NRC PERSPECTIVES ON THE DIGITAL SYSTEM REVIEW PROCESS

J.L. MAUCK
Instrumentation and Controls Branch
Division of Reactor Controls and Human Factors
Office of Nuclear Reactor Regulation
United States Nuclear Regulatory Commission
Washington, D.C., USA

Abstract

Since about 1988, the USNRC has been involved in the review of digital retrofits to instrumentation and control (I&C) systems in nuclear power plants. Initially, this involvement was limited but with the advent of the 1990s, NRC involvement has become greater because of increased interest in and application of digital systems as existing analog systems become obsolete. Criteria for the design of such systems to ensure safety has been promulgated over the years and the USNRC has been actively involved both nationally and internationally with this effort. With the publication of the Zion Eagle 21 Safety Evaluation Report in 1992, Generic Letter 95-02 in April 1995 which endorses EPRI guidance document TR-102348 on digital upgrades and the latest revision to Regulatory Guide 1.152 which endorses IEEE 7.4.3.2-1993; a basic digital system review process was established. The NRC supplemented this review process with recently issued inspection procedures for use by NRC inspectors when conducting onsite reviews of digital modifications. In addition, the NRC undertook a major effort to codify the above guidance and the experience gained from digital system reviews of both operating plant modifications and advanced reactor designs, over these years into a revision to Standard Review Plan, (SRP), NUREG-0800, Chapter 7, Instrumentation and Control. This SRP revision was published in June, 1997, and included new SRP sections, branch technical positions and six new regulatory guides endorsing IEEE standards on software quality. The NRC staff believes that a stable digital system review process is now in place.

1. INTRODUCTION

Actual implementation of digital systems modifications to US nuclear power plants is not new - such systems have been in use since the late 1970's. Activity on the part of licensees in the 1980's and early 1990's highlighted the need to update NRC staff review criteria. The publication of the NRC Safety Evaluation report dated June 9, 1992, on the Eagle 21 Reactor Trip System modification at Zion provided a comprehensive digital system review framework for operating reactor digital modifications. Additionally, during this same time period, the NRC was completing reviews of the advanced light water reactor digital instrumentation and control systems designs. It was decided to codify both the operating reactor digital modification and advanced reactor instrumentation and control system design reviews into a revision to the Standard Review Plan.

The challenge for the NRC was to balance the advantages of digital systems with the potential problems they create and maintain the level of safety prescribed in the existing regulations and individual plant licensing bases. The experience gained from the reviews of digital system operating plant upgrades, the reviews of the advanced light water reactor designs, and

the interactions with experts in academia, industry and government (here and abroad) led to what the NRC believes is a stable licensing approach, for use in future upgrade proposals.

2. STANDARD REVIEW PLAN

The USNRC has recently completed a several year task to update the regulatory framework and review guidance for nuclear power plant digital I&C systems. This update consists of a revision to the SRP, NUREG-0800 Chapter 7, Instrumentation and Control, which incorporates six new regulatory guides endorsing IEEE standards on software quality, new branch technical positions addressing review aspects of digital systems, and new sections in Chapter 7 on diverse I&C systems and data communication systems. Also included are references to USNRC endorsement of key EPRI topical reports dealing with specific topics of concern in digital systems including EPRI TR-102348 on digital system upgrades, TR-106439 dedication of commercial-off-the-shelf software, and TR-102323 on electromagnetic interference protection. The framework sets out an acceptable approach to implementation of digital I&C systems, but is not a requirement. Licensees may provide alternative approaches with appropriate justification. There are also twenty publicly available USNRC technical reports that provide background and support for the SRP guidance and cover such digital I&C issues as: diversity analysis; software reliability and safety; environmental effects; programming languages; human-system interface; and software verification and validation.

The major revision to SRP Chapter 7 was the addition of detailed review guidance and acceptance criteria for digital computer-based I&C systems. The guidance covers the regulatory basis, information to be reviewed, and basis for acceptance. The staff's acceptance of software for digital computer-based I&C systems is based upon three factors for ensuring software quality. The first factor is confirmation that the software was developed in accordance with acceptable software development plans. The second factor is evidence that the plans were followed in an acceptable software life cycle process. The third factor is evidence that the life cycle process produced acceptable design outputs.

The review approach for digital systems is similar to that used by most industry and regulatory authorities concerned with the safe application of digital technology. It consists of a two-fold demonstration--provision for a high quality software and hardware design development process, and a level of defense-in-depth and diverse capability to offset the recognition that software cannot be made error free despite this high quality process. The software development process calls for effective documentation of the software life cycle including the requirements specification, and verification and validation program. The principle feature of the NRC criteria for this demonstration is endorsement of industry standards on the quality of the software development process and other industry guidelines on digital system implementation.

The following discussion describes the content of the update to SRP Chapter 7 and highlights the major differences between the 1997 version and the previous version (1981). These differences are due mainly to the issues involved in the use of digital technology as discussed above and in part due to new safety issues that have occurred over the years.

Chapter 7 of the SRP provides guidance for the review of the instrumentation and control (I&C) portions of (1) applications for nuclear reactor licenses or permits and (2) amendments to existing licenses. The SRP guidance may also be applied in the review of topical reports submitted to NRC by vendors and industry groups requesting generic acceptance of systems

or components and specific topics that may be used in and are applicable to nuclear power plant I&C systems.

SRP Section 7.0 provides an overview of the process used by the NRC to review both the I&C portion of license applications and the I&C portions of generic safety evaluations of specific topics. Guidance is provided to the reviewer in applying Chapter 7 of the SRP to these reviews.

Figure 7.0-2 illustrates the life cycle for any I&C system, and relates the application types to the life-cycle activities that should be addressed by the application. The review of any application should involve all the applicable life-cycle activities. Reviews should confirm the acceptability of system requirements and the adequacy with which the final system meets these requirements. Review of non-digital computer-based system implementation may focus on component and system requirements, design outputs, and validation (e.g., type testing). Review of digital computer-based systems should focus on confirming the acceptability and correct implementation of the life-cycle activities. Appendix 7.0-A describes a generic process for reviewing the unique aspects of computer-based systems, including hardware/software integration.

The guidance in Appendix 7.0-A is used in conjunction with the remaining sections of SRP Chapter 7 when applied to a digital system for review of (1) the overall I&C system design described in Section 7.0, (2) the design criteria and commitments described in Section 7.1, and (3) the individual I&C systems described in Sections 7.2 through 7.9. This appendix illustrates how the review activities interact with each other and with the overall I&C system review process described in Sections 7.1 through 7.9. Additional information relevant to the review process can be found in the references in Section D of this appendix.

SRP Section 7.1 discusses the review of the overall I&C system concept and generic system requirements. Appendices 7.1-A, 7.1.-B, and 7.1-C discuss the review procedures for each acceptance criterion relevant to I&C systems.

The fundamental acceptance criteria for I&C systems are described in 10 CFR 50.55a, which refers to ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations;" Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations;" and Appendix A of 10 CFR Part 50, General Design Criteria (GDC). Appendix B of 10 CFR Part 50 Quality Assurance Criteria provides criteria for quality assurance programs to be applied to the design, fabrication, construction, and testing of I&C safety systems. The criteria of 10 CFR Part 50 apply to safety-related digital I&C systems and are sufficient to support licensing of such systems. Specific guidance for digital systems designs is contained in IEEE Std. 7-4.3.2 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" which is endorsed by Reg. Guide 1.152 "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants". For applications for standardized plant design certification under 10 CFR Part 52, the technical acceptance criteria of 10 CFR 50 apply.

Certain characteristics of digital I&C systems necessitate that augmented review approaches and different review perspectives be used in assessing compliance with the fundamental acceptance criteria of 10 CFR Part 50. These characteristics are important to the valuation of (1) design qualification of digital systems, (2) protection against common-mode failure, and (3) selected functional requirements of IEEE Std 603 and the GDC that pose new assurance

challenges when implemented using computers. These issues are discussed in more detail below and are the basis for the guidance in SRP Section 7.1 for digital I&C system reviews.

Digital I&C systems require additional design and qualification approaches that are not typically employed for analog systems. The performance of analog systems can typically be predicted by the use of engineering models. These models can also be used to predict the regions over which an analog system exhibits continuous performance. The ability to analyze the system design using models based upon physics principles, and the ability to use these models to establish a reasonable expectation of continuous performance over substantial ranges of input conditions are important factors used in the qualification of analog system designs. These factors enable extensive use of type testing, acceptance testing, and inspection of design outputs in qualifying and verifying the design of analog systems and components. If the design process ensures continuous behavior over a fixed range of inputs, and testing at a finite sample of input conditions in each of the continuous ranges demonstrates acceptable performance, then performance at intermediate input values between the samples test points can be inferred to be acceptable with a high degree of confidence.

Digital I&C systems are fundamentally different from analog I&C systems in that use of software codes create a virtually unlimited number of pathways for inputs and outputs, and minor errors in design and implementation can cause them to exhibit unexpected behavior. Consequently, the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing at a sample of input conditions. The use of inspections, type testing, and acceptance testing of digital systems and components does not alone accomplish design qualification and verification at high confidence levels. To address this issue, the NRC approach to the review of design qualification for digital systems focuses, to a large extent, upon confirming that the applicant/licensee employed a high-quality development process that incorporated disciplined specification and implementation of design requirements. Inspection and testing is used to verify correct implementation and to validate desired outputs (functionality) of the final product, but confidence that isolated, discontinuous point failures will not occur derives from the discipline of the development process.

SRP Sections 7.2 through 7.9 describe the review of system-specific requirements, system design, and implementation. In the SRP Chapter 7 updates, the content of SRP Section 7.2 through 7.7 is basically the same as in the previous version of the SRP with the exception of reference to SRP Section 7.1 for digital system applications guidance. Two new sections of SRP Chapter 7, Section 7.8 and 7.9 have been added to provide specific guidance for I&C systems not previously addressed in the SRP.

SRP Section 7.8 describes the review process and acceptance criteria for the diverse I&C systems and equipment provided for the express purpose of protecting against potential common-mode failures of protection systems. The following systems are covered by this section:

1. Anticipated transient without scram (ATWS) mitigation systems required for compliance with 10 CFR 50.62. As defined in 10 CFR 50.62 which was promulgated in 1985, an ATWS event is an anticipated operational occurrence followed by failure of the reactor trip portion of the protection system. 10 CFR 50.62 identifies design requirements for ATWS mitigation systems and equipment in pressurized and boiling water reactor designs.

2. Diverse manual controls and displays provided to comply with the NRC position on defense-in-depth and diversity (D-in-D&D) for digital I&C systems as described in the Staff Requirements Memorandum (SRM) regarding SECY-93-087. These systems are to be independent and diverse from the safety digital computer system, located in the main control room, and provide for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.

3. Diverse actuation systems (DAS) are those automatic systems provided solely for the purpose of meeting the NRC position on D-in-D&D for digital I&C systems. DAS and ATWS mitigation system functions may be combined into a single system. The reactor trip system (RTS), engineered safety features actuation system (ESFAS), control systems, or other diverse I&C systems may perform DAS functions to meet the NRC position on D-in-D&D. Diverse I&C system functions performed by the RTS, ESFAS and other systems are not within the scope of this section. The diverse I&C functions of these systems should meet the criteria applicable to the systems as a whole. The criteria for these system designs are found in the appropriate SRP sections for the individual systems.

SRP Section 7.9 describes the review process and acceptance criteria for data communication systems (DCSs) that are part of or support the systems described in Sections 7.2 through 7.8. The scope and depth of the review and the acceptance criteria will vary according to the importance to safety of the system that the DCS is supporting.

The objectives of the review are to confirm that the DCS is of comparable qulaity and reliability to the system it supports, will perform the safety functions assigned, and will tolerate the effects of random transmission failures. A particular concern is that the transmission of multiple signals over a single path may constitute a single point of failure that may have a larger impact on plant safety than would occur in previous analog system designs.

SRP Chapter 7 contains technical positions (BTPs) that provide guidance on specific aspects of I&C system design. The first nine of the BTPs are the same as those presented in the 1981 version of SRP Chapter 7. There are four new BTPs based on new operating reactor issues and six new BTPs based on the application of digital based I&C systems. The more significant of these new BTPs are discussed below.

BTP 10 provides additional guidelines for reviewing an applicant/licensee's post-accident monitoring system. These guidelines are based on previous reviews of applicant/licensee design submittals that contained approved interpretations and alternative design features to the guidance identified in Reg. Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident."

BTP 11 provides guidelines for reviewing the use of isolation devices in I&C systems. These acceptance guidelines are based on experience in the review of applicant/licensee submittals for electrical qualification and application of isolation devices used to protect safety I&C systems from faults in non-safety I&C systems.

BTP 12 provides guidelines for reviewing the process an applicant/licensee follows to establish and maintain instrument setpoints. These guidelines are based on reviews of applicant/licensee submittals and vendor topical reports describing setpoint assumptions,

terminology, and methodology, and experience gained from NRC inspections of operating plant setpoint programs.

BTP 13 provides guidelines on the use of cross-calibration techniques for surveying the performance of resistance temperature detectors (RTDs). These guidelines are based on experience in the detailed reviews of applicant/licensee submittals describing the application of in-situ cross-calibration procedures for reactor coolant RTDs, as well as NRC research activities. Other methods, such as using a diverse parameter to provide a cross-correlation reference, can be used if adequate justification is provided.

BTP 14 provides guidance for the review and confirmation that an acceptable level of software quality is provided for computer-based I&C systems. The NRC's acceptance of software for safety system functions is based upon (1) confirmation that acceptable plans were prepared to control software development activities, (2) evidence that the plans were followed in an acceptable software life cycle, and (3) evidence that the process produced acceptable design outputs. These guidelines are based on reviews of licensee submittals, industry standards for software development, and the analysis of standards and practices documented in NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems." The structure of BTP 14 is derived from the review process described in Appendix 7.0-A.

BTP 17 provides guidelines for reviewing the design of self-test and surveillance test provisions in digital computer-based I&C systems. These guidelines are based on reviews of applicant/licensee submittals and vendor topical report submittals describing self-test and surveillance test assumptions, terminology, methodology and experience gained from NRC inspections of operating plants.

BTP 18 provides guidelines for reviewing the use of programmable logic controllers (PLCs) in digital instrumentation and control (I&C) systems. These guidelines are based on reviews of licensee submittals and the analysis of PLC-related issues documented in NUREG/CR-6090, "The PLC and Its Application in Nuclear Reactor Protection Systems."

BTP 19 discusses common-mode failure concerns in digital computer-based systems due to a potential software error which defeats the redundancy achieved by hardware architecture. In NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," the NRC documented a D-in-D&D analysis of a digital computer-based reactor protection system, in which defense against common-mode failures was based upon an approach using a specified degree of system separation between echelons of defense. Subsequently, in SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors," the NRC included discussion of its concerns about common-mode failures in digital protection systems and documented its position with respect to common-mode failures in digital systems and defense-in-depth. This position was formally implemented in accordance with the SRM for Item II.Q of SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." Based on the above and experience in the detailed reviews of digital protection systems, the NRC staff has established acceptance guidelines for D-in-D&D assessments as described in this branch technical position.

BTP 20 provides guidelines for reviewing digital system real-time performance and system architectures. These guidelines are based on reviews of licensee submittals and the analysis

of these issues documented in NUREG/CR-6083, "Reviewing Real-Time Performance of Nuclear Reactor Safety Systems," and NUREG/CR-6082, "Data Communications."

3. GENERIC DIGITAL ISSUES

At the present time, there are few safety-related digital modifications being proposed for plant-specific applications. However, the NRC has been and continues to remain active in the review of generic proposals.

The NRC is currently reviewing several generic digital-based programs concerned with modifications to operating plant I&C systems. These are (1) programmable logic controllers for use in safety-related systems (EPRI sponsored), (2) Application Specific Integrated Circuits for replacement of existing Westinghouse plant reactor trip systems (Westinghouse sponsored) and (3) Ovation safety-related digital based system (Westinghouse sponsored). We are currently applying the updated SRP Chapter 7 to the review of these generic proposals. These programs are scheduled for completion over the next several years.

4. FUTURE ISSUES

The NRC recognizes that the rapid evolution of computer technology will mean further changes in systems proposed for nuclear power plant implementation in the future. Maintaining the review criteria for these evaluations current is important. In order to address anticipated digital system issues for the future, the NRC identified a number of research efforts to help cope with future evaluations. These are as follows:

a. Use of ISO 9000

   The international computer vendor community (including US nuclear suppliers) is increasing the use of ISO 9000 and ISO 9000-3 for general quality assurance and software quality assurance respectively due to the international recognition of these standards and regulatory requirements in much of the European community. NRR audits of ISO 9000 certified systems have raised several questions regarding its guidance when compared to the quality assurance requirements of 10 CFR 50, Appendix B. Some computer-based systems are certified to the general ISO 9000 criteria but are not certified to the software-related ISO 9000-3 criteria. Information received from the Software Productivity Consortium and other industry publications notes that an ISO 9000 certification may not assure the necessary level of quality assurance for safety systems due to variance between the certifying entity and the specific regulatory requirements. The NRC will develop a comparison of these quality standards.

b. Domain Engineering Guidance

   Domain engineering is increasing in popularity with vendors because it facilitates the reuse of software with the resultant economic benefits. The establishment of a domain model allows the development of standard software requirements specifications and architectures that can be used for multiple systems. The NRC will develop guidance on application of domain engineering.

c. Quantitative Assessment of Digital System Reliability

A longstanding goal of the computer industry has been the attempt to quantify the reliability of software-based systems. The NRC will survey the state-of-the-practice methods for assessment of quantitative reliability prediction, and incorporation of quantitative reliability in PRAs. One candidate for review is the Statistical Modeling and estimation of Reliability Functions for Software (SMERFS) produced by the Naval Surface Warfare Center. The project should include a review of European and Canadian nuclear industry and domestic computer industry efforts in this area. The NRC will attempt to identify means for quantification of digital system reliability.

d. Guidance on Formal Methods and Applicable Tools

Formal methods have been presented by their proponents in the computer industry and academia as a method to mathematically prove that the software will contain no errors. Several formal methods academic projects and a few commercial projects were reviewed by the staff several years ago. Since then, the literature has described several improvements. The NRC will survey recent formal methods development and state of the practice with a focus on formal requirements specifications and their effectiveness in practical commercial applications. Verification of timing considerations via formal methods will also be addressed. The NRC will develop guidance for use of formal methods as appropriate.

e. Review of IEEE Std 1498 Guidance

In August 1995, ISO/IEC 12207, "Software Lifecycle Processes," was released as an approved international standard. The Joint International Standards Working Group (JISWG) is adapting ISO/IEC 12207 for use in the United States including the technical content found in J-STD-016. The scope of ISO/IEC 12207 includes the computer development process of IEEE 1498 as well as acquisition, supply operation, and maintenance processes. The US 12207-1996 guidance focuses on the overlap between IEEE 1498 and ISO/IEC 12207 and includes supporting processes such as documentation, quality assurance, configuration management, and peer review. The NRC will develop a comparison of IEEE 1498 and US version of ISO/IEC 12207 against the SRP Chapter 7 guidance and, if acceptable, a regulatory guide will be prepared to endorse both standards.

5. YEAR 2000 CONCERN

Another important topic that is being pursued is the problems associated with the Year 2000 (Y2K) issue. The Y2K problem has the potential to affect any computer system, any hardware that is microprocessor-based (embedded software), and any software and data base at nuclear power plants.

As of this date the NRC has not received notification from vendors of digital protection systems, (Westinghouse, General Electric, Combustion Engineering, Foxboro, Allen Bradley, and Framatome/Babcock & Wilcox), that a Y2K problem exists with their safety-related initiation and actuation systems. However, non-safety, but important computer-based systems, primarily data bases and data collection necessary for plant operation which are date driven, may need modification for Y2K compliance. Some examples of systems that may be affected by Y2K problems are:

Security computers
Plant process (data scan, log, and alarm)/Safety parameter display system computers)

Emergency response systems
Radiation monitoring systems
Dosimeters/readers
Plant simulators
Engineering programs
Communications systems
Inventory control system
Surveillance and maintenance tracking systems
Control systems

The NRC issued Information Notice 96-70, "Year 2000 Effect on Computer System Software," to alert NRC licensees, certificate holders, and registrants of the potential problems their computer systems and software may encounter as a result of the change to the new century. The information notice (IN) contained a discussion of how the Y2K issue may affect NRC licensees. The IN encouraged licensees to examine their uses of computer systems and software well before the turn of the century and suggested that licensees consider actions appropriate to examine and evaluate their computer systems related to the Y2K issue. Also, the final version of the updated SRP Chapter 7, incorporates wording that addresses the need for recognition of the Y2K issue. .

The NRC is currently working with various industry groups to ensure that individual licensees are developing proper plans for each nuclear plant to address the Y2K issue and to provide confidence to the NRC that come the year 2000, nuclear plants in the United States will continue to operate in a safe manner.

6. CONCLUSION

Meetings of this type are important to the fostering of international cooperation in addressing common problems, sharing solutions, and determining future research needs on issues associated with the implementation of digital technology which is itself a rapidly changing technology. Although the specific approaches to acceptance of digital technology in nuclear power plants may differ from country to country, the overall objective is largely the same: ensure an appropriate level of safety has been achieved.

As discussed above, the NRC undertook a major effort to codify the guidance developed and the large amount of regulatory experience expended in digital system reviews over the past few years in a revision to the SRP that was published in June 1997. Although, the NRC believes that a stable digital review process is now in place, the NRC will continue to maintain its review criteria current as digital-based I&C system technology advances.

Session 4:

Experiences in Implemented Computerized Safety and Safety Related Systems.