements” and 3.3, “Software Quality Assurance”, are designed to provide improvements to the regulatory review process that reduces the time it takes NRR to review digital I&C system packages, while at the same time, maintaining the level of plant safety and improving the scrutability of the regulatory process. The research products that will be provided under the tasks in section 3.4, “Risk Assessment of Digital I&C Systems”, will support the development of new capabilities to use risk informed regulatory approaches in the review of digital I&C applications. Therefore, with all tasks, primary focus is on (1) maintaining/improving plant safety, (2) regulatory efficiency, and (3) reducing unncessary regulatory burden. The research products that will be provided under the tasks in section 3.5, “Emerging I&C Technology and Applications”, will shorten the time it takes to develop regulatory guidance for the implementation and review of emerging technology in the digital area, thereby reducing the time it takes for licensees to get their systems in the field. Additionally as part of the tasks in section 3.5, “Emerging I&C Technology and Applications”, is a program of looking forward to develop an understanding of how future advances in digital I&C will effect the nuclear industry.

This will be done by both review of current and future trends in other industries and countries and by interactions with the research community.

It is important to note that although there is not a specific program that looks at commercial-off-the-shelf (COTS) digital equipment in the digital I&C research plan, the research program as a whole includes the important issues associated with them. One major aspect that distinguishes COTS equipment from custom-built digital equipment is the difficulty in obtaining design, implementation, and testing detail. In return, COTS digital equipment often has operating experience beyond that of custom-built systems. Outside of these two aspects, the same issues facing custom-built digital systems also face COTS digital systems. For example, software quality, reliability assessment, and electromagnetic interference are issues that face both types of systems. Rather than addressing the aspects of COTS through an individual research area or issue, it is more efficient and practical to ensure that all research products are capable of addressing both COTS and custom-built systems. Therefore, while it may not be explicitly mentioned in each task description, aspects of COTS digital equipment will be addressed in each research activity.

3.2 Systems Aspects of Digital I&C Technology

Systems aspects of digital I&C technology involve those factors external to the digital I&C system, or the system's architecture, impacting the system's performance. This plan discusses four types of system aspects that have the potential to impact plant safety and future regulatory decisions.

- **Environmental Stressors** – includes electromagnetic interference/radio-frequency interference (EMI/RFI), temperature, humidity, smoke, and lightning.

- **Digital Requirements Specifications** – describe the function expected out of the digital I&C system and how the system is to interface with other plant systems and components.

- **Diagnostics and Fault-Tolerance** – many digital I&C systems have the capability to detect internal problems and either avoid, or handle the problem, and alert the operator to the problem.

- **Operating Systems** – software that controls the basic functions of a digital I&C system, including communications, memory management, and task scheduling.

The following sections provide the regulatory and technical background on the issue, a description of the research issue, and tasks to address those issues for each type of system aspect.

3.2.1 Verify Electromagnetic-Interference/Radio-Frequency Interference (EMI/RFI) Qualification Levels

Background and Issues

EMI/RFI is a type of environmental stressor in which electric fields, magnetic fields, or radio-frequency waves interfere with the operation of an electrical or electronic device. The

electric/magnetic fields and radio-frequency waves are generated from sources such 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 nuclear power plants have demonstrated how EMI/RFI can cause unexpected behavior in digital I&C systems (USNRC, 1994).

10 CFR 50, Appendix A - General Design Criteria 4, 10 CFR 50.49, and IEEE Standard 603 (by reference from 10 CFR 50.55a(h)) call for environmental qualification of I&C in nuclear safety systems (IEEE, 1991). At one time, the NRC lacked a complete set of regulatory guides pertaining to EMI/RFI qualification for digital I&C systems. To meet that need, RES developed RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," to provide an acceptable process for EMI/RFI qualification. However, experience in the nuclear industry has indicated that the qualification levels outlined by the RG may be overly conservative for COTS equipment. Therefore, to address this possible over conservatism, the qualification levels identified in the RG need to be re-evaluated.

In addition, past EMI/RFI research did not look at the potential for EMI/RFI to impact electric signals coming into and out of digital safety systems. EMI/RFI that is conducted on signal lines needs to be evaluated to determine the impact, if any, on digital safety system operation. Recently, the International Electrotechnic Commission (IEC) developed an industry consensus standard on EMI/RFI qualification. This standard will be considered as a potential candidate for providing regulatory guidance.

Issues related to EMI/RFI qualification of advance instrumentation and wireless communications will be investigated as part of emerging technologies.

Tasks

Part 1: Investigate the potential for endorsing the new IEC consensus standard on EMI/RFI qualification. If the standard is acceptable, proceed to modify the RG on EMI/RFI qualification to endorse the standard.

Part 2: Investigate claims concerning over conservatism in the proposed EMI/RFI qualification levels. To carry out this portion of the task, re-evaluate nuclear power plant EMI/RFI data and make necessary (if any) adjustments to the qualification RG. Additional data collection may be necessary.

Part 3: Investigate EMI/RFI conduction through I&C signal lines and include appropriate guidelines into the RG. Experiments should consider digital I&C equipment similar to that used in a nuclear safety system and similar operational/accident environments. Results of the experiment and recommended maximum levels for EMI/RFI conducted through I&C signal lines are to be reported. RG 1.180 would be modified if the results warrant a revision.

Outputs

Appropriate revisions to RG 1.180 on EMI/RFI qualification will provide clear guidelines for NRR and licensees on EMI/RFI qualification of digital I&C equipment. Results of the proposed

research will help meet NRC goals of reducing unnecessary regulatory burden and maintaining safety by preventing EMI/RFI qualification over-conservatism and resolving issues related to EMI/RFI conducted through signal lines. For example, re-evaluating the EMI/RFI qualification levels for over-conservatism would prevent the exclusion of qualified COTS digital systems from entering nuclear power plants. This action, in turn, prevents undue burden on licensees in trying to find an over-qualified digital system as a replacement.

3.2.2 Complete Environmental Qualification Guidelines

Background and Issues

As mentioned in section 3.2.1, regulations require digital safety systems to be environmentally qualified for expected and postulated environmental scenarios. Environmental stressors (i.e., temperature, humidity, and smoke) are known to cause digital I&C failures (USNRC, 1994). To address this issue, the NRC has performed research to arrive at acceptable qualification levels. While the majority of this work is completed, important steps remain to fill certain gaps.

Tasks

Complete on-going studies on the effects of smoke on digital I&C systems and provide recommendations for smoke qualification. Consider the results and recommendations from temperature, humidity, and smoke studies, and develop regulatory guidance that identifies the procedures and levels necessary for qualifying digital safety systems against such stressors.

Outputs

A RG on environmental qualification of digital I&C equipment for temperature, humidity, and smoke will provide guidance to the NRC staff and nuclear industry. By providing such guidance, NRC goals of maintaining safety and reducing unnecessary regulatory burden are being met by providing stability and consistency in the licensing process. The proposed guidance would provide criteria to determine the minimum operating temperature range for such systems. In doing so, safety is maintained by preventing unqualified digital equipment from entering nuclear power plants, and unnecessary regulatory burden is reduced since acceptance criteria are made clearer.

3.2.3 Develop Lightning Protection Guidelines

Background and Issues

Like other environmental stressors, lightning has the potential to cause failure in digital I&C systems. To protect against lightning, certain design measures can be taken to prevent or minimize its impact. Currently, Chapter 7 of the SRP, states that lightning protection should be addressed as part of the review of electromagnetic compatibility. It also states that lightning protection features should conform to the guidance of NFPA Standard. 78, "Lightning Protection Code," and IEEE Standard. 665, "Guide for Generation Station Grounding." However, it is unclear whether the guidance in these standards is sufficient for ensuring the protection of digital safety systems from lightning because of the much lower operating voltages that modern digital I&C systems use.

Tasks

Investigate lightning protection research, practices, and standards by surveying previous research in the area of lightning protection for digital systems. Where necessary, conduct experiments and analysis to obtain missing data. Using the results, develop (or incorporate) applicable guidance for qualifying digital safety systems against lightning effects.

Outputs

A RG on lightning protection will provide needed guidance to the NRC staff and nuclear industry. This guidance would help meet NRC's goal of reducing unnecessary regulatory burden by removing the licensing uncertainty associated with qualifying digital safety systems against lightning effects. For example, licensees consider lightning as a potential environmental stressor, however there is no guidance on how to analyze its potential effects The proposed guidance would provide licensees with qualification criteria and remove unnecessary burden that is associated with regulatory uncertainty.

3.2.4 Investigate Requirements Specification Assessment Methods

Background and Issues

As defined earlier, digital system requirements specifications state the expected response of the digital I&C system for given inputs and conditions. System requirements specifications also dictate the interface between the digital I&C system and other plant systems, including the operator. While the specification of system requirements appears to be a relatively simple task, experts have indicated that unclear, incorrect, and incomplete requirements are a leading cause of digital-related failures in high integrity systems (NAS, 1997; USNRC, 1999a). Typical errors in requirements specifications include omission of timing requirements, inability to handle all possible data loads, and no instruction for handling unanticipated inputs/conditions that could arise. Assessing system requirements specifications for these types of errors is difficult because of the complex operating patterns that are characteristic of digital I&C systems. Furthermore, experts have also indicated that the translation from system requirements specifications to hardware and software requirements specifications can introduce errors if the proper information is not communicated.

The SRP provides discussion on software quality assurance criteria for digital safety systems in nuclear power plants. These criteria flow primarily from 10 CFR 50.55a(h); 10 CFR 50, Appendix A – GDC 1 & 21; and 10 CFR 50, Appendix B – Criterion III. RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 830-1993, "IEEE Recommended Practice for Software Requirements Specifications." Both the standard and the SRP state criteria that software requirements specifications should possess, which include completeness, traceability, and correctness. For criteria like traceability, it is fairly straightforward for the staff to assess whether the criteria were met. However, for other criteria (completeness and correctness in particular) it is difficult for the staff to determine whether these criteria have been met in the system, hardware, or software requirements specifications.

As the nuclear industry begins to use more COTS digital equipment, it is vital for requirements specifications to be complete, correct, and clear. The reason for this diligence is because most of the development effort is shifted from design of custom equipment, to the specification and selection of generalized COTS equipment. Since COTS equipment is designed to meet multiple applications, including those outside of the nuclear industry, it is important to ensure that all system requirements for digital safety systems are accomplished. Additionally the use of auto code generation tools in software production is becoming more and more prevalent, especially in COTS products. This presents additional concerns because not only does the code need to meet the system requirements, but the code generation tool needs to be reviewed to ensure additional unwanted functions are not added to the code and there is no potential for common-cause failure modes. It is speculated that COTS equipment can meet the majority of system requirements, but some modifications may be required in order to fully meet all requirements. Therefore, the NRC staff will need the data, methods, and tools to be able to gain adequate confidence that the stated system, hardware, and software requirements specifications are complete, correct, consistent, traceable, unambiguous, and verifiable. As hardware becomes more capable and complex, and as systems are required to do more this issue will continue to be important. (One common complexity that is added to systems is self testing and diagnostics, which is discussed in section 3.2.5.)

Tasks

Investigate the experience and use of requirements specification assessment methods/tools used in other industries having high integrity systems. For example, methods/tools have been developed at the U.S. Naval Research Laboratory (SCR tool) and Safeware Engineering Corp. (SpecTRM tools) and used to assess the requirements of avionics systems. As part of the investigation, look at digital failure data to identify the most probable types of requirements specification errors. Assess the various methods/tools and provide recommendations for a method/tool which the NRC staff and licensees may use to review requirements specifications. Also, provide guidelines for the proper assessment of requirements specifications. To ensure that the recommended methods and tools are suitable for use with nuclear safety applications, conduct a pilot project using the requirements for a nuclear I&C system and the selected methods/tools.

Outputs

Technical report(s) will be developed which discuss and provide guidelines for the review of system, hardware, and software requirements specifications. The report(s) will also describe available methods/tools for assessing the correctness of specifications, make recommendations for NRC uses these methods/tools, and results of the pilot project. The report(s) will catalog and rank the types of requirements specification errors as found from digital failure data. The material in the technical reports will help the NRC make its activities and decisions more effective, efficient, and realistic by supporting the timely review of digital safety systems, particularly those that incorporate COTS systems. For example, the methods/tools identified in the proposed project would make NRC's activities more efficient by reducing the time and effort required to assess requirements specifications. In a typical digital system review of one staff year, it is estimated that use of requirements assessment methods/tools could provide a five to ten percent decrease in staff effort**.**

3.2.5 Diagnostics and Fault-Tolerance Techniques

Background and Issues

One of the unique features setting digital technology apart from analog technology is the enhanced capability to respond to internal faults, or problems. The facilities that detect internal faults are called diagnostics. Once the digital I&C system detects a fault, it can take appropriate action, such as alert the operator, avoid an unsafe situation by failing to a safe state, or attempt to correct the fault. These actions are commonly called fault-tolerance techniques.

The use of diagnostics and fault-tolerance techniques can improve upon the availability of digital safety systems. Many digital I&C systems, including those being placed in nuclear power plants, contain diagnostics and fault-tolerant techniques to detect and handle internal system faults. However, one of the issues behind these techniques is that they introduce a large amount of complexity to the system. With greater complexity, there is a greater opportunity for software errors. The NRC staff is concerned that software errors in the diagnostics and fault-tolerant techniques may prevent the safety functions from executing properly when called upon. Furthermore, the staff needs information on how to assess whether the diagnostics and fault-tolerance techniques are able to meet their claims. Being able to assess what the diagnostics and fault-tolerance techniques can and cannot do will help the NRC determine the amount of credit that an application can receive for increased availability claims.

Tasks

Investigate the best engineering practices and performance of digital diagnostics and fault-tolerant techniques. The results of the investigation will state the proper use of such techniques, including the types of faults they can recognize and act upon. The investigation will also provide recommended acceptance criteria for the design, test, and verification of diagnostics such that they will not interfere with safety function performance, and determine whether the complexity introduced by the fault tolerance techniques is compensated for.

Outputs

A technical report will provide the technical information and guidance that NRC staff needs when reviewing a digital I&C system that contains diagnostics and fault-tolerant techniques. The guidance and technical information will help meet NRC's goal of making its activities and decisions more effective, efficient, and realistic by improving the timeliness of digital I&C reviews. For example, by having guidance on how much credit to give COTS digital systems containing diagnostics and fault-tolerant techniques, the NRC staff will be able to form more realistic decisions on the acceptance of such systems.

3.2.6 Operating Systems

Background and Issues

Operating systems (such as Windows 98, NT, DOS, etc.) control most aspects of a computer's operation. For example, operating systems perform memory management, control certain

aspects of computer communication, schedule tasks on the processor, and provide an interface between the application programs and the computer hardware. In the past, operating systems for digital controllers were often custom programmed for the controller. The regulatory review of operating systems is becoming more difficult for two reasons. First, the computing capability of digital I&C systems is increasing, which in turn, causes the operating systems to become more complex. Second, many custom and COTS digital systems now contain COTS operating systems, versus custom-made systems. For proprietary reasons, the NRC and licensees are not able to access the COTS operating system development information which they typically use to determine software quality.

Operating systems control all aspects of a computer's operation making their quality critical to the computer's quality. Therefore, the NRC staff needs a technically sound and alternate method of determining operating system quality, in light of complexity and lack of adequate documentation. This area would be a possible candidate for a cooperative program, including cost sharing, with industry or other federal agencies that share this common concern.

Tasks

Investigate the characteristics and performance of operating systems (particularly COTS operating systems). In the investigation, perform the following steps: (1) examine past performance of operating systems and rank the causes of computer failures due to operating system failure; (2) determine and assess the possibility of using operational history of an operating system as an indication of its quality; (3) perform tests on several of the most widely used COTS operating systems to determine their strengths and weaknesses; and (4) identify the configurations and usage of operating systems that would minimize the potential for operating system-induced errors or failures.

Outputs

A technical report will provide the technical information and guidance that NRC staff needs when reviewing operating systems in digital I&C equipment. The results stated in the report will help the NRC meet its goal of maintaining safety at nuclear power plants. For example, the NRC staff will use the information in the report to identify those features and aspects of COTS operating systems that could negatively affect the safe operation of digital systems.

3.3 Software Quality Assurance

Software quality assurance is (1) a planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements, or (2) a set of activities designed to evaluate the process by which products are developed or manufactured (IEEE, 1991). The NRC currently has a set of software quality assurance activities identified in Chapter 7 of the SRP. While these activities satisfy the quality assurance requirements of 10 CFR 50, Appendix B, they are resource-intensive for both the NRC and the industry. For example, there are hundreds of acceptance criteria outlining the software quality assurance procedure. In addition, current guidance on software testing activities does not specify how these activities should be performed or how much testing should

be conducted. This leads to an inconsistency in the amount of testing and testing methods for similar digital I&C systems.

The following sections outline research tasks which explore the state-of-the-art for software quality assurance. The objective of these tasks is to identify methods, measures, and criteria that would provide both an objective and efficient method for software quality assurance.

3.3.1 Investigate Objective Software Engineering Criteria

Background and Issues

During the infancy of software engineering, it was difficult to assess software quality because it was impossible to test every possible input and condition that a digital system may encounter (NAS, 1997; USNRC, 1999a). As an alternative to complete verification and validation, software engineers relied upon the assessment of the software development process to determine software quality. The premise for this decision suggested that high quality software would result from a quality development process. In evaluating the software development process, software engineers would look at the way documentation was written, organization structure, procedures, and budget. The difficulty with evaluating software quality using this method is that (1) it is difficult to set a minimum acceptance level for process activities, (2) it is difficult to measure the process, (3) a high quality process does not necessarily guarantee quality software, and (4) it is often resource-intensive to review any but the most simple software systems. However, due to the limitations in software quality assessment techniques, this method became the state-of-the-practice and many industries, software certification groups, and regulatory agencies adopted this method, including the NRC.

As the software engineering discipline matures, various software quality assessment methods are being proposed as a way to determine software quality. These quality assessment methods attempt to measure software quality through the means of objective criteria and measures. For example, the number of defects (software errors) found during code inspections and testing is one measure that may be used to determine software quality. The benefit of using objective software measures is that it allows the development of minimum acceptance criteria that can be consistently applied to all software systems under review. Furthermore, to ensure that software quality has been achieved, the NRC staff only needs to check and see if the measurement procedures are correctly applied and the measurement results meet the minimum level of acceptance. In order to use software measures, the NRC must (1) ensure that the measurement technique provides a technically sound method for software quality assurance, (2) identify the minimum acceptance criteria, (3) identify the proper use of the measurement technique, and (4) ensure that it is applicable to the nuclear industry and our regulatory framework. While the objective criteria and methods will not determine that software is 100% error free, they possess the potential to increase the confidence in software quality while demanding fewer resources. As newer, more complex systems are added to ever increasing number of plant systems (including safety systems) this will create an ever increasing need for objective criteria to support the review and inspection of digital systems.

Tasks

The goal of this task is to increase confidence in software quality and decrease the average amount of effort (one staff year) for a digital system review by fifteen to twenty percent.

Phase 1: Investigate various objective criteria and software engineering techniques that hold the potential to be used as a software quality assessment method. For example, the Software Engineering Institute has developed two methods, Personal Software Process and Team Software Process, which use software measures to help improve the quality of developed software. From a number of experiments and applications, the methods appear to reduce the number of software defects by at least one-half the normal defect rate. Candidate software measures and techniques are to be analyzed in the following areas: (1) ability to show software quality and (2) can the measure be used in the nuclear industry and our regulatory framework. As a result of the investigation, recommend software measures (if possible) that could be used to indicate software quality. With the recommendation, provide minimum acceptance criteria that should be met for nuclear safety software and the guidelines for proper use of the measurement technique. Compare these methods and measurement techniques to approaches currently used to determine software quality (such as the Capability Maturity Model).

Outputs

A technical report will provide recommendations and criteria on the use of objective software measurement techniques as a software quality assessment method. If an adequate software measure is found, the technique will help the NRC in making its activities and decisions more effective, efficient, and realistic by reducing the amount of resources needed for digital I&C reviews, while maintaining safety. In contrast, subjective assessment of software quality increases unpredictability in the licensing process and requires additional review effort to consider the various factors that influence subjective assessment techniques.

Phase 2: Investigate various new methods for software measures and software validation and verification methods that present possible advantages over traditional methods.

Outputs

A technical report will provide recommendations on the feasibility of using this method for software quality metrics in the regulatory arena. If a method is found feasible, it would provide benefits to the NRC that are similar to the outputs of Phase 1 above.

3.3.2 Investigate Criteria for Software Testing

Background and Issues

Test coverage is the number of inputs and conditions tested compared to the total number of inputs and possible conditions.

Software quality assurance is heavily dependent on how software is tested. The quality of software tests are determined by the methods and test cases used. For example, most software is tested to see if it will perform the correct function when given the corresponding inputs and conditions. However, most software is not tested to see how it would handle

unexpected, but credible, inputs or conditions. Furthermore, most software is not tested to see how it would react in response to a software error or a hardware failure. Software testing experts recommend that these three types of testing be carried out on high integrity systems, which include digital safety systems in nuclear power plants (Voas, 1999).

The SRP outlines acceptance criteria for software tests, while RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," and RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," provide an acceptable method for carrying out software tests. While these documents specify the desired characteristics, process, and documentation for carrying out software tests, they do not indicate the test coverage or type of testing for minimum acceptance. The type of testing and the coverage are important parameters in software testing since they dictate what test cases will be exercised and the stopping condition for testing. Types of tests and test coverage have been dictated by other agencies and organizations. An example is the Federal Aviation Administration who lists test type and coverage criteria in DO-178B, “Software Considerations in Airborne Systems and Equipment Certification” (RTCA, 1992).

Tasks

Investigate software testing to determine the types of testing and test coverage required to achieve acceptable software quality. In particular, address the testing criteria for COTS software. Provide recommendations on the type of testing that should be executed, the test coverage, and the minimum acceptance criteria for the coverage. Conduct a pilot project on a complex nuclear I&C system to determine the effectiveness and amount of resources needed to implement the recommendations. This could be a candidate for cooperative research with industry.

Outputs

A technical report will describe which testing methods and criteria are best suited for software quality assurance purposes. The research results will help the NRC meet its goals of maintaining safety and reducing unnecessary regulatory burden by improving the consistency of regulatory reviews and the quality of submitted software. For example, if minimum criteria are established for the type and depth of software tests, there would be little variance in the level of regulatory scrutiny between two different systems that have been submitted for review.

3.4 Risk Assessment of Digital I&C Systems

As stated in the NRC's policy statement on the use of PRA, the NRC intends to increase the use of PRA technology in "all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data (USNRC, 1995)." Since I&C systems play an important role in nuclear power plant safety, and with the entry of digital technology, the need for digital risk assessment methods becomes more evident. A recent Accident Sequence Precursor (ASP) database study demonstrates the prevalence of embedded (digital) I&C components and its impact on plant safety. This database study is summarized in Appendix A, and it identifies the contribution of I&C failures to events with large increases ($> 10^{-5}$) in conditional core damage

probability. Several of the identified ASP events involved the failure of digital controls that were embedded in larger plant systems (e.g., circuit breakers, transformers, and diesel generators). Because of its prevalence and potential impact on plant safety, future risk-informed regulatory decisions are likely to involve the risk assessment of digital I&C systems.

NRR is interested in digital risk assessments because the NRC currently does not endorse, or possess the tools or methods, for quantitative risk assessment of digital computers or systems incorporating them in safety systems. RG 1.152, "Criteria For Digital Computers In Safety Systems Of Nuclear Power Plants," endorses IEEE Std. 7-4.3.2, "IEEE Standard Criteria For Digital Computers In Safety Systems Of Nuclear Power Generating Stations (USNRC, 1996; IEEE, 1993)." IEEE Std. 7-4.3.2 makes provision for quantitative goals for digital I&C systems. However, RG 1.152 states that "the NRC staff's acceptance of the reliability of the computer system is based on deterministic criteria for both the hardware and software rather than on quantitative reliability goals." Recently the NRC issued a revision to 10 CFR 50.59, which requires a license amendment if the modification results in more than a minimal increase in the frequency of occurrence of an accident or the likelihood of occurrence of a malfunction of a structure, system, or component (SSC) important to safety. Determining the frequency or likelihood of such events involving digital modifications, in any but a purely qualitative way, would require capabilities in digital system performance and reliability.

The objectives of risk assessment methods are to identify (1) the failures that can occur, (2) the impact of those failures, and (3) the frequency of those failures. The research in this area will provide the methods, tools, and criteria to meet these three objectives for digital risk assessment. The research issues center around digital failure assessment (what kinds of digital failures can occur and how they occur), risk-importance of I&C systems (impact of digital failures on plant safety), and digital reliability assessment methods (frequency of failures), and develop and analyze the data needed to support this work.

3.4.1 Perform Data Analysis on Digital I&C Failures

Background and Issues

Analyzing digital I&C failure data provides many helpful insights to the NRC. First, by analyzing I&C failures, the NRC can determine which digital failures would have the largest impact on plant safety and focus review efforts accordingly. Second, analysis of failure data also provides feedback on the effectiveness of NRC regulatory programs. Third, digital I&C failure data supports the risk assessment of digital I&C systems. However, there are several issues related to accessibility of the data, as follows:

Accessibility to meaningful digital I&C failure data: The first issue with analysis of digital I&C failure data is not necessarily the lack of data, but the inability to access the data with the current tools and means. For example, licensee event reports provide some clue to digital I&C failures, but often it is difficult to determine if it was a digital failure and what was the cause. Being able to access the root cause of the failure, its affects, and how it could have been prevented is the type of analysis the NRC needs to support the regulatory review and risk analysis of digital I&C systems. Most licensees keep a log of I&C failures which provides most of this information. Access to this information would prove beneficial to the nuclear industry as well as the NRC.

Accessibility to outside digital I&C experience: Another issue is the lack of knowledge concerning digital I&C performance in other industries. For example, the process industry uses similar COTS digital equipment that nuclear power plants use. If they have failure data, the NRC could utilize it to supplement the data from nuclear power plants. Another potential source of COTS failure data is the Department of Defense(DoD) and NASA. Both agencies have made a strong effort to implement COTS equipment in their high integrity systems. Some of the same COTS problems found in defense and aerospace systems may translate to nuclear systems. Using the experience of other industries would help the NRC in addressing potential digital I&C problems before they occur.

The NRC has conducted studies on I&C performance in nuclear power plants. One example is a reliability study on Westinghouse reactor protection systems(USNRC, 1999b). While these studies provide useful information on I&C systems, they do not address digital-specific failures. RES recently conducted informal data analysis on the ASP and LER databases and concluded that much of the detailed information on digital failures is lacking in the databases.

Tasks

The purpose of this task is to access data on digital I&C failures, either from existing databases or by constructing a database. The task consists of two parts, which involve gathering failure data from within and without the nuclear industry. In both parts, the collected data should be analyzed to identify the frequency, severity, cause, and possible prevention of digital I&C failures.

Part 1: Obtain digital I&C failure data for domestic and foreign nuclear power plants. This part of the task would be carried out by identifying both domestic and foreign sources that could provide digital I&C failure data. One example source is nuclear industry research groups. Coordinate with other research groups to centralize the data, appoint a custodian(s) over the data, and provide the data to NRC staff.

Part 2: Obtain failure data for COTS and embedded digital equipment belonging to industries that have I&C systems of similar safety and integrity level. Contact appropriate persons in those industries to access that data. Example industries include fossil power generation, petroleum, chemical, aerospace, and defense in addition to the nuclear industry.

Outputs

The output of this project is a database(s) for digital I&C failures, along with an analysis of that database. The databases will help the NRC make its activities and decisions more effective, efficient, and realistic by providing the NRC feedback on its regulatory programs involving digital I&C systems, provide insights into which failures are most significant from a safety standpoint, and provide supporting information to risk-informed decisions involving digital I&C systems.

3.4.2 Investigate Criteria for Digital Failure Assessment Methods

Background and Issues

A key part of risk assessment is the identification of potential failures and their impact on plant safety. Because of the complex design and operation of digital I&C systems, there is a large number of potential failures. However, not all of these failures are significant in terms of plant safety. For example, a digital reactor protection system may not be able to correctly time stamp an event, but if it is still capable of initiating a reactor trip at the moment one is required, then the digital failure is not safety-significant. When looking at a digital I&C system as a "black-box" in the plant PRA, the primary concern is that the digital system perform on demand, complete its safety function, not prevent the function from happening, not perform unintended functions, and not initiate its safety functions until they are required (no spurious operation). Therefore, when the risk assessment of digital I&C systems is performed, those failures that affect the safety function are of most interest. Once those failures are identified, it is necessary to understand how they impact the safety function. Identification of the critical digital failures and their impact provide the first two steps in risk assessment of digital I&C systems.

Licensees are currently required by 10 CFR 50.55a(h) to perform an analysis of the I&C system in the event of a single failure and a design basis event. With digital I&C systems, proof of the single failure criterion is difficult since it is difficult to prove the absence of any software errors which may affect redundant safety channels and trains. Using a defense-in-depth and diversity analysis, it is often assumed that the digital safety system has failed, and an analysis is performed to show that the plant can handle the digital failure. However, this type of analysis does not provide the information required for risk assessment of digital I&C systems because it does not identify the failures within system, or how the failure might affect other systems. Therefore, the research issue is the identification of digital I&C failures, how they arise, and their impact on the required safety functions.

Tasks

Identification of digital I&C failures can be performed either through data analysis or by analytical means. By analyzing data, potential digital failures are recognized since most failures have occurred in other systems. While some failures may not be applicable to the digital system under analysis, those identified through data analysis provide a baseline in the identification process. The tasks listed under the section, "Data Analysis and Lessons Learned," will identify potential digital failures and their impact on system functionality.

Digital failures are also identified through analytical means. There are various analytical methods to identify digital failures and their impact on plant safety. Some of the common methods include hazard analysis, failure modes and effects analysis, fault tree analysis, and operability analysis. At this time, the guidance and criteria on the use of these methods (depth of analysis, scope, etc.) and how they might be used to support digital risk assessments is not defined.

Part 1: Survey the analytical methods for identifying digital failures and their impact on safety. For each method document the advantages and disadvantages of using that method.

Part 2: Provide recommendations for a digital failure assessment technique(s). Also, provide criteria for using the technique(s) and applying them to digital risk assessments.

Part 3: Conduct at least two case studies using the recommended digital failure assessment technique(s). The case studies will determine (1) the amount of effort associated with the proposed criteria and methods, (2) the effectiveness of the criteria, and (3) the suitability of the criteria and methods to nuclear applications. Following the case studies, necessary adjustments to the proposed criteria will be made. Digital safety systems for nuclear power plants are to be used in the case studies.

Outputs

Task results will be published in a technical report. The proposed criteria for identifying digital failures and their impact will be included in a RG. This RG will provide an acceptable method for digital I&C risk assessment. The results of this task provide an acceptable means to carry out part of the digital I&C risk assessment process, and it identifies the level of detail the NRC would expect in licensee submittals. The results published in the report help the NRC make its activities and decisions more effective, efficient, and realistic since a consistent method for identifying digital failures would help the NRC staff easily recognize those failures that have greater impact on plant safety versus those that have little impact.

3.4.3 Identify the Risk-Importance of Digital I&C Systems

Background and Issues

A large number of I&C systems exist within nuclear power plants, but only a portion are important in terms of risk. It would be helpful to determine the risk importance[2] of I&C systems for two reasons. First, risk importance helps determine the required level of regulatory review. In situations where the I&C system is not risk important, less review effort is applied. It will also help focus research efforts on the aspects of those digital I&C systems having a significant impact on plant safety. Second, risk-importance identifies those I&C systems that are significant in terms of risk, but may be overlooked. This situation is particularly true of digital systems embedded in circuit breakers, diesel generators, and other plant systems/components.

The risk-importance of I&C systems has been looked at in part by general risk studies (i.e., individual plant examinations) and reactor protection system studies (USNRC, 1999b). While the studies identify the risk associated with some of the major I&C protection systems, they do not sufficiently look at I&C systems across the plant (including those embedded in larger plant systems). While the capability exists to determine the risk significance of I&C systems, only informal work has been performed to date. Therefore, the research issue consists of modeling I&C systems (where models do not exist) and calculating the risk-importance of I&C systems, including those that are embedded in larger, risk-important plant systems.

Tasks

Phase 1, Part 1: Identify and develop necessary risk models of I&C systems. Identification of I&C systems can be performed through the analysis of piping and instrumentation diagrams and other technical information on plant systems. One avenue that would identify embedded

[2]Risk importance is determined independent of whether the I&C system is analog or digital. Risk importance is dependent upon the I&C system's function and the plant configuration.

I&C systems, particularly those that are digital, would be to use systems identified as part of the Y2K assessments at nuclear power plants. Since the design and layout of nuclear power plants vary, the calculation of risk importance will be performed on a generic basis by using the NUREG-1150 plants or another group of reference plants. The approach is to utilize a complete PRA of several plants as a baseline. Identification of I&C systems would be performed on a generic level according to plant type. If an identified I&C system does not exist in a plant PRA model, establish and document the necessary assumptions in order to calculate the risk importance as if it were in the plant PRA. Risk models only need to be developed to the point where the I&C system is a "black box."

Phase 1, Part 2: Calculate the risk importance for generic I&C systems in nuclear power plants. By treating the I&C systems as a "black box," determine the change in plant risk if the I&C system fails. All credible digital failure modes are to be considered.

Phase 2: Some of the high risk-important I&C systems may be large or complex in nature. In such cases, develop the I&C risk models beyond the "black box" level in Phase 1. By developing the I&C risk models beyond the "black box" level, the NRC is better able to identify sub-components of I&C systems that may warrant special regulatory and/or research attention.

Outputs

The results of the risk-importance study will be documented in a technical report. This report will be used by NRC staff involved in both I&C and PRA reviews and will help the NRC make its activities and decisions more effective, efficient, and realistic. For example, as licensees conduct more digital modifications for safety systems, the NRC staff will be able to adjust the depth of their reviews and better allocate resources to those digital modifications having the highest risk importance. From a PRA perspective, knowing the risk importance of I&C systems will help determine the level of detail required for I&C models. The results support future research efforts by pointing to risk important areas and issues.

3.4.4 Investigate Digital Reliability Assessment Methods

Background and Issues

The third part of digital risk analysis is determining the likelihood of failure for a digital I&C system. Since I&C systems play a key role in the operation of safety systems (and therefore impact plant risk), occasions will arise in which the reliability of digital systems needs to be evaluated. First, data for analog safety systems is not necessarily applicable to digital safety systems and, therefore, that data cannot be used to estimate the reliability of digital safety systems. The data cannot be used because the two systems operate and fail differently. The reliability of digital components may or may not be better than analog components but, digital equipment is more complex in design, offering a greater potential for design errors.

A second reason for evaluating the reliability of digital systems involves the reduction of uncertainty in plant PRAs. RG 1.174 “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the licensing Basis,” mentions two types of uncertainty, aleatory and epistemic uncertainty. Aleatory uncertainty involves the

randomness of events, and epistemic uncertainty involves, to a degree, a lack of knowledge about the PRA model and its parameters. Therefore, epistemic uncertainty can be reduced by gaining knowledge about the PRA model and its parameters. Current plant PRAs do not model the majority of I&C systems, but include them within other plant systems. To reduce the epistemic uncertainty associated with plant PRAs, it may become necessary to model and estimate the likelihood of I&C failures.

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

Industry and academia have worked to develop digital reliability estimation methods. Some of the basic methods estimate digital hardware reliability using available data and then estimate software reliability according to software test results. The hardware and software reliability are then added to generate a digital system reliability. Other methods consider both the hardware and software as an integrated unit in order to account for their interactions and dependencies. At present, the NRC does not have standard methods for determining the failure probability of digital I&C systems. If these standard methods were available the evaluation of new technology would be simplified and the review of systems could be generalized to a greater extent. The challenge for the NRC is to identify digital reliability assessment method(s) that (1) provide adequate model completeness, (2) do not require an excessive amount of effort, and (3) can be applied to digital equipment in nuclear safety systems, particularly commercial off-the-shelf equipment. The research issue is identifying methods for determining the likelihood of failure for complete digital I&C systems (hardware and software). The acceptance criteria for using those methods needs to be identified also.

Tasks

Since digital reliability assessment is state-of-the-art, the proposed task is phased and expected to be a several year effort. The NRC has already begun work on these tasks through the cooperative agreement at UVa. By participating in the cooperative agreement, the NRC is able to better leverage its resources to achieve the desired outputs, and it is able to tap into the experience and knowledge gained by academia, other government agencies, and industry.

Phase 1: The following activities are planned through UVa cooperative agreement: Identify digital reliability assessment methods and analyze their benefits and shortcomings (i.e., judge according to effectiveness in estimating digital system reliability and effort required for assessment). During this phase, there may arise a need to further develop some of the promising reliability assessment methods to a state that would be suitable for NRC use. In

particular, reliability assessment methods should be developed to the state where they can handle commercial off-the-shelf equipment. Case studies involving nuclear applications should be used to identify the suitability and required modifications to the identified reliability assessment methods.

The following activity will not be performed as part of the cooperative agreement: Investigate software reliability measures which may be used to calculate digital I&C system reliability. In particular, consider how software reliability measures would be incorporated with hardware reliability to arrive at a digital system reliability.

Phase 2: The following activities are planned through the UVa cooperative agreement: Recommend a digital reliability assessment method(s) suitable for nuclear power plants. Along with the recommendation, provide guidelines and acceptance criteria for using the identified method(s). Before the second phase is executed, results of the first phase are assessed to determine the probable success of using the identified methods. Perform a pilot project using the recommended digital reliability assessment method(s) to determine its applicability to nuclear systems, its effectiveness at determining reliability, and its ease of use.

Outputs

The results of these tasks will be a series of technical reports describing digital I&C reliability assessment methods and their acceptable use. The guidance and acceptance criteria for digital reliability assessment methods will be included in the RG that states an acceptable method(s) for digital risk assessment. The results of these tasks will prepare the NRC for risk-informed regulatory activities and decisions by: (1) supporting the review of digital risk assessments, (2) allowing the calculation of risk change associated with digital I&C upgrades, and (3) providing the capability to reduce plant PRA uncertainty where digital I&C systems play a significant role in safety. By meeting these three points, the results of this task will help the NRC make its activities and decisions more effective, efficient, and realistic. For a typical digital system review of one staff year, the NRC estimates that it may be able to reduce staff review effort by 20 to 30 percent using the research information gained in the above mentioned tasks.

3.5 Emerging I&C Technology and Applications

New innovations in the area of digital I&C technology have the potential to help nuclear power plants in both operating efficiency and safety. As an example, a licensee recently requested a power uprate based on an advanced flowmeter (leading-edge or ultrasonic flowmeter). When the nuclear power plants were constructed, a two percent safety margin was applied to the operating power limit because of inaccuracies in measuring and calculating reactor power. Based on the improved accuracy of the advanced flowmeter, the licensee claimed that the power operating limit design margin could be reduced by one percent. Many other new technology and applications of established technology will be proposed for introduction into nuclear power plants in the future. As part of this research, those areas that have been shown to be likely to be applied in plants in the future and areas of research that have the potential to raise safety issues but have not yet been addressed are included in this area of research. By becoming informed of the design, operation, and reliability of emerging I&C technology and applications, the NRC is better prepared to make future regulatory decisions in these areas.

3.5.1 Review of Future Applications of Digital I&C and Research Infrastructure

Background and Issues

As discussed in the introduction, the rate of change of technology in the area of digital systems is a significant challenge to the NRC's capability to keep current, and to be prepared to effectively and efficiently regulate digital systems. Because of the speed at which entirely new systems are developed and fielded and because of the new capabilities in hardware and software that can make methods more feasible, it is important that the NRC engage in research in this area to understand the application of these emerging technologies and applications. The other parts of this section address specific areas that have been identified as probable areas in which new reactor applications will emerge. The research object for this area includes activities that are needed to keep current with the state-of-the-practice in the areas of digital system reliability, systems analysis, and quality. An important part of this research is the identification of new research areas. These areas will be developed into new programs, as it becomes apparent that identified technologies will probably be used in U.S. nuclear reactors. Keeping up with the state-of-the-practice involves three aspects. First, developing and maintaining contact with the industrial, academic and regulatory communities and maintaining technical capabilities within the staff. In section 4 “Interactions and Interfaces with Relevant Digital I&C activities” the work that will be done to develop and utilize information from other areas and sources are discussed in detail. The second aspect is participation in the consensus standard’s area. Additionally, work in this area will include coordination with other NRC activities, such as the Human Performance Plan and the PRA Implementation Plan. The third aspect is active review of new technology to determine what technology might be used in future digital I&C applications and the development of the RES technical staff.

Tasks

Phase 1 Develop and maintain interactions and interfaces with the industrial, academic and regulatory communities with relevant digital I&C applications. This will include formal and informal interactions with the organizations listed in section 4. It will also include development of information sources and exchange of information as recommended in the National Academy of Science report (NAS, 1997).

Outputs

Reports and information on how other industries and organizations regulate digital systems for safety critical applications allows us to learn from their experience. Applying those lessons-learned to our regulatory structure helps the NRC meet its goal of making its activities and decisions more effective, efficient, and realistic.

Phase 2: Participate on national and international standards working groups and committees to develop and update standards (This will include IEEE Standard. 1498, IEEE Standard. 603, IEEE Standard 384, IEEE Standard 1012, IEEE Standard 7-4.3.2, etc.). Revise existing RGs, as appropriate to endorse updated standards.

Outputs

The staff will actively participate in consensus standard organizations and revise existing RGs referenced in SRP Chapter 7, to incorporate revisions of IEEE and other standards. Again, these activities will help make NRC's activities more effective, efficient, and realistic.

Phase 3: Review new technology as it becomes available by (1) obtaining new tools and methods for trial use by RES staff; (2) attend professional meetings; and (3) develop new technical capabilities and knowledge through training.

Outputs

Periodic reports on the status of emerging technology in the digital area will be issued and used to determine when new areas should be developed for research. An additional output will be a more technically capable staff. Again, these activities will help make NRC's activities more effective, efficient, and realistic.

3.5.2 Predictive Maintenance/On-Line Monitoring

Background and Issues

New digital I&C systems are being developed which have the capability to automatically determine system/component failure or the need for maintenance. For example, some systems can detect an eventual bearing failure in a pump by monitoring the pump's vibrations. Other systems are capable of monitoring safety signals and determining when a protection channel is drifting out of the allowable tolerance.

Predictive maintenance and on-line monitoring systems have the potential to alter surveillance and maintenance practices at nuclear power plants. For example, in one type of on-line monitoring system, if an instrument fails, the system can create an artificial signal from other plant variables. The potential implication is the ability to use the artificial signal until the next refueling outage when the instrument can be replaced. Such an implication would save licensees from having to shutdown the plant in order to repair an instrument. Other examples that would impact regulatory decisions include the ability to perform maintenance when it is required and not on a scheduled basis. An in-house ASP database study showed that maintenance errors resulted in approximately 27% of I&C failures. If maintenance activities were reduced to only those systems requiring maintenance, there is a potential improvement in plant safety. The NRC needs to understand the characteristics of preventive maintenance and on-line monitoring systems to determine the best way to inspect and license these systems.

Tasks

Provide technical information on predictive maintenance and on-line monitoring systems, identify the best engineering and operational practices of such systems, and provide appropriate review guidelines. Specifically, identify the advantages and the potential negative safety impacts of using such systems.

Outputs

A technical report will be provided that helps NRC staff evaluate the safe use of predictive maintenance and on-line monitoring systems. The report would support the NRC's goal of making its activities and decisions more effective, efficient, and realistic and reducing unnecessary regulatory burden by enhancing the ability to make timely regulatory decisions and remove uncertainty in the licensing process. For example, predictive maintenance techniques may lead to changes in maintenance practices at nuclear power plants. The report would prepare the NRC to make timely decisions on the degree of confidence that can be placed on such automated techniques.

3.5.3 Advanced Instrumentation

Background and Issues

The introduction of advanced instrumentation for measuring flow, temperature, pressure, neutron flux, and other plant variables hold the potential to improve upon plant efficiency, safety, or both. For example, obtaining the capability to accurately map the neutron flux distribution in a PWR using the incore instruments may provide the potential for power uprates. As mentioned earlier, the use of an advanced flowmeter over the venturi flowmeter provided the ability to request a power uprate. To make timely and informed regulatory decisions involving advanced instrumentation (e.g., power uprates), the NRC needs the technical bases surrounding this emerging technology.

Tasks

Investigate advanced instrumentation that is expected to enter nuclear power plants and identify characteristics that either enhance or degrade safety. Provide review guidelines for licensing such systems.

Outputs

A series of technical reports will aid the NRC staff in the safety evaluation of plant and technical specification modifications involving advanced instrumentation. The report would support the NRC's goal of making its activities and decisions more effective, efficient, and realistic and reducing unnecessary burden by enhancing the ability to make timely regulatory decisions and remove uncertainty in the licensing process. For example, licensees may submit power uprate requests based on the accuracy of advanced instrumentation. The report would prepare the NRC to make timely decisions on the degree of accuracy that advanced instrumentation can achieve.

3.5.4 Smart Transmitters

Background and Issues

Smart transmitters provide much of the computational capability currently found in controllers. For example, some transmitters can provide feedback control for simple control systems. Smart transmitters are also capable of communicating over digital networks to other computers. The advantages that smart transmitters bring include (1) decreased number of I&C components and wiring (due to the consolidation of I&C functions currently performed by controllers and

other I&C equipment) and (2) the potential for higher accuracy by taking into account instrument characteristics and other error factors. While smart transmitters provide several benefits, the NRC must determine the capability of these instruments to perform in a nuclear environment. For example, could the transmitters operate within containment, particularly during post-accident situations? How reliable are the smart transmitters compared to the transmitters used today? These questions and others face the NRC as smart transmitters move into nuclear power plants.

Tasks

Investigate smart transmitters and provide technical information on such systems, their application in nuclear power plants, and their potential impacts on safety. In particular, provide the following information:

Provide a general description of smart transmitters in terms of type, functions, operation, installation, and maintenance.

- Identify the acceptable operating environment, reliability, and failure modes of smart transmitters through tests and data. Make maximum use of vendor data where possible.
- Provide review guidelines for licensing smart transmitters.

Outputs

The output of this task is a report containing smart transmitter descriptions, reliability, acceptable operating environment conditions, and failure modes. The technical bases and review guidelines gained from this task will help the NRC make its activities and decisions more effective, efficient, and realistic by preparing the NRC to make timely regulatory decisions regarding smart transmitters. For example, the report would help NRC staff identify potential I&C architecture changes, using smart transmitters, that would eliminate defense-in-depth measures originally built into the plant.

3.5.5 Wireless Communications

Background and Issues

Wireless communication systems are being used in industrial settings today to reduce the amount of wiring and increase the transfer rates for data. If wireless communications could be successfully used in nuclear power plants, it would reduce the large amount of cables and the issues associated with them. Most wireless communication systems utilize commercial communication protocols, which allow the transmission of large amounts of data.

Although wireless communication systems hold many advantages over current cables, their reliability in a nuclear power plant environment is questionable. For example, how would wireless communication systems perform in accident situations? Also, how would the security and quality of the data transmission be ensured? The NRC staff requires technical knowledge and an understanding of those wireless communications aspects that will impact the safe operation of nuclear power plants.

Tasks

Investigate the design, operation, and failure mechanisms of wireless communications and provide appropriate review guidance to the NRC staff.

Outputs

A technical report will be published to support NRC review efforts when wireless communications are concerned. The report will help the NRC make its activities and decisions more effective, efficient, and realistic and reduce unnecessary burden by providing the technical information that supports timely regulatory decisions and alleviate licensing uncertainty.

3.5.6 Firewalls

Background and Issues

Recent attacks by hackers preventing access by overloading commercial sites and penetrations into secure DoD computers illustrate the potential for hackers to cross firewalls and corrupt data stored in computers. This ability poses a potential threat to nuclear power plant safety and security because plant computer systems are not isolated from the outside world. For example, communication outside the plants is provided to key personnel such as the plant manager via modems and computer networks.

Tasks

Investigate on-going worldwide efforts to develop preventive design techniques and develop appropriate review guidance for identifying vulnerabilities to the NRC staff.

Outputs

A technical report will be published to support NRC review efforts when communication from outside nuclear power plant boundaries is permitted. The information in the report will help the NRC meet its goal of maintaining safety by identifying potential access routes to computers and providing information on computer security techniques.

4 INTERACTIONS AND INTERFACES WITH RELEVANT EXTERNAL DIGITAL I&C ACTIVITIES AND ASSOCIATED ACTIVITIES

4.1 Objectives

The application of digital I&C technology extends far beyond nuclear power plants. Indeed, today one can find many process industries that include nothing but digital I&C and have gained a substantial amount of experience developing and using the technology. The staff intends to tap this resource to the extent possible in order to leverage its research dollars. In doing so, the staff hopes to identify and acquire products of research in other industries that can support the NRC mission, and would otherwise require an investment of NRC resources to develop. In addition, the staff will investigate potential opportunities for collaborative efforts and pilot projects with parties that share a common goal with the NRC. Such efforts in areas other than digital I&C have been helpful in the past in reducing the cost and lead time for achieving research goals. Reducing lead time for digital I&C research projects is especially important because a nuclear industry decision to modernize I&C could come at any time and with it, a high volume of requests for NRC review and approval of new instrumentation infrastructures to support a digitally monitored and controlled plant, as well as replacement of specific analog I&C components with digital versions. Last, the staff will investigate the types and sources of training and expertise the NRC will need to address emerging technologies that are likely to require NRC review and approval in the future.

4.2 Potential Contacts

4.2.1 Federal Agencies

With the introduction of its *Information Technology for the Twenty-First Century* initiative, the executive branch of the federal government has proposed a dramatic new commitment to research in information technology [NSTC, 1999]. This is a multi-agency information technology research initiative that increases federal investment in a number of areas including the development of reliable software for high confidence and safety-critical applications, security of software systems, human-computer interaction and fundamental research on emerging technologies. The following agencies each play a major role in this program: National Aeronautics and Space Administration (NASA), National Science Foundation (NSF), Department of Energy (DOE), Defense Advanced Research Projects Agency (DARPA); as such, they represent a potential resource for NRC's digital I&C research program. Other federal agencies that are potential resources for the NRC include those charged with regulation of potentially hazardous products and services that are produced or implemented with the aid of digital technologies, such as the Federal Aviation Administration (FAA), the Federal Railroad Administration (FRA) and the Food and Drug Administration (FDA). These agencies are faced with challenges similar to those faced by the NRC; namely, to develop processes that allow regulators to make an objective determination of the acceptability of safety-critical applications of digital I&C. The staff will review and assess the work of these agencies with the objective of identifying on-going research that supports the NRC’s research goals, and determining if joint research is appropriate.

4.2.2 International Organizations

For over ten years the NRC has been interacting regularly with international organizations who also have a stake in the performance of digital I&C in nuclear power plants. These contacts include regulatory authorities and nuclear electricity producers in other, countries as well as umbrella organizations such as the OECD Nuclear Energy Agency (NEA), the International Atomic Energy Agency (IAEA) and the OECD Halden Project. One international contact of particular interest is the Swedish Nuclear Power Inspectorate (SKI). They have approved the use of a programmable protection system in the Ringals plant that is considered to have complete functional diversity in that each protection channel is performed by a distinct processor [Dahll, 1998]. The staff is interested in gaining a full understanding of the benefits of a multiprocessor design over a single processor design and any unique technical issues associated with the safety review of a multiprocessor design.

4.2.3 Academic Institutions

Research in the many facets of digital technology can be found at the engineering colleges of most major universities. Some of the work is funded by government agencies such as DARPA, DOE, NSF and NASA, some is funded by private organizations and the remainder by the universities themselves. The staff is currently engaged cooperatively with the University of Virginia (UVA), and is following the work of other universities, such as the University of Maryland. UVA has number of research projects that relate directly to the issues the NRC faces in evaluating the acceptability of digital I&C systems and components in safety-critical applications, including: (1) methods and tools for software reliability analysis using fault trees; (2) development of a fault simulation methodology for the validation and verification (V & V) of safety-critical systems and application of the methodology in development of an embedded control system for the railway industry (see section 4.3.2.1).

4.2.4 Nuclear Industry Organizations

The staff continues to interact publically with the Electric Power Research Institute (EPRI) I&C Steering Committee. At a recent meeting for the exchange of operating experience, the benefits of a joint EPRI, DOE and NRC workshop on digital I&C research activities was discussed. One strategy for such a workshop, would have each of the three groups present their research plans with the goal of identifying common areas that could be addressed with joint research activities. All representatives at the meeting agreed to raise the idea within their respective organizations for further consideration.

4.3 Topical Areas

4.3.1 Data Analysis

4.3.1.1 Activities in Other U.S. Government Agencies

The staff recognizes that the Department of Defense (DOD) has considerable experience with COTS software in its high integrity software applications. As discussed in section 3.4.1, the staff will make contact with DOD with the intent of collecting applicable experience/failure data that can be used in reliability and risk assessments of digital I&C systems.

4.3.1.2 Activities in Other Countries

The NRC staff will continue its ongoing activities involving the exchange of operating experience involving digital systems. These exchanges involve foreign regulatory authorities with which we have bilateral agreements (e.g., France, Canada, etc.) and umbrella organizations such as OECD/NEA and OECD Halden Reactor Project.

4.3.1.3 Activities in Other Industries

Both COTS software and embedded software in digital equipment are used extensively in other process industries, such as fossil power generation, petroleum processing and other chemical processing. As discussed in section 3.4.1, the staff will investigate activities in other process industries with the intent of collecting applicable experience/failure data that can be used in reliability and risk assessments of digital I&C systems.

4.3.2. Software Quality Assurance

4.3.2.1 Activities in Other U.S. Government Agencies

The U.S. government is a heavy user and developer of high integrity and safety-critical software and has issued a number of standards for software development over the past ten years (See Table 4.1). The staff intends to contact some of these agencies to see what their experience has been in implementing these standards, with emphasis on the methods and criteria used to assure quality. This will be done in addition to the ongoing standards work that is described in section 3 of this Plan.

Table 4.1 Standards for Development of Safety-Critical Software

Topic	Sponsor	Reference
software used in safety systems in nuclear power plants	International Electro technical Commission (IEC)	IEC 880, 1986
system safety program requirements	U.S. Department of Defense (DOD)	MIL-STD-882B, 1984
development of software safety plans	Institute of Electrical and Electronics Engineers (IEEE)	IEEE Standard 1228-1994
software system safety	U.S. Air Force Boeing Corp.	AFISC SSH 1-1, Sept. 1995
QA programs for software used in critical applications	Canadian Standards Association (CAN)	CAN/CSA-Q396.1.2-89
guidance for computer controlled medical devices	U.S. Food and Drug Administration (FDA)	FDA 91

software in general industrial safety-related systems	IEC	IEC/TC65A WG9, IEC 65A, Ver. 1, 1991
analysis of safety-critical hazards	Ministry of Defense, UK	Interim Defense Standard 00-56, April 1991
security requirements for COMSEC software development	U.S. National Security Agency (NSA)	NSA Spec. 86-16
software systems safety design	U.S. Naval Surface Warfare Center (NSWC)	NSWC TR 89-33, 1989
software reliability and safety in nuclear reactor protections systems	U.S. Nuclear Regulatory Commission	NUREG/CR-6101, 1993
software in protection and control systems	Atomic Energy Control Board, Canada (AECB)	Draft RG C-138, 1996
criteria for digital computers in safety systems of nuclear power plants	U.S. Nuclear Regulatory Commission	RG 1.152, Rev. 1, 1996.

U.S. research and development activities in the area of software engineering and high confidence software systems are being pursued under the President's FY 2000 *Information Technology for the Twenty-First Century* initiative. A core group of government agencies will conduct this research, including DARPA, DOE, NASA and NSF. The staff will establish points of contact in these agencies in order to follow this work and evaluate its usefulness in meeting NRC research goals.

National Aeronautics and Space Administration (NASA)

NASA's goal regarding the development of high confidence software is "behavioral predictability", i.e., no surprises [CCCIC, 1997] To achieve this goal, they place heavy emphasis on testing by designing testability into the product from the start and then testing comprehensively throughout the development process. NASA is also considering the usefulness of automated tools for software V&V and ways of removing human errors in software development by making modeling activities formal syntactic processes. Such practices are not specifically identified in current NRC standards. The staff's interest in these practices is in support of potential regulatory improvements. NASA appears to be an especially good resource with respect to software quality because (1) they have experience developing and assuring the quality of safety-critical software and evaluating appropriateness of COTS in safety-critical applications; (2) they use their own technical standards that address safety in more detail than IEEE standards. Their experience and the lessons learned from their experiences represent potentially valuable resources for the NRC in preparing to meet the potential challenge of a nuclear industry modernization that includes a substantial amount of software-based control.

Federal Railroad Administration (FRA)

Given today's research activities, future railway systems may eventually become totally automated with distributed computer systems performing train routing, signaling and switching and train velocity and acceleration control. Clearly, such systems must perform their hardware and software operations in a safe manner. In the railway industry, the quality of safety-critical software is assured via extensive testing and simulation of a train control system The staff is currently following work at UVa on verifying newly developed fault-tolerant architectures and modeling techniques in the design of advanced rail systems for Union Switch and Signal, Inc. The techniques developed by UVa for ensuring digital system safety include a design process that involves simulation of the hardware and software behavior in the presence of software- and hardware-based faults inserted into the simulations. These simulations are an integral part of the design process – not a one time effort that is done at the end of design. UVa has also developed a technique for assessing the ability of the completed design to safely tolerate faults and verified the technique with testing on the as built system for Union Switch and Signal. The staff intends to initiate contact with the FRA and its licensees to better understand the factors motivating considerable investment in these technologies. In addition, the staff is currently funding research at UVa to better understand how their assessment method could be applied in safety assessments of digital systems proposed for new or modernized nuclear power plants.

4.3.2.2 Activities in Other Countries

Canada (AECB, AECL and Ontario Hydro)

Canada's Atomic Energy Control Board (AECB) licensed a computerized shutdown system at AECL'S Darlington plant operated by Ontario Hydro. Ontario Hydro used formal methods to verify the consistency of the software and the requirements and also used a large number (7000) of tests randomly chosen to model one of six accident scenarios to provide a measure of the system's reliability. The use of formal methods and random testing offer potentially greater objectivity in assuring the acceptability of software that can impact nuclear safety . The use of such practices is not specifically identified in current NRC standards; and accordingly, the staff's interest in these practices is in support of potential improvements in RGs. Proposed NRC research on software testing is described in section 3.3.2 of this plan.

Halden Reactor Project

The OECD Halden Reactor Project (HRP) is an international institution with participation from 19 countries. A main research topic over the last twenty years has been software dependability. Particular emphasis has been placed on software in safety critical systems. Recently, HRP produced a guideline for reviewing and assessing safety critical software in nuclear power plants for the Swedish Nuclear Power Inspectorate (SKI). These guidelines were applied in the licensing of the exchange of an analog protection system with a functionally equivalent programmable system in the Swedish nuclear power plant Ringhals. In addition, the HRP has developed a formal method for software development that can be applied in the development software requirements specification and the software design. The staff's interest in these practices is in support of potential improvements in NRC RGs. Proposed NRC research in the area of assessment of software requirements specification is described in section 3.2.4 of this plan.

4.3.3 Risk Assessment

4.3.3.1 International Activities

OECD Nuclear Energy Agency

Principle Working Group 5 (PWG5) of the NEA/CSNI is currently developing a proposed set of activities related to the use and licensing of programmable systems in safety critical applications. If approved by member states, these activities may include a survey of experience and practices in member states regarding the use of programmable systems in nuclear power plants. The scope of this survey would cover operating experience with programmable systems, guidelines and procedures in place for using such systems, and experience in using probabilistic risk assessment techniques to evaluate the risks associated with using programmable systems in nuclear power plants. As a member of PWG5, the RES representative will stay abreast of the experience and practices at nuclear facilities and among safety experts in NEA member countries as they might apply to research at the NRC in the areas of reliability and safety assessment of digital systems.

OECD Halden Reactor Project

One activity at the Halden Reactor Project (HRP) of particular interest to the staff is the work they have done together with ABB-Atom of Sweden and the VTT Corp. of Finland exploring new probabilistic techniques for assessing software quality. Recent advances in technology have lead to techniques for building large logic models using data and information from the software development process to compute a figure-of-merit that can be associated with the software development process. This work includes an investigation of applying these techniques in the evaluation of COTS software. The staff is interested in this work because it offers the potential for a more objective method for evaluating COTS software than that referenced in current NRC standards.

5 SCHEDULE

The schedule for the research that will need to be done to accomplish the goals of the program are outlined in this section. A short summary of the tasks and outputs discussed in section 3 has been provided as part of the schedule for the work to make it easer to reference back to the detailed discussion of the work in section 3.

The most recent user need request for research in this area is "User Need for Digital Instrumentation and Controls Research" Memorandum to Ashok C. Thadani, from Samuel J. Collins, February 29, 2000.

Schedule for Research Activities

In prioritizing the research, described in section 3, as part of the Planning Budget and Performance Management process the NRC strategic performance goals were used as to determine what projects would be assigned resources and in what priority as input to the RES prioritization process. Each program area discussed below includes a priority, and an indication as to how that priority was established (for example an NRR user need).

For each of the tasks in section 3, a schedule has been developed based on the process described above with the start dates or anticipated start dates for work on the projects and the anticipated resource and completion dates. The process for the scheduling of the research activities uses four criteria. In order of importance they are; (1) regulatory need (as evaluated for stakeholder input, primarily NRR user needs), (2) dependance of activities on one another, (3) time needed to complete the research, and (4) completion of needed work that has already been initiated.

The research products will include review guidance for emerging technology, new methods and models for assessing digital system reliability, qualification guidelines for environmental stressors, and software assessment methods.

Systems Aspects of Digital Technology (3.2)

Verify EMI/RFI Qualification Levels (3.2.1)

Task A: Re-evaluate nuclear power plant EMI/RFI data and make necessary adjustments to the regulatory guidance.

Output: Revision of Reg Guide 1.180

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY00 **Completion Date:** 3Q FY02 **Current Activity:** Yes

Task B: Investigate EMI/RFI conduction through I&C signal lines and include appropriate standards into the regulatory guidance to include conducted EMI/RFI susceptibility.

Output: Revision of Reg Guide 1.180

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY00 **Completion Date:** 4Q FY01 **Current Activity:** Yes

Task C: Investigate the potential for endorsing the new IEC consensus standards on EMI/RFI qualification.

Output: Revision of Reg Guide 1.180

Priority: High priority (NRR user need (2000-6))

Start Date: 1Q FY01 **Completion Date:** 4Q FY01 **Current Activity:** Yes

Complete Environmental Qualification Guidelines (3.2.2)

Task: Complete current work on developing environmental qualification guidelines.

Output: A RG on environmental qualification of digital I&C equipment

Priority: High priority (NRR user need (2000-6))

Start Date: 1Q FY98 **Completion Date:** 4Q FY01 **Current Activity:** Yes

Develop Lightning Protection Guidelines (3.2.3)

Task: Research is currently planed to investigate lightning protection practices and standards and develop/incorporate applicable guidance.

Output: A RG on lightning protection to provide needed guidance to the NRC staff and nuclear industry.

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY00 **Completion Date:** 3Q FY03 **Current Activity:** Yes

Investigate Requirements Specification Assessment Methods (3.2.4)

Task: Investigate the experience and use of requirements specification assessment methods/tools for use with nuclear software systems, and develop acceptance criteria for requirements specifications assessment.

Output: A technical report outlining the criteria for requirements specification assessment and explaining the use and success of requirements specification assessment methods/tools in finding inconsistency, incompleteness, and ambiguity requirements.

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY99 **Completion Date:** 4Q FY01 **Current Activity:** Yes

Diagnostics and Fault Tolerance Techniques (3.2.5)

Task: Investigate the design and performance of digital diagnostics and fault-tolerant techniques and provide appropriate technical information and review guidance.

Output: A technical report will provide the technical information and guidance that NRC staff needs when reviewing a digital I&C system that contains diagnostics and fault-tolerant techniques.

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY02 **Completion Date:** 4Q FY03 **Current Activity:** No

Operating Systems (3.2.6)

Task: Investigate the characteristics and performance of operating systems (particularly COTS operating systems) and provide appropriate review guidance to ensure their safe use.

Output: A technical report that provides the technical information and guidance that NRC staff needs when reviewing operating systems in digital I&C equipment.

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY01 **Completion Date:** 4Q FY02 **Current Activity:** No

Software Quality Assurance (3.3)

Investigate Objective Software Engineering Criteria (3.3.1)

Task A: Research is currently planned to Investigate the performance and applicability of software measures to nuclear power plant software.

Output: A technical report providing review guidance on the use of objective software measures as a software quality assurance method.

Priority: High priority (NRR user need (2000-6))

Start Date: 3Q FY98 **Completion Date:** 3Q FY01 **Current Activity:** Yes

Task B: Investigate various new methods for software measures and software validation and verification methods that present possible advantages over traditional methods, such as “formal methods”.

Output: A technical report will provide recommendations on the feasibility of using this methods for software quality metrics in the regulatory arena.

Priority: High priority (NRR user need (2000-6) and RES initiative)

Start Date: 1Q FY02 **Completion Date:** 3Q FY03 **Current Activity:** No

Investigate Criteria for Software Testing (3.3.2)

Task: Investigate software testing to determine the types of testing and test coverage required to achieve acceptable software quality.

Output: A technical report describing which testing methods, along with their criteria for use, are best suited for software quality assurance purposes.

Priority: High priority (NRR user need (2000-6) and RES initiative)

Start Date: 3Q FY02 **Completion Date:** 3Q FY03 **Current Activity:** No

Risk Assessment of Digital I&C Systems (3.4)

Perform Data Analysis on Digital I&C Failures (3.4.1)

Task A: Obtain digital I&C failure data for domestic and foreign nuclear power plants.

Output: Database(s) for digital I&C failures, along with an analysis of that database.

Priority: Medium priority (RES initiative)

Start Date: 1Q FY99 **Completion Date:** on-going **Current Activity:** Yes

Task B: Obtain failure data for COTS and embedded digital equipment belonging to industries that have I&C systems of similar safety and integrity level.

Output: Database(s) for digital I&C failures, along with an analysis of that database.

Priority: Medium priority (NRR user need (2000-6))

Start Date: 2Q FY03 **Completion Date:** 4Q FY04 **Current Activity:** No

Investigate Criteria for Digital Failure Assessment Methods (3.4.2)

Task A: Survey the analytical methods for identifying digital failures and their impact on safety. For each method document the advantages and disadvantages of using that method.

Output: The proposed criteria for identifying digital failures and their impact will be included in a RG. This RG provides an acceptable method for digital I&C risk assessment. The results of this task provide an acceptable means to carry out part of the digital I&C risk assessment process, and it identifies the level of acceptance the NRC would expect in license submittals.

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY99 **Completion Date:** 4Q FY02 **Current Activity:** Yes

Task B: Provide recommendations for a digital failure assessment technique(s). Also, provide criteria for using the technique(s) and applying them to digital risk assessments.

Output: A NUREG document containing the recommendations for digital failure assessment techniques and criteria for their application.

Priority: High priority (NRR user need (2000-6))

Start Date: 1Q FY01 **Completion Date:** 4Q FY03 **Current Activity:** Yes

Task C: Conduct at least two case studies using the recommended digital failure assessment technique(s).

Output: A NUREG report containing the results of the case studies.

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY03 **Completion Date:** 4Q FY04 **Current Activity:** Yes

Identify the Risk-Importance of Digital I&C Systems (3.4.3)

Task A: Identify and develop necessary risk models of I&C systems.

Output: The results of the risk-importance study will be documented in a technical report. This report will be used by NRC staff involved in both I&C and PRA reviews.

Priority: High priority (NRR user need (2000-6))

Start Date: 1Q FY01 **Completion Date:** 1Q FY02 **Current Activity:** No

Task B: Calculate the risk importance for generic I&C systems in nuclear power plants.

Output: Provide results of the calculations in a NUREG document.

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY02 **Completion Date:** 4Q FY02 **Current Activity:** No

Task C: Develop risk models beyond the "black box" level for complex systems.

Output: Provide description of modeling effort in a NUREG document, including the lessons learned.

Priority: High priority (NRC user need (2000-6))

Start Date: 1Q FY03 **Completion Date:** 4Q FY04 **Current Activity:** No

Investigate Digital Reliability Assessment Methods(3.4.4)

Task A: Identify digital reliability assessment methods and analyze their benefits and shortcomings.

Output: The result is a series of technical reports describing digital I&C reliability assessment methods and their acceptable use.

Priority: High priority (NRR user need (2000-6))

Start Date: 3Q FY00 **Completion Date:** 4Q FY02 **Current Activity:** Yes

Task B: Validate digital reliability assessment method(s) suitable for nuclear power plants.

Output: Reports that provide test case examples of the use of assessment methods identified or developed in Task A.

Priority: High priority (NRR user need (2000-6)

Start Date: 1Q FY02 **Completion Date:** 4Q FY03 **Current Activity:** Yes

Emerging I&C Technology and Applications (3.5)

Review of Future Applications of Digital I&C and Research Infrastructure (3.5.1)

Task A: Develop and maintain interactions and interfaces with the industrial, academic and regulatory communities with relevant digital I&C applications.

Output: Reports and information on how other industries and organizations regulate digital systems for safety critical applications, and what lessons, we can learn from their examples.

Priority: High priority (RES initiative)

Start Date: n/a **Completion Date:** on-going **Current Activity:** Yes

Task B: Participate on national and international standards working groups and committees to develop and updated standards.

Output: The staff will activity participate in consensus standard organizations and revise existing RGs referenced in SRP Chapter 7 to incorporate revised versions of IEEE and other standards.

Priority: High priority (NRR user need (2000-6) and RES initiative)

Start Date: n/a **Completion Date:** on-going **Current Activity:** Yes

Task C: Review new technology as it becomes available including abstaining tools and methods for trail use by RES staff.

Output: Periodic reports on the status of emerging technology in the digital area, which will be used to determine when new areas should be developed for research. A more technically capable staff.

Priority: High priority (NRR user need (2000-6) and RES initiative)

Start Date: n/a **Completion Date:** on-going **Current Activity:** Yes

Predictive Maintenance/On-Line Monitoring (3.5.2)

Task: Provide technical information on predictive maintenance and on-line monitoring systems, and identify the proper design and operation of such systems to ensure adequate safety.

Output: A technical report that helps NRC staff evaluate the safe use of predictive maintenance and on-line monitoring systems.

Priority: Medium priority (RES initiative)

Start Date: 3Q FY02 **Completion Date:** 2Q FY03 **Current Activity:** No

Advanced Instrumentation (3.5.3)

Task: Investigate advanced instrumentation that is expected to enter nuclear power plants and identify characteristics that either enhances or potentially degrades safety.

Output: Technical reports that will aid the NRC staff in the safety evaluation of plant modifications involving advanced instrumentation.

Priority: Medium priority (RES initiative)

Start Date: 1Q FY03 **Completion Date:** 4Q FY04 **Current Activity:** No

Smart Transmitters (3.5.4)

Task: Investigate smart transmitters and provide technical information on such systems, their application in nuclear power plants, and their potential impacts on safety.

Output: A technical report to support the review of smart transmitters and their application to nuclear power plants.

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY03 **Completion Date:** 4Q FY04 **Current Activity:** No

Wireless Communications (3.5.5)

Task: Investigate the design, operation, and failure mechanisms of wireless communications and provide appropriate review guidance to the NRC staff.

Output: A technical report to support NRC review efforts when wireless communications are concerned.

Priority: High priority (NRR user need (2000-6))

Start Date: 2Q FY03 **Completion Date:** 4Q FY04 **Current Activity:** No

Firewalls (3.5.6)

Task: Investigate on-going worldwide efforts to develop preventive design techniques and develop appropriate review guidance for identifying vulnerabilities to the NRC staff.

Output: A technical report will be published to support NRC review efforts when communication from outside nuclear plant boundaries is permitted.

Priority: High priority (RES initiative)

Start Date: 1Q FY03 **Completion Date:** 4Q FY04 **Current Activity:** No

Table 5.1, on the next page, summarizes the schedule for te digital I&C research program.

Table 5.1 Proposed Schedule for the Digital I&C Research Program

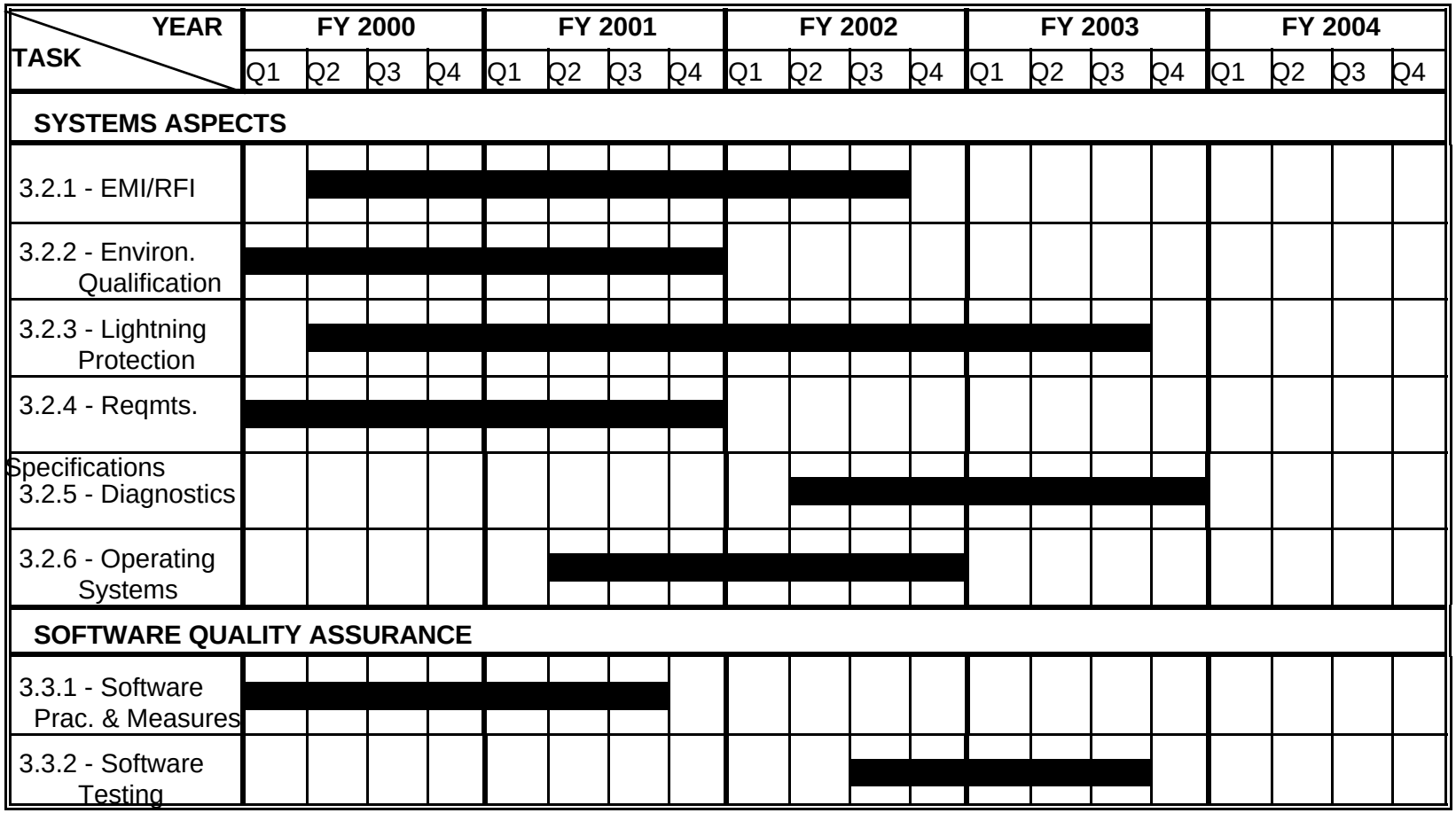

Table 5.1 Proposed Schedule for the Digital I&C Research Program (cont.)

TASK \ YEAR	FY 2000				FY 2001				FY 2002				FY 2003				FY 2004			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RISK ASSESSMENT OF DIGITAL SYSTEMS																				
3.4.1 - Data Analysis	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
3.4.2 - Digital Failure Assessments	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
3.4.3 - Risk Import. of I&C Sys.					■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
3.4.4 - Digital Reliability Assess.			■	■	■	■	■	■	■	■	■	■	■	■	■	■				
EMERGING TECHNOLOGY																				
3.5.1 - Future Applications	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
3.5.2 - Pred. Maint. & On-Line Monitor.											■	■	■	■						
3.5.3 - Advanced Instrumentation													■	■	■	■	■	■	■	■
3.5.4 - Smart Transmitters														■	■	■	■	■	■	■
3.5.5 - Wireless Communication														■	■	■	■	■	■	■
3.5.6 - Firewalls													■	■	■	■	■	■	■	■

6 REFERENCES

CCCIC. “Research Challenges in High Confidence Systems, Proceedings of the Workshop sponsored by the Congressional Committee on Computing, Information, and Communications, August 6-7, 1997.

Dahll, G. “Combining Disparate Sources of Information in the Safety Assessment of Software Based Systems, proceedings of 25th Annual Water Reactor Safety Information Meeting, NUREG/CP-0162, Vol. 3 April 1998.

IEEE. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std. 603. New York: Institute of Electrical and Electronics Engineers, 1991.

IEEE. "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Std. 7-4.3.2. New York: Institute of Electrical and Electronics Engineers, 1993.

Leveson, Nancy G., *Safeware, System Safety and Computers,* Addison-Wesley Publishing, New York, New York, 1995

NAS. *Digital Instrumentation and Control Systems in Nuclear Power Plants*, National Research Council. Washington, D.C.: National Academy of Science Press, 1997.

NSTC. “Information Technology for the Twenty-first Century: A Bold investment in America’s Future: Implementation Plan; National Science and Technology Council, Office of the President, June 1999.

RTCA. "Software Considerations in Airborne Systems and Equipment Certification," RTCA/ DO-178B. Washington, D.C.: Radio Technical Commission for Aeronautics, 1992.

USNRC. "Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Nuclear Reactors," NUREG/CR-5904. Washington, D.C.: U. S. Nuclear Regulatory Commission, 1994.

USNRC. "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," *Federal Register*, Vol. 60, p. 42622 (60 FR 42622), 16 August 1995.

USNRC. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152. Washington, D.C.: U.S. Nuclear Regulatory Commission, 1996.

USNRC. "Expert Panel on Digital System Research: Transcript," Office of Nuclear Regulatory Research. Washington, D.C.: U.S. Nuclear Regulatory Commission, 1999a.

USNRC. "Reliability Study: Westinghouse Reactor Protection System, 1984 -1995," NUREG/CR-5500. Washington, D.C.: U.S. Nuclear Regulatory Commission, 1999b.

USNRC. "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Regulatory Guide 1.180. Washington, D.C.: U. S. Nuclear Regulatory Commission, 2000.

Voas, J. "A Recipe for Certifying High Assurance Software," *IEEE Software*, Vol. 16, No. 4, July 1999.

APPENDIX A:
I&C CONTRIBUTIONS TO CORE DAMAGE PROBABILITY

For some nuclear power plant events, I&C system failure contributes to an increase in conditional core damage probability (CCDP). The CCDP is the probability of core damage given that certain system failures have occurred. This appendix summarizes a study using the Accident Sequence Precursor (ASP) database[3]. The ASP database provides the CCDP for high risk-significant[4] licensee event reports (LERs). Using the database, those LERs involving I&C failures[5] are collected and general conclusions are drawn concerning their effect on nuclear power plant safety. The following observations are made:

- the number of ASP events affected by I&C failures versus the total number of ASP events
- the number of ASP events initiated by an I&C failure
- location of I&C failures among plant systems
- types of I&C failures (component failure, degraded performance, design error, maintenance error, and spurious operation)
- the frequency of I&C-related ASP events per year

As RES defines future research plans for digital I&C systems, it is important to look at past nuclear industry experience and recognize important safety trends. This appendix summarizes one effort in using nuclear power plant data to identify digital I&C research needs.

The ASP Database

ASP LERs between 1984 and 1997 were observed since this time period captures events associated with a mature nuclear industry. The number of events with a CCDP of 1×10^{-5} or larger is 217. Out of this total, 86 events are impacted by I&C failures. Of the 86 I&C-related ASP events, 65 are initiated by I&C failures. Table A.1 breaks down the number of I&C-related ASP events versus all ASP events by CCDP ranking.

Characterization by I&C System and Subsystem

In this study, four types of I&C systems are considered: safety, control, monitoring, and support. I&C safety systems are those structures, systems, and components that are relied upon to remain functional during and following design basis events (taken from the definition of safety-related structures, systems and components in 10 CFR 50.2). Control systems are those systems that manage normal balance-of-plant operation, and support systems are those systems that provide a support function such as electric power, instrument air, HVAC, control power, and cooling water. Monitoring systems include alarm and display systems providing plant status to operators.

---

3 Version 1.97 of the ASP database was used in the study.

4 In the study, high risk-significant events are those with a CCDP of 1×10^{-5} or larger.

5 No distinction is made between analog and digital I&C failures. The type of I&C technology does not affect CCDP calculations. Also, I&C-related events are those events where the failure of an I&C component is part of the progression of events leading to a high CCDP.

Table A.1. I&C-related events vs. the total number of ASP events.

CCDP	Total ASP Events	I&C Related ASP Events	Percent I&C-related ASP Events
$1\times10^{-1} < x \leq 1$	0	0	-
$1\times10^{-2} < x \leq 1\times10^{-1}$	1	1	100%
$1\times10^{-3} < x \leq 1\times10^{-2}$	7	3	43%
$1\times10^{-4} < x \leq 1\times10^{-3}$	93	34	37%
$1\times10^{-5} < x \leq 1\times10^{-4}$	116	48	41%
Total:	217	86	40%

Table A.2 provides the number and location of I&C failures contributing to a CCDP of $1x10^{-5}$ or greater. The number of I&C-related ASP events and I&C failures do not coincide because some ASP events contain multiple I&C failures among different plant systems. I&C components in safety systems contribute the most to CCDPs of $1x10^{-5}$ or larger with 46 associated failures. However, support and control system I&C failures, when combined, contribute to more than half of the I&C failures with a total of 60.

For the total number of I&C failures in safety systems, 38 failures are associated with pumps, valves, or diesel generators. Examples of these failures include spurious closure of valves, failure of emergency diesel generator exciter and load control circuits, and various I&C maintenance and design errors preventing the automatic operation of pumps and valves. The remaining 8 safety-related I&C failures occur in the reactor protection systems or radiation monitoring.

Considering the 38 I&C failures in support systems, 31 failures involve power supply failures. Power supplies include breaker and inverter circuitry and instrument power supplies for both safety and non-safety systems. The other 7 I&C failures falling under support systems involve instrument air, service water, and HVAC systems.

Considering the 22 I&C failures in control systems, 12 failures involve feedwater control. Feedwater control failures only include control system malfunctions, and not any failures associated with support systems such as the power supply. Other I&C control system failures include main generator/ turbine control (6 events), steam dump control (2 events), reactor pressure control (1 event), and a plant multiplexer (1 event).

Monitoring and alarm system failures contribute to approximately 3% of all ASP I&C failures. While this appears to be a low percentage, several safety-related monitoring and alarm systems are included in the safety system classification (e.g. radiation monitoring).

Table A.2. ASP I&C failures categorized by system and subsystem type.

System Type	System Subtype	Number of I&C Failures	Percent of Total I&C Failures
Monitoring	Generator/Turbine Protection Circuits	2	1.83%
	Hotwell Level Measurement	1	0.92%
	Subtotal:	**3**	**2.75%**
Safety	Engineered Safety Features Systems	25	22.94%
	MSIVs, PORVs, and SRVs	7	6.42%
	Reactor Protection System(RPS)	7	6.42%
	Emergency Diesel Generators	6	5.5%
	Radiation Monitoring	1	0.92%
	Subtotal:	**46**	**42.2%**
Support	Power Supply	31	28.44%
	Instrument Air	4	3.67%
	Service Water System	2	1.83%
	HVAC	1	0.92%
	Subtotal:	**38**	**34.86%**
Control	Feedwater Control	12	11.01%
	Generator/Turbine Control	6	5.5%
	Steam Dump Control	2	1.83%
	Reactor Pressure Control	1	0.92%
	Plant Multiplexer	1	0.92%
	Subtotal:	**22**	**20.18%**
	Total:	**109***	**100%**

* Of the 86 I&C-related ASP events, some contained multiple I&C failures.

Characterization by I&C Failure Categories

I&C failures are catalogued into five categories: component failure, degraded performance, design error, maintenance error, and spurious operation. In component failure, the I&C equipment does not function. Degraded performance refers to the incomplete accomplishment of the I&C system's function. Spurious operation are those instances where the I&C system actuates when it is not necessary. Finally, design[6] and maintenance errors involve those incorrect actions performed by technicians, developers, and operators that prevent the I&C system from accomplishing its full task.

Table A.3 lists the types of I&C failures found in the ASP database study and how many occurred. Component failures comprise the majority of I&C failures with 37 out of the 109 total I&C failures. There are various types of component failures, but it is interesting to note that 10 of the 37 component failures are power supply failures, while another 6 are attributed to relay failures. Another point of interest is that out of 19 degraded performance incidents, 18 are associated with safety and control systems.

Table A.3. Types of I&C failures for the I&C-related ASP events.

Types of Systems	Component Failure	Degraded Performance	Design Error	Maintenance Error	Spurious Operation
Control	9	6	1	5	1
Monitoring	1	0	0	1	1
Safety	12	12	4	12	6
Support	15	1	6	11	5
Total:	**37**	**19**	**11**	**29**	**13**

Characterization of I&C-related ASP Events By Year

Figure A.1 compares the number of I&C-related ASP events with all ASP events having a CCDP greater than $1x10^{-5}$. To draw conclusions from this data, it is better to consider the percentage of I&C-related events versus all events, as shown in Figure A.2. Figure A.2 also illustrates a regression plot of percent I&C-related ASP events for all ASP events within a year. While the percentage is decreasing (-0.96 percent/year), the average number of I&C-related events is 40% of the total ASP events as shown in Table A.1.

The actual I&C safety performance trend is difficult to determine from the ASP database for two reasons. First, there are not many data points in the latter years (1993 - 1997), which results in a large variance between those data points. Second, most ASP events are composed of

---

[6] Design error refers to human error in system development when good engineering practices are observed versus design error related to the use of poor design procedures.

multiple failures involving I&C, mechanical, and electrical components. Since many ASP events involve multiple system failures, it is difficult to determine the trend of one type of system, such as I&C.

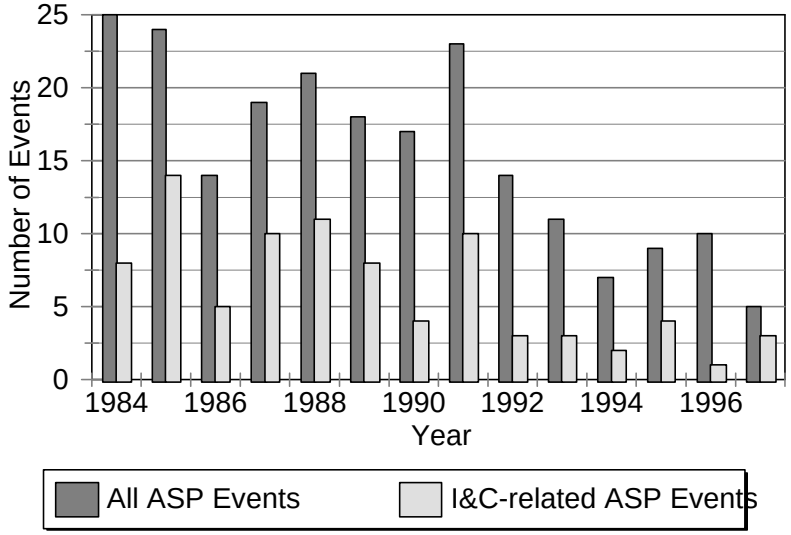

Figure A.1. Number of I&C-related ASP events compared by year.

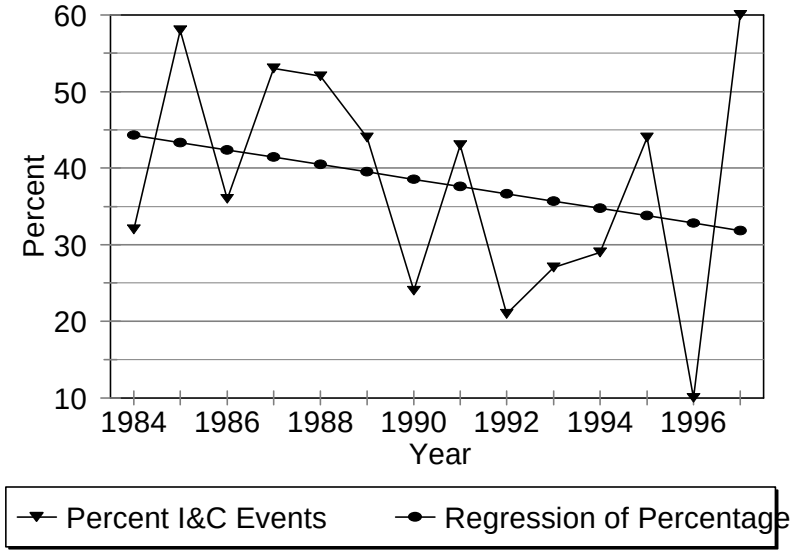

Figure A.2. I&C-related ASP events versus all ASP events.

Comments and Research Suggestions

While the ASP database provides insights into I&C system impact on nuclear power plant safety, it cannot answer the following key question: "What is the risk-importance of I&C systems in relation to overall plant safety?" The main reason the risk-importance of I&C systems cannot be found in the ASP database is the way the CCDP is calculated. Like most nuclear power plant probabilistic risk assessments, the risk modeling of the plant only goes to the system level (e.g. reactor protection system, auxiliary feedwater, and diesel generator). However, as shown in the ASP events, the majority of I&C failures are associated with I&C systems embedded in those plant systems. For example, the circuitry to start and load the emergency diesel generator is not modeled for CCDP calculations, but rather the diesel generator is modeled as a "black-box." I&C, mechanical, and electrical components contribute to the diesel generator's reliability, but the extent of their contribution to that reliability cannot be found with the ASP database. Since the risk contribution of I&C components to the reliability of plant systems is not known, neither can the risk-importance of I&C components be determined through the ASP database.

Although the ASP database does not provide sufficient information to determine the exact risk-importance of I&C systems, it does provide many indicators showing that I&C systems have a considerable impact on plant safety. The following observations support this statement:

- Only ASP events with a CCDP of $1x10^{-5}$ or greater are considered in this study. Of these events, 40% have at least one I&C failure contributing to the progression of events leading to a high CCDP and 30% of these events were initiated by an I&C failure.

- I&C failures in safety systems make up 42% of all I&C failures in ASP events having a CCDP of $1x10^{-5}$ or greater.

The first observation shows considerable I&C failure contribution to risk-significant, nuclear power plant events, and the second observation links I&C failures to risk-important plant systems. Therefore, based on the findings of this report, it appears that I&C systems have a considerable impact on plant safety and steps should be taken to better identify that contribution.

Besides pointing to the risk-significance of I&C systems, the ASP database also brings to light certain issues impacting I&C safety research. The following lists some observations made in the report:

- I&C components in support and control systems contribute to 55% of I&C failures in ASP events having a CCDP of $1x10^{-5}$ or greater.

- Of the safety-related I&C failures in this study, 83% involve pumps, valves, or diesel generators.

- Of the support system I&C failures in this study, 80% involve power supplies.

- Together, design and maintenance errors comprise 37% of the total I&C failures found in this study. Component failures alone comprise 34% of the total I&C failures.

The first observation indicates that some I&C components in non-safety systems have risk-significance. This same point was also noted in the Individual Plant Examinations (USNRC, 1997). The second observation suggests a closer look at I&C components embedded in safety systems. Often, the scope of safety-related I&C components is limited to reactor protection instruments and logic. However, many safety systems and components, such as pumps, valves, and diesel generators, depend upon I&C components to function correctly. The third observation points to the risk-significance of embedded I&C components in breakers, inverters, and other required power supply components for both safety and non-safety systems. The final observation shows design and maintenance errors having as much impact on I&C reliability as component failure.

Nuclear power plants and other commercial nuclear facilities are taking advantage of digital and advanced I&C components for performance and economic reasons. In the future, many of the NRC's regulatory decisions, such as reduced surveillance of safety equipment and power uprates for plants, may be based upon the capabilities of advanced I&C equipment. It is imperative for the NRC to understand the safety impact of new I&C technology and how digital and advanced I&C systems can either improve, maintain, or degrade plant safety. The following summarizes the research suggestions given in this section:

- Develop the methods and capability to identify the risk-importance of I&C systems

- Identify risk-important I&C components in support and control systems, particularly power supply equipment

- Identify risk-important I&C components in safety systems, particularly pumps, valves, and emergency diesel generators

- Ensure that I&C safety research address component failure, design error, and maintenance error.

Through I&C safety research, the NRC can provide valid methods, data, technical bases, and review guidance to facilitate timely, risk-informed decisions.