



**U.S.NRC**

UNITED STATES NUCLEAR REGULATORY COMMISSION

*Protecting People and the Environment*

**DIGITAL INSTRUMENTATION AND CONTROLS  
Digital I&C-ISG-06**

**Task Working Group #6:  
Licensing Process**

**Interim Staff Guidance**

*Revision 1  
(Initial Issue for Use)*



# U.S. NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

*Protecting People and the Environment*

**DIGITAL INSTRUMENTATION AND CONTROLS  
Digital I&C-ISG-06**

**Task Working Group #6:  
Licensing Process**

**Interim Staff Guidance**

*(Initial Issue for Use)*

**ML110140103**

**\*CONCURRENCE VIA E-MAIL**

<b>OFFICE</b>	DI&C/TWG-6	DI&C/TWG-6	DI&C/TWG-6	DI&C/TWG-6	RES/DE	NRO/DE
<b>NAME</b>	GMILLER	NCARTE (S.ARNDT FOR)	SARNDT	LJAMES (PHILAND FOR)	MCASE* (SRICHARDS FOR)	TBERGMAN *
<b>DATE</b>	01/14/11	1/14/11	1/14/11	1/18/11	1/11/11	1/13/11

<b>OFFICE</b>	NMSS/FCSS/SPTSD	NSIR/DSP	OGC	NRR/ADES
<b>NAME</b>	MBAILEY*	RCORREIA (CERLANGER FOR)*	BMIZUNO *	JGROBE (PHILAND FOR)
<b>DATE</b>	1/12/11	1/10/11	1/12/11	01/ 19 /11

**OFFICIAL FILE COPY**

# **DIGITAL INSTRUMENTATION AND CONTROLS**

## **DI&C-ISG-06**

### **Task Working Group #6: Licensing Process**

#### **Interim Staff Guidance**

*(Initial Issue for Use)*

#### **A. INTRODUCTION**

This Interim Staff Guidance (ISG) describes the licensing process that may be used in the review (against licensing criteria – the Standard Review Plan, NUREG-0800) of license amendment requests associated with digital I&C (I&C) system modifications in operating plants originally licensed under Part 50. This guidance is consistent with current NRC policy on digital I&C systems and is not intended to be a substitute for Nuclear Regulatory Commission (NRC) regulations, but to clarify one way that a licensee may efficiently request NRC approval to install a digital I&C system. This ISG may be used, in part or in whole, for more than license amendment requests (e.g., digital platform topical reports, Part 50 licensing of Watts Bar Unit 2, and Bellefonte).

This ISG also covers activities prior to submittal of the license amendment request (LAR). Except in those cases in which a licensee has established an approach for complying with specified portions of NRC regulations or proposes an alternative approach, the NRC staff may use the process described in this ISG to evaluate compliance with NRC regulations.

The purpose of the NRC review is to assess whether the facility and equipment, the proposed use of the equipment, the processes to be performed, and other technical criteria will comply with the regulations (i.e., 10 CFR 50) and that public health and safety will be protected. It is not intended that the review or audit activities by the reviewer include an evaluation of all aspects of the design and implementation of the I&C system. The review scope is of sufficient detail to allow the reviewer to conclude the LAR complies with the regulations.

Reviews should assess the adequacy with which the system meets the regulations. Review of non-digital computer-based system implementation may focus on component and system requirements, system design, and associated validation analyses. Review of digital computer-based systems should also include assessing the acceptability and correct implementation of life-cycle activities; while process is important, it is not a substitute for a detailed review of the hardware and software architectures to conclude that they meet the four fundamental principles of redundancy, independence, deterministic behavior, and diversity and defense-in-depth, as well as the more subjective principle of simplicity of design.

Section 7.1 of the Standard Review Plan (SRP) describes the review of the overall I&C system concept and generic system requirements. SRP Sections 7.2 through 7.9 describe the review of system-specific requirements, system design, and implementation. For systems or components with embedded computers, SRP Appendix 7.0-A describes a generic process for reviewing the unique aspects of computer-based systems, including hardware/software integration.

## **B. PURPOSE**

The purpose of this ISG is to provide guidance for the NRC staff's review of license amendments supporting installation of digital I&C equipment in accordance with current licensing processes (LIC-101, "License Amendment Review Procedures" – Non-Publically Available). This ISG also identifies the information the NRC staff should review for digital I&C equipment and when the information should be provided. This documentation should allow technical reviewers to quickly assess digital I&C upgrade applications to ensure that they sufficiently address the areas that are within the I&C scope of review (e.g., during the acceptance review per LIC-109, "Acceptance Review Procedures" - Agencywide Documents Access and Management System (ADAMS) Accession No. ML091810088).

Use of this ISG is designed to be complementary to the NRC's longstanding topical report review and approval process (LIC-500, "Topical Report Process" – ADAMS Accession No. ML091520370). Where a licensee references an NRC-approved topical report, the NRC staff should be able to, where appropriate, limit its review to assessing the application of the digital I&C upgrade falls within the envelope of the topical report approval. Additionally, this ISG was developed based upon, and is designed to work in concert with, existing guidance. Where appropriate, this ISG references other guidance documents and provides their context with respect to the digital I&C license amendment process for operating reactors.

### **B.1 Background**

The NRC staff should review proposed digital I&C equipment to ensure that the equipment will perform the required functions; this review should use the guidance in the SRP, Chapter 7, and other associated guidance including ISGs. Licensees should provide a description of the licensing basis functions of the I&C equipment and include a description of the equipment that implements the functions. Additionally, licensees should clearly identify those parts of the licensing basis they are updating as a result of the proposed change.

The SRP Appendix 7.0-A and Branch Technical Position 7-14 (BTP 7-14) have been established to guide NRC staff in performing reviews of digital safety systems (DSS). While the NRC staff does not perform an independent design review of the DSS, the staff reviews the design and the development process to conclude that the design meets regulatory requirements (e.g., independence / redundancy, deterministic behavior, defense-in-depth and diversity,...) and that the process is of sufficient high quality to produce systems and software suitable for use in safety-related applications in nuclear power plants. In addition the staff may perform thread audits (in accordance with LIC-111, "Regulatory Audits" – ADAMS Accession No. ML082900195) to conclude that the DSS implementation activities are consistent with the DSS planning activities. The NRC staff then depends on the proper application of this high quality development process to produce acceptable systems and software. Therefore, in addition to review of system hardware and software architecture a portion of the NRC staff review is of documentation of plans and processes which describe the life-cycle development of the software to be used by and/or in support of the digital I&C system. The NRC staff should review the development process, and the associated implementation, with the intent of determining that the process described is the process that was used, that the process was used correctly, and that it was used in such a manner as to produce software suitable for use in safety-related applications at nuclear power plants.

### B.1.1 Principles of Review

The NRC staff recognizes two different ways that a component can be approved for use in safety-related applications:

- (1) If a basic component has critical characteristics that **cannot** be verified, then it **must** be designed and manufactured under a quality assurance program.
- (2) If a basic component has critical characteristics that **can** be verified, then it **may** be designed and manufactured as commercial grade item and then commercially dedicated under a quality assurance program.

These approaches are implied by the definitions in 10 CFR 21.3:

*“Basic component... Basic components are items designed and manufactured under a quality assurance program complying with appendix B to part 50 of this chapter, or commercial grade items which have successfully completed the dedication process.*

...

*Commercial grade item... means a structure, system, or component, or part thereof that affects its safety function, that was not designed and manufactured as a basic component. Commercial grade items do not include items where the design and manufacturing process require in-process inspections and verifications to ensure that defects or failures to comply are identified and corrected (i.e., one or more critical characteristics of the item cannot be verified).*

...

*Critical characteristics... are those important design, material, and performance characteristics of a commercial grade item that, once verified ... the item will perform its intended safety function.”*

Since some critical characteristics of software cannot be verified, no commercially developed software could be used in any safety-related application; however, software developed under a 10CFR50 Appendix B quality assurance program could be. This position seems to conflict with the fact that some commercially available software is highly reliable. Therefore, the NRC staff has concluded that a high quality software development process is a critical characteristic of all safety-related software. A high quality software development process is one that is equivalent to the development process for software developed under an Appendix B quality assurance program. Consistent with this principle, the Safety Evaluation (ML092190664) for EPRI TR-106439, “Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” the staff stated (see Section 2.0, “Background,” subsection “Commercial Dedication per CFR Part 21”): “The staff considers verification and validation activities common to software development in digital systems to be a critical characteristic that can be verified as being performed correctly following the completion of the software development by conducting certain dedication activities such as audits, examinations, and tests.”

### B.1.2 Documentation Reviewed

The organization responsible for the review of I&C, generally does not review procedures; however, the organization responsible for the review of I&C should review sufficient information to make an evaluation against the review criteria in the SRP. If the only place such information exists is inside procedures, then the organization responsible for the review of I&C should

request and review those procedures. The organization responsible for the review of I&C, reviews the information necessary to make an evaluation against the review criteria in the Chapter 7 of the SRP; this information should be docketed. If the necessary information is contained in proprietary or larger documents, then the organization responsible for the review of I&C should request those documents. If a licensee chooses, the information may be extracted or reproduced in another format convenient for docketing.

This ISG does not describe the development process; a licensee is allowed to determine its own development process (e.g., per RG 1.173 and IEEE Std 1074). However, this ISG makes certain assumptions (consistent with 10 CFR 50 Appendix B), about that development process. For example, if there exists a regulatory requirement that a safety-system has a certain property (e.g., IEEE Std 603-1991 Clause 5.1, "Single-Failure Criterion"), then the licensee should ensure that there is a documented design analysis that demonstrates that the safety system meets this regulatory requirement. The licensee should also ensure that the verification and Validation (V&V) team evaluates this design documentation and documents the evaluation. Enclosure B sometimes asks for this analysis using a generic name. In some cases it may be appropriate to summarize this analysis (in sufficient detail for the regulator to independently determine that the regulatory requirement is met) in the LAR; simply stating that the regulatory requirement is met is not sufficient for the regulator to determine that the system is designed to meet the regulations.

The SRP (NUREG-0800 Chapter 7 Section 7.0, "Instrumentation and Controls – Overview of Review Process") describes the interfaces that the organization responsible for the review of I&C has with other organizations. Several other organizations are identified as evaluating the adequacy of protective, control, display, and interlock functions and that these functions meet certain identified General Design Criteria (GDCs). The organization responsible for the review of I&C is essentially responsible for independently evaluating whether the equipment will perform the described functions. The material that is reviewed is documentation associated with the equipment and application.

### **B.1.3 I&C Review Scope**

The organization responsible for the review of I&C should review sufficient information to make an evaluation that the equipment will perform the required safety functions; sufficiently detailed functional diagrams and explanatory discussion should be provided so that a detailed review can be accomplished to ensure that the four fundamental principles are inherent in the hardware and software DI&C architectures. The organization responsible for the review of I&C does not, in general, review the adequacy of the required functions.

Licensees should be aware of the potential for a digital I&C upgrade to impact other systems, programs, or procedures. For instance, licensees should evaluate the impact of the upgrade on their Emergency Plan and associated Emergency Action Levels (NRC Information Notice (IN) 2005-19, "Effects of Plant Configuration Changes on the Emergency Plan," informed licensees of the importance of properly evaluating changes to procedures, equipment, and facilities for potential impact on the licensee's ability to maintain an effective emergency plan).

SRP Section 7.0 states that the organization responsible for review of I&C should coordinate with other NRC technical organizations in the review of the adequacy of certain I&C system design features. The coordinated reviews include the following:

The organization responsible for review of reactor systems evaluates the adequacy of protective, control, display, and interlock functions and concludes that they are consistent with the accident analysis, the operating criteria of the I&C systems, and the requirements of 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 10, 15, 28, 33, 34, and 35.

The organization responsible for the review of plant systems evaluates the adequacy of the criteria for the auxiliary supporting features and other auxiliary features to assess whether they satisfy the applicable acceptance criteria. These features include, for example, compressed (instrument) air, cooling water, boration, lighting, heating, and air conditioning. This review concludes that (1) the design of the auxiliary supporting features and other auxiliary features is compatible with the single-failure criteria of the I&C systems, and (2) the auxiliary supporting features and other auxiliary features will maintain the necessary environmental conditions in the areas containing I&C equipment. This review includes the design criteria and testing methods employed in the seismic design and installation of equipment implementing auxiliary supporting features and other auxiliary features. The organization responsible for review of plant systems also evaluates the adequacy of protective, control, display, and interlock functions, and concludes that they are consistent with the operating criteria of the supported system and the requirements of GDC 41 and 44.

The organization responsible for the review of containment systems reviews the containment ventilation and atmospheric control systems provided to maintain necessary environmental conditions for I&C equipment located inside containment. This organization also evaluates the adequacy of protective, control, display, and interlock functions associated with containment systems and severe accidents, and concludes they are consistent with the accident analysis, operating criteria, and the requirements of GDC 16 and 38.

The organization responsible for the review of electrical systems (1) evaluates the adequacy of physical separation criteria for cabling and electrical power equipment, (2) determines that power supplied to redundant systems is supplied by appropriate redundant sources, and (3) concludes the adequacy of the I&C associated with the proper functioning of the onsite and offsite power systems.

The organization responsible for the review of environmental qualification reviews the environmental qualification of I&C equipment. The scope of this review includes the design criteria and qualification testing methods for I&C equipment.

The organization responsible for the review of seismic qualification reviews the seismic qualification demonstration for I&C equipment including the design criteria and qualification testing methods.

The organization responsible for the review of human-machine interface evaluates the adequacy of the arrangement and location of instrumentation and controls, and concludes that the capabilities of the I&C are consistent with the operating procedures and emergency response guides.

The organization responsible for the review of maintenance provisions reviews the adequacy of administrative, maintenance, testing, and operating procedure programs as part of its primary review responsibility for SRP Sections 13.5.1.2 and 13.5.2.2.

The organization responsible for the review of quality assurance reviews design, construction, and operations phase quality assurance programs, including the general methods for addressing periodic testing, maintenance, and reliability assurance, as part of its primary review responsibility for SRP Chapter 17. This organization also reviews the proposed preoperational and startup test programs to assess whether they are in conformance with the intent of Regulatory Guide 1.68, Revision 2, "Initial Test Programs for Water-Cooled Nuclear Power Plants," as part of its primary review responsibility for SRP Section 14.2.

#### **B.1.4 Regulatory Redundancy**

NUREG-1412 (ADAMS Accession No. ML080310668), "Foundation for the Adequacy of the Licensing Bases," states:

"Initially the regulatory requirements came from the need to develop highly reliable instrumentation and control systems to monitor and control the operation of nuclear reactors and other critical systems. In response to this need, concepts and methods such as the single failure criterion, failure mode and effects analysis, reliability, failure rates, sneak circuit analysis, redundancy, and diversity were developed and applied. In August 1968, these concepts and methods were originally collected into proposed IEEE Standard 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," which was incorporated into 10 CFR 50.55a(h) in 1970. In addition, these concepts and methods were made part of the Commission regulations governing the design, fabrication, construction, installation, testing, and operation of these highly reliable instrumentation and control systems for nuclear reactors."

In addition, IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations –Description," states:

"This standard was evolved from IEEE Std 603-1980, Standard Criteria for Safety Systems for Nuclear Power Generating Stations. ... The series began with IEEE Std 279-1968 ..."

It is clearly recognized that there is some redundancy in regulatory requirements. Because of this regulatory redundancy, certain topics are addressed in more than one place in this ISG.

#### **B.1.5 Endorsed Industry Standards**

The NRC endorses industry standards through regulatory guides. These industry standards address various topical areas such as V&V and configuration management. Each standard represents a view from a defined perspective (e.g., configuration management). Therefore some of the various endorsed industry standards address some of the same topics (see subsections below). For example, it would be difficult to write a standard regarding configuration management that did not include the associated verifications, configurations audits, and reviews (some of which may be performed by the V&V team).

Chapter 7 of the SRP includes pointers to the various guidance documents and allows the licensee the design freedom to develop a set of development processes. The result being that a licensee should understand SRP Chapter 7 and all associated guidance in order to address any particular topical area. Industry requested that this ISG integrate into one place all of the



guidance associated with particular topical areas; however, this is not possible without significantly restricting development process freedom.

The following two subsections provide examples of how the same topic is addressed in various guidance documents.

### **Verification and Validation**

Regulatory Guide (RG) 1.168 Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," subject to exceptions listed in the Regulatory Positions in the RG. IEEE Std 1012 contains normative clauses regarding V&V.

RG 1.152 Revision 2, "Criteria for use of Digital Computers in Safety Systems of Nuclear Power Plants," Endorses IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," subject to exceptions listed in the Regulatory Positions in the RG. IEEE Std 7-4.3.2 Clauses 5.3.3 and 5.3.4 contain normative material regarding V&V.

Regulatory Guide (RG) 1.169 "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 828-1990, "IEEE Standard for Software Configuration Management Plans," subject to exceptions listed in the Regulatory Positions in the RG. IEEE Std 828 contains normative clauses regarding verification activities, configuration audits, and reviews.

### **Configuration Management**

Regulatory Guide (RG) 1.169 "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 828-1990, "IEEE Standard for Software Configuration Management Plans," subject to exceptions listed in the Regulatory Positions in the RG. IEEE Std 828-1990 contains normative clauses regarding configuration management (e.g., configuration audits and changes).

RG 1.152 Revision 2, "Criteria for use of Digital Computers in Safety Systems of Nuclear Power Plants," Endorses IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," subject to exceptions listed in the Regulatory Positions in the RG. IEEE Std 7-4.3.2-2003 Clause 5.3.5 contains normative material regarding configuration management.

Regulatory Guide (RG) 1.168 Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," subject to exceptions listed in the Regulatory Positions in the RG. IEEE Std 1012-1998 contains normative clauses regarding a Installation Configuration Audit and Change Assessment.

## **C. DIGITAL I&C REVIEW PROCESS**

The SRP provides guidance to NRC staff performing safety reviews of license amendments under 10 CFR Part 50. The SRP references some standards that are not endorsed by regulatory guides as sources of information for NRC staff. These standards are referenced in

the SRP as sources of good practices for NRC staff to consider. References to these standards in the SRP alone do not imply endorsement of these standards as a method acceptable to the NRC for meeting NRC regulations.

It is the intent of this plan to make information about regulatory matters widely available and to improve communication between the NRC, interested members of the public, and the nuclear power industry, thereby increasing understanding of the NRC's review process.

The review process described in this document is the current process used by the Office of Nuclear Reactor Regulation (NRR) to perform reviews of requests for amendments to operating licenses issued in accordance with Part 50. Specifically, Enclosure B identifies the documents and information to be submitted in a typical LAR that seeks to install a digital I&C safety system.

Precedent licensing actions are those with a similar proposed change and regulatory basis. Searching for, identifying, and using precedents in the review process maximizes staff efficiency, minimizes requests for additional information and ensures consistency of licensing actions. However, approval of a function or DSS at one plant does not serve as the basis for approving the same at another plant. Each LAR is a plant specific licensing action.

The staff's acceptance of a safety system is based on the system's ability to perform design basis functions (e.g., trip on high level, display of proper indications,...) and the system's conformance with regulatory requirements (e.g., redundancy, independence,...). This information is contained in a description of the design and in analysis reports that indicate the design meets requirements. In some cases it may be necessary to include testing and associated documentation to demonstrate that a certain design criterion has been achieved.

The staff's acceptance of software for safety system functions is based upon (1) conclusion 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. Branch Technical Position No. 14 (BTP 7-14) provides guidelines for evaluating software life-cycle processes for digital computer-based instrumentation and control (I&C) systems. The technical evaluation section for software development (i.e., Section D.4.4) is organized in the same manner as BTP 7-14. In some cases, the staff does not review docketed material, but rather performs audits or inspections of the associated documentation and development products. Subsections (e.g., D.4.4.2.4) clearly indicate the type (e.g., licensing review, licensing audit, & regional inspection) and timing (e.g., Phase 1, 2, & 3 – See Enclosure C) of regulatory oversight activities.

## **C.1 Process Overview**

Recognizing that digital I&C upgrades represent a significant licensee resource commitment, a phased approach is appropriate where critical, fundamental, system information is initially vetted through the NRC staff prior to undertaking subsequent steps in the digital I&C system development and licensing process. Therefore, the NRC staff encourages the use of public meetings prior to submittal of the LAR in order to discuss issues regarding the system development scope. The intent of this activity is to reduce regulatory uncertainty through the early resolution of major issues that may challenge the staff's ability to assess the systems compliance with NRC regulations. The NRC staff recognizes that some information may not be available upon initial submittal of the LAR, thus it is not expected that information sufficient to address all review topics be submitted until at least 12 months prior to the requested approval

date; the timing of specific exceptions may be a topic for discussions during the Phase 0 meetings.

A flow chart of the overall review process is included in Enclosure C and the various review phases are further discussed in Sections C.2 through C.5.

Additionally, the NRC staff recognizes that there are different approaches available to licensees regarding use and application of previously-approved digital platforms. Therefore, the NRC staff should consider applications to be within one of three tiers of review.

Tier 1 is applicable to license amendments proposing to reference a previously approved topical report (regarding a digital I&C platform or component(s) – hardware, software, and developmental tools) within the envelope of its generic approval as described in the topical report. A Tier 1 review would rely heavily upon previous review efforts. The list of documents that typically should be submitted by the licensee in support of a Tier 1 review is contained in Enclosure B, Column 1. This list would not include those documents already reviewed and approved by the NRC staff. Tier 1 generally addresses: (1) Application Specific Action Items (ASAI) identified in the safety evaluation, (2) post-SE regulatory changes, (3) post-Safety Evaluation (SE) regulatory guidance changes (e.g., DI&C-ISG-04), (4) evaluation of the equipment for performing application or plant specific functions, and (5) assembling, programming, integrating, and configuring the platform components to perform the application specific functions.

Tier 2 is applicable to license amendments proposing to reference a previously approved topical report with deviations to suit the plant-specific application. Deviations could include, for example, a revised software development process or new hardware. The deviations from the approved topical report should receive a significant review effort. Typically, an application citing licensing experience from another plant's previous approval would also be considered a Tier 2 review; this, however, is dependent upon the similarities of the application. The list of documents that would typically be submitted by the licensee in support of a typical Tier 2 review is contained in Enclosure B, Column 2. However for any particular submittal, the actual list of documents should be determined by the changes from the previously approved topical report as determined in the Phase 0 meetings. Tier 2 evaluations generally include Tier 1 review scope and any deviations from the approved SE or topical report.

Tier 3 is applicable to license amendments proposing to use a new digital I&C platform or component(s) with no generic approval. Licensees should expect that a Tier 3 review should receive a significant review effort within all review areas. The list of documents, that would typically be submitted by the licensee in support of a Tier 3 review, is contained in Enclosure B, Column 3. Tier 3 evaluations generally include Tier 1 review scope and topical report review scope. The typical topical review scope includes hardware, software, developmental tools, and associated developmental methods (e.g., application restrictions and integration methods).

These tier labels are used as a general guide for defining the scope or complexity of a review. It is expected that not all reviews will be in one tier or another. It is expected that systems with greater complexity should receive greater review effort.

Enclosure B is only an example list of "information to be provided," which has been explained throughout this ISG, that is reviewed. A licensee may have different names for similar documents. Regardless of the titles of the documents submitted, the actual LAR should contain sufficient information to address the criteria discussed in the technical evaluation

sections of Section D. It is possible that the plant specific application of a digital system may obviate the review of certain listed documents and necessitate the inclusion of other, unlisted, documents.

This guidance divides the whole of the review into a number of conceptual review areas. Doing this allows the review to be handled in a more regimented manner that fosters better tracking of outstanding information and communication of the associated status to the licensee. Additionally, this method supports knowledge transfer by allowing new reviewers to better conceptualize what should be reviewed versus a single large list of criteria. Not all of the review areas directly address meeting regulatory requirements, instead, some lay the groundwork for evaluating the criteria of others; this information subsequently feeds into the NRC staff's evaluation against the acceptance criteria (e.g., IEEE Std 603-1991).

## **C.2 Pre-Application (Phase 0)**

Prior to submittal of a LAR for a digital I&C upgrade, it is beneficial to have an overall design concept that adequately addresses NRC regulatory requirements and policy with regard to key issues (e.g., communication independence, defense-in-depth and diversity, demonstration of deterministic behavior, etc.). To this end, the NRC staff intends to use the public meeting process to engage licensees in a discussion of how their proposed digital I&C upgrade LAR should address: (1) key issues such as, defense-in-depth and diversity, (2) significant variances from current guidance, (3) NRC's determination of the appropriate "Tier" of review, and (4) other unique or complex topics associated with the proposed design. Such unique or complex topics could include, for example, a large scale system application with multiple interconnections and communication paths or major human-machine interface changes. These meetings are intended to be two-way discussions where, in addition to the licensee presentation of concept, the NRC staff can provide feedback on the critical aspects of the proposed design that are likely to affect (both positively and negatively) the NRC staff's evaluation.

As a minimum, the communication independence discussions should include whether the system will have: (1) interdivisional digital communications, or (2) nonsafety-related data diodes. As a minimum, the defense-in-depth and diversity discussions should include whether the system will have built-in diversity for all applicable events or whether the licensee will rely on: (1) a diverse actuation system or (2) diverse manual actions. Further, these discussions should include whether the licensee is proposing the use of an approved topical report, any planned deviations from NRC staff positions, and specifics of the software quality assurance plan. Licensees are encouraged to discuss topics from other review areas as well as how any best-estimate evaluations utilize realistic assumptions (or models) and address uncertainty associated with the results.

All proposed deviations from the document list and associated schedule described in Enclosure B should be discussed in the Phase 0 meeting(s). Any associated agreements should be documented in the Phase 0 meeting minutes. Delays by a licensee in meeting these commitments can result in an application being denied (see 10 CFR 2.108, "Denial of application for failure to supply information") or delay the evaluation completion date.

Following each meeting the NRC staff should capture the topics discussed via a meeting summary. This summary should include a preliminary NRC staff assessment of the licensee's concept (or those sub-parts of the overall concept discussed) and identify the areas that are

significant to this preliminary assessment. Additionally, as appropriate, the NRC staff should include a preliminary assessment of which review tier would be applicable for the proposed upgrade. The licensee should be provided a draft copy of the meeting summary comment prior to its issuance. An example meeting summary is included in Enclosure A to this document.

### **C.3 Initial Application (Phase 1)**

Once a licensee believes it has a design that adequately addresses NRC criteria, including, for example: (1) independence / redundancy, (2) defense-in-depth and diversity, (3) deterministic behavior, (4) variances to existing guidance, and (5) any unique or complex design features, it should prepare and submit a LAR (e.g., see Enclosure B, Information to be provided with the LAR). It is incumbent upon the licensee to identify any design features and concepts that may impact the NRC staff's preliminary assessment made during Phase 0. These features and concepts may adversely impact the NRC staffs acceptance of the LAR for review.

To the extent possible, the LAR should address the criteria associated with the following areas, which are discussed in further detail in the referenced sections:

- System Description (Section D.1)
- Hardware Development Process (Section D.2)
- Software Architecture (Section D.3)
- Software Development Process (Section D.4)
- Environmental Equipment Qualifications (Section D.5)
- Defense-in-Depth & Diversity (Section D.6)
- Communications (Section D.7)
- System, Hardware, Software, and Methodology Modifications (Section D.8)
- Compliance with IEEE Std 603 (Section D.9)
- Conformance with IEEE Std 7-4.3.2 (Section D.10)
- Technical Specifications (Section D.11)
- Secure Development and Operational Environment (Section D.12)

Initially, the NRC staff should review the application in accordance with the NRR Office Instruction, LIC-109, "Acceptance Review Procedures," (ADAMS Accession No. ML091810088), to determine whether the application is sufficient for NRC staff review; the acceptability of an application is normally documented in a letter (e.g., ADAMS Accession Nos. ML081070521, ML082460632, ML102220073, ML103130160). It is recognized that some sets of information may not be available upon initial application and the review process may be more efficiently administered by beginning prior to their availability. Therefore, a digital I&C upgrade application may be found to be sufficient for review provided a clear schedule for submission of omitted information is included. Any proposed changes to the schedule should be agreed upon by the

NRC staff prior to a given due-date. Licensees should be made aware that the NRC staff intends to adhere to the schedule set forth and failure to submit information in accordance with the schedule may result in denial of the application pursuant to 10 CFR 2.108.

During Phase 1, the NRC staff should draft the SE and issue requests for additional information (RAI) for the information that is necessary to finish the review of the docketed material. These activities should be conducted in accordance with LIC-101, "License Amendment Review Procedures" (Non-Publically Available). The NRC staff should also communicate those areas of review that, based upon the currently available information, appear to be acceptable. The licensee should respond to the RAIs prior to the submittal of the Phase 2 information. Although the NRC staff may have additional questions based on the responses to the Phase 1 RAI response, the licensee should not delay submission of the Phase 2 information. It is important to maintain close communications between the NRC staff and the licensee such that both parties remain cognizant of deliverables and due-dates. Use of a tracking system is encouraged.

As further discussed in Section C.4, the NRC staff and the licensee should be aware that some information may be in documentation available at licensee's facility (e.g., Enclosure B, table of documents to be available for audit 12 months prior requested approval date). The information examined in this manner should be documented and the NRC Project Manager, in consultation with the licensee and technical staff, should schedule the audit. While the information discussed in Section D.1 through D.12 indicates which process may be used (i.e., RAI or Audit), individual circumstances should dictate the appropriate vehicle for the NRC staff to obtain the information.

One of the reasons for a publically available safety evaluation is so members of the public can have confidence in the review process by understanding what was approved, and the basis for that approval. This is addressed, in part, in Information Notice 2009-07. Sufficient non-proprietary information, including some system design details and design methods, should be provided as non-proprietary by the licensee and vendor to make this possible. To satisfy this concern, non-proprietary versions of documents should limit the material that is redacted to only specific portions that are necessary (i.e., a document containing proprietary information does not make the entire document proprietary).

#### **C.4 Continued Review and Audit (Phase 2)**

Following response to the Phase 1 RAIs but at least 12 months prior to the requested approval date, the licensee should submit a supplement containing sufficient information to address aspects of the review areas not submitted in the initial LAR or subsequent RAIs (e.g., see Enclosure B, table of documents to be submitted 12 months prior to requested approval date). Although 12 months is the minimum lead time, the NRC staff should expect the licensee to adhere to the submittal schedules established earlier.

During Phase 2, the NRC staff should continue the RAI process until sufficient information has been provided for a decision to be rendered on the acceptability of the proposed digital I&C upgrade. If necessary, during the Phase 2 process, the NRC staff should conduct one or more audits in accordance with LIC-111, "Regulatory Audits," (ADAMS Accession No. ML082900195).

Audits may cover information from both Phase 1 and Phase 2, and may result in further requests for information to be docketed. It is the NRC staff's intent to perform the audits as

early in the process as is reasonable, but the performance of an effective and efficient audit necessitates that the LAR and supplements be sufficiently detailed about the later phases of the system development lifecycle. Although the use of an audit is discussed in Phase 2, this does not preclude the performance of an audit during Phase 1 if it is determined to be beneficial.

Some documentation may not be available 12 months prior to the anticipated issuance of the amendment. Although the plans and other available information should be submitted as early as possible, it is acceptable to submit certain documentation as mutually agreed in the Phase 0 meetings, but prior to the due date of the SE.

During the review of a digital I&C LAR, certain items may be identified that are applicable to the system configuration, testing or operation that contribute to approval of the system. These items should be identified within the SE as “potential items for inspection” after the system is installed.

Phase 2 should conclude with the issuance of a SE documenting the approval or denial of the licensee’s proposed digital I&C upgrade. The licensing process covered by this ISG ends at the issuance of the SE.

### **C.5 Implementation and Inspection (Phase 3)**

Following regulatory approval of the digital I&C system, licensees may implement the upgrade by installing the system, implementing associated procedural and technical specification changes, and completing startup testing.

The startup testing is conducted in accordance with the plan submitted during Phase 2. NRC regional staff may review the startup testing as an inspection function conducted by the appropriate regional staff in accordance with IP-52003, “Digital Instrumentation and Control Modification Inspection.”

Changes after approval of the LAR (i.e., starting in Phase 3) are controlled and implemented by licensee programs which, in turn, are governed by 10 CFR 50 Appendix B and other regulatory requirements. The need for prior NRC review and approval is governed by 10 CFR 50.59.

### **D. Review Areas**

The review of complex digital I&C system should be conducted both from the perspective of individual system characteristics as well as from an integrated hardware and software perspective to ensure an understanding of the system. Hardware design decisions can drive software complexity and, thus, exacerbate potential common cause failure concerns. For example, when plant parameters are input to a processor whose digital output is sent to a separate processor-based voting unit, the system is sending digital data to another digital processing platform; whereas, if the same data were sent to an analog platform, a different software interface would be used.

The twelve review areas described in the major subsection below address different aspects of the licensing review. Certain subsections are primarily concerned with an integrated system perspective, for example: Sections D.1, “System Description;” and D.9.4.2, “IEEE Std 603, Clause 5, System.” Other subsections are primarily concerned with a single aspect of a digital safety system review, for example, Sections D.4, “Software Development Process,” and D.5, “Environmental Equipment Qualification.”

## **D.1 System Description**

### **D.1.1 Scope of Review**

Reviewing the system description allows the NRC staff to understand how the components of the system interact to accomplish the design function; this description should be from an integrated hardware/software perspective in order to develop a clear understanding of the overall complexity of the system. Understanding the system provides a solid foundation for the subsequent detailed reviews and evaluation against the acceptance criteria.

### **D.1.2 Information to be Provided**

**Review (Phase 1):** (1) LAR Section 4.1 – System Description  
(2) Hardware Architecture Descriptions

The licensee's submittal should provide sufficient documentation and descriptions to allow the NRC staff to identify the hardware being used, how the hardware items function, how the various hardware items are interconnected, and any software in the system. The digital hardware items should be identified to the revision level. In those cases where the hardware, software, or their integration has previously been described by the vendor and evaluated by the NRC staff, the licensee should provide reference to the description and evaluation, including the ADAMS accession numbers if available. All changes to previously approved aspects should be evaluated (See Section D.8).

The documentation and description should be on two levels. First, the individual channels or divisions should be described, including a description of the signal flows between the various hardware items. Second, there should be a description of the overall system, with particular emphasis on additional hardware items not included in the description of the channels or divisions, such as voters, communications with workstations or non-safety systems, bypass functions/switches, and diverse actuation systems. The description of data communication pathways also should be reviewed in detail using the guidance in Section D.7, "Communications."

### **D.1.3 Regulatory Evaluation**

The licensee's description of the system should be documented in the NRC staff's SE to explain system operation and to support the technical evaluations of other sections. No specific technical or regulatory evaluations are made under this section.

Regulatory guidance for reviewing digital system real-time system architectures in I&C systems is contained in BTP 7-21, "Guidance on Digital Computer Real-Time Performance." Additional guidance applicable to architectural descriptions is contained in the SRP BTP 7-14 Section B.3.3.2, "Design Activities - Software Architecture Description." Section B.3.3.2 states that the Architecture Description should support the understanding of the functional and performance characteristics credited, and that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.3.1 "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance.



#### **D.1.4 Technical Evaluation**

The NRC staff should provide a description of the system that describes how the required functions of the system are accomplished. This description should include the key parts of the system that should be further evaluated against regulatory requirements and criteria in later sections of the SE.

#### **D.1.5 Conclusion**

The NRC staff should find that the information provides a comprehensive explanation of the system. From this the NRC staff should determine the scope of review, identify which portions of the system already approved by previous licensing actions, and identify any other constraints on the approval of the system.

### **D.2 Hardware Development Process**

#### **D.2.1 Scope of Review**

Supported by the review of the high-level interactions from Section D.1, the NRC staff reviews the development process used during the development of individual hardware items and the overall system under review. Also, the NRC staff reviews the licensee and vendor quality control programs associated with the hardware development.

#### **D.2.2 Information to be Provided**

**Review (Phase 1):** (1) LAR Section 4.2 – Hardware Development Process  
(2) Quality Assurance Plan for Digital Hardware

The licensee's submittal should provide sufficient information to allow the NRC staff to understand and document the hardware development process and the quality control methods used during that development process. This documentation should cover both the development methods used during the design of individual hardware modules during the development process and the design of the application specific system to be used in implementing the safety function. In those cases where the hardware development process and quality control methods used have previously been described by the vendor and evaluated by the NRC staff, the licensee should provide reference to the description and evaluation; any deviations or revision changes should be identified and adequately justified. If commercial grade dedication of existing components (or application framework) is being performed, the program administering the dedication should be provided or the process described in sufficient detail for the NRC staff to evaluate its conformance with regulatory criteria.

The review by the technical review branch responsible for I&C is predicated on the licensee being an Appendix B compliant organization; therefore, the hardware should be developed or dedicated in accordance with Appendix B compliant processes. This information would typically be in quality assurance plans and reports or commercial grade dedication plans and reports (if commercial grade dedication is used).

#### **D.2.3 Regulatory Evaluation**

The following regulatory requirements are applicable to the review of digital I&C upgrades with respect to the hardware development process:

10 CFR 50.55a(a)(1) addresses Quality Standards for Systems Important to Safety: "Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed."

10 CFR 50.55a(h)(3), "Safety Systems" states: "Applications filed on or after May 13, 1999 ... must meet the requirements for safety systems in IEEE Std 603-1991, and the correction sheet dated January 30, 1995."

IEEE Std 603 Clause 5.3 requires that components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates, and that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

GDC 1, "Quality Standards and Records" states: "Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed..."

#### **D.2.4 Technical Evaluation**

The NRC staff should provide a description of the development process and the quality control process that governed that development process. This description should cover both development of the individual functional units and modules and how those units and modules were used in the application-specific safety function design. Since this description should be contained in a publically available safety evaluation, portions of the licensee's description should be non-proprietary.

#### **D.2.5 Conclusion**

The NRC staff should find that the information provides a comprehensive explanation of the hardware development process. From this the NRC staff should determine the scope of review, identify portions of the system already approved by previous licensing actions, and identify any other constraints on the approval of the system.

### **D.3 Software Architecture**

#### **D.3.1 Scope of Review**

Reviewing the software architecture of the digital I&C system allows the NRC staff to understand how the high-level coded functions of the system interact to accomplish the safety function(s). Evaluation of the system at a high-level provides a foundation for subsequent detailed reviews and evaluation against the acceptance criteria. The architecture of the platform software (i.e., application independent software) also should be described.

Some digital technologies, such as a field-programmable gate arrays (FPGAs), do not utilize software while the system is in operation (BTP 7-14 should be used to review the associated development process). Instead, these systems use software to generate a hardware layout to be implemented in the FPGA. In these situations, the NRC staff's review of the software tools used to generate, implement, and maintain the FPGAs should be guided by IEEE Std 7-4.3.2-2003 Clause 5.3.2.

EPRI TR-106439 "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," states that operating history alone is not sufficient for commercial dedication of equipment. Operating history should be used in combination with one or more of the other three commercial dedication approaches (i.e., special tests and inspections, source evaluations, and supplier surveys).

See also NUREG/CR-7006 (ADAMS Accession No. ML100880142), "Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems," for guidance on reviewing FPGA-based safety systems.

### **D.3.2 Information to be Provided**

**Review (Phase 1):** (1) LAR Section 4.3 – Software Architecture  
(2) Software Architecture Descriptions

The licensee's submittal should provide sufficient documentation and descriptions to allow the NRC staff to identify the software used in the computer (or platform) and the application software, how the software functions, how the various software components are interrelated, and how the software utilizes the hardware. The software should be identified to the revision level. In those cases where the software has been described by the vendor and evaluated by the NRC staff previously, the licensee should provide reference to the description and evaluation. Any deviations or revision changes should be identified and adequately justified.

Similar to the information provided for Section D.1, "System Description," the description should be on two levels. First, the individual software operating within individual channels or divisions should be described, including a description of the signal flows between the various channels or divisions. Second, there should be a description of the overall system, with particular emphasis on any additional software not included in the description of the channels or divisions, such as voters, and communications with workstations or non-safety systems. The description of data communication pathways should be reviewed in detail by Section D.7, "Communications."

This information would typically be in the platform and application software architecture description, the platform and application software requirements specification, the platform and application software design specification, and in the commercial grade dedication plans and reports (if commercial grade dedication of software is used).

These descriptions should allow the NRC staff to understand and adequately document the software used in the safety-related application and to understand the functional interactions within the system. This should be used subsequently in support of addressing the criteria of the following sections.

### **D.3.3 Regulatory Evaluation**

The acceptance criteria for the software architecture description are contained in the Standard Review Plan, BTP 7-14 Section B.3.3.2, "Design Activities - Software Architecture Description." This section states that the Software Architecture Description should describe all of the functional and software development process characteristics listed, and that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.3.1 "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance. (see Section D.4.4.3.2).

### **D.3.4 Technical Evaluation**

The NRC staff should provide a description of the software architecture that describes how the function of the system is accomplished. This description should include the key parts of the system that should be further evaluated against regulatory requirements and criteria in later sections of the SE.

### **D.3.5 Conclusion**

The NRC staff should find that the information provides a comprehensive explanation of the software architecture. From this the NRC staff should determine the scope of review, identify portions of the system already approved by previous licensing actions, and identify any other constraints on the approval of the system.

## **D.4 Software Development Processes**

There may be several development processes to consider (e.g., platform developer, application developer, and the nuclear power plant licensee). Each entity may have its own processes that are different from those of the other entities; for example, each corporation should have its own software configuration management processes. However, not all twelve plans identified in BTP 7-14 should be docketed from each entity. In some cases a licensee has combined many of the generic aspects of the twelve plans, described in BTP 7-14, into a software program manual (SPM). In these cases project specific aspects (e.g., budget and schedule) are described in project plans. These SPMs can be reviewed and approved independent of a specific project, and any approval should generally contain application-specific action items to address project-specific aspects.

The NRC typically reviews the software development plans of the platform developer (unless it is a commercially dedicated platform) and the application developer during the licensing process. Changes that the licensee makes (e.g., per 10 CFR 50.59) and the associated documentation is addressed by the reactor oversight process.

### **D.4.1 Scope of Review**

The software development process describes the life-cycle of the development of the software to be used by and/or in support of the digital I&C system. It is important that this be a disciplined process where the necessary system performance is well defined and the management aspects of the system development project demonstrate that a high quality product should be the result of a deliberate, careful and high-quality development process. The NRC staff review of the development process products should evaluate against applicable standards and criteria that the licensee and vendor plans and software development activities are sufficiently disciplined to accomplish this goal.

Parallel to the development process, a verification and validation program should be implemented to monitor, evaluate, and document the development process. Verification is defined as the process of determining whether the products of a given phase of the development cycle fulfill the criteria established during the previous phase. Validation is defined as the test and evaluation of the integrated computer system to ensure compliance with the functional, performance, and interface criteria. Combined, verification and validation is the process of determining whether the criteria for a system or component are adequate, the products of each development phase fulfill (i.e., implements) the criteria imposed by the

previous phase, and the system or component complies with specified criteria. This determination may include analysis, evaluation, review, inspection, assessment, and testing of products and processes.

#### **D.4.2 Information to be Provided**

The licensee's submittal should provide sufficient documentation to support and justify the adequacy of the software life-cycle associated with the digital I&C system. The documentation should provide sufficient justification to allow the staff to conclude that the development process and product meet the applicable criteria, as discussed in Section D.4.4. The information provided should clearly delineate the roles and responsibilities of the various organizations contributing to the development, operation, and maintenance of the software. Additionally, the interactions and boundaries between these organizations should be clearly described.

#### **D.4.3 Regulatory Evaluation**

The NRC staff uses the following guidance to review digital I&C upgrades with respect to the software development process:

10 CFR 50.55a(a)(1) addresses Quality Standards for Systems Important to Safety: "Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed."

10 CFR 50.55a(h)(3), "Safety Systems" incorporates IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995 into the federal regulations by reference.

Regulatory Guide 1.152, Revision 2, "Criteria for Use of computers in Safety Systems of Nuclear Power Plants,," endorsed IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Clause 5.3.1 of IEEE Std 7-4.3.2, "Software Development," provides guidance. (see also Section D.10.4.4.2.3.1)

GDC 1, "Quality Standards and Records" states: "Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed..."

SRP Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."

IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," as endorsed by Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

IEEE Std 1028-1997, "IEEE Standard for Software Reviews and Audits," as endorsed by Regulatory Guide 1.168 Revision 1, "Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants."

IEEE Std 1012-1998, "IEEE Standard for Software Versification and Validation," as endorsed by Regulatory Guide 1.168 Revision 1, "Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants."

IEEE Std 828-1990, "IEEE Standard for Configuration Management Plans," as endorsed by Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

IEEE Std 829-1983, "IEEE Standard for Software Test Documentation," as endorsed by Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing," as endorsed by Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

#### **D.4.4 Technical Evaluation**

##### **D.4.4.1 Software Planning Documentation**

This subsection addresses acceptance criteria for planning activities. The acceptance criteria address specific software development planning activities and products (e.g., plans). These plans, when found to be acceptable, provide the reviewer with additional criteria for reviewing the process implementation and products of subsequent life cycle activities, as discussed in Subsections D.4.4.2 and D.4.4.3 below.

##### **D.4.4.1.1 Software Management Plan (SMP)**

#### **Review (Phase 1): Software Management Plan**

SRP BTP 7-14, in Section B.3.1.1, provides acceptance criteria for a software management plan. This section states that Regulatory Guide 1.173 endorses IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" and that Clause 3.1.6, "Plan Project Management," contains an acceptable approach to software project management. Clause 3.1.6 states that the plan should include planning for support, problem reporting, risk management (e.g., see Section D.10.4.2.3.6), and retirement. These criteria are applied to both licensee and vendor programs.

The purpose of the NRC staff review of the SMP is to conclude that the management aspects of the software development project are such that high quality software should result, if the plans are followed. This necessitates a deliberate and careful development process. There are several management characteristics that are of particular interest to the staff, and the SMP should cover these aspects in detail. The software development may be performed by a vendor and not by the licensee; therefore, the interface between the licensee and vendor, and the method by which the quality of the vendor effort should be evaluated by the licensee is critical. It is important that licensee oversight of the vendor software development program exists and is effective. Software or system vendors may not be familiar with regulatory requirements or with specific plant criteria, and therefore, one of the more important aspects is oversight by the licensee that is effective and meets 10 CFR Part 50, Appendix B. The SMP should describe the interaction, the checks and audits the licensee should perform, and the standard by which the success of the audit should be judged.

Another important aspect of the SMP is the relationship between the software development group and the group(s) that check the quality of both the software development program and the software. Generally, these checking functions are quality assurance, software safety, and

verification and validation. It is important that these functions maintain independence from the development organization. The independence of quality assurance, software safety, and verification and validation processes, activities, and tasks should be described in terms of technical, managerial, schedule, technical capabilities, and financial aspects. If these independence aspects are described in the planning documents of these organizations, such as the V&V Plan, Safety Plan, or QA plan; the SMP should provide a pointer to the appropriate section of those plans.

The NRC staff may review the responsibilities of each position of the project's management and technical teams. The review should conclude (during subsequent audits) that the personnel responsible for various items have the experience or training to perform those duties. This information should be included in the SMP.

The SMP should include sufficient information about the secure development and operational environment (see Section D.12) for the reviewer to conclude that the methods used are consistent with Regulatory Guide 1.152 (see also RG 1.152 Draft Rev. 3 – DG 1249) and that the methods are used effectively; this should be an actual description of the secure environment described in RG 1.152, and not just a statement that all secure environment criteria should be met. The review of how those criteria are being met may be addressed in separate NRC guidance on this issue, as indicated in Section D.12.

The adequacy of the budget and personnel for the quality assurance organization, the software safety organization, and the software verification and validation organization is of interest, and should ensure that those groups have adequate resources to support a high quality development effort. This may necessitate some judgment, and it may necessitate a justification by the licensee or vendor. In addition, software safety and V&V personnel should be competent in software engineering in order to ensure that software safety and software V&V are effectively implemented. A general rule of thumb is that the V&V personnel should be at least as qualified as the development personnel.

#### D.4.4.1.2 Software Development Plan (SDP)

##### **Review (Phase 1):** Software Development Plan

The SDP should clearly state which tasks are a part of each life cycle activity, and state the task inputs and outputs. The review, verification, and validation of those outputs should be defined.

The acceptance criteria for a software development plan are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.2. This section states that Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," subject to exceptions listed, as providing an approach acceptable to the staff, for meeting the regulatory requirements and guidance as they apply to development processes for safety system software and that Clause 5.3.1 of IEEE Std 7-4.3.2-2003 contains additional guidance on software development.

The NRC staff review of the software development is primarily intended to confirm that use of the SDP results in a careful and deliberate process, which should result in high quality software, suitable for use in safety-related systems in nuclear power plants. The details on how this should be done may be found in other plans, such as the Software Verification and Validation Plan (SVVP), and the Software Configuration Management Plan (SCMP). If this is done, the

SDP should provide pointers to the appropriate sections of those other plans. An important aspect of the software development plan is the method to be used to make sure these other plans are being applied. This would generally include a provision for effective oversight, where the strategy for managing the technical development is specified. The SDP should discuss these aspects in detail, to allow the reviewer to conclude that the software development plan allows the licensee or vendor to adequately monitor the software development process, and that any deviations from the software development process should be discovered in time to take corrective action.

Risks that should be specifically discussed are those associated with risks due to size and complexity of the product, and those associated with the use of pre-developed software. Complexity of the product should be explicitly addressed. The reviewer should conclude that the licensee has considered this risk. The use of commercial software and hardware may be attractive due to cost, schedule, and availability, but there is some risk that a commercial grade dedication process could show the items to lack the quality necessary for use in safety-related systems in nuclear power plants, and that risk should be described and discussed (see also Sections D.10.4.2.3.6 and D.10.4.2.4.2).

Under the resource characteristics, the methods and tools to be used should be evaluated. Of particular interest to the staff is the method by which the output of software tools, such as code generators, compilers, assemblers, or testers, etc., are verified to be correct. This aspect of tool usage should be specifically covered in the SDP. The criterion from IEEE Std 7-4.3.2-2003 is that software tools should be used in a manner such that defects not detected by the software tool are detected by V&V activities. If this is not possible, the tool itself should be designed as safety-related (see also Section D.10.4.2.3.2).

The SDP should list the international, national, industry, and company standards and guidelines, including regulatory guides, that are to be followed, and whether these standards and guidelines have been approved by the NRC staff. If the standards have not been reviewed and approved, the staff may review the standard to confirm that adherence to the standard will result in meeting regulatory requirements. Coding standards should follow the suggestions contained in NUREG/CR-6463, "Review Guidance for Software Languages for Use in Nuclear Power Plant Safety Systems," or as appropriate NUREG/CR-7006, "Review Guidelines for Field Programmable Gate Arrays in Nuclear Power Plant Safety Systems."

#### D.4.4.1.3 Software Quality Assurance Plan (SQAP)

##### **Review (Phase 1):** Software QA Plan

Quality assurance is required by 10 CFR Part 50, Appendix B. The Software Quality Assurance Plan (SQAP) should be implemented under an NRC approved Quality Assurance (QA) program. 10 CFR Part 50, Appendix B, allows the licensee to delegate the work of establishing and executing the quality assurance program, but the licensee shall retain responsibility. The plan should identify which QA procedures are applicable to specific software development processes, and identify particular methods chosen to implement QA procedures. There are several Regulatory Guides and Standards that offer guidance: The acceptance criteria for a SQAP are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.3.

1. Regulatory Guide 1.28, Revision 3, "Quality Assurance Program Requirements (Design and Construction)," that endorses ANSI/ASME NQA-1-1983, "Quality Assurance Program



Requirements for Nuclear Facilities,” and the ANSI/ASME NQA-1a-1983 Addenda, “Addenda to ANSI/ASME NQA-1-1983 “Quality Assurance Program Requirements for Nuclear Facilities.”

2. Regulatory Guide 1.152, Revision 2, “Criteria for Use of computers in Safety Systems of Nuclear Power Plants,,” endorsed IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Clause 5.3.1 of IEEE Std 7-4.3.2, “Software Development,” provides guidance (see Section D.10.4.2.3.1).

3. Regulatory Guide 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems in Nuclear Power Plants” endorses IEEE Std 1074-1995, “IEEE Standard for Developing Software Life cycle Processes,”

4. NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.1.2, “Software Quality Assurance Plan,” and Section 4.1.2, “Software Quality Assurance Plan,” contain guidance on these plans.

The SQAP is one of the more important plans that should be reviewed by the staff. The staff reviewer should conclude not only that the SQAP exhibits the appropriate management, implementation and resource characteristics, but also that following the SQAP will result in high quality software that will perform the intended safety function. The NRC staff should review the development process and products to evaluate the effectiveness of the licensee or vendor QA and V&V efforts, and to assess whether the licensee or vendor QA and V&V efforts were performed correctly. If errors not already discovered and documented by either the QA organization or the V&V team are found, this indicates a potential weakness in the effectiveness of the QA organization and would merit further review.

The software QA organization should be described in sufficient detail to show that there is sufficient authority and organizational freedom, including sufficient independence from cost and schedule to ensure that the effectiveness of the QA organization is not compromised.

#### D.4.4.1.4 Software Integration Plan (SIntP)

**Review (Phase 1):** Software Integration Plan (Phase 1)

**Audit (Phase 2):** Software Integration Report

The acceptance criteria for a software integration plan are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.4, “Software Integration Plan.” This section states that Regulatory Guide 1.173, endorses IEEE Std 1074-1995, and that within that standard, Clause 5.3.7, “Plan Integration,” contains an acceptable approach relating to planning for software (code) integration. Clause 5.3.7 states that the software criteria and the Software Detailed Design should be analyzed to assess the order for combining software components into an overall system, and that the integration methods should be documented. The integration plan should be coordinated with the test plan. The integration plan should also include the tools, techniques, and methodologies to perform the software (code) integrations. The planning should include developing schedules, estimating resources, identifying special resources, staffing, and establishing exit or acceptance criteria.

Software integration actually consists of three major phases: integrating the various software modules together to form single programs, integrating the result of this with the hardware and instrumentation, and testing the resulting integrated product. In the first phase, the various

object modules are combined to produce executable programs. The second phase is when these programs are then loaded into test systems that are constructed to be as nearly identical as possible to the ultimate target systems, including computers, communications systems, and instrumentation. The third phase consists of testing the resulting system. Multiple levels of integration may be necessary, depending on the complexity of the software system that is being developed. Several integration steps may be necessary at some levels. Without a Software Integration Plan, it is possible that the computer system could lack important elements, or that some integration steps could be omitted.

The staff should review and audit the software integration plan to assess the adequacy of the planned software integration effort. The software integration organization is generally the same group as the software developers, but this is not always the case. If there is more than one group of software developers, or if some of the software is dedicated commercial grade or a reuse of previously developed software, the methods, and controls for software integration become more critical, and should be described in sufficient detail to allow the reviewer to conclude that the integration effort is sufficient.

With regard to management characteristics, the Software Integration Plan should include a general description of the software integration process, the hardware/software integration process, and the goals of those processes. It should involve a description of the software integration organization and the boundaries between other organizations. Reporting channels should be described and the responsibilities and authority of the software integration organization defined.

The implementation characteristics should include a set of indicators to confirm the success or failure of the integration effort. Data associated with the integration efforts should be taken and analyzed to assess the error rate.

The resource characteristics of the software integration plan should include a description of the methods, techniques, and tools that are to be used to accomplish the integration function. The plan should necessitate that integration tools be qualified with a degree of rigor and a level of detail appropriate to the safety significance of the software being created.

#### D.4.4.1.5 Software Installation Plan (SInstP)

##### **Inspect (Phase 3):** Software Installation Plan

The Software Installation Plan may not be reviewed in the staff SE. Application installation is not a part of the licensing process. The Software Installation Plan, may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the installation prior to the system being put into operational use.

Guidance for this plan is contained in the Standard Review Plan, BTP 7-14, Section B.3.1.5, "Software Installation Plan."

#### D.4.4.1.6 Software Maintenance Plan (SMaintP)

##### **Inspect (Phase 3):** Software Maintenance Plan

The Software Maintenance Plan may not be reviewed in the staff SE. Licensee maintenance is not a part of the licensing process. The Software Maintenance Plan may be inspected as part of

the regional inspection program. The licensee should be prepared to support any regional inspections of the maintenance plan prior to the system being put into operational use.

Guidance for this plan is contained in the Standard Review Plan, BTP 7-14, Section B.3.1.6, "Software Maintenance Plan."

#### D.4.4.1.7 Software Training Plan (STrngP)

##### **Inspect (Phase 3):** Software Training Plan

The software training plan may not be reviewed in the staff SE. Licensee training is not a part of the licensing process. Instead, it falls under the regional inspection purview. The licensee should be prepared to support any regional inspections of the training done in preparation for use of the proposed system prior to the system being put into operational use.

Guidance for this plan is contained in the Standard Review Plan, BTP 7-14, Section B.3.1.7, "Software Training Plan."

#### D.4.4.1.8 Software Operations Plan (SOP)

##### **Inspect (Phase 3):** Software Operations Plan

The Software Operations Plan may not be reviewed in the staff SE. Licensee operations are not a part of the licensing process. The Software Operations Plan may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.

Guidance for this plan is contained in the Standard Review Plan, BTP 7-14, Section B.3.1.8, "Software Operations Plan."

#### D.4.4.1.9 Software Safety Plan (SSP)

##### **Review (Phase 1):** Software Safety Plan

The acceptance criteria for a software safety plan are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.9, "Software Safety Plan." This section states that the Software Safety Plan should provide a general description of the software safety effort, and the intended interactions between the software safety organization and the general system safety organization. It further states that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.1.5 "Software Safety Plan," and Section 4.1.5 "Software Safety Plan," contain guidance on Software Safety Plans. Further guidance on safety analysis activities can be found in Regulatory Guide 1.173, Section C.3, "Software Safety Analyses."

The Software Safety Plan should describe the boundaries and interfaces between the software safety organization and other organizations. It should show how the software safety activities are integrated with other organizations and activities. It should also designate a single safety officer that has clear responsibility for the safety qualities of the software being constructed. Each person or group responsible for each software safety task should be specified. Further, the Software Safety Plan should include measures to confirm the success or failure of the software safety effort and analyze its effectiveness.

The plan should show how the licensee should handle the various issues. It is also possible, that the elements of software safety may be addressed in another plan such as the Software Management Plan. As long as the concepts discussed above are addressed, either approach is acceptable, however if the elements of software safety are addressed in other plans, the software safety plan should contain pointers to the appropriate sections of those other plans.

The plan should designate a group that specifically considers the safety issues of the digital system to confirm the acceptability of the system, and the software safety plan should define that group. The safety organization should consider the secure development and operational environment (see Section D.12) risk as well as the risk to the plant if the digital system malfunctions. Since the NRC staff should assess whether the proper risks were considered (i.e., that the licensee addresses these risks in an appropriate manner and stayed consistent with the software safety strategy), the software safety plan should specifically address these issues in the risk evaluations.

#### D.4.4.1.10 Software Verification and Validation Plan (SVVP)

##### **Review (Phase 1):** Software V&V Plan

The acceptance criteria for software verification and validation plans are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.10, "Software Verification and Validation Plan," and Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities." These sections state that Regulatory Guide 1.168 Revision 1, "Verification, Validation, Reviews, And Audits for Digital Computer Software Used in Safety Systems Of Nuclear Power Plants," endorses IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," as providing methods acceptable to the staff for meeting the regulatory requirements as they apply to verification and validation of safety system software, subject to the exceptions listed in these Regulatory Positions. Section B.3.2.2 states that further guidance can be found in Regulatory Guide 1.152, Revision 2, Section C.2.2.1, "System Features," and NUREG/CR-6101 (ADAMS Accession No. ML072750055), Sections 3.1.4 and 4.1.4. (See also Sections D.10.4.2.3.3 and D.10.4.2.3.4)

Verification and Validation (V&V) is the process of determining whether the criteria for a system or component are adequate, the products of each development phase fulfill (i.e., implements) the criteria imposed by the previous phase, and the system or component complies with specified criteria. This determination may include analysis, evaluation, review, inspection, assessment, and testing of products and processes.

The NRC staff considers the Software Verification & Validation Plan one of the key documents among the various plans reviewed. The NRC staff expects the licensee or vendor to develop and implement a high quality process to ensure that the resultant software is of high quality. The SVVP should demonstrate a V&V effort that is sufficiently disciplined and rigorous to ensure a high quality software development process. The V&V plan should demonstrate to the staff that the V&V effort should identify and solve the problems which could detract from a high quality design effort. The NRC staff should review the Software Verification & Validation Plan, as well as the various V&V reports, in great detail to reach this determination.

One of the most critical items in the Software Verification & Validation Plan is the independence of the V&V organization. Per IEEE Std 1012-1998, the V&V team should be independent in management, schedule, and finance. The plan should specifically show how the V&V team is independent, and how the V&V personnel are not subject to scheduling constraints or to

pressure from the software designers or project managers for reports or review effort. The SVVP should illustrate that the V&V team should report to a high enough level of management within the company to ensure that deficiencies discovered by the V&V organization should be resolved effectively. The plan should also show how the V&V effort is sufficiently independent to adequately perform the tasks without undue influence to schedule and financial pressure.

A second important issue is the number and quality of the V&V personnel. There is no specific criteria for the number of V&V personnel, but generally, equal effort is necessary for a sufficient V&V process as for original design. Thus, there should be rough parity between the two groups in terms of manpower and skill level. If the design group has significantly more resources than the V&V group, either the V&V effort may fall behind, or the V&V effort may not be able to perform all the items necessary. The plan should illustrate how the vendor or licensee management will confirm if the output from the V&V team and the overall V&V quality is acceptable, or if some functions are not being performed.

The training and qualification of the V&V personnel is also important. If a V&V engineer is to judge the output of a software design engineer, the V&V engineer should be qualified to understand the process, technology, and the software. If the V&V engineer is not qualified, the V&V effort may not be effective. The plan should address how the training and qualification of the V&V personnel was verified.

The Software Verification & Validation Plan should also address how the results of the V&V effort are to be fully and carefully documented, and that each of the discrepancies be documented in a report that includes how they were resolved, tested, and accepted by the V&V organization. Experience has shown that problems found in products can result from fixes to earlier problems, where a fix itself did not go through the V&V process, was not properly tested, and subsequently creates additional problems or does not fully address the original issue. The SVVP should specifically address the V&V criteria for discrepancy fixes, including the verification that the regression testing used was adequate.

The Software Verification & Validation Plan should describe reporting criteria. It should necessitate that reports document all V&V activities, including the personnel conducting the activities, the applicable procedures, and associated results. This includes V&V review of the documentation criteria, evaluation criteria, error reporting processes, and anomaly resolution processes. V&V reports should summarize the positive practices and findings as well as negative practices and findings. The reports should summarize the actions performed and the methods and tools used.

In general, the SVVP should document how IEEE Std 1012 is met, and for any IEEE Std 1012 normative material which is not being met, what compensatory actions are being used to demonstrate an equivalent level of verification and validation.

#### D.4.4.1.11 Software Configuration Management Plan (SCMP)

##### **Review (Phase 1):** Software Configuration Management Plan

The acceptance criteria for a software configuration management plan is contained in the Standard Review Plan, BTP 7-14, Section B.3.1.11, "Software Configuration Management Plan," and Section B.3.2.3, "Acceptance Criteria for Software Configuration Management Activities." These sections states that both Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power

Plants” that endorses IEEE Std 1074-1995, Clause 7.2.4, “Plan Configuration Management,” and Regulatory Guide 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” that endorses IEEE Std 828-1990, “IEEE Standard for Configuration Management Plans,” provide an acceptable approach for planning configuration management. BTP 7-14, Section B.3.1.11 further states that additional guidance can be found in IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems on Nuclear Power Generating Stations,” Clause 5.3.5, “Software configuration management,” and in Clause 5.4.2.1.3, “Establish configuration management controls,” (see Section D.10.4.2.3.5). NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.1.3 “Software Configuration Management Plan,” and Section 4.1.3, “Software Configuration Management Plan,” also contain guidance.

Configuration management provides the methods and tools to identify and control the system and programming throughout its development and use. Activities include 1) the identification and establishment of baselines, 2) the review, approval, and control of changes, 3) the tracking and reporting of such changes, 4) the audits and reviews of the evolving products, and 5) the control of interface documentation. Configuration management is the means through which the integrity and traceability of the system are recorded, communicated, and controlled during both development and maintenance. The configuration management plan should include an overview description of the development project and identify the configuration items that are governed by the plan. The plan should also identify the organizations, both technical and managerial, that are responsible for implementing configuration management.

The Software Configuration Management Plan is another important plan because the system can malfunction if the wrong version of the software is modified, or the changes are not sufficiently tested to ensure that they do not introduce new errors. Configuration management starts once the initial product (i.e., the specification, design or software) is initially released by the group responsible for that product.

One of the critical items which should be discussed in the SCMP is an exact definition of who controls the software. There should be a software librarian or equivalent group who is responsible for keeping the various versions of the software, giving out the current version for test or modification, and receiving back the modified and tested software.

Another critical item is what items are under configuration control. The plan should specify that all design inputs and products, including software; not just the operational code to be used in the safety application, is controlled. This would include any software or software information which affects the safety software, such as software components essential to safety; support software used in development; libraries of software used in testing; test results used to qualify software; analyses and results used to qualify software; software documentation; databases and software configuration data; pre-developed software items that are safety system software; software change documentation; and tools used in the software project for management, development or assurance tasks. Each of these can affect the product if a wrong version is used during the software development process.

The Software Configuration Management Plan may be three different plans: platform development, application development, and one used by the licensee during the operational phase of the project. Licensing review should address the handoff from platform development SCMP to the application development SCMP. The licensee plan may be contained in an overall plant configuration management plan. If this is the case, the licensee should check that software specific issues have been addressed in the plant configuration management plan. The

operation and maintenance phase SCMP may not be reviewed and approved with the LAR, but may be subject to regional inspection of the system. Regional oversight may also address the handoff from application development SCMP to the operational phase SCMP.

#### D.4.4.1.12 Software Test Plan (STP)

##### **Review (Phase 1):** Software Test Plan

The acceptance criterion for a software test plan is contained in the Standard Review Plan, BTP 7-14, Section B.3.1.12, "Software Test Plan," and in Section B.3.2.4, "Acceptance Criteria for Testing Activities." These sections state that both Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," that endorses IEEE Std 829-1983, "IEEE Standard for Software Test Documentation," and Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," that endorses IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing," identify acceptable methods to satisfy software unit testing criteria.

The purpose for the test plan is to prescribe the scope, approach, resources, and schedule of the testing activities; to identify the items being tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the risks associated with the plan. The Software Test Plan should cover all testing done to the software, including unit testing, integration testing, factory acceptance testing, site acceptance testing, and installation testing. If any of these types of testing is not being performed, this exception should be specifically discussed and justified, and the additional actions taken to compensate for this lack of testing explained. The test plan should be examined to ensure the test planning is understandable, that testing responsibilities have been given to the appropriate personnel, and that adequate provisions are made for retest in the event of failure of the original test. Since modifying software after an error occurs can result in a new error, it is important that the Software Test Plan specifies the full set of tests be run after any modification to the software.

A significant portion of the testing is considered a part of the V&V activities. Section 5.4.5 of IEEE Std 1012-1998, the IEEE Standard for Software Verification and Validation, endorsed by RG 1.168 Revision 1, discusses V&V test. This section states, "the V&V effort [should] generate its own V&V software and system test products (e.g., plans, designs, cases, and procedures), execute and record its own tests, and verify those plans, designs, cases, procedures, and test results against software [criteria]." Since this testing is considered a V&V test, the Software Test Plan should assign the responsibility of the definition, test design, and performance to the V&V group. The NRC staff should specifically be reviewing the test plan to ensure that the specified V&V test is generated and performed by the V&V group, and not done by a design or test group, and merely checked by V&V personnel.

#### D.4.4.2 Software Plan Implementation

This subsection addresses acceptance criteria for implementation activities. The acceptance criteria address specific software life cycle process implementation activities and documentation. These activities and products, when found to be acceptable, provide the reviewer with confidence that the plans have been carried out. The NRC staff reviewer assesses whether the plans have been followed by the software developer. The detailed acceptance criteria are provided by the software developer and evaluated by the NRC staff in its acceptance of the plans.

#### D.4.4.2.1 Software Safety Analysis (SSA)

##### **Review (Phase 2):** Safety Analysis

The acceptance criteria for a software safety analysis are contained in the Standard Review Plan, BTP 7-14, Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities." This section states that the SSP (see Section D.4.4.1.9) describes the safety analysis (SA) implementation tasks that are to be performed. The acceptance criterion for software safety analysis implementation is that the tasks in that plan have been carried. The SA shows that the safety analysis activities have been successfully accomplished for each life cycle activity group and that the proposed digital system is safe. In particular, the SA shows that the system safety criteria have been adequately addressed for each activity group; that no new hazards have been introduced; that the software criteria, design elements, and code elements that can affect safety have been identified; and that all other software criteria, design, and code elements should not adversely affect safety.

Regulatory Guide 1.168 Revision 1, "Verification, Validation, Reviews, And Audits for Digital Computer Software Used in Safety Systems Of Nuclear Power Plants," endorses IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," as providing methods acceptable to the staff for meeting the regulatory requirements as they apply to verification and validation of safety system software, subject to the exceptions listed in the Regulatory Positions. IEEE Std 1012 states:

"Some V&V activities and tasks include analysis, evaluations, and tests that may be performed by multiple organizations (e.g., software development, project management, quality assurance, V&V). For example, risk analysis and hazard analysis are performed by project management, the development organization, and the V&V effort. The V&V effort performs these tasks to develop the supporting basis of evidence showing whether the software product satisfies its criteria. These V&V analyses are complementary to other analyses and do not eliminate or replace the analyses performed by other organizations. The degree to which these analyses efforts are coordinated with other organizations [should] be documented in the organizational responsibility section of the SVVP."

It is preferable to docket the safety analysis associated with each phase as soon as it has been finished; however, the analysis should be docketed by the start of Phase 2.

#### D.4.4.2.2 V&V Analysis and Reports

##### **Review (Phase 2):** V&V Reports

**Audit (Phase 2):** (1) Individual V&V Problem Reports up to FAT  
(2) Software Integration Report

SRP Chapter 7 BTP 7-14 Section B.3.2.2 contains SRP acceptance criteria and references to applicable guidance:

Regulatory Guide 1.168, Revision 1, endorses IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," as providing methods acceptable to the staff for meeting the regulatory requirements as they apply to verification and validation of safety system software, subject to the exceptions listed.



Regulatory Guide 1.168, Revision 1, also endorses IEEE Std 1028-1997, "IEEE Standard for Software Reviews and Audits," as providing an approach acceptable to the staff for carrying out software reviews, inspections, walkthroughs and audits, subject to the exceptions listed.

Clause 5.3.3, "Verification and Validation" and Clause 5.3.4, "Independent V&V (IV&V) requirements," of IEEE Std 7-4.3.2-2003 which is endorsed by Regulatory Guide 1.152, Revision 2, contain guidance on V&V.

The SVVP (see Section D.4.4.1.10) describes the V&V implementation tasks that are to be carried out. The acceptance criterion for software V&V implementation is that the tasks in the SVVP have been carried out. Documentation should exist that shows that the V&V tasks have been successfully accomplished for each life cycle activity group. In particular, the documentation should show that the requirements, design, code, and integration design outputs satisfy the appropriate software development functional and process characteristics.

Problems identified by the verification effort should be documented, together with any action items necessary to mitigate or eliminate each problem. A record should be kept of actions taken in response to the action items and the appropriate CM activities should be performed.

As part of the software V&V effort, a traceability analysis should be performed and documented. This traceability analysis documentation should clearly show the linkage between each criterion imposed on the software by the system specification document and system design documents, and one or more criterion in the SRS. The analysis documentation should allow traceability in both directions. It should be organized so that as design, implementation, and validation take place, traceability information can be added for these activities. It should be updated at the completion of each life cycle activity group. The analysis documentation should permit tracing from the system specification and design through the software specification, design, implementation, integration, and validation.

The integration V&V activities should demonstrate that all unit and subsystem tests specified by the SVVP were successful. Any anomalies or errors found during the tests should be resolved and documented. Integration tests should be documented. Reports should be written for each test run. These reports should include any anomalies found and actions recommended. The integration V&V report should describe the procedures followed and the tests performed during integration. This report should be consistent with the SIntP.

The software validation activities should demonstrate that all validation tests specified by the SVVP were successful. The testing process should contain one or more tests for each criterion in the SRS, as well as the acceptance criteria for each test. The result of each test should clearly show that the associated criterion has been met. Each test procedure should contain detailed information for the test setup, input data specification, output data expectations, and completion time. Documentation should be produced for each test.

Procedures should be included for handling errors and anomalies that are encountered during the testing. These procedures should include correction procedures (including configuration management), and provision for re-test until such time as the problems are resolved. A report summarizing the validation testing should be provided. The report should contain a summary of problems and errors encountered during testing, and the actions taken to correct the problems encountered. The report should contain a statement that the validation testing was successful and that the software tested met all of the criteria of the SRS.

It is preferable to docket the V&V reports associated with each phase as soon as they are completed; however, they all should be docketed by the start of Phase 2.

#### D.4.4.2.3 Configuration Management Activities

**Review (Phase 2):** As-Manufactured, System Configuration Documentation

**Audit (Phase 2):** Configuration Management Reports

SRP Chapter 7 BTP 7-14 Section B.3.3 contains SRP acceptance criteria and references to applicable guidance:

Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 1042-1987, "IEEE Guide to Software configuration management," subject to specific provisions identified in the regulatory guide, as providing guidance that is acceptable for carrying out software configuration management.

There are many configuration management tools available for software. A particular tool should be selected, evaluated, and used properly for software configuration control.

The SDP describes the software and documents that should be created and placed under configuration control. The software configuration control system should be described. The SCMP describes the implementation tasks that are to be carried out. The acceptance criterion for software CM implementation is that the tasks in the SCMP (see Section D.4.4.1.11) have been carried out.

Documentation should exist that shows that the configuration management tasks for that activity group have been successfully accomplished. In particular, the documentation should show that configuration items have been appropriately identified; that configuration baselines have been established for the activity group; that an adequate change control process has been used for changes to the product baseline; and that appropriate configuration audits have been held for the configuration items created or modified for the activity group.

Each configuration item should be labeled unambiguously so that a basis can be established for the control and reference of the configuration items defined in the SCMP. Configuration baselines should be established for each life cycle activity group, to define the basis for further development, allow control of configuration items, and permit traceability between configuration items. The baseline should be established before the set of activities can be considered complete. Once a baseline is established, it should be protected from change. Change control activities should be followed whenever a derivative baseline is developed from an established baseline. A baseline should be traceable to the baseline from which it was established, and to the design outputs it identified or to the activity with which it is associated.

Configuration control actions should be used to control and document changes to configuration baselines. A configuration control board (CCB) should exist with the authority to authorize all changes to baselines. Problem reports should be prepared to describe anomalous and inconsistent software and documentation. Problem reports that necessitate corrective action should invoke the change control activity. Change control should preserve the integrity of configuration items and baselines by providing protection against their change. Any change to a configuration item should cause a change to its configuration identification. This can be done via a version number or attached change date. Changes to baselines and to configuration items under change control should be recorded, approved and tracked. If the change is due to a problem report, traceability should exist between the problem report and the change. Software changes should be traced to their point of origin, and the software processes affected by the change should be repeated from the point of change to the point of discovery. Proposed changes should be reviewed by the CCB for their impact on system safety.

Status accounting should take place for each set of life cycle activities prior to the completion of those activities. The status accounting should document configuration item identifications, baselines, problem report status, change history and release status.

The configuration management organization should audit life cycle activities to confirm that configuration management procedures were carried out in the life cycle process implementation.

#### D.4.4.2.4 Testing Activities

**Review (Phase 2):** (1) Test Design Specification  
(2) Summary Test Reports (Including FAT)  
(3) Summary of Test Results (Including FAT)

**Audit (Phase 2):** (1) Test Procedures Specification  
(2) Completed Test Procedures and Reports  
(3) Test Incident Reports

**Inspect (Phase 3):** Site Test Documentation

SRP Chapter 7 BTP 7-14 Section B.3.4 contains SRP acceptance criteria and references to applicable guidance (see also Section D.4.4.1.12):

Regulatory Guide 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," with a few noted exceptions, identifies an acceptable methods for addressing computer system qualification testing (See: IEEE Std 7-4.3.2-2003 Clause 5.4.1, "Computer System Testing" – see Section D.10.4.2.4.1).

Regulatory Guide 1.168, Revision 1, Section 7.2, "Regression Analysis and Testing," and 7.4, "Test Evaluation," contain guidance related to testing activities. Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 829-1983, "IEEE Standard for Software Test Documentation," with a few noted exceptions, identifies an acceptable method for addressing test documentation.

Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing," with a few noted exception, identifies an acceptable method for addressing software unit testing.

Thorough software testing consists of testing the smallest testable units, and then integrating those units into larger testable units, and testing that integrated unit. This process is repeated until the system is tested after installation. There is no generally accepted, precise definition of a unit, module, and system. It is therefore understood that Regulatory Guide 1.171 applies to all testing before integrated system testing.

The software validation activities should demonstrate that all validation tests specified by the SVVP were successful; FAT is one of those activities.

#### D.4.4.3 Design Outputs

This subsection describes the criteria that should be used to assess whether the software has each of the characteristics important to safety system software.

#### D.4.4.3.1 Software Requirements Specification (SRS)

##### **Review (Phase 1):** Software Requirements Specification

The acceptance criteria for a software requirements specification (SRS) is contained in the Standard Review Plan, BTP 7-14, Section B.3.3.1, "Requirements Activities - Software Requirements Specification." This section states that Regulatory Guide 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," and that standard describes an acceptable approach for preparing software requirements specifications for safety system software. Section B.3.3.1 also states that additional guidance can be found in NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.2.1 "Software Requirements Specification," and Section 4.2.1, "Software Requirements Specifications."

The SRS documents the results of the requirements phase activities by the design team and documents the aspects of the safety system that are to be addressed in the software design documentation. It is not appropriate to include planning information (e.g., see Section D.4.4.1) in an SRS.

Errors in the specification of criteria or misunderstanding of their intent are a major source of software errors. The SRS should be carefully examined to ensure that criteria are consistent, correct, understandable, traceable, unambiguous, and verifiable. The complexity of the SRS is, of course, dependant on the complexity of the system being proposed, and the level of detail should reflect the level of complexity.

If the platform has not previously been reviewed, or if there are changes in the platform since the previous review, there may be two Software Requirements Specifications which should be reviewed, one for the platform software and another for the applications software. Each of these may be reviewed separately.

Since the staff may use the SRS during the thread audit each criterion should be traceable to one or more safety system criteria, and the requirements traceability matrix should show where in the software the action is being performed. The key to an adequate SRS is its understandability.

The NRC staff should review the SRS against the acceptance criteria in BTP 7-14 and should review a limited number of criteria during the thread audit. The NRC staff should expect to find sufficient V&V documentation to show that there was a 100% verification and validation of the software criteria by the V&V organization.

If any criteria (related to regulatory requirements) in the SRS change, then the SRS should be re-submitted.

The SRS should include criteria that specifically address functional requirements in the regulations, for example:

- IEEE Std 603-1991 Clause 5.2, "Completion of Protective Action"
- IEEE Std 603-1991 Clause 5.6, "Independence"
- IEEE Std 603-1991 Clause 5.7, "Capability for Test and Calibration"
- IEEE Std 603-1991 Clause 5.8, "Information Displays"
- IEEE Std 603-1991 Clause 5.10, "Repair"

IEEE Std 603-1991 Clause 6.5, "Capability for Test and Calibration"  
IEEE Std 603-1991 Clause 7.3, "Completion of Protective Action"

#### D.4.4.3.2 Software Architecture Description (SAD)

**Review (Phase 1):** (1) LAR Section 4.3 – Software Architecture  
(2) Software Architecture Description

The acceptance criteria for the software architecture description are contained in the Standard Review Plan, BTP 7-14 Section B.3.3.2, "Design Activities - Software Architecture Description." This section states that the Software Architecture Description should describe all of the functional and software development process characteristics listed, and that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.3.1 "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance. Standard Review Plan, BTP 7-21, "Guidance on Digital Computer Real-Time Performance," provides guidance for reviewing deterministic performance and associated digital system architectures.

The SAD should explain how the software works, the flow of data, and the deterministic nature of the software. The architecture should be sufficiently detailed to allow the reviewer to understand the operation of the software. This is further addressed in Section D.3, "Software Architecture." There may be SAD for both the platform and the application, if appropriate.

#### D.4.4.3.3 Software Design Specification

**Review (Phase 1):** Software Design Specification

The acceptance criteria for the Software Design Specification are contained in the Standard Review Plan, BTP 7-14, Section B.3.3.3, "Design Activities - Software Design Specification." This section states that the software design specification should accurately reflect the software requirements specification, and that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.3.2 "Software Design Specification," and Section 4.3.2, "Software Design Specifications," contain relevant guidance.

The Software Design Specification is primarily used by the V&V team and the staff to ensure that the software accurately reflects the software requirements specification, and should be detailed enough for the V&V team to check the criteria and follow them through the code. The Software Design Specification should be understandable, and contains sufficient information for the staff to make the determinations shown above.

The NRC staff should review the SDS using the criteria in BTP 7-14 and should review a limited number of criteria during the thread audit. The NRC staff should expect to find sufficient V&V documentation to show that there was a 100% verification and validation of the software design by the V&V organization.

The SDS should include design details that specifically address functional requirements in the regulations, for example:

- IEEE Std 603-1991 Clause 5.2, "Completion of Protective Action"
- IEEE Std 603-1991 Clause 5.6, "Independence"
- IEEE Std 603-1991 Clause 5.7, "Capability for Test and Calibration"
- IEEE Std 603-1991 Clause 5.8, "Information Displays"

IEEE Std 603-1991 Clause 5.10, "Repair"  
IEEE Std 603-1991 Clause 6.5, "Capability for Test and Calibration"  
IEEE Std 603-1991 Clause 7.3, "Completion of Protective Action"

#### D.4.4.3.4 Code Listings

##### **Audit (Phase 2):** Code Listings

See SRP Chapter 7 BTP 7-14 Section B.3.3.4 for SRP acceptance criteria and references to applicable guidance. NUREG/CR-6463, Revision 1, "Review Guidelines for Software Languages for Use in Nuclear Power Plant Safety Systems," contains relevant guidance.

Thread audits may be used to examine code listing in order to support the evaluation of exceptions to approved guidance.

#### D.4.4.3.5 System Build Documents (SBDs)

##### **Review (Phase 2)** System Build Documents

The acceptance criteria for the system build documentation are contained in the SRP, BTP 7-14, Section B.3.3.5, "Integration Activities -System Build Documents." This section states that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.5.1, "System Build Documents," and Section 4.5.1, "System Build Documents," contain relevant guidance.

The information to confirm the system build may be contained in the configuration tables, logic diagrams, or in the system and software configuration documentation. Experience (e.g., Oconee RPS/ESPS LAR) has shown that a system may be built at the vendor factory (i.e., "As-Manufactured") and again at the licensee's facilities (i.e., "As-Built"). The licensing process includes review of documentation up to the completion of factory acceptance testing (and associated analysis activities).

The build documentation is generally used verify that the programs delivered and installed on the safety system are the programs that underwent the V&V process and that they were tested. Any future maintenance, modifications or updates may necessitate that the maintainers know which version of the programming to modify and, therefore, the system build documentation is closely tied to the configuration management program. The items included in the system build documentation should be sufficient to show that the programming listed in the build documentation is identified by version, revision, and date, and that this is the version and revision that was tested and found appropriate.

The NRC staff should review the SBDs against the acceptance criteria in BTP 7-14 and should review a limited number of criteria during the thread audit. The NRC staff should find sufficient V&V documentation to show that there was a 100% verification and validation of the software by the V&V organization.

#### D.4.4.3.6 Installation Configuration Tables

##### **Inspect (Phase 3)** Installation Configuration Tables

The Installation Configuration Tables should not be reviewed in the staff SE. Licensee operations are not a part of the licensing process, but they may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional

inspections of the preparation for use of the proposed system prior to the system being put into operational use.

Guidance for this plan is contained in the Standard Review Plan, BTP 7-14, Section B.3.3.6, "Installation Activities - Installation Configuration Tables (ICTs)."

Experience (e.g., Oconee RPS/ESPS LAR) has shown that cycle specific parameter values are usually defined as typical values (during the development process) since it is not certain which cycle may first include the digital safety system. The "As-Manufactured" system is the system as configured and tested (e.g., Factory Acceptance Test) at the vendor facility (including typical values). The licensing process includes review of documentation up to the completion of factory acceptance testing (and associated analysis activities). The "As-Built" system includes cycle specific values.

#### D.4.4.3.7 Operations Manual

##### **Inspect (Phase 3):** Operations Manuals

The Operations Manual should not be reviewed in the staff SE. Licensee operations are not a part of the licensing process. The Operations Manual may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.

#### D.4.4.3.8 Software Maintenance Manuals

##### **Inspect (Phase 3):** Software Maintenance Manuals

The Software Maintenance Manuals should not be reviewed in the staff SE. Licensee maintenance is not a part of the licensing process, they may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.

#### D.4.4.3.9 Software Training Manuals

##### **Inspect (Phase 3):** Software Training Manuals

The Software Training Manuals should not be reviewed in the staff SE. Licensee training is not a part of the licensing process, they may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.

### **D.4.5 Conclusion**

The NRC staff should find that the information describes a well-defined, disciplined process which should produce a high quality product. The NRC staff should also find that the V&V process described should provide acceptable analysis, evaluation, review, inspection, assessment, and testing of the products and processes. The NRC staff should review the development process information/documents produced during the development of the DSS. The NRC staff should also perform thread audits of the software under review, with the intent of concluding that the process described was the process that was used, and that the process was used correctly and in such a manner as to produce high quality software suitable for use in safety-related applications at nuclear power plants.

## **D.5 Environmental Equipment Qualifications**

### **D.5.1 Scope of Review**

The NRC staff should review the information provided to conclude that the equipment has been demonstrated to be able to operate within the specified environment. This includes both the normal operating conditions and the worst conditions expected during abnormal and accident conditions where the equipment is expected to perform its safety function. The equipment is tested with respect to a wide range of parameters, such as temperature, humidity, seismic, and electromagnetic, based on the environment in which the equipment is located. Furthermore, as stated in RG 1.209, for environmental qualification of safety-related computer-based I&C systems, type testing is the preferred method. The type tests may be manufacturer's tests that document performance to the applicable service conditions with due consideration for synergistic effects, if applicable.

### **D.5.2 Information to be Provided**

**Review (Phase 1):** Equipment Qualification Testing Plans (Including EMI, Temperature, Humidity, and Seismic)

**Review (Phase 2):** (1) Qualification Test Methodologies  
(2) Summary of EMI, Temp., Humidity, and Seismic Testing Results

**Audit (Phase 2):** Completed Test Procedures and Reports

The licensee's submittal should provide sufficient documentation to support the assertion that a proposed digital I&C system is adequately robust to perform its safety function within its design basis for normal and adverse environments. This information should be found in the equipment qualifications test plans, methodologies, and test reports. The results of the qualification testing should be documented in the summary. The information necessary to address the various aspects of environmental qualification are elaborated in Section D.5.4.

The equipment qualification program and the qualification of equipment for harsh environments (i.e., 10 CFR 50.49) is not within the scope of the technical review branch for I&C. The technical review branch for I&C is primarily interested in the qualification of digital equipment in mild environments.

### **D.5.3 Regulatory Evaluation**

Regulatory criteria for environmental qualifications of safety-related equipment are provided in:

**Harsh Environment:** 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants,"

10 CFR Part 50, Appendix A:

GDC 2, "Design Bases for protection Against Natural Phenomena," and  
GDC 4, "Environmental and Dynamic Effects Design Bases."

10 CFR 50.55a(h) incorporates (based on the date of that the construction permit was issued):  
IEEE Std 279-1971 (see Clause 4.4, "Equipment Qualification"), and  
IEEE Std 603-1991 (see Clause 5.4, "Equipment Qualification").



RG 1.152 Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," endorses IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"; Clause 5.4, "Equipment Qualification" contains guidance on equipment qualification (see Section D.10.4.2.4).

RG 1.180 Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," endorses several standards.

**Harsh Environment:** RG 1.89 Revision 1, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plant," endorses IEEE Std 323-1974, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations," subject to the regulatory positions described in the RG, and as supplemented by RG 1.209.

**Mild Environment:** RG 1.209 dated March 2007, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," endorses IEEE Std 323-2003 subject to five enhancements and exceptions.

SRP (NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition") Chapter 7, "Instrumentation and Controls,"

Appendix 7.0-A "Review Process for Digital Instrumentation and Control Systems" Section B.1, "Qualification of Digital Instrumentation and Control Systems and Components," contains guidance on equipment qualification.

Appendix 7.1-B "Guidance for Evaluation of Conformance to IEEE Std 279" Section 4.4, "Equipment Qualification," contains guidance on equipment qualification.

Appendix 7.1-C "Guidance for Evaluation of Conformance to IEEE Std 603" Section 5.4, "Equipment Qualification," contains guidance on equipment qualification.

Appendix 7.1-D "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2" Section 5.4, "Equipment Qualification," contains guidance on equipment qualification.

Regulatory Guide 1.209 endorses guidance for compliance with IEEE Std 323-2003. Mild environment qualification should conform with the guidance of IEEE Std 323-2003. The information provided should demonstrate how the equipment was tested, or what analysis was done. The resultant test data or analysis should also be provided to allow the NRC staff to make a determination that the testing or analysis was adequate and demonstrate that the environmental qualification envelopes the worst case accident conditions in the location where the equipment should be located for any event where the equipment is credited for mitigation. Additionally, the licensee should show why a single failure within the environmental control system, for any area in which safety system equipment is located, should not result in conditions that could result in damage to the safety system equipment, nor prevent the balance of the safety system not within the area from accomplishing its safety function. In this regard, the loss of a safety-related environmental control system is treated as a single failure that should not prevent the safety system from accomplishing its safety functions. Non safety-related environmental control systems should be postulated to fail.

Because the loss of environmental control systems does not usually result in prompt changes in environmental conditions, the design bases may rely upon monitoring environmental conditions

and taking appropriate action to ensure that extremes in environmental conditions are maintained within non-damage limits until the environmental control systems are returned to normal operation. If such bases are used, the licensee should demonstrate that there is independence between environmental control systems and sensing systems that would indicate the failure or malfunctioning of environmental control systems.

Regulatory Guide 1.151 dated July 1983, "Instrument Sensing Lines," may be used to ensure that the environmental protection of instrument sensing lines is addressed.

EMI qualification in accordance with the guidance of Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," is an acceptable means of meeting the qualification requirements for EMI and electrostatic discharge.

Lightning protection should be addressed as part of the review of electromagnetic compatibility. Regulatory Guide 1.204, "Guidelines for Lightning Protection of Nuclear Power Plants," provides additional guidance.

Additional disciplines should be involved in the review of equipment qualification to harsh environments, seismic events, evaluation of conformance to the requirements of GDC 2 and 4 and 10 CFR 50.49 to ensure the requirements for equipment qualification to harsh environments and seismic events are met. Guidance for the review of this equipment qualification is given in SRP Sections 3.10 and 3.11.

SRP Appendix 7.1-D subsection 5.4 provides additional guidance on environmental qualification of digital computers for use in safety systems. (See also Section D.10.4.2.4)

The information necessary to address the various aspects of environmental qualification are elaborated in Section D.5.4.

#### **D.5.4 Technical Evaluation**

To comply with the regulatory requirements, the information provided should demonstrate through environmental qualification that the I&C systems meet design-basis and performance criteria when the equipment is exposed to normal and adverse environments. The testing should include exposure to expected extremes of temperature, humidity, radiation, electromagnetic and radio interference, and seismic input. While testing against all of these stressors, the system should be functioning with the software and diagnostics that are representative of those used in actual operation. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces.

For harsh environments, prior to the performance of testing, the system should be reviewed to identify significant aging mechanisms. For digital systems located in mild environments RG1.209 Regulatory Position 1 states that the NRC does not consider the age conditioning in IEEE Std 323-2003 Section 6.2.1.2 to be applicable because of the absence of significant aging mechanisms. However, if significant aging mechanisms are identified, they should be addressed in the qualification program. An aging mechanism is significant if in the normal or abnormal service environments causes degradation during the installed life of the system that progressively and appreciably renders the equipment vulnerable to failure. Such mechanisms may be addressed by testing (e.g., preconditioning prior to testing), operating experience, or

surveillance and maintenance. Where feasible the preconditioning and surveillance / maintenance assessments should be based on quantifiable acceptance criteria. If the system has one or more significant aging mechanisms, preconditioning is necessary prior to testing to the degree that the mechanism is not accounted for by surveillances and maintenance. For example, if an aging mechanism exists and there is a surveillance performed to quantify the progress of the aging mechanism, the system should be preconditioned sufficient to account for the acceptance criteria of the surveillance plus the expected aging until the next performance of the surveillance. Additional criteria pertinent to environmental qualification are referenced in D.5.3.

The NRC staff should evaluate the various test plans to ensure that they are rigorous enough to support the conclusion that the environment should not have a negative effect on the ability of the system to perform its safety function in the worst case environment in which it needs to operate. Environmental criteria are not generally absolute, but are plant dependent. A digital system may, for example, have a degree of seismic hardening which makes it suitable for use in a plant with a small design basis earthquake, but may be unsuitable for use in another plant where the design basis earthquake is more severe. The same may be true of the worst case temperature environment. If a system is tested to be able to withstand 120° F, it is suitable for use in a plant where the worst case temperature reaches only 118° F, but unsuitable for use in a plant where the worst case temperature may be 125° F. The NRC staff should be looking for the comparison that shows that the equipment qualifications envelopes the worst case plant conditions for each environmental stressor.

#### D.5.4.1 Atmospheric

IEEE Std 323-2003 (endorsed per RG 1.209 dated March 2007) defines the mild environment as an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences. The system should be qualified in the most severe environment to which it may be exposed and is relied upon to perform its safety function.

Typically, the most limiting combination of temperature and humidity occurs at high values of both (i.e., high temperature and high humidity). Therefore, unless another more limiting combination of these parameters exists, the test should be performed at the upper extreme of both.

#### D.5.4.2 Radiation

RG 1.209 dated March 2007 contains guidance regarding the significant differences between analog and digital technologies with respect to radiation. The system should be qualified in the most severe environment to which it may be exposed and is relied upon to perform its safety function.

Radiation exposure has a negative effect on digital I&C equipment and at sufficient doses can cause a degradation in performance. Since the effect of radiation on the system performance is cumulative (i.e., it does not return to its original state upon removal of the stressor) radiation exposure equivalent to the total dose expected during the system's service life should be applied as an aging mechanism.

Because different types of radiation affect electronic components differently and are differently attenuated by shielding, the source or sources used to radiologically age the system should be

representative of the actual in-plant source. If one type of radiation (e.g., gamma) is used to simulate the effects of another type of radiation (e.g., beta), then the basis for the equivalency should be clearly established.

Given that digital I&C systems are typically installed in areas with low levels of radiation, it may be possible to preclude the need for radiation stressing if the service-life dose is low enough. For a particular technology, if there is a known threshold for radiation exposure, below which, no degradation of performance is possible, radiation aging may not be necessary. The information provided should provide adequate references to support this conclusion.

#### D.5.4.3 Electromagnetic Interference/Radio Frequency Interference

RG 1.180 provides guidance on evaluating a digital I&C system with respect to EMI and RFI. This section also includes testing the system for robustness against static discharges and power surges. The RG endorses MIL-STD-461E and IEC 61000 to evaluate EMI & RFI, static discharges, and power surges. The NRC staff has also found EPRI TR-102323-A to be an acceptable method of addressing EMI/RFI. Although both sets of test methods, those found in MIL-STD-461E and those in IEC 61000 are acceptable to the NRC staff, each set of tests should be used in its entirety (i.e., no mixing or matching of various parts of the standards).

##### D.5.4.3.1 Susceptibility

The susceptibility portions of the testing verify that the digital I&C system is able to function properly in the maximum expected electromagnetic environment of the plant. Additionally, the static discharge and power surge portions of the tests verify robustness against these hazards.

##### D.5.4.3.2 Interference

To ensure that the EMI/RFI envelope used in the susceptibility testing remains valid with the addition of the digital I&C system to the plant environment, the EMI/RFI emissions of the device are also tested. The electromagnetic emissions of the system should be below the thresholds defined in the standard to which the system is qualified.

#### D.5.4.4 Sprays and Chemicals

Digital I&C systems whose design basis includes exposure to sprays (e.g., fire sprinkler systems) or chemicals should be protected from or qualified to the effects of such sprays and chemicals. If such exposures occur during normal operation, including maintenance and surveillance, they should be treated as an aging mechanism.

##### D.5.4.5 Seismic

The digital I&C system should be able to perform its safety function both during and after the time it is subjected to the forces resulting from one Safe Shutdown Earthquake. This test should be performed after the system has been exposed to the effects of a number of Operating Basis Earthquakes. The seismic testing should also include a resonance search test where a slow sweep through input frequencies expected to produce a resonance.

## **D.5.5 Conclusion**

The NRC staff should review the information provided on the environmental qualification of the system proposed for use, and should compare this to the plant accident analysis environmental conditions in the location where the equipment should be installed. The staff should evaluate each design basis event where the equipment is required to perform its safety function. The information should show that for each environmental stressor, the equipment qualification is greater than the associated plant environment.

## **D.6 Defense-in-Depth & Diversity**

### **D.6.1 Scope of Review**

The principle of defense-in-depth may be thought of as an arrangement of protective barriers or means that provide overlapping or compensating means of addressing faults in other defensive barriers. In the context of digital instrumentation and control (I&C) defense-in-depth is conceptually achieved through four echelons of defense. The first is the control system echelon which functions under normal operations of the plant and either through automatic control or manual control maintains the plant in safe regimes of operation. If the control system echelon fails or is otherwise unable to maintain the plant in a safe operating regime, the reactor trip echelon acts to rapidly reduce reactivity and minimize any excursion. In turn, if the reactor trip system (RTS) echelon is unable to maintain the plant within safe conditions, the engineered safety features actuation system (ESFAS) echelon activates systems designed to maintain or return the reactor to a subcritical and safe configuration. If these three levels fail, the monitoring and indicator echelon is available to allow operators to make informed decisions regarding response to the transient.

Diversity, in the context of digital I&C, is a principle of using different technologies, equipment manufacturers, logic processing equipment, signals, logic, and algorithms, development teams and personnel, and functions to provide a diverse means of accomplishing a safety function. Diversity complements defense-in-depth by increasing the probability that a particular echelon will function appropriately. The diversity of a system can be subdivided into seven areas: human diversity, technology diversity, equipment and manufacturer diversity, logic processing equipment diversity, signal diversity, and logic diversity.

Diversity in digital I&C systems is necessitated by their potential vulnerability to common-cause failures (CCFs) in software and systems even though CCFs are considered by the NRC to be beyond design basis. This criterion is documented in the SRM to SECY 93-087 and in SRP Chapter 7, BTP 7-19. The NRC staff review of a digital I&C system modification should ensure that sufficient diversity is provided to accomplish the safety function subject to potential CCF vulnerabilities.

Additional information regarding the use of diversity to mitigate or prevent CCFs diversity is provided in NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems" (ADAMS Accession No. ML100880143).

## D.6.2 Information to be Provided

**Review (Phase 1):** (1) LAR Section 4.6 - Defense-in-Depth and Diversity  
(2) D3 Analysis

The licensee's D3 analysis submittal should provide sufficient documentation for the NRC staff to independently reach a conclusion that the plant I&C systems are sufficiently robust against CCF. As further discussed in Section D.6.3, the NRC staff should evaluate the licensee's proposed diversity evaluation using Branch Technical Position 7-19 Rev. 6, which contains four points to be addressed. To satisfy these four points, the NRC staff would expect a submittal to include:

- A description and analysis of the diversity credited within the safety system or backup system(s), with respect to the seven areas (human diversity, technology diversity, equipment manufacturer diversity, logic processing equipment diversity, signal diversity, and logic diversity) discussed in Section D.6.1.
  - An evaluation of all common elements or signal sources shared by two or more system echelons.
  - Identification of all interconnections between the safety systems and with non-safety systems provided for system interlocks and justification that functions required by 10 CFR 50.62 are not impaired by the interconnections.
  - Description and demonstration of components credited to have no potential for CCF and the plan for demonstrating no potential for CCF (i.e., sufficient diversity or fully tested)
- For credited backup systems, description of compliance with BTP 7-19 and SRP Section 7.8
  - A best-estimate-based (e.g., normal operating plant conditions for the event being analyzed) evaluation of each anticipated operational occurrence (AOO) event in the design basis occurring in conjunction with each single postulated common-cause failure.
  - A best-estimate based (e.g., normal operating plant conditions the event being analyze) evaluation of each postulated accident in the design basis occurring in conjunction with each single postulated common-cause failure.
  - A list of all manual actions credited for coping with a common cause failure.
  - Detailed justification for manual actions.
- For credited operator actions
  - D3 HFE analysis and preliminary validation for credited operator actions
  - D3 HFE integrated system validation for credited operator actions (see SRP Chapter 18 Appendix 18-A, ADAMS Accession No. ML092950353)

Licenses should be aware that the specific situations and applications of a system may necessitate additional justification or, in some cases, may not apply to each design basis AOO or accident.

### **D.6.3 Regulatory Evaluation**

As a result of the reviews of advanced light-water reactor (ALWR) design certification applications that incorporated digital protection systems, the NRC position is documented in the SRM on SECY 93-087, "Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Design," with respect to common-mode failure (i.e., CCF) in digital systems and defense-in-depth. This position was also documented in BTP 7-19 Rev. 6, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer Based Instrumentation and Control Systems." Points 1, 2, and 3 of this position are applicable to digital system modifications for operating plants.

While the NRC considers CCFs in digital systems to be beyond design basis, the digital I&C system should be protected against CCFs. The NRC staff's review of defense-in-depth and diversity in digital I&C systems is focused on ensuring that the safety functions can be achieved in the event of a postulated CCF in the digital system. The NRC staff's review considered the following regulatory requirements:

GDC 22, "Protection System Independence," requires, in part, "that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions not result in loss of the protection function. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

GDC 24, "Separation of Protection and Control Systems," requires in part that "[i]nterconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

GDC 29, "Protection Against Anticipated Operational Occurrences," requires in part defense against anticipated operational transients "to assure an extremely high probability of accomplishing safety functions."

The NRC staff intends to provide a preliminary determination on the acceptability of approaches for demonstrating a sufficient level of defense-in-depth and diversity as part of the Phase 0 meetings and acceptance review of the amendment request. This should be done to provide the licensee with an appropriate level of assurance that the proposed digital I&C system design development and implementation may proceed as planned.

### **D.6.4 Technical Evaluation**

Branch Technical Position 7-19 Rev. 6 provides guidance to the NRC staff on performing an evaluation of the defense-in-depth and diversity of a digital I&C system. BTP 7-19 has the objective of concluding that vulnerabilities to CCF have been addressed:

Conclude that adequate diversity has been provided in a design to meet the criteria established by NRC regulations.

Conclude that adequate defense-in-depth has been provided in a design to meet the criteria established by NRC regulations.

Conclude that the displays and manual controls for critical safety functions initiated by operator action are diverse from digital systems used in the automatic portion of the protection systems.

#### D.6.4.1 Adequate Safety System Diversity and Manual Actions

Branch Technical Position 7-19 Rev. 6 and SRP Chapter 18, "Human Factors," Section 18-A, "Guidance for Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses," provide guidance to the NRC staff for reviewing the defense-in-depth and diversity of a digital I&C upgrade with respect to adequate safety system diversity and manual actions.

If the docketed D3 analysis demonstrates that sufficient diversity exists in the protection system<sup>1</sup> or that an adequate automatic Diverse Actuation System<sup>2</sup> (DAS) is provided (which may be non-safety-related), then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

If sufficient diversity does not exist in the protection system, and sufficient time exists for operators to reliably perform manual actions (see SRP Section 18-A) then manual actions may be credited for addressing CCF.

#### D.6.4.2 Diverse Displays and Controls for System Level Actuations

The four-point positions of BTP 7-19 are based on the NRC concern that software based or software logic based digital system development errors are a credible source of CCF. In BTP 7-19, the term "common software" includes software, firmware, and logic developed from software-based development systems. Generally, digital systems cannot be proven to be error-free and, therefore, are considered susceptible to CCF because identical copies of the software based logic and architecture are present in redundant channels of safety-related systems. Also, some errors labeled as "software errors" (for example) actually result from errors in the higher level specifications used to direct the system development that fail in some way to represent the actual process. Such errors further place emphasis on the use of diversity to avoid or mitigate CCF.

BTP 7-19 Rev. 6, Position 4 states:

In addition to the above three points, a set of displays and controls (safety or non-safety) should be provided in the main control room (MCR) for manual system level actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal from the primary system, RCS integrity, and containment isolation and integrity. The displays and controls should be independent and diverse from the safety systems in Points 1-3 to the extent that postulated CCFs in the safety systems do not affect the manual controls. In this case, these displays and controls could be those used for manual action. Where they serve as backup capabilities, the displays and controls also should be able to function downstream of the lowest-level components subject to the CCF that necessitated the use of the diverse backup system or function.

---

<sup>1</sup> Sufficient diversity in the reactor trip system is not adequate for satisfying 10 CFR 50.62.

<sup>2</sup> A single diverse actuation system may be built to meet the requirements of both D3 and 10 CFR 50.62.



One example would be the use of hard-wired connections. For digital system modifications to operating plants, retention of existing analog displays and controls in the MCR could satisfy this point.... However, if existing displays and controls are digital and/or the same platform is used this point may not be satisfied.

## **D.6.5 Conclusion**

The NRC staff should review the proposed system and any proposed diverse system to conclude that sufficient diversity exists, whether within the system itself or between the system and the proposed diverse system, to protect against common-mode/common-cause failure. The NRC staff should specifically address the positions in BTP 7-19 Rev. 6 to assess whether adequate diversity exists.

## **D.7 Communications**

### **D.7.1 Scope of Review**

Digital systems have the capability for individual channels of a control or protection function to be aware of the status of its redundant channels. While this ability can be utilized to provide additional capabilities, it also presents the potential that erroneous data from a malfunctioning channel or failure of a communications pathway could adversely impact system performance. Therefore, a digital I&C system should be designed and constructed such that individual channels of a function are robust against propagating an error in another channel. Additionally, the same considerations are applied to potential communications between the system and other safety-related and non-safety related equipment.

The NRC staff should review the overall design as discussed in the following subsections. As part of this review, the NRC staff should evaluate applicability and compliance with SRP Section 7.9, "Data Communication Systems," SRP Chapter 7, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," and Branch Technical Position 7-11, "Guidance on Application and Qualification of Isolation Devices."

If signal communication exists between different portions of the safety system, the evaluation should include an assessment of whether a malfunction in one portion affects the safety functions of the redundant portion(s). If the safety system is connected to a digital computer system that is non-safety, the evaluation should include a review to confirm if a logical or software malfunction of the non-safety system could affect the functions of the safety system. These reviews should be done by examination of the communication methods used, and comparing these methods to each staff position within DI&C-ISG-04 Revision 1, "Interim Staff Guidance on Highly-Integrated Control Rooms – Communications Issues (HICRc)," March 2009.

### **D.7.2 Information to be Provided**

**Review (Phase 1):** Design Analysis Report (Inter-division communication description and DI&C-ISG-04 compliance analysis)

The licensee's submittal should provide sufficient documentation to support and justify the ability of the digital I&C system to limit the effect of a failed channel from adversely affecting separate channels or divisions. The documentation should provide sufficient justification to allow the conclusion that the plan meets the standards of IEEE Std 603-1991 Clause 5.6, IEEE Std 7-

4.3.2 Clause 5.6, and BTP 7-11. Typically, this involves a detailed discussion of where communications are possible, the nature of those communications, and the features of the system that provide the ability to preclude or account for errors.

The information to confirm adequate data isolation should be contained in the system, hardware and software specifications, architecture, and descriptions. Depending on the complexity of the proposed communications, the NRC staff also may have to examine the actual circuitry as described in the circuit schematics and in the software code listings, and in detailed system and hardware drawings. The licensee should provide documentation on how each clause in DI&C-ISG-04 has been met, or what alternative and proposed alternatives when an individual clause is not met.

### **D.7.3 Regulatory Evaluation**

IEEE Std 603-1991 Clause 5.6, "Independence," requires independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design basis events, and (3) safety systems and other systems. SRP, Chapter 7, Appendix 7.1-C, Section 5.6

"Independence" provides acceptance criteria for this requirement, and among other guidance, provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and that if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system should not be able to affect the functions of the safety system.

IEEE Std 7-4.3.2-2003, endorsed by Regulatory Guide 1.152 Revision 2, Clause 5.6, "Independence," provided guidance on how IEEE Std 603 requirements can be met by digital systems. This clause of IEEE Std 7-4.3.2 specifies that, in addition to the requirements of IEEE Std 603-1991, data communication between safety channels or between safety and non-safety systems not inhibit the performance of the safety function. SRP, Chapter 7, Appendix 7.1-D, Section 5.6, "Independence" provides acceptance criteria for equipment qualifications. This section states 10 CFR Appendix A, GDC 24, "Separation of protection and control systems," states that "the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

BTP 7-11 provides guidance for the application and qualification of isolation devices. BTP 7-11 applies to the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety and non-safety systems. Therefore, this safety evaluation only considers applicability between safety and non-safety systems.

SRP Section 7.9, "Data Communications Systems," also contains guidance for data communication systems.

Additional Guidance on interdivisional communications is contained in DI&C-ISG-04 Rev. 1, "Highly-Integrated Control Rooms – Communication Issues," (ADAMS Accession No. ML083310185).

## **D.7.4 Technical Evaluation**

The communication pathways of the system, including internal communications (one independent channel to another) between other safety-related systems, and between safety-related systems and non-safety-related systems should be evaluated to conclude that a failure or malfunction in one channel or in a connected non-safety system does not adversely affect successful completion of the safety function. Assessment whether the system is sufficiently robust against improper operation due to these communications is further discussed in DI&C-ISG-04.

The technical evaluation should address each applicable section of DI&C-ISG-04, and should show that the system is or is not in compliance with each clause. For those clauses where the system does not comply with the guidance provided in DI&C-ISG-04, the NRC staff should review the proposed alternative, and assess if the alternative meets regulatory requirements.

Section 1 of DI&C-ISG-04 provides guidance on the review of communications, which includes transmission of data and information, among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related;. this ISG section does not apply to communications within a single division.

Section 2 of DI&C-ISG-04 provides guidance applicable to a prioritization device or software function block, that receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device.

Section 3 (of DI&C-ISG-04 provides guidance concerning workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division. The guidance applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.

## **D.7.5 Conclusion**

The NRC staff should review the design and implementation of digital I&C systems to conclude that data communications meet the criteria of IEEE Std 603-1991, IEEE Std 7-4.3.2 and DI&C-ISG-04. The NRC staff should find that the proposed digital I&C upgrade either is acceptable with respect to data communications, or is not acceptable and necessitates revision to the data communications architecture.

## **D.8 System, Hardware, Software, and Methodology Modifications**

### **D.8.1 Scope of Review**

LIC-101 Revision 3 (Non-Publically Available), "License Amendment Review Procedures," Appendix B, "Guide for Processing License Amendments," Section 4.2, "Using Precedent Safety Evaluations & References to Topical Reports," states: "If a licensee in their application or the NRC staff during its review identifies a deviation from the process or limitations associated with a topical report, the staff should address the deviation in its SE for the plant-specific license amendment application." Section D.8 does not have an inherent scope of review. This review area describes how the NRC staff should assess the significance of deviations from previously approved systems, hardware, software, or methodologies. If there has been no previous review

of the proposed system, or there have been no changes in the system, hardware, software, or design lifecycle methodology since the previous review, this section is not applicable.

## **D.8.2 Information to be Provided**

**Review (Phase 1):** (1) LAR Section 4.8 – System, Hardware, Software and Methodology Modifications  
(2) Design Analysis Report (System, Hardware, Software and Methodology Modifications)

The information provided should identify all deviations to the system, hardware, software, or design lifecycle methodology from a previous NRC approval of a digital I&C system or approved topical report. The intent is to eliminate NRC staff reviews of items that have been reviewed and approved, and also to allow the NRC staff to conclude that any changes do not invalidate conclusions reached by a previous review. Completion of this review should result in an update of the previous digital I&C system; however, for topical reports (TRs), it is strongly encouraged that the updated TRs be submitted for approval before a LAR is submitted referencing the TR.

Where appropriate, the licensee and vendor should discuss each of the documents listed in Enclosure B of this ISG. For each document, the licensee and vendor should state whether this document has changed since the last review. If the document has not changed, the licensee and vendor should show the date when the document was previously submitted, and the ADAMS accession number where the document can currently be found. For documents, including system, hardware and software descriptions that have changed, the licensee should submit, on the docket, the new version of that document. In cases where the changes are minor, the licensee can choose to submit a description of the change. The information provided should provide adequate justification to allow the NRC staff to evaluate the acceptability of the change. Additionally, the licensee should justify how the pertinent features of the subject plant conform to those of the existing approval. The amount of information should be proportional to the significance of the change.

## **D.8.3 Regulatory Evaluation**

The NRC staff generally uses the current version of the SRP to perform regulatory evaluations. The basis on which the new system, hardware, software, or design lifecycle methodology should be evaluated may be the same as the evaluation of the original version of that item; for example, having one component in a system that is environmentally qualified to a higher standard than all of the other components does not appreciably increase the reliability of the system. The various acceptance criteria are discussed throughout this ISG.

## **D.8.4 Technical Evaluation**

The NRC staff should assess the adequacy of each described change when the licensee or vendor determines the change is minor, and the full document does not need to be submitted. The change should be sufficiently minor that it can be fully explained in one or two paragraphs. Corrections of typographical errors, changes in personnel, or minor component or procedural changes are suitable for this type of description. The NRC staff should review significant hardware changes such as a new microprocessor requiring re-compiling of software changes that modify the software design description, or changes in methods which would result in a different way of complying with regulatory guidance, even if the licensee or vendor believes the change(s) should continue to comply with regulatory requirements. In each of the instances

described above, new documentation should be submitted to the NRC for review. Additionally, the licensee should justify how the pertinent features of the subject plant conform to those of the existing approval.

#### **D.8.5 Conclusion**

In the interest of efficiency, the NRC staff does not re-review items or documents that have been previously reviewed and approved. This process allows the licensee to limit the documentation submitted for review to only those documents that need a new review, and eliminate reviews of documentation that have only minor changes or modifications. If the NRC staff reviews the change description and concludes the change is not minor, and should be reviewed, the Request for Additional Information process should identify the documents to be reviewed, which should result in a longer review than if the document had been submitted originally. In order for the licensee to reduce the overall review time and effort, licensees are encouraged to submit documentation where the change is not clearly a minor change. The specific changes made related to various documents and programs can be identified during Phase 0 meetings.

#### **D.9 Compliance with IEEE Std 603**

##### **D.9.1 Scope of Review**

The scope of IEEE Std 603-1991 includes all I&C safety systems (i.e., those typically described in Sections 7.2 through 7.6 of the UFSAR). Except for the requirements for independence between control systems and safety systems, IEEE Std 603-1991 does not apply directly to non-safety systems such as the control systems and diverse I&C systems (i.e., those typically described in Sections 7.7 and 7.8 of the UFSAR). Although intended only for safety systems, the criteria for IEEE Std 603-1991 *can be* applicable to any I&C system. Therefore, for non-safety I&C systems that have a high degree of importance to safety, the reviewer may use the concepts of IEEE Std 603-1991 as a starting point for the review of these systems. Applicable considerations include design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing. Digital data communication systems as described in SRP Section 7.9 are support systems for other I&C systems. As such, they inherit the applicable requirements and guidance that apply to the supported systems. Consequently, IEEE Std 603-1991 is directly applicable to those parts of data communication systems that support safety system functions.

Additionally, the review may necessitate coordination with other organizations as appropriate to address the following considerations:

- Many of the auxiliary supporting features and other auxiliary features defined in IEEE Std 603-1991, as typically described in Chapters 4, 5, 6, 8, 9, 10, 12, 15, 18, and 19 of the UFSAR, should be considered for coordination with other technical disciplines.
- The site characteristics, systems (both physical and administrative), and analyses described in other sections of the UFSAR may impose additional criteria on the digital I&C system.
- Digital I&C systems may impose additional criteria on other plant systems and analyses.
- Other plant systems may impose additional criteria on the digital I&C systems.

IEEE Std 603-1991 provides the following operational elements as examples of auxiliary supporting features and other auxiliary features: room temperature sensors, component temperature sensors, pressure switches and regulators, potential transformers, undervoltage relays, diesel start logic and load sequencing logic, limit switches, control circuitry, heating ventilation and air conditioning fans and filters, lube pump, component cooling pumps, breakers, starters, motors, diesel start solenoids, crank motors, air compressors and receivers, batteries, diesel generators, inverters, transformers, electric buses, and distribution panels. IEEE Std 603-1991 Figure 3, "Examples of Equipment Fitted to Safety System Scope Diagram," provides a matrix with an extensive list of auxiliary supporting features and other auxiliary features. IEEE Std 603-1991 Appendix A, "Illustration of Some Basic Concepts for Developing the Scope of a Safety System," also provides examples of the elements of a safety system used to achieve a safety function.

## **D.9.2 Information to be Provided**

**Review (Phase 1)** (1) LAR Section 4.9 – Compliance with IEEE Std 603  
(2) System Description (To block diagram level)

The LAR should provide sufficient information to support the assertion that a proposed digital I&C system meets the requirements of IEEE Std 603-1991; this information is typically embedded within the LAR documentation (e.g., see Enclosure E). To assist the NRC staff in making the determination that the licensee submittal meets the requirements of IEEE Std 603, the licensee may also submit a document showing where within the other submitted documentation the confirmatory information can be found. While this is not a regulatory requirement, it should result in a faster review requiring less NRC staff time. The information necessary to address the various clauses of the standard are elaborated in Section D.9.4.

## **D.9.3 Regulatory Evaluation**

For nuclear plants with construction permits issued before January 1, 1971, 10 CFR 50.55a(h) requires that protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued after January 1, 1971, but before May 13, 1999, 10 CFR 50.55a(h) requires that protection systems must meet the requirements stated in either IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE Std 603-1991 and the correction sheet dated January 30, 1995. Applications filed on or after May 13, 1999 for construction permits and operating licenses, must meet the requirements for safety systems in IEEE Std 603-1991 and the correction sheet dated January 30, 1995. SRP Appendix 7.1-C contains guidance for the evaluation of conformance to IEEE Std 603-1991.

10 CFR 50.55a(a)(3)(i) allows licensees to propose alternatives to paragraph (h), amongst others, provided that the proposed alternative would provide an acceptable level of quality and safety. Where a licensee wishes to demonstrate compliance with another standard in lieu of IEEE Std 603-1991, including a later edition of IEEE 603 (e.g., the 1998 edition), a request to use a proposed alternative must be submitted with the digital I&C LAR. This request must justify why, and the NRC staff must be able to conclude that, meeting the alternate standard provides an equivalent level quality and safety as meeting IEEE Std 603-1991. The additional

review time and effort to approve the alternative (per LIC-102, "Relief Request Reviews" – ML091380595) should depend on how different the alternate standard is from IEEE Std 603-1991.

## **D.9.4 Technical Evaluation**

### **D.9.4.1 IEEE Std 603, Clause 4, Design Basis**

Clause 4 of IEEE Std 603-1991 requires, in part, that a specific design basis be established for the design of each safety system. If this is an upgrade to a digital system from an existing system, the design basis for the new digital system may be the same as the existing system. In this case, a simple description of the design basis should be provided (organized in accordance with the subsections below). The new digital system may, however, have a different design basis. For example the new digital systems may need a diverse actuation system, which would become part of the system design basis. The design basis for the old system and a comparison to the design basis for the new system should be specifically addressed in the information provided.

The plant accident analysis and technical specifications should be compared to the system description, hardware architecture description, theory of operations description, detailed system and hardware drawings, vendor build documentation, systems and hardware requirements specification, and in the commercial grade dedication plans and reports if commercial grade dedication is used. This comparison should allow the licensee and NRC staff reviewer to assess whether the proposed system meets the existing design basis, or if additional review as shown in sections D.9.4.1.1 through D.9.4.1.9 is needed.

#### **D.9.4.1.1 IEEE Std 603, Clause 4.1, Design basis events**

Clause 4.1 requires the identification of the design bases events applicable to each mode of operation. This information should be consistent with the analyses of UFSAR, Chapter 15, events. SRP BTP 7-4 provides specific guidance on the failures and malfunctions that should be considered in identification of design bases events for systems that initiate and control auxiliary feedwater systems. SRP BTP 7-5 provides specific guidance on the reactivity control malfunctions that should be considered in the identification of design basis events. The malfunctions postulated should be consistent with the control system failure modes described in the UFSAR (typically Sections 7.6 and 7.7).

The organization responsible for review of I&C should coordinate with other NRC technical organizations in the evaluation of the proper identification of the design basis events applicable to each operating mode.

#### **D.9.4.1.2 IEEE Std 603, Clause 4.2, Safety Functions and Protective Actions**

Clause 4.2 requires documentation of the safety functions and corresponding protective actions of the execute features for each design basis event. If these have not changed, this should be clearly identified in the information provided.

The organization responsible for review of I&C should coordinate with other NRC technical organizations in the evaluation of the proper identification of the protective actions of the execute features for each design basis event.

#### D.9.4.1.3 IEEE Std 603, Clause 4.3, Permissive Conditions

Clause 4.3 requires documentation of the permissive conditions for each operating bypass capability that is to be provided. If these have not changed, this should be clearly identified in the information provided.

The organization responsible for review of I&C should coordinate with other NRC technical organizations in the evaluation of the proper identification of the permissive conditions for each operating bypass capability.

#### D.9.4.1.4 IEEE Std 603, Clause 4.4, Variables monitored

Clause 4.4 requires the identification of variables that are monitored in order to provide protective action. Performance criteria, including system response times, system accuracies, ranges, and rates of change, should also be identified in the system description. The analysis, including the applicable portion provided in Chapter 15 of the USFAR, should conclude that the system performance criteria are adequate to ensure completion of protective actions. Clause 4.4 also requires the identification of the analytical limit associated with each variable. Review considerations in assessing that an adequate margin exists between analytical limits and setpoints are discussed in Clause 6.8.

#### D.9.4.1.5 IEEE Std 603, Clause 4.5, Criteria for manual protective actions

Clause 4.5 requires the documentation of the minimum criteria under which manual initiation and control of protective actions may be allowed, including the points in time and the plant conditions during which manual control is allowed, the justification for permitting initiation or control subsequent to initiation solely by manual means, the range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations are to be performed, and that the variables in Clause 4.4 be displayed for use in taking manual action. If these have not changed, this should be clearly identified in the information provided. SRP BTP 7-6 provides specific guidance on determining if the timing margins for changeover from injection to recirculation mode are sufficient to allow manual initiation of the transition. Additionally, SRP Section 18-A contains guidance for evaluating manual actions.

The information documented under this clause should be used in assessing conformance with Clause 6.2.2 as well.

#### D.9.4.1.6 IEEE Std 603, Clause 4.6, Minimum number and location of sensors

Clause 4.6 requires the identification of the minimum number and location of sensors for those variables in Clause 4.4 that have spatial dependence (i.e., where the variable varies as a function of position in a particular region). The analysis should demonstrate that the number and location of sensors are adequate. If these have not changed, this should be clearly identified in the information provided. The specification of the minimum number and location of sensors is used in evaluating the acceptability of single failures addressed by Clause 5.1.

#### D.9.4.1.7 IEEE Std 603, Clause 4.7, Range of Conditions

Clause 4.7 requires, in part, that the range of transient and steady-state conditions be identified for both the energy supply and the environment during normal, abnormal, and accident



conditions under which the system must perform. If these have not changed, this should be clearly identified in the information provided. The range of conditions specified is used in evaluating the adequacy of the design and qualification of the equipment.

#### D.9.4.1.8 IEEE Std 603, Clause 4.8, Conditions Causing Functional Degradation

Clause 4.8 requires the identification of conditions having the potential for causing functional degradation of safety system performance, and for which provisions must be incorporated to retain necessary protective action. This information should feed into additional evaluations, including Clause 5.5.

#### D.9.4.1.9 IEEE Std 603, Clause 4.9, Methods used to determine reliability

Clause 4.9 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design, and the identification of the methods used to verify that reliability goals imposed on the system design have been met. NRC staff acceptance of system reliability is based on the deterministic criteria described in IEEE Std 603-1991, and IEEE Std 7-4.3.2-2003.

The NRC staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the NRC's regulations for reliability of safety systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience can provide an added level of confidence, but alone is not sufficient.

For safety systems that include digital computers, both hardware and software reliability should be considered. Software errors that are not the consequence of hardware failures are caused by design errors and, therefore, do not follow the random failure behavior used for hardware reliability analysis. Consequently, different methodologies may be used to assess the unreliability introduced by hardware and software.

#### D.9.4.1.10 IEEE Std 603, Clause 4.10, Critical Points in Time or Plant conditions

Clause 4.10 requires that the minimum design basis documentation include the critical points in time or plant conditions, after the onset of a design basis event. The documentation of critical points in time for the initiation of protective actions is used to derive certain performance criteria (e.g., response time); the ability of the digital safety system to meet certain performance criteria is evaluated under Clause 5.4.

Clause 4.10.3 requires the documentation of information that will be used in Clause 6.1.

The information documented under this clause should also be used in assessing conformance with Clause 6.2.3.

#### D.9.4.1.11 IEEE Std 603, Clause 4.11, Equipment Protective Provisions

Clause 4.11 requires the documentation of the equipment protective provisions that prevent a safety system from accomplishing their safety function.

#### D.9.4.1.12 IEEE Std 603, Clause 4.12, Special Design Basis

Clause 4.12 requires the documentation of any other special design basis.

#### D.9.4.2 IEEE Std 603, Clause 5, System

##### **Review (Phase 2):** Requirements Traceability Matrix

Clause 5 of IEEE Std 603-1991 requires that the safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established by design basis events. This evaluation should confirm that the general functional criteria have been appropriately allocated to the various system components. The review in this regard should conclude that the system design fulfils the system design basis criteria established; this review should be from an integrated hardware/software perspective.

The licensee should ensure that the Requirements Traceability Matrix (RTM) is written such that each criteria and sub-criteria (whether hardware or software) is traceable throughout the design. The traceability should be possible both forwards and backwards, that is, the staff should be able to take any criterion, and trace it through from the system requirements specification to the design and associated validation tests or analysis. Tracing backwards, it should be possible to confirm what requirement is responsible for any aspect of the system. One of the things this should be used for is to assess whether there is no unnecessary code in the product. Any application code which is not traceable back to a system or plant criteria is unnecessary and should be removed.

In addressing Clauses 5.1 through 5.15, the following additional considerations should be taken into account:

##### D.9.4.2.1 IEEE Std 603, Clause 5.1, Single Failure Criterion

Clause 5.1 requires that any single failure within the safety system shall not prevent proper protective action at the system level when needed. The analysis<sup>3</sup> should confirm that the single-failure criterion is satisfied. Guidance in the application of the single-failure criterion is provided in RG 1.53 Rev. 2, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," which endorses IEEE Std 379-2000, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

Components and systems not qualified for seismic events or accident environments and non-safety-grade components and systems are postulated to fail to function if failure adversely affects safety system performance. Conversely, these components and systems are postulated to inadvertently function in the worst manner if functioning adversely affects safety system performance. All failures in the safety system that can be predicted as a result of an event for which the safety system is designed to provide a protective function are postulated to occur if the failure adversely affects the safety system performance. In general, the lack of equipment qualification or a less than high quality development process may serve as a basis for the assumption of certain failures. After postulating the failures of non-safety-grade, non-qualified equipment and those failures caused by a specific event, a random single failure within the safety-related system is postulated. With these failures postulated, the safety system must be capable of performing the protective functions that are necessary to mitigate the consequences of the specific event. The information to reach a determination of adequate compliance with the single failure criterions with respect to equipment qualification should be contained in the system and hardware specifications, architecture, and descriptions, and in the Equipment

---

<sup>3</sup> The analysis is sometimes documented in a Failure Modes and Effects Analysis (FMEA) report; see Section D.9.4.2.1.1.

Qualification Testing Plans, methods, Failure Modes and Effects Analysis (FMEA), and test results.

Digital computer-based I&C systems share data, data transmission, functions, and process equipment to a greater degree than analog systems. Although this sharing forms the basis for many of the advantages of digital systems, it also raises a key concern with respect to I&C system vulnerability to a different type of failure. The concern is that a design using shared databases and process equipment has the potential to propagate a common-cause failure of redundant equipment. DI&C-ISG-04, Section 1, "Interdivisional Communications," Staff Position 3, states that "A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system." In order to comply with this staff position, the licensee or vendor should demonstrate what support or enhancement to the safety function is provided by the communications and that any communications failure should not allow a single failure within one channel to defeat the single failure concept. This demonstration is further discussed in Section D.7, "Communications." Per Section D.7, the information to reach a determination of adequate data isolation should be contained in the system, hardware and software specifications, architecture, and descriptions. Depending on the complexity of the proposed communications, the NRC staff may also have to examine the actual circuitry as described in the circuit schematics and in the software code listings, and in detailed system and hardware drawings.

Another concern is that software programming errors can defeat the redundancy achieved by the hardware architectural structure. Because of these concerns, the NRC staff has placed significant emphasis on defense-in-depth against common-cause failures within and between functions. The principle of defense-in-depth is to provide several levels or echelons of defense to challenges to plant safety, such that failures in equipment and human errors should not result in an undue risk to public safety. This is addressed further in Section D.6.

#### D.9.4.2.1.1 Failure Modes and Effects Analysis (FMEA)

##### **Review (Phase 2): FMEA**

There is no specific regulatory guidance on the format, complexity or conclusions concerning the FMEA. Each system must be independently assessed to conclude that the FMEA is sufficiently detailed to provide a useful assessment of the potential failures and the effects of those failures. For example, an FMEA is a method for documenting a single failure analysis which is conducted in accordance with IEEE Std 379-2000 as endorsed by RG 1.53 Rev. 2.

The FMEA is a method of analysis of potential failure modes within a system for determination of the effects on the system. This information can then be used to assess the potential for an undetectable failure. The overall staff expectation is that each potential failure mode should be identified, and the effects should be determined. For a complex system, this is expected to be a complex analysis.

The review with respect to the failure of software is addressed in: (1) Section D.4.4.1.9, "Software Safety Plan", (2) Section D.4.4.2.1, "Safety Analysis", and (3) D.6, "Defense-in-Depth & Diversity".

#### D.9.4.2.2 IEEE Std 603, Clause 5.2, Completion of Protective Action

Clause 5.2 requires that the safety systems be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features continue until completion, and that deliberate action is necessary to return the safety systems to normal. Appendix 7.1-C, Section 5.2, of the SRP provides acceptance criteria for this requirement.

In addition to a description of how “seal-in” features ensure that system-level protective actions go to completion, the information provided may include functional and logic diagrams to demonstrate this feature. The information should clearly demonstrate that deliberate action is needed to return the safety systems to normal operation. The information needed by the NRC staff to reach a determination that the “seal-in” features of the system are sufficient, should be contained in the system hardware and software specifications and associated descriptions. Depending on the complexity of the proposed seal-in features, the NRC staff may also have to examine (audit) the actual circuitry as described in the circuit schematics and in the software code listings.

#### D.9.4.2.3 IEEE Std 603, Clause 5.3, Quality

Clause 5.3 requires that components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates, and that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

The information provided should confirm that the quality assurance provisions of Appendix B to 10 CFR, Part 50, are applicable to the safety system. The adequacy of the quality assurance program is addressed further in the evaluation against Clause 5.3 of IEEE Std 7-4.3.2-2003. It may be beneficial for a licensee to conduct a 10 CFR, Part 50, Appendix B audit of the vendor to assess the adequacy of their quality assurance program. The information needed by the NRC staff to reach a determination that the vendor is planning to provide adequate quality should be contained in the quality assurance plans. The implementation of these plans may be audited by the NRC staff.

#### D.9.4.2.4 IEEE Std 603, Clause 5.4, Equipment Qualification

**Review (Phase 1):** System Response Time Analysis Report

**Review (Phase 2):** System Response Time Confirmation Report

IEEE Std 603 Clause 5.4 states that safety system equipment shall be qualified<sup>4</sup> by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it should be capable of meeting the performance criteria as specified in the design basis (e.g., IEEE Std 603 Clause 4.10), while being exposed to specified environmental conditions (e.g., IEEE Std 603 Clause 4.7). Appendix 7.1-C, Section 5.4, of the SRP provides acceptance criteria for Clause 5.4. The information provided should confirm that the safety system equipment is designed to meet the performance criteria over the range of normal, abnormal, and accident conditions. SRP Chapter 7, BTP 7-21, “Guidance on Digital Computer

---

<sup>4</sup> The information needed by the NRC staff to reach a determination of adequate environmental equipment qualification is discussed in Section D.5.

Real-Time Performance,” provides guidance for reviewing the deterministic behavior of a digital Safety System (DSS).

Typically an environmental equipment qualification test specimen is not in the identical configuration as a plant specific application; therefore, equipment qualification is generally addressed in three parts:

- (1) Qualifying the equipment to specified environmental conditions. See Section D.5, “Environmental Equipment Qualifications,” for detailed guidance on environmental equipment qualifications.
- (2) Ensuring that the environmental equipment qualification envelop bounds the plant specific application.
- (3) Ensuring that the application specific functional and performance criteria are achieved by the specific equipment and configuration proposed.

The licensee’s submittal should provide sufficient documentation to support the assertion that a proposed digital I&C system is qualified to perform its safety function within its design-basis normal and adverse environments (e.g., as required to be documented by IEEE Std 603 Clause 4.7). The results of the qualification testing should be documented in a summary report.

The NRC staff should review the information provided to conclude that the plant specific application has been demonstrated to be able to meet functional and performance criteria within the expected environment. This includes both the normal operating conditions and the worst conditions expected during abnormal and accident conditions where the equipment is expected to perform its safety function. The system is tested with respect to a wide range of parameters, such as temperature, humidity, seismic, and electromagnetic, based on the environment in which the equipment is located.

#### D.9.4.2.5 IEEE Std 603, Clause 5.5, System Integrity

**Review (Phase 1):** Design Report on Computer integrity, Test and Calibration, and Fault Detection

Clause 5.5 requires that the safety systems be designed such that the system can accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.5, “System Integrity,” provides acceptance criteria for system integrity. This acceptance criteria states that the NRC staff may assess whether tests have been conducted on safety system equipment components and the system racks and panels as a whole to demonstrate that the safety system performance is adequate to ensure completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment. The test should show that if the system does fail, it fails in a safe state, and that failures detected by self-diagnostics should also place a protective function into a safe state.

The information provided should be sufficient for the NRC staff to conclude that adequate testing and analysis has been performed on the system as a whole and its components. This testing and analysis should be sufficient to demonstrate that the safety system performs its protective actions over the range of transient and steady-state conditions of both the power supply and the environment. Further, the test should demonstrate that if the system does fail, it

fails in a safe state and failures detected by self-diagnostics should also place a protective function into a safe state. The information needed by the NRC staff to reach a determination of adequate system qualification is discussed in Section D.5 of this ISG, and the NRC staff determination that the system adequately meets IEEE Std 603 Clause 5.5 should reference the testing section of the NRC staff SE.

A special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure completion of protective action within the critical points of time identified as required by Clause 4.10 of IEEE Std 603-1991. SRP BTP 7-21 provides supplemental guidance on evaluating response time for digital computer-based systems, and discusses design constraints that allow greater confidence in the results analyses or prototype testing to determine real-time performance.

Evaluation of computer system hardware integrity should be included in the evaluation against the requirements of IEEE Std 603-1991. Computer system software integrity (including the effects of hardware-software interaction) should be demonstrated by the licensee's software safety analysis activities.

The review of system integrity should conclude that the design provides for safety systems to fail in a safe state, or into a state that has been demonstrated to be acceptable on some other defined basis, if conditions such as disconnection of the system, loss of energy, or adverse environments, are experienced. This aspect is typically evaluated through evaluation of the licensee's failure modes and effects analysis. The analysis should justify the acceptability of each failure effect. Reactor trip system (RTS) functions should typically fail in the tripped state. Engineered safety feature actuation system (ESFAS) functions should fail to a predefined safe state. For many ESFAS functions this predefined safe state should be that the actuated component remains as-is.

Computer-based safety systems should, upon detection of inoperable input instruments, automatically place the protective functions associated with the failed instrument(s) into a safe state (e.g., automatically place the affected channel(s) in trip), unless the affected channel has already been placed in a bypass mode (this would change a two-out-of-four logic to a two-out-of-three logic). Hardware failures or software errors detected by self-diagnostics should also place a protective function into a safe state or leave the protective function in an existing safe state. Failure of computer system hardware or software error should not inhibit manual initiation of protective functions or the performance of preplanned emergency or recovery actions. During either partial or full system initialization or shutdown after a loss of power, control output to the safety system actuators should fail to a predefined, preferred failure state. A system restart upon restoration of power should not automatically transfer the actuators out of the predefined failure state. Changes to the state of plant equipment from the predefined state following restart and re-initialization (other than changes in response to valid safety system signals) should be in accordance with appropriate plant procedures.

#### D.9.4.2.6 IEEE Std 603, Clause 5.6, Independence

##### **Review (Phase 1):** Design Analysis Report

Clause 5.6 requires independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design bases events, and (3) safety systems and other systems.<sup>5</sup>

Guidance for evaluation of physical and electrical independence is provided in RG 1.75, Revision 3, "Criteria for independence of Electrical Safety Systems," which endorses IEEE Std 384-1992, "IEEE Standard Criteria for independence of Class 1E Equipment and Circuits." The safety system design should not have components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features that could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence is attained by physical separation and physical barriers. Electrical independence should include the utilization of separate power sources. Transmission of signals between independent channels should be through isolation devices.

SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence," provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety function of the redundant portions. Further, if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system must not be able to affect the functions of the safety system. Section D.7 and DI&C-ISG-04 provide additional information on this topic.

##### D.9.4.2.6.1 IEEE Std 603, Clause 5.6.1, Between Redundant Portions

Clause 5.6.1 states that the safety systems shall be designed so that there is sufficient independence between redundant portions of a safety system such that the redundant portions are independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. SRP Chapter 7, Appendix 7.1-C does not provide any additional acceptance criteria beyond that in Clause 5.6.1. The information provided should demonstrate the independence between redundant portions of the safety system. Section D.7 and DI&C-ISG-04 describes the criteria for demonstration of this independence.

##### D.9.4.2.6.2 IEEE Std 603, Clause 5.6.2, Effects of Design Basis Event

Clause 5.6.2 states that the safety systems necessary to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of IEEE Std 603. Clause 5.6.2 further states that equipment qualification in accordance with Clause 5.4 is one method that can be used to meet this requirement. The

---

<sup>5</sup> An independence design analysis report provides sufficient detail to support and justify independence: (1) between redundant portions of a safety systems, (2) from the effects of design basis events, and (3) from other systems. Some of the supporting analysis is sometimes documented in a Failure Modes and Effects Analysis (FMEA) report; see Section D.9.4.2.1.1.

information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that the degree of independence is sufficient.

#### D.9.4.2.6.3 IEEE Std 603, Clause 5.6.3, Other Systems

Clause 5.6.3 states that the safety systems shall be designed such that credible failures in and consequential actions by other systems do not prevent the safety systems from meeting the requirements of IEEE Std 603. Clause 5.6.3 is subdivided into sub-clauses for interconnected equipment, equipment in proximity, and the effects of a single random failure. Each of the sub-clauses should be addressed in the following paragraphs.

Clause 5.6.3.1 of IEEE Std 603, "Interconnected Equipment" states that equipment that is used for both safety and non-safety functions, as well as the isolation devices used to affect a safety system boundary, shall be classified as part of the safety systems. This clause further states that no credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance criteria during and following any design basis event needing that safety function and that a failure in an isolation device will be evaluated in the same manner as a failure of other equipment in a safety system. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that the degree of independence is sufficient.

Clause 5.6.3.2 of IEEE Std 603, "Equipment in Proximity," states that equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, will be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment, and that physical separation may be achieved by physical barriers or acceptable separation distance. This clause further states that the physical barriers used to form a safety system boundary shall meet the requirements of Clause 5.3, Clause 5.4, and Clause 5.5 for the applicable conditions specified in Clause 4.7 and Clause 4.8 of the design basis. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that the degree of independence is sufficient.

Clause 5.6.3.3 of IEEE Std 603, "Effects of a Single Random Failure," requires that where a single random failure in a non-safety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. IEEE Std 379 provides additional guidance for the application of this requirement.

The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that the degree of independence is sufficient.

#### D.9.4.2.7 IEEE Std 603, Clause 5.7, Capability for Test and Calibration

**Review (Phase 1):** Design Report on Computer integrity, Test and Calibration, and Fault Detection

Clause 5.7 requires the capability for testing and calibration of the safety system equipment be provides while retaining the capability of the safety systems to accomplish their safety functions. It is expected that safety systems should be periodically tested and calibrated.



Guidance on periodic testing of the safety system is provided in RG 1.22, "Periodic Testing of Protection System Actuation Functions," and in RG 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems," which endorses IEEE Std 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems." The extent of test and calibration capability provided bears heavily on whether the design meets the single-failure criterion. Any failure that is not detectable must be considered concurrently with any random postulated, detectable single failure. Periodic testing should duplicate, as closely as practical, the overall performance of the safety system. The test should confirm operability of both the automatic and manual circuitry. The capability should be provided to permit testing during power operation. When this capability can only be achieved by overlapping tests, the reviewer should conclude that the test scheme overlaps leave no gaps.

The tests should address the increased potential for subtle system failures such as data errors and computer lockup. The system design should also support the compensatory actions documented in the Technical Specifications when limiting conditions for operation are not met. Typically, this should allow for tripping or bypass of individual functions in each safety system channel. SRP BTP 7-17 describes additional considerations regarding these topics.

In addition, if self-contained diagnostics within the digital system are being used as a reason for elimination of existing surveillances, or less frequent performance of existing surveillances, the information provided should show exactly what components and safety functions were previously tested, and how the new diagnostic functions will test these components to the same degree.

D.9.4.2.8 IEEE Std 603, Clause 5.8, Information Displays

**Review (Phase 1):** Theory of Operation Description

Clause 5.8 has four sub-clauses.

Clause 5.8.1 requires that display instrumentation provided for manually controlled actions for which no automatic control is provided and that are necessary for the safety systems to accomplish their safety functions will be part of the safety systems. The design should minimize the possibility of ambiguous indications.

Clause 5.8.2 requires that display instrumentation provide accurate, complete, and timely information pertinent to safety system status, and that this information shall include indication and identification of protective actions of the sense and command features and execute features. Further, the design should minimize the possibility of ambiguous indications. The review of information displays for manually controlled actions should include assessment whether the displays will be functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary.

Clause 5.8.3 requires that protective actions that have been bypassed or deliberately rendered inoperative for any other purpose be continuously indicated in the control room; this display instrumentation does not need to be considered a part of the safety system. The indication must be automatically actuated if the bypass or otherwise inoperative condition is expected to occur more frequently than once per year and is expected to occur when the affected system is specified to be operable. Safety system bypass and inoperable status indication should conform with the guidance of Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

Clause 5.8.4 requires that information displays be located such that they are accessible to the operator and that if the information display is provided for manually controlled protective actions, that it be visible from the controls used to effect the actions.

The information provided in the system, hardware and software specification and design documentation should sufficiently describe the hardware and software such that the NRC staff is able to conclude that the four sub-clauses have been met. The NRC staff should review the factory acceptance testing to assess that these design features have been tested. The staff also should review the summary reports to conclude that the testing showed these features were acceptable.

D.9.4.2.9 IEEE Std 603, Clause 5.9, Control of Access

**Review (Phase 1):** Theory of Operation Description

Clause 5.9 requires that the safety system be designed to permit administrative control of access to the equipment. Administrative access limited to qualified plant personnel is acceptable if done with the permission of the control room operator. The system should be designed with alarms and locks to preclude inappropriate access. Additionally, electronic access to the system (e.g., via a network connection) should be sufficiently restricted. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that Clause 5.9 has been met. The Secure Development and Operational Environment Review area (see Section D.12) discusses this aspect in further detail. The information needed by the NRC staff to reach a determination that the system is designed such that administrative controls of access to the equipment is adequate should be contained in the system, hardware and software specifications, architecture, and descriptions.

Depending on the complexity of the proposed features, the NRC staff may examine (audit) the actual circuitry as described in the circuit schematics and in the software code listings, and in detailed system and hardware drawings. The auditors should evaluate whether the administrative controls are such that they adequately limit access to qualified and authorized plant personnel.

D.9.4.2.10 IEEE Std 603, Clause 5.10, Repair

**Review (Phase 1):** (1) Design Report on Computer Integrity, Test and Calibration, and Fault Detection  
(2) Theory of Operation Description

Clause 5.10 requires that the safety system be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. It important to note that the acceptance criteria states that while digital safety systems may include self-diagnostic capabilities to aid in troubleshooting, the use of self-diagnostics does not replace the need for the capability for test and calibration systems as required by Clauses 5.7 and 6.5. The hardware and software descriptions, and descriptions of the surveillance testing and self-diagnostics should be sufficient to allow the NRC staff to conclude that this requirement has been met.

#### D.9.4.2.11 IEEE Std 603, Clause 5.11, Identification

##### **Review (Phase 1):** Theory of Operation Description

Clause 5.11 requires that the safety system equipment and documentation be distinctly identified for each redundant portion of a safety system. Regulatory Guide 1.75 Rev. 3, "Criteria for Independence of Electrical Safety Systems," endorses IEEE 384-1992, "IEEE Standard for Independence of Class 1E Equipment and Circuits," subject to the exceptions listed. IEEE 384 contains guidance regarding identification (e.g., Clause 6.1.2, "Identification"). Further, the safety system equipment must be distinguishable from any identifying markings placed on the equipment for other purposes, that the identification methods not necessitate the frequent use of reference materials (i.e., be "user friendly"), and that the associated documentation be distinctly identified. However, components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not, themselves, need identification.

The information provided should sufficiently describe the identification of hardware, software, and documentation such that the NRC staff is able to conclude that the Clause 5.11 has been met.

#### D.9.4.2.12 IEEE Std 603, Clause 5.12, Auxiliary Features

Clause 5.12 requires that auxiliary supporting features meet all requirements of IEEE Std 603. Those auxiliary features that perform functions that are not necessary for the safety system to accomplish its safety function and are not isolated from the safety system shall be designed to meet those criteria necessary to ensure that these components, equipment, or systems do not degrade the safety systems below an acceptable level.

The auxiliary supporting features need to be designed to the same high quality standards as the rest of the safety-related system, and the same demonstration that all requirements are being met is required. In addition, DI&C-ISG-04, Section 1, "Interdivisional Communications," Staff Position 3 states that "Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system". In order to comply with this staff position, the licensee or vendor should demonstrate that any auxiliary supporting features are necessary to perform the safety function. If the licensee or vendor cannot show that the supporting feature is needed, a detailed description of the feature, how it is designed and how it functions should be needed for the NRC staff to conclude that having this feature should not compromise the safety or functionality of the system. This detailed description may necessitate the NRC staff to review actual schematics or software code to reach its conclusion.

#### D.9.4.2.13 IEEE Std 603, Clause 5.13, Multi-Unit Stations

##### **Review (Phase 1):** Theory of Operation Description

Clause 5.13 requires that any shared structures, systems, or components between multi-unit generating stations be capable of simultaneously performing all necessary safety functions in any or all units. Guidance on the sharing of electrical power systems between units is contained in RG 1.32 Revision 3, "Criteria for Power Systems for Nuclear Power Plants," which endorses IEEE Std 308-2001, and guidance on application of the single-failure criterion to shared systems is contained in RG 1.53 Rev. 3 which endorses IEEE 379-2000.

The information provided should sufficiently describe the shared components such that the NRC staff is able to conclude that the Clause 5.13 has been met.

#### D.9.4.2.14 IEEE Std 603, Clause 5.14, Human Factors Considerations

##### **Review (Phase 1):** Theory of Operation Description

Clause 5.14 requires that human factors be considered at the initial stages and throughout the development process to assure that the functions allocated in whole or in part to the users and maintainers can be successfully accomplished to meet the safety system design goals.

The information provided should be sufficient to demonstrate that the guidance contained in NUREG-0700, NUREG-0711, and SRP Section 18-A has been met.

#### D.9.4.2.15 IEEE Std 603, Clause 5.15, Reliability

##### **Review (Phase 2):** Reliability Analysis

Clause 5.15 requires that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved.<sup>6</sup> The information provided should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed. For computer systems, both hardware and software should be included in this analysis. The NRC staff considers software that complies with the quality criteria of Clause 5.3, and that is used in safety systems that provide measures for defense against common-cause failures as described in D.6, also complies with the fundamental reliability requirements of GDC 21, IEEE Std 279-1971, and IEEE Std 603-1991.

Further, the assessment against Clause 5.15 should consider the effect of possible hardware failures and software errors and the design features provided to prevent or limit their effects, and that hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of the communications systems. This should include hard failures, transient failures, sustained failures, and partial failures. With respect to software, common-cause failures, cascading failures, and undetected failures should be considered. Quantitative reliability goals alone are not sufficient as a means of meeting the regulations for the reliability of digital computers used in safety systems.

#### D.9.4.3 IEEE Std 603, Clause 6, Sense and Command Features

Clause 6 of IEEE Std 603-1991 provides the requirements for sensors and command features. In addressing Clauses 6.1 through 6.8, the additional considerations contained within those clauses should be taken into account:

##### D.9.4.3.1 IEEE Std 603, Clause 6.1, Automatic Control

Clause 6.1 requires that for each design basis event, all protective actions should automatically initiate, with the exception of those justified in Clause 4.5. The information provided should

---

<sup>6</sup> A reliability analysis provides sufficient detail to support and justify that the system meets the reliability requirements.

sufficiently describe the hardware and software such that the NRC staff is able to conclude that the automatic initiation will be precise and reliable. The description of this precision and reliability needs to address factors such as setpoints, margins, errors, and response times. Further, the description should demonstrate that the functional criteria have been appropriately allocated into hardware and software. The description should confirm that the system's real-time performance is deterministic and known. The information needed by the NRC staff to a conclusion that the protective action will be automatically initiated should be contained in the system, hardware and software specifications, architecture, and descriptions.

The information to show that these features are adequately tested should be contained in the factory acceptance test Design Specification.

D.9.4.3.2 IEEE Std 603, Clause 6.2, Manual Control

**Review (Phase 1):** Theory of Operation Description

Clause 6.2 requires that means be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions, that the means will minimize the number of discrete manipulations, and will depend on the operation of a minimum of equipment consistent with the constraints of Clause 5.6.1. RG 1.62 provides further guidance on this topic.

Clause 6.2 also requires implementation of manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 5.2 of IEEE Std 603, with the information provided to the operators, the actions needed of these operators, and the quantity and location of associated displays and controls be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators, in an environment suitable for the operator, and suitably arranged for operator surveillance and action.

The information needed by the NRC staff to reach a determination that the means to implement manual actions at the division level may be contained in the system, hardware and software specifications, as well as the architecture descriptions. The information to show that these features are adequately tested may be contained in the factory acceptance test design specification. Test reports may be reviewed in making this assessment.

The manual controls required by Clause 6.2 may be different from manual actions that could be used as an acceptable diverse actuation to address BTP 7-19 Rev. 6, as defense against common cause software failure (CCSF). The manual initiation and indicators to tell when to use the manual initiation required by Clause 6.2 are required to be at a system level and safety-related. These controls may or may not be the ones used in the event of CCSF (due to the design of these manual controls and their susceptibility to CCF), and therefore the CCSF controls should be independent and therefore downstream of the digital portion of the safety system that is subject to the CCSF. The SRM to SECY 93-087, as reflected in BTP 7-19 Rev. 6, addresses diverse automatic or manual controls in the event of CCSF. The CCSF manual controls may be system level or component level, and may be non-safety, but must be independent of any CCSF, and therefore downstream of any digital portion of the digital safety system. It is possible for one set of manual controls to meet both of these criteria, by making those controls safety-related, system level, and downstream of any digital portion of the safety system that could be affected by a CCSF.

#### D.9.4.3.3 IEEE Std 603, Clause 6.3, Interaction with Other Systems

Clause 6.3 requires that if a single credible event can both cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designed to provide principal protection against the condition, either alternate channel or alternate equipment not subject to this failure be provided, or equipment not subject to failure caused by the same single credible event be provided. If the event of concern is a single failure of a sensing channel shared between control and protection functions, isolating the safety system from the sensing channel failure by providing additional redundancy or isolating the control system from the sensing channel failure by using data validation techniques to select a valid control input is acceptable.

The information provided should be sufficient to describe the hardware and software such that the NRC staff is able to conclude that Clause 6.3 has been met. Additionally, the FMEA should contain information to address this clause.

#### D.9.4.3.4 IEEE Std 603, Clause 6.4, Derivation of System Inputs

Clause 6.4 requires that, to the extent feasible and practical, sense and command feature inputs be derived from signals that are direct measures of the desired variables as specified in the design basis. If indirect parameters are used, the indirect parameter must be shown to be a valid representation of the desired direct parameter for all events. Further, for both direct and indirect parameters, the characteristics of the instruments that produce the safety system inputs, such as range, accuracy, resolution, response time, and sample rate should be described.

The information provided in the system, hardware and software specifications, architecture, and descriptions should sufficiently describe the hardware and software such that the NRC staff is able to conclude that the Clause 6.4 has been met.

#### D.9.4.3.5 IEEE Std 603, Clause 6.5, Capability for Testing and Calibration

**Review (Phase 1):** (1) Design Report on Computer Integrity, Test and Calibration, and Fault Detection  
(2) Theory of Operation Description

Clause 6.5 requires that it must be possible to check, with a high degree of confidence, the operational availability of each sense and command feature input sensors needed for a safety function during reactor operation, including the availability of each sense and command feature needed during the post-accident period. SRP Chapter 7, Appendix 7.1-C, Section 6.5, "Capability for Testing and Calibration," provides acceptance criteria for Clause 6.5.

The information provided should confirm that the operational availability can be checked by varying the input to the sensor or by cross checking between redundant channels. Additionally, when only two channels of a readout are provided, the information provided must justify why it is expected that an incorrect action will not be taken if indications from the two channels are different.

#### D.9.4.3.6 IEEE Std 603, Clause 6.6, Operating Bypass

##### **Review (Phase 1):** Theory of Operation Description

Clause 6.6 requires that if the applicable permissive conditions are not met, a safety system must automatically prevent the activation of an operating bypass or initiate the appropriate safety function. Further, if plant conditions change such that an activated bypass is no longer permissible, the safety system must either remove the appropriate active operating bypass, restore plant conditions to the permissive conditions, or initiate the appropriate safety functions. The requirement for automatic removal of operational bypasses means that the reactor operator may not have a role in such removal; however, the operator may take action to prevent the unnecessary initiation of a protective action.

The information provided in the system, hardware and software specifications, architecture, and descriptions should sufficiently describe the hardware and software such that the NRC staff is able to conclude that Clause 6.6 has been met.

#### D.9.4.3.7 IEEE Std 603, Clause 6.7, Maintenance Bypass

##### **Review (Phase 1):** Theory of Operation Description

Clause 6.7 requires that the safety system be designed such that while sense and command features equipment is in maintenance bypass, the capability of a safety system to accomplish its safety function must be retained, and during such operation, the sense and command features must continue to meet the Clauses 5.1 and 6.3. Additionally, provisions for a bypass must be consistent with the Technical Specification action statements.

The information provided in the system, hardware and software specifications, architecture, and descriptions should sufficiently describe the hardware and software such that the NRC staff is able to conclude that Clause 6.7 has been met.

#### D.9.4.3.8 IEEE Std 603, Clause 6.8, Setpoints

##### **Review (Phase 1):** Setpoint Methodology (If changing TS Setpoints)

##### **Review (Phase 2):** Setpoint Calculations (If changing TS Setpoints)

Clause 6.8 requires that the allowance for uncertainties between the process analytical limit documented in Clause 4.4 and the device setpoint must be determined using a documented methodology. Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design must provide a positive means of ensuring that the most restrictive setpoint is used. The setpoint analysis should confirm that an adequate margin exists between operating limits and setpoints, such that there is a low probability for inadvertent actuation of the system. Furthermore, the analysis should confirm that an adequate margin exists between setpoints and safety limits.

Additional guidance on the establishment of instrument setpoints can be found in RG 1.105 and RIS 2006-0017. Where it is necessary to provide multiple setpoints as discussed in Clause 6.8.2, the NRC staff interpretation of "positive means" is that automatic action is provided to ensure that the most restrictive setpoint is used. SRP BTP 7-3 provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that Clause 6.8 has been met.

#### D.9.4.4 IEEE Std 603, Clause 7, Execute Features

##### **Review (Phase 1):** Theory of Operation Description

Clause 7 provides the requirements for actuators and other executable features.

#### D.9.4.4.1 IEEE Std 603, Clause 7.1, Automatic Control

Clause 7.1 requires that the safety system have the capability incorporated into the execute features to receive and act upon automatic control signals from the sense and command features consistent with Clause 4.4.

The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that the Clause 7.1 been met.

#### D.9.4.4.2 IEEE Std 603, Clause 7.2, Manual Control

Clause 7.2 requires that if manual control of any actuated component in the execute features is provided, the additional features needed to accomplish such manual control shall not defeat the requirements of Clauses 5.1 and 6.2, and that any capability to receive and act upon manual control signals from the sense and command features is consistent with the design basis.

The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that Clause 7.2 has been met. The review of manual controls should include conclusion that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified), accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary. RG 1.62 provides guidance on this topic.

#### D.9.4.4.3 IEEE Std 603, Clause 7.3, Completion of Protective Action

Clause 7.3 requires that the design of the execute features be such that once initiated, the protective actions of the execute features shall go to completion. However, this requirement does not preclude the use of equipment protective devices identified in Clause 4.11 of the design basis or the provision for deliberate operator interventions. Additionally, when the sense and command features reset, the execute features shall not automatically return to normal, but shall need separate, deliberate operator action to be returned to normal.

The information provided should include functional and logic diagrams. The NRC staff notes that the seal-in feature may incorporate a time delay as appropriate for the safety function. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that Clause 7.3 has been met.

#### D.9.4.4.4 IEEE Std 603, Clause 7.4, Operating Bypass

Clause 7.4 contains identical requirements to Clause 6.6. The information provided for meeting Clause 6.6 may e referenced.



#### D.9.4.4.5 IEEE Std 603, Clause 7.5, Maintenance Bypass

Clause 7.5 contains similar requirements as Clause 6.7, but also requires that portions of the execute features with a degree of redundancy of one must be designed such that when a portion is placed in maintenance bypass, the remaining portions provide acceptable reliability.

The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that Clause 7.5 has been met.

#### D.9.4.5 IEEE Std 603, Clause 8, Power Source Requirements

Clause 8 provides the requirements for the power sources supporting the digital I&C system. Clause 8 requires that those portions of the Class 1E power system that are needed to provide the power to the many facets of the safety system are governed by the criteria of IEEE Std 603-1991 and are considered a portion of the safety systems. Clauses 8.1 and 8.2 apply the requirements of IEEE Std 603-1991 to electrical and non-electrical power sources, respectively.

Clause 8.3 requires that the capability of the safety system to accomplish its safety function be retained when the power source is in maintenance bypass. Additionally, portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass, the remaining portions provide acceptable reliability.

The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that Clauses 8.1, 8.2, and 8.3 have been met.

### D.9.5 Conclusion

The NRC staff should review the licensee's submittal against the requirements of IEEE Std 603-1991 to assess whether the proposed implementation would be acceptable with respect to IEEE Std 603-1991 and 10 CFR 50.55a(h)(2).

### D.10 Conformance with IEEE Std 7-4.3.2

#### D.10.1 Scope of Review

The scope of IEEE Std 7-4.3.2-2003 includes all I&C safety systems that are computer-based. IEEE Std 603-1991 does not directly discuss digital systems, but states that guidance on the application of its criteria for safety systems using digital programmable computers is provided in IEEE/ANS Std 7-4.3.2-1982. IEEE/ANS Std 7-4.3.2-1982 was subsequently revised into IEEE Std 7-4.3.2-2003 and endorsed by RG 1.152, Revision 2. IEEE Std 7-4.3.2-2003 serves to amplify the criteria in IEEE Std 603-1991. Within the context of IEEE Std 7-4.3.2-2003, the term computer is a system that includes computer hardware, software, firmware, and interfaces.

#### D.10.2 Information to be Provided

**Review (Phase 1):** (1) LAR Section 4.10 – Conformance with IEEE Std 7-4.3.2  
(2) System Description (To block diagram level)

The licensee's LAR should provide sufficient information to support the assertion that a proposed digital I&C system follows the guidance of IEEE Std 7-4.3.2-2003; this information is typically embedded within the LAR documentation. To assist the NRC staff in making the

determination that the licensee submittal follows the guidance provided in IEEE Std 7-4.3.2, the licensee may also submit a document showing where within the other documentation submitted the confirmatory information can be found; this should result in a faster review needing less NRC staff time. The information necessary to address the various clauses of the standard are elaborated in Section D.10.4.

### **D.10.3 Regulatory Evaluation**

For nuclear plants with construction permits issued before January 1, 1971, 10 CFR 50.55a(h) requires that protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued after January 1, 1971, but before May 13, 1999, 10 CFR 50.55a(h) requires that protection systems must meet the requirements stated in either IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE Std 603-1991 and the correction sheet dated January 30, 1995. Applications filed on or after May 13, 1999 for construction permits and operating licenses, must meet the requirements for safety systems in IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

IEEE Std 603-1991 does not directly discuss digital systems, but states that guidance on the application of the criteria in IEEE Std 603-1991 for safety systems using digital programmable computers is provided in IEEE/ANS Std 7-4.3.2-1982, "American Nuclear Society and IEEE Standard Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations." IEEE/ANS Std 7-4.3.2-1982 has been revised into IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." Guidance on applying the safety system criteria to computer based safety systems is provided by IEEE Std 7-4.3.2-2003, as endorsed by Regulatory Guide 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." IEEE Std 7-4.3.2-2003 specifies computer-specific criteria (incorporating hardware, software, firmware, and interfaces) to supplement the criteria in IEEE Std 603-1998. Although IEEE Std 7-4.3.2-2003 references IEEE Std 603-1998, IEEE Std 603-1991 and the correction sheet dated January 30, 1995 remains the requirement for safety systems in accordance with 10 CFR 50.55a(h). SRP Appendix 7.1-D contains guidance for the evaluation of conformance to IEEE Std 7-4.3.2-2003.

While IEEE Std 7-4.3.2 is not codified in 10CFR50.55a, it is the principal standard used by the NRC staff in evaluating digital I&C upgrades. The standard is endorsed by RG 1.152 Rev. 2 dated 2003 (i.e., RG 1.152 & IEEE Std 7-4.3.2 are SRP acceptance criteria). To demonstrate conformance with another standard in lieu of IEEE Std 7-4.3.2, the licensee should include an evaluation that allows the NRC staff to conclude that conformance provides a high quality system. This activity should be expected to take a significant amount of additional review time and effort.

### **D.10.4 Technical Evaluation**

#### **D.10.4.1 IEEE Std 7-4.3.2, Clause 4, Safety System Design Basis**

Clause 4 does not provide any additional criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.1.

D.10.4.2 IEEE Std 7-4.3.2, Clause 5, System

Clause 5 contains no additional criteria beyond those in IEEE Std 603-1991; however, some of the sub-clauses contain additional criteria. The sub-clauses are described in 5.1 through 5.15.

D.10.4.2.1 IEEE Std 7-4.3.2, Clause 5.1, Single-failure criterion

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.1.

D.10.4.2.2 IEEE Std 7-4.3.2, Clause 5.2, Completion of protective action

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.2.

D.10.4.2.3 IEEE Std 7-4.3.2, Clause 5.3, Quality

Clause 5.3 states that hardware quality is addressed by IEEE Std 603-1991. This clause also describes the typical digital system development life cycle. The licensee should describe the development life cycle actually used for the development of the system being proposed, and compare this to the typical life cycle. Any difference in the life cycle should be explained and justified.

Clause 5.3 contains 6 sub-parts that are discussed in further detail below.

D.10.4.2.3.1 IEEE Std 7-4.3.2, Clause 5.3.1, Software development

**Review (Phase 1):** Vendor Software Plan

Computer system development activities should include the development of computer hardware and software. The integration of the computer hardware and software and the integration of the computer with the safety system should be addressed in the development process.

The computer system development process typically consists of the following computer lifecycle phases:

- Concepts
- Requirements
- Design
- Implementation
- Test

Licensing Review

- Inspection
- Installation, Checkout and Acceptance Testing
  - Operation
  - Maintenance
  - Retirement

The NRC staff's licensing review, for operating reactors, of the development process should assess the first five of these phases, and include all activities through factory acceptance tests. Installation, operation, maintenance and retirement phases are not part of the licensing process, hence these items may be assessed by regional personnel after receipt of the system at the plant site. The licensee must address and document the following activities:

- Creating the conceptual design of the system, translation of the concepts into specific system criteria
- Using the criteria to develop a detailed system design
- Implementing the design into hardware and software
- Analyzing, Reviewing, and Testing to assure the criteria have been correctly implemented

SRP BTP 7-14 describes the characteristics of a software development process that the NRC staff should use when assessing the quality criteria of this clause.

Specifically, Clause 5.3.1 requires an approved quality assurance (QA) plan for all software that is resident at run time. In addition, the NRC staff considers this to include software, that while not itself resident at run time, is used to program the system (e.g., software used to generate hardware based logic).

To meet this clause, the licensee must provide a software QA plan. This plan should clearly show what software is subject to that plan. Software that is not resident at run time, such as software tools used to program the system, maintain configuration control, or track criteria for the requirement traceability matrix are generally not safety-related and therefore do not require the same degree of quality assurance as safety-related software, however these software tools should still be discussed in and subject to the QA plan. The software QA plan should describe the method used to determine that this software was evaluated and found suitable for use. It should also be noted that if the software QA plan specifies the use of separate documents, those documents should also be provided.

To facilitate a timely review of a proposed system, the software QA plan should be submitted for NRC staff review as early as possible in the application process. Because of the length of time necessary to review a software QA plan, changes to the software QA plan that are needed as a result of the NRC staff review should be applied to all products produced during the period the NRC staff was reviewing the software QA plan. As necessary, the licensee may need to perform regression testing and verification and validation of all changes necessitated by software QA plan changes.

Clause 5.3.1.1 specifies that the use of software quality metrics be considered throughout the software lifecycle to assess whether software quality criteria are being met. The basis for the metrics selected to evaluate the software quality should be included in the software development documentation. The metrics methodology should use diverse software measures that appropriately aggregate the measurement data to provide a quantitative assessment of the quality of the outputs.

This recommends the use of software quality metrics. If metrics are used to justify software quality, the licensee should demonstrate how those metrics actually measure software quality, and how use of the metrics should demonstrate that the quality requirements of 10 CFR Appendix B are being met.

Licensees should be careful when making claims on the effectiveness of any software metric. The licensee should evaluate what that metric actually measures and what conclusion can be reached based on these measurements. The metric may, for example, be useful to the

software vendor to show diminishing returns on continued testing, but unless the quality and thoroughness of the testing program is evaluated, it may not be sufficient to demonstrate that the software is of high quality. Quality becomes more visible through a well conceived and effectively implemented software metrics program. A metrics methodology using a diversity of software measures and that appropriately aggregates the measurement data could provide quantitative data giving insight into the rigor of the safety software development process and resulting quality of the life cycle outputs.

D.10.4.2.3.2 IEEE Std 7-4.3.2, Clause 5.3.2, Software tools

**Review (Phase 1):** Software Tool Verification Program

**Review (Phase 2):** Software Tool Analysis Report

Clause 5.3.2 specifies that software tools used to support software development processes and V&V processes be controlled under the configuration management plan. The tools are further specified to be either developed to a similar standard as the safety-related software or the tools be used in a manner such that defects not detected by the tools should be detected by V&V activities.

Software tools should be used in a manner such that defects not detected by the software tools should be detected by V&V activities. If, however, it cannot be proven that defects not detected by software tools or introduced by the software tools should be detected by V&V activities, the software tools should be designed as Appendix B quality software, with all the attendant regulatory requirements for software developed under an Appendix B program.

A test tool validation program should be developed to provide confidence that the necessary features of the software tool function as specified. This basically means that if the output cannot or is not subject to full V&V, the tool needs to be developed as if it were safety-related, and needs to be reviewed by the NRC staff in the same manner.

SRP BTP 7-14 states that the resource characteristics that the software development plan should exhibit include methods/tools and standards. Methods/tools specifies a description of the software development methods, techniques and tools to be used. The approach to be followed for reusing software should be described. The plan should identify suitable facilities, tools and aids to facilitate the production, management and publication of appropriate and consistent documentation and for the development of the software. It should describe the software development environment, including software design aids, compilers, loaders, and subroutine libraries.

The plan should specify that tools are to be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be developed using the tools. Methods, techniques and tools that produce results that cannot be verified to an acceptable degree or that are not compatible with safety criteria should be prohibited, unless analysis shows that the alternative would be less safe.

Reviewers should evaluate tool usage, including a sufficient number of tool products for the NRC staff to conclude that the tools function as described. Tools used for software development may reduce or eliminate the ability of the vendor to evaluate the output of those tools, and therefore rely on the tool, or on subsequent testing to show the software should perform as intended. Testing alone can only show that those items tested can operate as

intended, and cannot be relied upon to show that no unintended functions exist, or that the software will function in conditions other than those specifically tested. The use of software tools should be evaluated in the overall context of the quality control and V&V process, and there should be a method of evaluating the output of the tool.

Operating experience may be used to provide confidence in the suitability of a tool, but may not be used to demonstrate that a tool is of sufficient quality to be the equivalent to safety-related software. If the first option is chosen, that the tool be developed in the same manner as safety-related software is developed, the NRC staff should review the tool development process in a similar manner as safety-related software would be reviewed. With the second option, where the tool is not developed and qualified similar to safety related software, the NRC staff should postulate that the output of that tool may contain errors, and therefore the output of the tools should undergo the full verification and validation process.

The information needed for the NRC staff to reach a determination that the software tools are adequate for their intended use should be contained in the documentation of the software tool verification program. The intended use of those tools should be described in the software development plan, the software integration plan, and software test plan, depending on how the tool will be used. Use of the tools may be audited by the NRC staff to assess the quality of the tools.

#### D.10.4.2.3.3 IEEE Std 7-4.3.2, Clause 5.3.3, Verification and validation

Clause 5.3.3 states that a V&V program should exist throughout the system lifecycle and that the software V&V effort should be performed in accordance with IEEE Std 1012-1998. As endorsed by RG 1.168, Revision 1, the criteria for the highest level of integrity (level 4) should be applied. The information provided should demonstrate that the V&V process provides an objective assessment of the software products and processes throughout the lifecycle and must address the computer hardware and software, integration of the digital system components, and the interaction of the resulting computer system with the plant.

As described in Section D.4.4.1.10 of this ISG, the licensee should submit the V&V plan (which is consistent with NRC endorsed standards) actually used during the development of the platform and the application software. If the V&V effort used documents that are not included as part of the V&V plan (i.e., V&V planning activities are contained within other documents), those documents must also be submitted for NRC staff review (per Section D.4.4.1.10).

The V&V plan, and the determination that the V&V effort meets regulatory requirements is one of the most significant parts of the NRC staff review of the design life cycle, and therefore should receive a thorough review. The V&V processes, activities, and tasks (PATs) should be described in the system and software development plans, and the products produced by these PATs should be contained in the V&V reports. The NRC staff should review these PATs and products to assess whether the V&V effort meets the criteria of RG 1.168 and IEEE Std 1012.

#### D.10.4.2.3.4 IEEE Std 7-4.3.2, Clause 5.3.4, Independent V&V (IV&V)

Clause 5.3.4 defines the levels of independence necessary for the V&V effort in terms of technical, managerial, and financial independence (see Section D.4.4.1.10). Oversight of the effort should be vested in an organization separate from the development and program management organizations, with resources allocated independent of the development resources. The information provided should demonstrate that:

- The V&V organization is independent and given sufficient time and resources.
- The V&V personnel are as qualified as the design personnel.
- The V&V organization is effective, such that errors not identified by the V&V organization can indicate a lack of IV&V effectiveness.
- Problems identified by the V&V organization are properly addressed.

The information necessary for the NRC staff to assess the adequacy of independence of the V&V effort should be contained in the management plans, QA plans and in the V&V plans. The NRC staff should audit the independence of the V&V during the vendor V&V and thread audits to assess whether the V&V products are acceptable, and that the various plans have been adequately implemented.

The reviewer of the V&V effort should evaluate the overall effectiveness of the V&V process, since the NRC staff cannot perform a review of every criteria and every line of code. With this in mind, the items the reviewer should check include, but are not limited to the following:

- Is the V&V organization independent and given sufficient time and resources to avoid pressure to perform in a hurried or insufficient review? The reviewer should interview the V&V personnel, and observe the relationship between the V&V staff and the design staff. There may be cases where the organizational relationship indicates there is independence, when in fact, the V&V personnel are subject to pressure to perform a rapid review and to show that the software product is of high quality when the level of effort or the quality of the effort does not justify that determination.
- Are the V&V personnel qualified to perform the task? The V&V personnel should be at least equally experienced and qualified as the design personnel.
- Is the V&V organization effective? If thread audits of selected functions reveals errors that were not found by the V&V effort, the indication is that V&V may not be finding other errors as well. In addition to checking the outputs of the various design stages to verify that the output properly reflects the criteria, and validates that the outputs are designed so that the product will fulfill its intended use, the V&V effort should determine that the design outputs function as specified. As an example, a filter may have been specified, and that filter properly designed and implemented. However, if the filter does not actually filter the specified frequencies, or does not actually reduce or eliminate the noise it is intended to filter, the quality of the V&V effort is suspect.
- Are the V&V problem reports properly addressed, corrections made, and the resulting correction itself properly checked? There have been cases where a V&V problem report was not effectively resolved, or that the correction resulting from a V&V problem report was in itself in error, and the analysis for the correction was so limited that the new error was not found. The reviewer should check a sufficient number of problem reports carefully, and conclude that each problem was addressed and that correction did, in fact, correct the problem without introducing new errors.

The review of the V&V products is an important step in the determination of high quality software and a high quality development process, and as such, any concerns the reviewer has about the quality of the V&V effort should be resolved prior to acceptance of the digital system. If the NRC reviewer identifies significant concerns with quality or effectiveness that are supported with information gathered during the review, those issues should be raised to NRC management to prepare the NRC for non-acceptance of the V&V effort of the safety-related digital system.

#### D.10.4.2.3.5 IEEE Std 7-4.3.2, Clause 5.3.5, Software configuration management

Clause 5.3.1.5 specifies that software configuration management be performed in accordance with IEEE Std 1042-1987, and that IEEE Std 828-1998 provides guidance for the development of software configuration management plans. RG 1.169 endorses these standards. (see Sections D.4.4.1.11 and D.4.4.2.3)

The licensee should ensure that the information provided in the configuration management plans should demonstrate that the software configuration management plan implements the following minimum set of activities:

- Identification and control of all software designs and code.
- Identification and control of all software design functional data.
- Identification and control of all software design interfaces.
- Control of all software design changes
- Control of software documentation
- Control of software vendor development activities for the supplied safety system software.
- Control of all tools and supporting equipment used to develop the software.
- Control and retrieval of qualification information associated with software designs and code.
- Software configuration audits.
- Status accounting.

It is possible that some of these activities may be performed by other QA activities; however, the plan should describe the division of responsibility.

A software baseline should be established at appropriate points in the software life cycle process to synchronize engineering and documentation activities. Approved changes that are created subsequent to a baseline should be added to the baseline.

The labeling of the software for configuration control should include unique identification of each configuration item, and revision and/or date time stamps for each configuration item. This labeling should be unambiguous, and clearly identify this particular product and version from all other products and versions.

Changes to the software/firmware should be formally documented and approved consistent with the software configuration management plan. The documentation should include the reason for the change, identification of the affected software/firmware, and the impact of the change on the system. Additionally, the documentation should include the plan for implementing the change in the system (e.g., immediately implementing the change, or scheduling the change for a future version).



There may be two or more different software configuration management programs to evaluate, that being used by the software vendor(s) during the development process, and that used by the licensee after the software has been delivered and installed in the nuclear power plant. All of these programs should be evaluated in sufficient detail for the NRC staff to conclude that the programs and plans are acceptable. Appendix B of 10 CFR Part 50, in Section I, "Organization," it states, "The applicant may delegate to others, such as contractors, agents, or consultants, the work of establishing and executing the quality assurance program, or any part thereof, but shall retain responsibility therefore." The reviewer should assess whether a vendor software configuration management program has been approved by the licensee, and if it fits into the licensee's overall software configuration management program.

IEEE Std 828-1990 and IEEE Std 1042-1987, which are endorsed by Regulatory Guide 1.169, provide acceptable guidance for a software configuration management system, but the use of these standards is not mandatory. If referenced by the licensee, the reviewer should make an independent determination that the software configuration management system as implemented is appropriate for safety-related software used in nuclear power plants. If the vendor or licensee is using methods other than that prescribed by IEEE Std 828-1990 and IEEE Std 1042-1987, the determination of adequacy should be more difficult. In this case, the reviewer should be familiar with the software configuration control objectives, and examine the methodology used by the vendor and licensee in sufficient detail to conclude that an equivalent level of control is provided as those that would have been provided by previously reviewed and approved methods, such as those found in IEEE Std 828-1990 and IEEE Std 1042-1987.

The reviewer of the software configuration management system should evaluate that the system used by both the vendor and the licensee ensures that any software modifications during the development process and after acceptance of the software for use should be made to the appropriate version and revision of the software. This should involve not only a review of the Software Configuration Management documentation, but also a review of the actual methods being used at both the vendor and licensee facilities, to ensure that the methods discussed in the plans are properly implemented.

D.10.4.2.3.6 IEEE Std 7-4.3.2, Clause 5.3.6, Software project risk management

**Review (Phase 1):** Software Project Risk Management Program

**Audit (Phase 2):** Software Project Risk Management Report

Clause 5.3.6 defines the risk management activities for a software project. The documentation expected is the documentation produced as a result of the risk management activities. Software project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems should be addressed to assure that software quality goals are achieved. Risk management should be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. Software project risks may include technical, schedule, or resource-related risks that could compromise software quality goals, and thereby affect the ability of the safety system to perform safety-related functions. Risk factors that should be addressed include system risks, mechanical/electrical hardware integration, risks due to size and complexity of the product, the use of pre-developed software, cost and schedule, technological risk, and risks from program interfaces (maintenance, user, associate contractors, subcontractors, etc.). Software project risk management differs from hazard analysis.

When analyzing the risk management program, it should be kept in mind that licensee acceptance of risk is not necessarily sufficient or acceptable. As an example, if the licensee decides to use highly complex software in lieu of a simpler system, the licensee should demonstrate that the complexity is acceptable. Alternative solutions, and analysis of those alternatives, should be considered and a reason why the complexity offered sufficient advantages to outweigh the disadvantages. The risk management program is intended to manage risk, not to only state that risk is acceptable. Risk management may also be addressed in the Software Management Plan (see Section D.4.4.1.1).

#### D.10.4.2.4 IEEE Std 7-4.3.2, Clause 5.4, Equipment qualification

Clause 5.4 defines the equipment qualification<sup>7</sup> for a software project. These criteria, as expanded in sub-clauses 5.4.1 and 5.4.2, are in addition to those given in IEEE Std 603-1991. Additionally, Section D.5, "System Qualifications," provides further guidance.

##### D.10.4.2.4.1 IEEE Std 7-4.3.2, Clause 5.4.1, Computer system testing

Clause 5.4.1 specifies that the system qualification testing be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces.

Licensees should ensure that the test plans include these criteria, and that the test reports show what software was running during the tests.

##### D.10.4.2.4.2 IEEE Std 7-4.3.2, Clause 5.4.2, Qualification of commercial computers

**Review (Phase 1):** Commercial Grade Dedication Plan(s)

**Review (Phase 2):** Commercial Grade Dedication Report(s)

Clause 5.4.2 defines the qualification of existing commercial computers for use in safety-related applications in nuclear power plants. The clause references EPRI TR-106439, as accepted by the NRC SE dated July 17, 1997, and EPRI TR-107330, as accepted by the NRC SE dated July 30, 1998, for specific guidance.

For commercial grade software intended for use in safety-related systems, one of the critical characteristics is implementation of a high quality development process. In essence, the licensee should show that the development process used to develop the commercial software was as rigorous as that for software used in safety-related applications. If this cannot be demonstrated, the commercial grade software may not be suitable for safety-related applications.

EPRI TR-106439, as accepted by the NRC safety evaluation dated July 17, 1997, (ADAMS Accession No. ML092190664) provides guidance for the evaluation of existing commercial computers and software to comply with the criteria of Sub-Clause 5.4.2 of IEEE Std 7-4.3.2-

---

<sup>7</sup> The information needed by the NRC staff to reach a determination of adequate system qualification is discussed in Section D.5.

2003. The guidance of SRP BTP 7-14 may be applied to the evaluation of vendor processes described in EPRI TR-106439.

EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," as accepted by the NRC safety evaluation dated July 30, 1998, (no Accession Number Available), provides more specific guidance for the evaluation of existing programmable logic controllers (PLC).

The fundamental criteria for demonstrating that a computer will perform its intended safety functions is presented in this portion of IEEE Std 7-4.3.2-2003 and additional guidance is provided in EPRI TR-106439 and EPRI TR-107330.

The qualification process (e.g., as described in the Commercial Grade Dedication Plan) should be accomplished by evaluating the hardware and software design using the criteria of IEEE Std 7-4.3.2-2003. Acceptance should be based upon evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its specified functions and has been developed in accordance with a high quality development process. The acceptance and its basis should be documented (e.g., in a Commercial Grade Dedication Report) and maintained with the qualification documentation.

In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify that a component is acceptable for use in a safety-related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR Part 50 Appendix B program.

The dedication process for the digital safety system (e.g., as described in the Commercial Grade Dedication Plan) should entail identification of the physical, performance, and development process criteria necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process should apply to the computer hardware, software, and firmware that are necessary to accomplish the safety function. The dedication process for software and firmware should include an evaluation of the development process and the implementation of the development process.

The preliminary and detailed phase activities for commercial grade item dedication are described in Sub-Clauses 5.4.2.1 through 5.4.2.2 of IEEE Std 7-4.3.2-2003.

The commercial grade dedication reports should be docketed by the start of Phase 2.

D.10.4.2.5 IEEE Std 7-4.3.2, Clause 5.5, System integrity

**Review (Phase 1):** Design Report on Computer integrity, Test and Calibration, and Fault Detection

Clause 5.5 specifies that in addition to the system integrity criteria provided by IEEE Std 603-1991, the digital system should be designed for computer integrity, test and calibration, and fault detection and self-diagnostic activities. Sub-clauses 5.5.1 through 5.5.3 provide further criteria.

#### D.10.4.2.5.1 IEEE Std 7-4.3.2, Clause 5.5.1, Design for computer integrity

Clause 5.5.1 specifies that the computer be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. The licensee should provide this demonstration, however this demonstration should generally credit the design, V&V, and test documentation. The NRC staff should review the development processes that were implemented and that the safety functions are in accordance with NRC regulations.

#### D.10.4.2.5.2 IEEE Std 7-4.3.2, Clause 5.5.2, Design for test and calibration

Clause 5.5.2 specifies that test and calibration functions not adversely affect the ability of the system to perform its safety function, and that it be verified that the test and calibration functions do not affect system functions that are not included in a calibration change. The clause further states that V&V, configuration management, and QA are necessary for test and calibration functions on separate systems such as test and calibration computers that provide the sole verification of test and calibration data. V&V, configuration management, and QA is not specified when the test and calibration function is resident on a separate system and does not provide the sole verification of test and calibration for the safety system.

Again, the licensee should provide this demonstration, however this demonstration should generally credit the design, V&V, and test documentation. The NRC staff should review the development processes that were implemented and that the test and calibration functions are in accordance with NRC regulations.

#### D.10.4.2.5.3 IEEE Std 7-4.3.2, Clause 5.5.3, Fault detection and self-diagnostics

Clause 5.5.3 specifies that if reliability criteria warrant self-diagnostics, then the software should contain functions to detect and report computer system faults and failures in a timely manner, and that these self-diagnostic functions not adversely affect the ability of the system to perform its safety function nor cause spurious actuations of the safety function. Licensees should ensure that the criteria for self-diagnostics are contained in the software specifications, and that the capability to actually detect and report faults is tested. The test plans should show how the testing of self-diagnostics will be performed, and the test report should show that the testing done was adequate to test these diagnostic features. NRC staff should review test plans and reports to conclude that the testing was performed appropriately.

#### D.10.4.2.6 IEEE Std 7-4.3.2, Clause 5.6, Independence

##### **Review (Phase 1):** Design Analysis Report

Clause 5.6 specifies that in addition to the requirements of IEEE Std 603-1991, data communication between safety channels or between safety and non-safety systems not inhibit the performance of the safety function.<sup>8</sup> The protection system should be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is

---

<sup>8</sup> An independent design analysis report provides sufficient detail to support and justify independence: (1) between redundant portions of a safety systems, (2) from the effects of design basis events, and (3) from other systems. Some of the supporting analysis is sometimes documented in a Failure Modes and Effects Analysis (FMEA) report; see Section D.9.4.2.1.1.

common to both systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. The interconnection of the protection and control systems should be limited so as to assure that safety is not impaired.

DI&C-ISG-04 discussed communications independence, and if the licensee can demonstrate compliance with DI&C-ISG-04, this demonstration should also suffice for compliance with this clause. The licensee should point to documentation on compliance with DI&C-ISG-04.

D.10.4.2.7 IEEE Std 7-4.3.2, Clause 5.7, Capability for test and calibration

**Review (Phase 1):** Design Report on Computer integrity, Test and Calibration, and Fault Detection

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.7.

The capability of the software to test itself should be clearly described. From experience with a number of digital failures, many failures were not in the operational code but in the diagnostic code. One of the reasons for this may be that the diagnostic code may be much more complex than the operational code.

Large amounts of test and diagnostic software increase the complexity of a system. This increase in complexity should be balanced against the potential gain in confidence in the system provided by the test and diagnostic software. This may also be balanced by the extensive previous use of these diagnostic routines. The test and diagnostic software may have been well tested and extensively used in the past, while the operational code is likely new for each application. The interaction of the diagnostic software with the operational software must be evaluated.

A non-software watchdog timer is critical in the overall diagnostic scheme. A software watchdog should cause the system to fail to operate if the system processor freezes and no instructions are processed. The hardware watchdog timer's only software input should be a reset after the safety processor performs its function. There must be no possibility of a software error causing a jump to the reset function, thereby nullifying the effectiveness of the watchdog timer.

D.10.4.2.8 IEEE Std 7-4.3.2, Clause 5.8, Information displays

Clause 5.8 states that there are no criteria beyond those found in IEEE Std 603-1991; however, this is limited to equipment that has only a display function. Some displays may also include control functions<sup>9</sup>, and therefore, need to be evaluated to show that incorrect functioning of the information display does not prevent the performance of the safety function when necessary.

In the past, information displays only provided a display function, and therefore did not necessitate two-way communications. Modern display systems may include control functions, and therefore the reviewer should ensure that incorrect functioning of the information displays does not prevent the safety function from being performed when necessary. This is the same issue as in subsection 5.6, "Independence," and similar methods are appropriate. If the communications path is one-way from the safety system to the displays, or if the displays and controls are qualified as safety related, the safety determination is simplified. Two-way

---

<sup>9</sup> See DI&C-ISG-04, Section 3, "Multidivisional Control and Display Stations."

communications with non-safety control systems have the same isolation issues as any other non-safety to safety communications.<sup>10</sup> The reviewer should conclude that the developer has ensured that inadvertent actions, such as an unintended touch on a touch sensitive display cannot prevent the safety function.

#### D.10.4.2.9 IEEE Std 7-4.3.2, Clause 5.9, Control of access

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.9.

#### D.10.4.2.10 IEEE Std 7-4.3.2, Clause 5.10, Repair

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.10.

#### D.10.4.2.11 IEEE Std 7-4.3.2, Clause 5.11, Identification

Clause 5.11 specifies that firmware and software identification be used to assure the correct software is installed in the correct hardware component. Means should be included in the software such that the identification may be retrieved from the firmware using software maintenance tools and that physical identification of hardware is implemented in accordance with IEEE Std 603-1991. The identification should be clear and unambiguous, include revision level, and should be traceable to configuration control documentation. Licensees should ensure that the configuration management plans are sufficient to meet this clause, and when discussing compliance with the clause, point to the sections of the configuration management plans where this is discussed. The NRC staff should review the development processes that were implemented and that the firmware and software identification is in accordance with NRC regulations.

#### D.10.4.2.12 IEEE Std 7-4.3.2, Clause 5.12, Auxiliary Features

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.12.

#### D.10.4.2.13 IEEE Std 7-4.3.2, Clause 5.13, Multi-unit Stations

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.13.

#### D.10.4.2.14 IEEE Std 7-4.3.2, Clause 5.14, Human Factor Considerations

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.14.

---

<sup>10</sup> See DI&C-ISG-04, Section 1, "Interdivisional Communications."

#### D.10.4.2.15 IEEE Std 7-4.3.2, Clause 5.15, Reliability

##### **Review (Phase 2): Reliability Analysis**

Clause 5.15 specifies that, in addition to the requirements of IEEE Std 603-1991, when reliability goals are identified, the proof of meeting the goals should include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing.<sup>11</sup>

As stated in RG 1.152, the NRC does not endorse the concept of quantitative reliability goals as the sole means of meeting the NRC's regulations for reliability in digital computers for safety-related applications. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the system.

Since there is not a widely accepted view on the determination of software reliability values, determining an error probability and therefore a reliability value may not be appropriate. The reviewer should be cautious if vendors or licensees offer such a value. The NRC staff relies on the vendor implementing a high quality process of software design to obtain high quality software. The reviewer should expect the software to be of the highest quality, but should not credit the software being perfect. The NRC staff should review software reliability calculations and that the firmware and software is in accordance with NRC reliability guidelines.

#### D.10.4.3 IEEE Std 7-4.3.2, Clause 6, Sense and Command Features

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.3.

#### D.10.4.4 IEEE Std 7-4.3.2, Clause 7, Execute Features

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.4.

#### D.10.4.5 IEEE Std 7-4.3.2, Clause 8, Power Source

There are no criteria beyond those in IEEE Std 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.5.

### **D.10.5 Conclusion**

The NRC staff should review the licensee's submittal against the criteria of IEEE Std 7-4.3.2-2003 and should assess whether or not the proposed implementation meets the clauses of that standard.

---

<sup>11</sup> A reliability analysis provides sufficient detail to support and justify that the system meets the reliability requirements.

## **D.11 Technical Specifications**

### **D.11.1 Scope of Review**

The scope of review includes the information necessary to ensure compliance with 10 CFR 50.36. SRP Chapter 7 BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," should be used by the staff in these evaluations.

As discussed previously, the complex nature of digital I&C systems allows for individual channels to be aware of other channels and system functions. This ability has the potential to obviate the need for some of the Surveillance Requirements (SRs) classically associated with I&C. Specifically, the need for channel checks, channel calibrations, etc, may no longer be necessary if these functions can be performed internally by the digital I&C system. While utilization of digital I&C systems may allow the deletion of some existing SRs, those that are necessary to assure that the quality of the system and its components is maintained need to be retained in TSs or proposed for addition to the TSs.

Additionally, if a licensee anticipates a later need to make changes to the digital I&C programming or system settings without prior NRC approval, it may be necessary for the appropriate development processes to be referenced in the administrative section of the TSs.

### **D.11.2 Information to be Provided**

**Review (Phase 1):** LAR Section 4.11, "Technical Specifications"

In addition to a mark-up copy of the TSs, the licensee should provide a justification for each change. This includes a detailed basis for how the digital I&C system internally accomplishes each SR proposed for deletion and provide the V&V documentation for each SR proposed for addition. These justifications, taken together, should demonstrate that the proposed TSs provide sufficient limits such that the digital I&C system will be able to maintain safe operation of the facility with respect to its associated functions.

### **D.11.3 Regulatory Evaluation**

10 CFR 50.36(c)(2)(i) states that limiting conditions for operation (LCO) are the lowest functional capability or performance levels of equipment required for safe operation of the facility. When a LCO of a nuclear reactor is not met, the licensee shall shut down the reactor or follow any remedial action required by the technical specifications until the condition can be met. A limiting condition for operation needs to be established for any condition that meets one or more of the four criterion given in 10 CFR 50.36(c)(2)(ii).

10 CFR 50.36(c)(3) states that the TSs must contain SRs relating to test, calibration, and inspection to assure the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met.

10 CFR 50.36(c)(5) states that administrative controls are the provisions relating to organization and management, procedures, recordkeeping, review and audit, and reporting necessary to assure operation of the facility in a safe manner.



#### **D.11.4 Technical Evaluation**

TS LCOs being proposed for deletion are evaluated against the four 10 CFR 50.36(d)(2)(ii) criteria that require establishment of a LCO for a system of function. If none of the criteria apply to the system of function addressed by an existing LCO, the LCO may be deleted. Additionally, LCOs being proposed for addition should adequately define the lowest functional capability or performance levels of the system required for safe operation of the facility. This review includes the adequacy of the proposed LCOs and the potential need for additional LCOs that have not been proposed for addition to the TSs.

The SRs associated with the LCOs that will govern system operation should be sufficient to test, calibrate, and inspect the system and its functions such that the necessary quality of the system is assured. As with the review of the LCOs, the staff should evaluate proposed SRs and the need for additional LCOs.

The NRC staff should ensure that the licensee has proposed to include the appropriate references to methods and processes in the Administrative section of the TSs.

#### **D.11.5 Conclusion**

The NRC staff should review proposed TS changes associated with the implementation of digital I&C system and should assess whether the LCOs and SRs that will govern the operations, test, and maintenance of the digital I&C system are adequate to conclude that the system will perform its design function. Additionally, the NRC staff should review the methods and processes that have been proposed for incorporation into the administrative section of the TSs and should assess the acceptability of the methods and processes. The NRC staff should disclose in the SE whether the proposed digital I&C upgrade is acceptable with respect to technical specifications.

### **D.12 Secure Development and Operational Environment**

#### **D.12.1 Scope of Review**

The scope of the review includes:

- Ensuring that the development processes and documentation are secure (from non-malicious acts or events) such that the system does not contain undocumented code (e.g., backdoor coding and dead code), unwanted functions or applications, and any other coding that could adversely impact the integrity or reliability of the digital safety system. Review of secure software design and development processes include the concepts phase through the factory acceptance tests.
- Ensuring that any undesirable behavior of connected systems do not prevent the safety system in the performance of its safety function.
- Ensuring that access to safety systems is controlled such that inadvertent access and or operator error does not adversely impact the performance of the safety function.

(Note: Site acceptance, installation, operation and maintenance, and retirement phases are not in the scope of a 10CFR50 licensing review.)

Any cyber security design features included as part of a safety system for the purposes of complying with 10 CFR 73.54 would be reviewed to ensure that their inclusion would not impact the reliable performance of the safety function. However, no evaluation of the adequacy of those cyber security features should be made as part of the licensing review.

#### **D.12.2 Information to be Provided**

**Review (Phase 1):** (1) LAR Section 4.12, "Secure Environment and Operational Environment"  
(2) Vulnerability Assessment  
(3) Secure Development and Operational Environment Controls

The licensee's submittal should provide documentation to support the assertion that a proposed digital I&C system is adequately robust to perform its safety function within its design-basis normal and adverse environments.

Development of a vulnerability assessment is a licensee's opportunity to identify those concerns that formed the basis for adoption of design features for the safety system to protect against undesirable behavior of connected systems and inadvertent access to the system. The vulnerability assessment should also identify those concerns with the development process that could have led to incorporation of undocumented and unwanted code. The vulnerability assessment should address vulnerabilities due to hardware, software, access control, and network connectivity and forms the basis for the overall system secure environment approach. The Secure Development and Operational Environment Controls includes (1) Secure Operational Environment Design Features, (2) Requirements Phase Requirements and Controls, (3) Design Phase Requirements and Controls, (4) Implementation Phase Requirements and Controls, and (5) Test Phase Requirements and Controls. The Vulnerability Assessment and the Secure Development and Operational Environment Controls address Regulatory Positions 2.1, Concepts Phase through 2.5, Test Phase of Regulatory Guide 1.152. The information necessary to address the various aspects of secure environment are elaborated in Section D.12.4.

#### **D.12.3 Regulatory Evaluation**

GDC 21, "Protection system reliability and testability", requires in part that "The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed."

10 CFR 50.55a(h) requires that protection systems for nuclear power plants meet the requirements of IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. With respect to the use of computers in safety systems, IEEE Std 7-4.3.2-2003 specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std 603. IEEE Std 7-4.3.2 reflects advances in digital technology and represents a continued effort by IEEE to support the specification, design, and implementation of computers in safety systems of nuclear power plants. In addition, IEEE Std 7-4.3.2-2003 specifies computer-specific criteria to supplement the criteria and requirements which are endorsed by RG 1.152.

IEEE Std 603-1991 Clause 4.8 requires that the design basis shall document as a minimum: "The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety

functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).” Furthermore, IEEE Std 603-1991 Clause 5.5, “System Integrity,” states, “The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.”

IEEE Std 603-1991 in Clause 5.6.3.1(2) under Interconnected Equipment states, “No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.” NRC staff should review the interconnected systems and equipment to conclude that the safe operation of the system will not be adversely impacted due to undesirable behavior of any interconnected systems or equipment.

IEEE Std 603-1991 in Clause 5.9 under Control of Access states, “The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.” NRC staff should review the control of access requirements to ensure reliable performance of the safety function.

#### **D.12.4 Technical Evaluation**

To meet the regulatory requirements, the information provided must demonstrate that appropriate measures have been taken throughout the development life cycle (from inception through the test phase) to ensure that the software is free from undocumented code (e.g., backdoor coding and dead code), unwanted functions or applications, and any other coding that could adversely impact the integrity or reliability of the digital safety system. Vulnerability assessment identifies the vulnerabilities that could affect the secure development and reliable and secure operation of a digital safety system. To protect against the identified vulnerabilities, adequate controls through the design and development phases, implementation phase, and test phase must be in place.

Following is the information that should be provided in support of the secure environment. It is recognized that every organizational entity may have a different name for the same document. In addition, it is conceivable that some of the licensees may address some of the documentation needs in another software related document. While including the secure environment criteria within another document is acceptable, the licensees are urged to devote a separate section of the LAR for such secure environment issues and provide a roadmap for the same in the application.

##### **D.12.4.1 Vulnerability Assessment**

The licensee should identify potential vulnerabilities during all phases of the project including both development and operations. Vulnerabilities for the development phases should provide the basis for protective actions, programs, processes and controls that are aimed at precluding the introduction of unwanted, unneeded and undocumented code in the operating system and application software. Vulnerabilities of the operational phases should be used to determine what design features or controls are appropriate to prevent (unintended) inadvertent access to the system and to protect the reliable operation of the system from undesired behavior from connected systems.

The licensee should be assessing the weaknesses (potential, actual, and perceived) in the physical or electronic configuration of a safety system or any other digital system that is or may be connected to the safety system that could allow an action that compromises the secure environment and, hence, the reliability of the safety system. All unintended actions must be considered as part of the vulnerability assessment. These actions may be caused by operator error, inadvertent operator access to the system, connection to a device or a network which had not been considered and included in the vulnerability analysis, and undesirable behavior of connected systems. Control of documentation, control of hardware, control of software, control of development activities, and control of test environment must be exercised to prevent introduction of unwanted, unneeded and undocumented code.

#### D.12.4.2 Concepts Phase

The design features adopted to address operational vulnerabilities (i.e., those deficiencies identified in the vulnerability assessment that could lead to degradation in reliable system operation due to either inadvertent access or undesirable behavior of connected systems) should be identified in the concepts phase.

#### D.12.4.3 Requirements Phase

Those secure operational environment design features identified to address any operational vulnerabilities should have criteria identified during this phase. These secure operational environment criteria may be included with the platform and/or application software specifications (with a specific section devoted to secure environment).

Activities involved with the development of criteria to preclude introduction of unwanted or unneeded criteria also must be addressed as part of the requirements phase. The secure development environment portion of the requirements documentation may be included in a specific section of another document; however, the controls should be clearly identified. Measures taken to secure the requirements and requirements development process should address the requirements phase vulnerabilities identified in the vulnerability assessment.

#### D.12.4.4 Design Phase

During the design phase, criteria are translated into system / software design. The protection of the design documents and the development activities pertaining to design phase must be appropriately addressed. Design of secure operational environment design features would be expected to trace to secure operational environment design criteria and to be included in the system design documentation.

The design phase activities aimed at precluding introduction of unwanted, unneeded and undocumented design features may be addressed in a separate document or as part of one or more of the other documents. Measures taken to secure the design documentation and development process should address the design phase vulnerabilities identified in the vulnerability assessment.

#### D.12.4.5 Implementation Phase

In the implementation phase the system design is translated into code, database structures, and related machine executable representations. Implementation of secure operational environment design features would be expected to trace back to the design documentation.

Measures taken to protect the implementation phase from the introduction of unwanted, unneeded and undocumented code may be addressed in a separate document or as part of one or more of the other documents. Measures taken to secure the developed code and implementation process should address the implementation phase vulnerabilities identified in the vulnerability assessment.

#### D.12.4.6 Test Phase

In the test phase the secure operational environment design features are tested. The test phase should not only verify and validate the secure operational environment design feature criteria and functions but must also be secure from inadvertent manipulation of the test environment and test results. The test phase activities may be addressed in a separate document or as part of one or more of the other documents. Measures taken to secure the test environment and processes should address the test phase vulnerabilities identified in the vulnerability assessment.

Test phase specifications and results should be available for review by NRC staff. The need to submit any of these documents should be determined during the licensing review.

#### D.12.5 Conclusion

The NRC staff should review the requested information to conclude that the system is designed, tested, and controlled against identified vulnerabilities and that the overall design, development controls, and testing should result in a system that should be free from undocumented code (e.g., backdoor coding and dead code), unwanted functions or applications, and any other coding that could adversely impact the integrity or reliability of the digital safety system. The staff may review and audit any of the documentation and/or testing to conclude that the digital safety system was developed in a secure environment and that it will be protected from inadvertent actions in its operational environment.

## **Enclosure A**

### **Sample Summary of Level 0**

#### **Public Meeting to Discuss Plans to Request NRC Approval in Support of a Digital I&C Upgrade License Amendment Request**

MEMORANDUM TO: [NAME], Director  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation  
[NAME], Director  
Division of Engineering  
Office of Nuclear Reactor Regulation

FROM: [NAME], Project Manager  
Plant Licensing Branch [X-X]  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation

SUBJECT: SUMMARY OF [MONTH DAY, YEAR], CATEGORY 1 PUBLIC MEETING TO DISCUSS [LICENSEE] PLANS TO REQUEST NRC APPROVAL OF A DIGITAL I&C UPGRADE OF [SYSTEM] USING [PLATFORM]

On [DATE], the Nuclear Regulatory Commission (NRC) staff conducted a Category 1 public meeting to discuss [LICENSEE]'s plans for upgrading the [PLANT] [SYSTEM] to the [PLATFORM] digital instrumentation and control (I&C) system.

The purpose of this meeting was to discuss the initial design concepts and any site specific issues identified by [LICENSEE]. These discussions focused on the how [LICENSEE] should address the review area of defense-in-depth and diversity.

In these discussions, the licensee identified the following characteristics and design specifications that contribute to the [PLATFORM]'s diversity and robustness against common cause failure (CCF).

- Item 1
- Item 2...

The NRC staff provided feedback to [LICENSEE] that the following aspects of the design seemed conducive to finding the proposed upgrade consistent with the NRC staff's position on defense-in-depth and diversity:

- Item 1
- Item 2...

Additionally, the NRC staff identified that the following aspects of the design would need additional review before finding the proposed upgrade fully consistent with the NRC staff's position on defense-in-depth and diversity:

- Item 1
- Item 2...

*Concurrence for this memorandum shall include the Chief, Instrumentation & Controls Branch, the Chief, Plant Licensing Branch X-X, and any other Branch Chiefs whose review authorities may have been discussed.*

## **Enclosure B**

# **Information to be Provided in Support of a Digital I&C Upgrade License Amendment Request**

Note: The list of information to be submitted is only a representation on one type of system modification. In this particular example, the microprocessor has been upgraded, and the printed circuit boards, support chip set, and memory have also been modified along with the new microprocessor. The operating system or platform software has been upgraded, and a different set of software tool was used to develop and test the new software. Most of the lifecycle documentation is the same; however the software development manual, the V&V plan, and the testing plan have been modified. Systems with a different type of modifications since the system was last reviewed should necessitate a different set of documentation to be submitted to the staff for review.

This enclosure can be used as a cross reference or checklist for addressing the descriptive material provided in the body of this ISG. This enclosure is intended to be used with the sections referenced.



	Tier			Submitted with LAR (Phase 1)
	1	2	3	
1.1	X	X	X	Hardware Architecture Descriptions (D.1.2)
1.2			X	Quality Assurance Plan for Digital Hardware (D.2.2)
1.3	X	X	X	Software Architecture Descriptions (D.3.2, D.4.4.3.2)
1.4	X	X	X	Software Management Plan (D.4.4.1.1)
1.5	X	X	X	Software Development Plan (D.4.4.1.2)
1.6	X	X	X	Software QA Plan (D.4.4.1.3, D.10.4.2.3.1)
1.7	X	X	X	Software Integration Plan (D.4.4.1.4)
1.8	X	X	X	Software Safety Plan (D.4.4.1.9)
1.9	X	X	X	Software V&V Plan (D.4.4.1.10)
1.10	X	X	X	Software Configuration Management Plan (D.4.4.1.11)
1.11	X	X	X	Software Test Plan (D.4.4.1.12)
1.12	X	X	X	Software Requirements Specification (D.4.4.3.1)
1.13	X	X	X	Software Design Specification (D.4.4.3.3)
1.14		X	X	Equipment Qualification Testing Plans (Including EMI, Temperature, Humidity, and Seismic) (D.5.2)
1.15	X	X	X	D3 Analysis (D.6.2)
1.16	X	X	X	Design Analysis Reports (D.7.2, D.8.2, D.9.4.2.6, D.10.4.2.6)
1.17	X	X	X	System Description (To block diagram level) (D.9.2, D.10.2)
1.18		X	X	Design Report on Computer integrity, Test and Calibration, and Fault Detection (D.9.4.2.5, D.9.4.2.7, D.9.4.2.10, D.9.4.3.5, D.10.4.2.5, D.10.4.2.7)
1.19	X	X	X	System Response Time Analysis Report (D.9.4.2.4)
1.20		X	X	Theory of Operation Description (D.9.4.2.8, D.9.4.2.9, D.9.4.2.10, D.9.4.2.11, D.9.4.2.13, D.9.4.2.14, D.9.4.3.2, D.9.4.3.5, D.9.4.3.6, D.9.4.3.7, D.9.4.4)
1.21	x	x	x	Setpoint Methodology (D.9.4.3.8, D.11)
1.22			X	Vendor Software Plan (D.10.4.2.3.1)
1.23		X	X	Software Tool Verification Program (D.10.4.2.3.2)
1.24	X	X	X	Software Project Risk Management Program (D.10.4.2.3.6)
1.25		X	X	Commercial Grade Dedication Plan (D.10.4.2.4.2)
1.26	X	X	X	Vulnerability Assessment (D.12.4.1)
1.27	X	X	X	Secure Development and Operational Environment Controls (D.12.2)

	Tier			Submitted 12 months prior to requested approval (Phase 2)
	1	2	3	
2.1	X	X	X	<b>Safety Analysis</b> (D.4.4.2.1)
2.2	X	X	X	<b>V&amp;V Reports</b> (D.4.4.2.2)
2.3	X	X	X	<b>As-Manufactured, System Configuration Documentation</b> (D.4.4.2.3)
2.4	X	X	X	<b>Test Design Specification</b> (D.4.4.2.4)
2.5	X	X	X	<b>Summary Test Reports (Including FAT)</b> (D.4.4.2.4)
2.6	X	X	X	<b>Summary of Test Results (Including FAT)</b> (D.4.4.2.4)
2.7	X	X	X	<b>Requirement Traceability Matrix</b> (D.9.4.2)
2.8		X	X	<b>FMEA</b> (D.9.4.2.1.1)
2.9	X	X	X	<b>System Build Documents</b> ( D.4.4.3.5)
2.10				
2.11		X	X	<b>Qualification Test Methodologies</b> (D.5.2)
2.12		X	X	<b>Summary of Digital EMI, Temp., Humidity, and Seismic Testing Results</b> (D.5.2)
2.13	X	X	X	<b>As-Manufactured Logic Diagrams</b> (D.9.2)
2.14	X	X	X	<b>System Response Time Confirmation Report</b> (D.9.4.2.4)
2.15	X	X	X	<b>Reliability Analysis</b> (D.9.4.2.15, D.10.4.2.15)
2.16	X	X	X	<b>Setpoint Calculations</b> (D.9.4.3.8)
2.17		X	X	<b>Software Tool Analysis Report</b> (D.10.4.2.3.2)
		X	X	<b>Commercial Grade Dedication Report(s)</b> (D.10.4.2.4.2)

	Tier			Available for audit 12 months prior to requested approval (Phase 2)
	1	2	3	
3.1	X	X	X	<b>Software Integration Report</b> (D.4.4.1.4, D.4.4.2.2)
3.2	X	X	X	<b>Individual V&amp;V Problem Reports up to FAT</b> (D.4.4.2.2)
3.3	X	X	X	<b>Configuration Management Reports</b> (D.4.4.2.3)
3.4	X	X	X	<b>Test Procedure Specification</b> (D.4.4.2.4)
3.5	X	X	X	<b>Completed Test Procedures and Reports</b> (D.4.4.2.4, D.5.2)
3.6	X	X	X	<b>Test Incident Reports</b> (D.4.4.2.4)
3.7	X	X	X	<b>Code Listings</b> (D.4.4.3.4)
3.8	X	X	X	<b>Software Project Risk Management Report</b> (D.10.4.2.3.6)
3.9	X	X	X	<b>Circuit Schematics</b>
3.10	X	X	X	<b>Detailed System and Hardware Drawings</b>

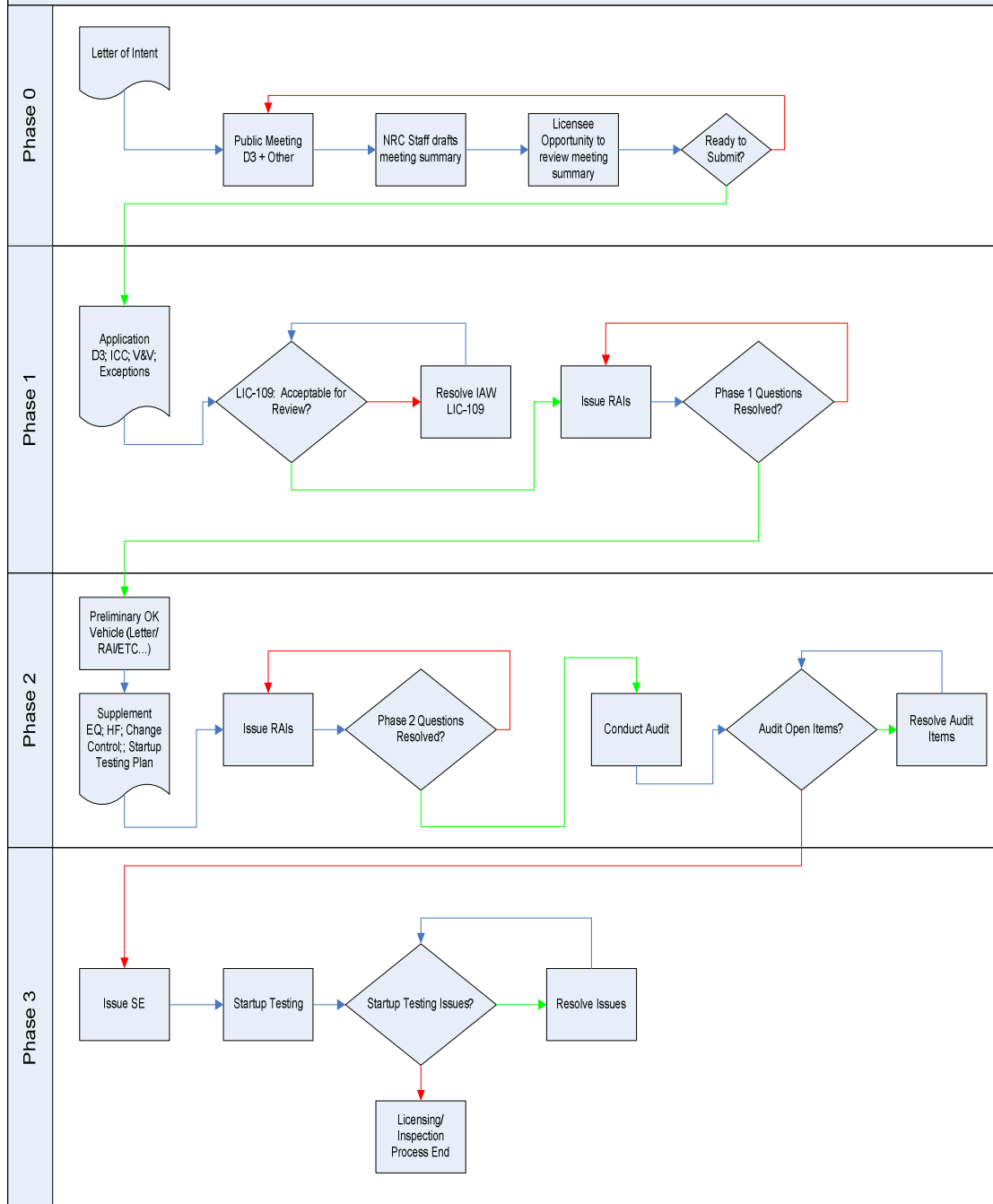
	Tier			Available for Inspection After Approval (Phase 3)
	1	2	3	
4.1	X	X	X	<b>Software Installation Plan</b> (D.4.4.1.5)
4.2	X	X	X	<b>Software Maintenance Plan</b> (D.4.4.1.6)
4.3	X	X	X	<b>Software Training Plan</b> (D.4.4.1.7)
4.4	X	X	X	<b>Software Operations Plan</b> (D.4.4.1.8)
4.5	X	X	X	<b>Site Test Documentation</b> (D.4.4.2.4)
4.6	X	X	X	<b>Operations Manual</b> (D.4.4.3.7)
4.7	X	X	X	<b>Software Maintenance Manuals</b> (D.4.4.3.8)
4.8	X	X	X	<b>Software Training Manuals</b> (D.4.4.3.9)
4.9		X	X	<b>Installation Configuration Tables</b> (D.4.4.3.6)

# **Enclosure C**

## **Digital I&C Licensing Process**

### **Flow Chart**

# Digital I&C Licensing Process Flow Chart



# **Enclosure D**

## **Sample Safety Evaluation for Digital I&C License Amendment**

Note: This is only a sample of what the Safety Evaluation Report may be. Since each digital system is somewhat different and each presents unique challenges to the review process, each SE should be unique and any particular SE should be different from the sample shown.

## Table of Contents

1.0	INTRODUCTION.....	5
2.0	REGULATORY EVALUATION.....	5
3.0	TECHNICAL EVALUATION .....	5
3.1	System Description .....	6
3.2	Hardware Development Process.....	6
3.3	Software Architecture .....	6
3.4	Software Development Process .....	6
3.4.1	Software Planning Documentation .....	6
3.4.1.1	Software Management Plan (SMP).....	6
3.4.1.2	Software Development Plan (SDP).....	6
3.4.1.3	Software Quality Assurance Plan (SQAP) .....	6
3.4.1.4	Software Integration Plan (SIntP).....	6
3.4.1.5	Software Installation Plan (SInstP).....	6
3.4.1.6	Software Maintenance Plan (SMaintP) .....	6
3.4.1.7	Software Training (STrngP).....	6
3.4.1.8	Software Operations Plan (SOP) .....	6
3.4.1.9	Software Safety Plan (SSP) .....	7
3.4.1.10	Software V&V Plan (SVVP).....	7
3.4.1.11	Software Configuration Management Plan (SCMP) .....	7
3.4.1.12	Software Test Plan (STP) .....	7
3.4.2	Software Implementation Documentation .....	7
3.4.2.1	Review of Safety Analyses.....	7
3.4.2.2	V&V Analysis and Reports .....	7
3.4.2.3	Configuration Management Activities.....	7
3.4.2.4	Testing Activities .....	7
3.4.3	Software Design Outputs .....	7
3.4.3.1	Software Requirements Specification .....	7
3.4.3.2	Software Architecture Description .....	7
3.4.3.3	Software Design Description (or Software Design Specification) .....	7
3.4.3.4	Software Design Review .....	7
3.4.3.5	Thread Audit of source Code Listings (CL) .....	8
3.4.3.6	System Build Documents (SBD) .....	8
3.5	Environmental Equipment Qualification .....	8
3.5.1	Environmental Qualification of System.....	8
3.5.1.1	Atmospheric .....	8
3.5.1.2	Interference .....	8
3.5.1.3	Susceptibility .....	8
3.5.1.4	Radiation.....	8
3.5.1.5	Electromagnetic Interference/Radio Frequency Interference .....	8
3.5.1.6	Seismic Qualification.....	9
3.5.2	Power Quality.....	9
3.5.3	Response time characteristics and testing .....	9
3.6	Defense-in-Depth and Diversity .....	9
3.7	Communications .....	9
3.7.1	DI&C-ISG-04 Compliance .....	9

3.7.1.1	DI&C-ISG-04, Section 1 – Interdivisional Communications.....	9
3.7.1.2	DI&C-ISG-04, Section 2 – Command Prioritization.....	9
3.7.1.3	DI&C-ISG-04, Section 3 – Multidivisional Control and Display Stations.....	9
3.8	System, Hardware, Software and Methodology Modifications .....	10
3.9	Review of System and IEEE Std 603 requirements .....	10
3.9.1	Clause 4. Design Basis .....	10
3.9.1.1	Clause 4.1 identification of the design basis events.....	10
3.9.1.2	Clause 4.2 Identification Of Safety Functions And Protective Actions.....	10
3.9.1.3	Clause 4.3 Permissive Conditions for Operating Bypasses .....	10
3.9.1.4	Clause 4.4 identification of variables monitored .....	10
3.9.1.5	Clause 4.5 minimum criteria for manual protective actions .....	10
3.9.1.6	Clause 4.6 identification of the minimum number and location of sensors.....	10
3.9.1.7	Clause 4.7 Range of Transient and Steady-State Conditions .....	10
3.9.1.8	Clause 4.8 Conditions Causing Functional .....	10
3.9.1.9	Clause 4.9 methods used to determine.....	10
3.9.1.10	Clause 4.10 Control after Protective Actions.....	11
3.9.1.11	Clause 4.11 Equipment Protective Provisions.....	11
3.9.1.12	Clause 4.12 Special Design Bases .....	11
3.9.2	Clause 5. System .....	11
3.9.2.1	Clause 5.1 Single-Failure Criterion .....	11
3.9.2.1.1	FMEA.....	11
3.9.2.2	Clause 5.2 Completion of Protective Action .....	11
3.9.2.3	Clause 5.3 Quality.....	11
3.9.2.4	Clause 5.4 Equipment Qualification .....	11
3.9.2.5	Clause 5.5 System Integrity .....	11
3.9.2.6	Clause 5.6 Independence .....	11
3.9.2.7	Clause 5.7 Capability for Test and Calibration.....	11
3.9.2.8	Clause 5.8 Information Displays.....	11
3.9.2.9	Clause 5.9 Control of Access .....	12
3.9.2.10	Clause 5.10 Repair .....	12
3.9.2.11	Clause 5.11 Identification.....	12
3.9.2.12	Clause 5.12 Auxiliary Features .....	12
3.9.2.13	Clause 5.13 Multi-Unit Stations.....	12
3.9.2.14	Clause 5.14 Human Factors Considerations.....	12
3.9.2.15	Clause 5.15 - Reliability .....	12
3.9.3	Clauses 6. - Sense and Command Features .....	12
3.9.3.1	Clause 6.1 - Automatic Control .....	12
3.9.3.2	Clause 6.2 - Manual Control.....	12
3.9.3.3	Clause 6.3 Interaction with Other Systems .....	12
3.9.3.4	Clause 6.4 Derivation of System Inputs .....	12
3.9.3.5	Clause 6.5 Capability for Testing and Calibration .....	12
3.9.3.6	Clauses 6.6 Operating Bypasses .....	13
3.9.3.7	Clauses 6.7 Maintenance Bypass .....	13
3.9.3.8	Clause 6.8 Setpoints .....	13
3.9.4	Clause 7 - Execute Features.....	13
3.9.4.1	Clause 7.1- Automatic Control .....	13



3.9.4.2	Manual Control.....	13
3.9.4.3	Clause 7.3 Completion of Protective Action .....	13
3.9.4.4	Clause 7.4 Operating Bypasses.....	13
3.9.4.5	Clause 7.5 Maintenance Bypass.....	13
3.9.5	Clause 8 Power Source .....	13
3.10	Review IEEE Std 7-4.3.2.....	13
3.10.1	Clause 5. System .....	13
3.10.1.1	Clause 5.3 Quality.....	13
3.10.1.1.1	Clause 5.3.1 Software Development.....	14
3.10.1.1.2	Clause 5.3.2 Software Tools.....	14
3.10.1.1.3	Clause 5.3.3 Verification and Validation .....	14
3.10.1.1.4	Clause 5.3.4 Independent V&V (IV&V) .....	14
3.10.1.1.5	Clause 5.3.5 Software Configuration Management.....	14
3.10.1.1.6	Clause 5.3.6 Software Project Risk Management.....	14
3.10.1.2	Clause 5.4 Equipment Qualification .....	14
3.10.1.2.1	Clause 5.4.1 Computer System Testing .....	14
3.10.1.2.2	Clause 5.4.2 Qualification of Existing Commercial Computers .....	14
3.10.1.2.3	Deterministic System Behavior .....	14
3.10.1.2.4	Performance – Response Time .....	14
3.10.1.3	Clause 5.5 System Integrity .....	14
3.10.1.3.1	Clause 5.5.1 Design for Computer Integrity .....	14
3.10.1.3.2	Clause 5.5.2 Design for Test and Calibration .....	15
3.10.1.4	Clause 5.6 Independence .....	15
3.10.1.5	Clause 5.7 Capability for Test and Calibration .....	15
3.10.1.6	Clause 5.8 Information Displays.....	15
3.10.1.7	Clause 5.11 Identification.....	15
3.10.1.8	Clause 5.15. Reliability.....	15
3.11	Technical Specification changes.....	15
3.12	Secure <i>Development and Operational</i> Environment .....	15
4.0	NRC FINDINGS .....	15
4.1	Summary of Regulatory Compliance.....	15
4.2	Limitations and Conditions .....	15
5.0	CONCLUSION .....	16
6.0	REFERENCES.....	16

Directions:

Fill in the **bolded** bracketed information. The *italicized* wording provides guidance on what should be included in each section. Delete the *italicized* wording from the safety evaluation (SE).

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION  
RELATED TO AMENDMENT NO. TO FACILITY OPERATING LICENSE NO. {NPF-XX}

AND AMENDMENT NO. TO FACILITY OPERATING LICENSE NO. {NPF-YY}

**{NAME OF LICENSEE}**

**{NAME OF FACILITY}**

**DOCKET NOS. 50-{XXX} AND 50-{YYY}**

## 1.0 INTRODUCTION

*Read DI&C-ISG-06 Sections A, B, & C.*

*Read and follow LIC-101 Rev. 3:*

- (1) Attachment 2 Section 4.5.1, "Introduction"*
- (2) Attachment 3 Section 1 (PDF page 62 of 64)*
- (3) SRP Chapter 7, Appendix 7.0-A*

## 2.0 REGULATORY EVALUATION

*Read:*

- (1) 10 CFR 50.34(h), "Conformance with the Standard Review Plan (SRP)"*
- (2) LIC-200 Rev. 1 Section 4.5 – Regarding the applicability of 10 CFR 50.34(h)*
- (3) RG 1.70 Section 7.1.2, "Identification of Safety Criteria"*
- (4) SRP Chapter 7, Appendix 7.1-A and Table 7-1*

*Read and follow:*

- (1) LIC-101 Rev. 3 Attachment 2 Section 4.5.2, "Regulatory Evaluation"*
- (2) LIC-101 Rev. 3 Attachment 3 Section 2, "Regulatory Evaluation" (PDF page 62 of 64)*

## 3.0 TECHNICAL EVALUATION

*Read and follow LIC-101 Rev. 3:*

- (1) Attachment 2 Section 4.5.3, "Technical Evaluation"*
- (2) Attachment 3 Section 3, (PDF page 63 of 64).*

*The information to be reviewed in this section may be taken from the "System Description (to Block Diagram Level)" (see DI&C-ISG-06 Enclosure B).*

### 3.1 System Description

*Read DI&C-ISG-06 Section D.1, "Hardware Description"*

### 3.2 Hardware Development Process

*Read DI&C-ISG-06 Section D.2, "Hardware Development Process"*

### 3.3 Software Architecture

*Read DI&C-ISG-06 Section D.3, "Software Architecture"*

### 3.4 Software Development Process

*Read DI&C-ISG-06 Section D.4, "Software Development Process"*

#### 3.4.1 Software Planning Documentation

*Read and follow:*

- (1) *SRP Chapter 7 Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems" Section C.1.E, "Life-cycle process planning"*
- (2) *SRP Chapter 7 BTP 7-14 Section B.3.1, "Acceptance Criteria for Planning"*

##### 3.4.1.1 Software Management Plan (SMP)

*Read DI&C-ISG-06 Section D.4.4.1.1, "Software Management Plan"*

##### 3.4.1.2 Software Development Plan (SDP)

*Read DI&C-ISG-06 Section D.4.4.1.2, "Software Development Plan"*

##### 3.4.1.3 Software Quality Assurance Plan (SQAP)

*Read DI&C-ISG-06 Section D.4.4.1.3, "Software Quality Assurance Plan"*

##### 3.4.1.4 Software Integration Plan (SIntP)

*Read DI&C-ISG-06 Section D.4.4.1.4, "Software Integration Plan"*

##### 3.4.1.5 Software Installation Plan (SInstP)

*Read ISG#6 Section D.4.4.1.5, "Software Installation Plan"*

##### 3.4.1.6 Software Maintenance Plan (SMaintP)

*Read ISG#6 Section D.4.4.1.6, "Software Maintenance Plan"*

##### 3.4.1.7 Software Training (STrngP)

*Read ISG#6 Section D.4.4.1.7, "Software Training Plan"*

##### 3.4.1.8 Software Operations Plan (SOP)

*Read ISG#6 Section D.4.4.1.8, "Software Operation Plan"*

3.4.1.9 Software Safety Plan (SSP)

*Read DI&C-ISG-06 Section D.4.4.1.9, "Software Safety Plan"*

3.4.1.10 Software V&V Plan (SVVP)

*Read DI&C-ISG-06 Section D.4.4.1.10, "Software Verification and Validation Plan"*

3.4.1.11 Software Configuration Management Plan (SCMP)

*Read DI&C-ISG-06 Section D.4.4.1.11, "Software Configuration Management Plan"*

3.4.1.12 Software Test Plan (STP)

*Read DI&C-ISG-06 Section D.4.4.1.12, "Software Test Plan"*

3.4.2 Software Implementation Documentation

3.4.2.1 Review of Safety Analyses

*Read DI&C-ISG-06 Section D.4.4.2.1, "Safety Analysis"*

3.4.2.2 V&V Analysis and Reports

*Read DI&C-ISG-06 Section D.4.4.2.2, "3.4.2.2 V&V Analysis and Reports"*

3.4.2.3 Configuration Management Activities

*Providing the results of the management and control of the software and the associated development environment, as well as document control.*

3.4.2.4 Testing Activities

*Providing the results of the software testing activities.*

3.4.3 Software Design Outputs

3.4.3.1 Software Requirements Specification

*Read DI&C-ISG-06 Section D.4.4.3.1, "Software Requirements Specification"*

3.4.3.2 Software Architecture Description

*Read DI&C-ISG-06 Section D.4.4.3.2, "Software Architecture Design"*

3.4.3.3 Software Design Description (or Software Design Specification)

*Read DI&C-ISG-06 Section D.4.4.3.3, "Software Design Specification"*

3.4.3.4 Software Design Review

*See SRP Chapter 7 BTP 7-14 Section B.3.3.4 "Code Listings" for SRP acceptance criteria and references to applicable guidance.*

#### 3.4.3.5 Thread Audit of source Code Listings (CL)

See SRP Chapter 7 BTP 7-14 Section B.3.3.4 for SRP acceptance criteria and references to applicable guidance.

*Write discussion of Thread Audit. The CL should have sufficient comments and annotations that the intent of the code developer is clear. This is not only so the reviewer can understand and follow the code, but also so future modifications of the code are facilitated. Undocumented code should not be accepted as suitable for use in safety-related systems in nuclear power plants. The documentation should be sufficient for a qualified software engineer to understand. If the reviewer does not have enough experience in this particular language or with the software tool being used, the reviewer may seek the assistance of other NRC personnel or independent contractor personnel to make this determination.*

#### 3.4.3.6 System Build Documents (SBD)

*Read DI&C-ISG-06 Section D.4.4.3.5, "System Build Documents"*

### 3.5 Environmental Equipment Qualification

*Read DI&C-ISG-06 Section D.5, "System Qualifications"*

#### 3.5.1 Environmental Qualification of System

*The environmental qualification includes temperature, humidity, electromagnetic compatibility (EMC), and radiation. For plant specific reviews, the qualifications must bound worst case plant conditions for all accidents and transients where the digital system is needed to mitigate or trip. Discuss test methodology.*

##### 3.5.1.1 Atmospheric

*Read DI&C-ISG-06 Section D.5.4.1, "Atmospheric"*

##### 3.5.1.2 Interference

*Read DI&C-ISG-06 Section D.5.4.3.2, "Interference"*

##### 3.5.1.3 Susceptibility

*Read DI&C-ISG-06 Section D.5.4.3.1, "Susceptibility"*

##### 3.5.1.4 Radiation

*Read DI&C-ISG-06 Section D.5.4.2, "Radiation"*

##### 3.5.1.5 Electromagnetic Interference/Radio Frequency Interference

*Read DI&C-ISG-06 Section D.5.4.3, "Electromagnetic Interference/Radio Frequency Interference"*

### 3.5.1.6 Seismic Qualification

### 3.5.2 Power Quality

### 3.5.3 Response time characteristics and testing

*This should include a discussion of the microprocessor cycle times, sampling rates, and testing methods.*

### 3.6 Defense-in-Depth and Diversity

*Read DI&C-ISG-06 Section D.6, "Defense-in-Depth and Diversity"*

### 3.7 Communications

*Read DI&C-ISG-06 Section D.7, "Communication"*

#### 3.7.1 DI&C-ISG-04 Compliance

*The NRC Task Working Group # 4, "Highly Integrated Control Rooms—Communications Issues," has provided interim NRC staff Guidance on the review of communications issues. DI&C-ISG-04 contains three sections, (1) Interdivisional Communications, (2) Command Prioritization, and (3) Multidivisional Control and Display Stations.*

##### 3.7.1.1 DI&C-ISG-04, Section 1 – Interdivisional Communications

*Section 1 of DI&C ISG 04 provides guidance on the review of communications, includes transmission of data and information, among components in different electrical safety divisions and communications between a safety division and equipment that is not safety related. This ISG does not apply to communications within a single division. This NRC staff position states that bidirectional communications among safety divisions and between safety- and nonsafety equipment may be acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems. It goes on to say that systems which include communications among safety divisions and/or bidirectional communications between a safety division and nonsafety equipment should adhere to the 20 points described.*

##### 3.7.1.2 DI&C-ISG-04, Section 2 – Command Prioritization

*Section 2 of DI&C-ISG-04 provides guidance applicable to a prioritization device or software function block, which receives device actuation commands from multiple safety and nonsafety sources, and sends the command having highest priority on to the actuated device.*

*Existing D3 guidance indicates that diverse actuation signals should be applied to plant equipment control circuits downstream of the digital system to which they are diverse, in order to ensure that the diverse actuation will be unaffected by digital system failures and malfunctions. Accordingly, the priority modules that combine the diverse actuation signals with the actuation signals generated by the digital system should not be executed in digital system software that may be subject to common cause failure (CCF).*

##### 3.7.1.3 DI&C-ISG-04, Section 3 – Multidivisional Control and Display Stations

*Section 3 of DI&C-ISG-04 provides guidance concerning safety-related and nonsafety operator workstations used for the control of safety-related plant equipment in more than one safety*

*division and for display of information from sources in more than one safety division, and applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.*

### 3.8 System, Hardware, Software and Methodology Modifications

*Read DI&C-ISG-06 Section D.8, "System, Hardware, Software and Methodology Modifications"*

### 3.9 Review of System and IEEE Std 603 requirements

*Read DI&C-ISG-06 Section D.9, "IEEE Std 603, Compliance"*

#### 3.9.1 Clause 4. Design Basis

*Read DI&C-ISG-06 Section D.9.4.1, "IEEE Std 603, Clause 4..."*

##### 3.9.1.1 Clause 4.1 identification of the design basis events

*Read DI&C-ISG-06 Section D.9.4.1.1, "IEEE Std 603, Clause 4.1..."*

##### 3.9.1.2 Clause 4.2 Identification Of Safety Functions And Protective Actions

*Read DI&C-ISG-06 Section D.9.4.1.2, "IEEE Std 603, Clause 4.2..."*

##### 3.9.1.3 Clause 4.3 Permissive Conditions for Operating Bypasses

*Read DI&C-ISG-06 Section D.9.4.1.3, "IEEE Std 603, Clause 4.3..."*

##### 3.9.1.4 Clause 4.4 identification of variables monitored

*Read DI&C-ISG-06 Section D.9.4.1.4, "IEEE Std 603, Clause 4.4..."*

##### 3.9.1.5 Clause 4.5 minimum criteria for manual protective actions

*Read DI&C-ISG-06 Section D.9.4.1.5, "IEEE Std 603, Clause 4.5..."*

##### 3.9.1.6 Clause 4.6 identification of the minimum number and location of sensors

*Read DI&C-ISG-06 Section D.9.4.1.6, "IEEE Std 603, Clause 4.6..."*

##### 3.9.1.7 Clause 4.7 Range of Transient and Steady-State Conditions

*Read DI&C-ISG-06 Section D.9.4.1.7, "IEEE Std 603, Clause 4.7..."*

##### 3.9.1.8 Clause 4.8 Conditions Causing Functional

*Read DI&C-ISG-06 Section D.9.4.1.8, "IEEE Std 603, Clause 4.8..."*

##### 3.9.1.9 Clause 4.9 methods used to determine

*Read DI&C-ISG-06 Section D.9.4.1.9, "IEEE Std 603, Clause 4.9..."*

3.9.1.10 Clause 4.10 Control after Protective Actions  
*Read DI&C-ISG-06 Section D.9.4.1.9, "IEEE Std 603, Clause 4.10..."*

3.9.1.11 Clause 4.11 Equipment Protective Provisions  
*Read DI&C-ISG-06 Section D.9.4.1.9, "IEEE Std 603, Clause 4.11..."*

3.9.1.12 Clause 4.12 Special Design Bases  
*Read DI&C-ISG-06 Section D.9.4.1.9, "IEEE Std 603, Clause 4.12..."*

3.9.2 Clause 5. System  
*Read DI&C-ISG-06 Section D.9.4.2, "IEEE Std 603, Clause 5..."*

3.9.2.1 Clause 5.1 Single-Failure Criterion  
*Read DI&C-ISG-06 Section D.9.4.2.1, "IEEE Std 603, Clause 5.1..."*

3.9.2.1.1 FMEA  
*Read DI&C-ISG-06 Section D.9.4.2.1.1, "Failure Modes and Effects Analysis"*

3.9.2.2 Clause 5.2 Completion of Protective Action  
*Read DI&C-ISG-06 Section D.9.4.2.2, "IEEE Std 603, Clause 5.2..."*

3.9.2.3 Clause 5.3 Quality  
*Read DI&C-ISG-06 Section D.9.4.2.3, "IEEE Std 603, Clause 5.3..."*

3.9.2.4 Clause 5.4 Equipment Qualification  
*Read DI&C-ISG-06 Section D.9.4.2.4, "IEEE Std 603, Clause 5.4..."*

3.9.2.5 Clause 5.5 System Integrity  
*Read DI&C-ISG-06 Section D.9.4.2.5, "IEEE Std 603, Clause 5.5..."*

3.9.2.6 Clause 5.6 Independence  
*Read DI&C-ISG-06 Section D.9.4.2.6, "IEEE Std 603, Clause 5.6..."*

3.9.2.7 Clause 5.7 Capability for Test and Calibration  
*Read DI&C-ISG-06 Section D.9.4.2.7, "IEEE Std 603, Clause 5.7"*

3.9.2.8 Clause 5.8 Information Displays  
*Read DI&C-ISG-06 Section D.9.4.2.8, "IEEE Std 603, Clause 5.8..."*



- 3.9.2.9            Clause 5.9    Control of Access  
*Read DI&C-ISG-06 Section D.9.4.2.9, "IEEE Std 603, Clause 5.9..."*
- 3.9.2.10          Clause 5.10   Repair  
*Read DI&C-ISG-06 Section D.9.4.2.10, "IEEE Std 603, Clause 5.10"*
- 3.9.2.11          Clause 5.11   Identification  
*Read DI&C-ISG-06 Section D.9.4.2.11, "IEEE Std 603, Clause 5.11..."*
- 3.9.2.12          Clause 5.12   Auxiliary Features  
*Read DI&C-ISG-06 Section D.9.4.2.12, "IEEE Std 603, Clause 5.12..."*
- 3.9.2.13          Clause 5.13   Multi-Unit Stations  
*Read DI&C-ISG-06 Section D.9.4.2.13, "IEEE Std 603, Clause 5.13..."*
- 3.9.2.14          Clause 5.14   Human Factors Considerations  
*Read DI&C-ISG-06 Section D.9.4.2.14, "IEEE Std 603, Clause 5.14..."*
- 3.9.2.15          Clause 5.15 - Reliability  
*Read DI&C-ISG-06 Section D.9.4.2.15, "IEEE Std 603, Clause 5.15..."*
- 3.9.3    Clauses 6. - Sense and Command Features  
*Read DI&C-ISG-06 Section D.9.4.3, "IEEE Std 603, Clause 6..."*
- 3.9.3.1            Clause 6.1 - Automatic Control  
*Read DI&C-ISG-06 Section D.9.4.3.1, "IEEE Std 603, Clause 6.1..."*
- 3.9.3.2            Clause 6.2 - Manual Control  
*Read DI&C-ISG-06 Section D.9.4.3.2, "IEEE Std 603, Clause 6.2..."*
- 3.9.3.3            Clause 6.3    Interaction with Other Systems  
*Read DI&C-ISG-06 Section D.9.4.3.3, "IEEE Std 603, Clause 6.3..."*
- 3.9.3.4            Clause 6.4    Derivation of System Inputs  
*Read DI&C-ISG-06 Section D.9.4.3.4, "IEEE Std 603, Clause 6.4..."*
- 3.9.3.5            Clause 6.5    Capability for Testing and Calibration  
*Read DI&C-ISG-06 Section D.9.4.3.5, "IEEE Std 603, Clause 6.5..."*

3.9.3.6 Clauses 6.6 Operating Bypasses  
*Read DI&C-ISG-06 Section D.9.4.3.6, "IEEE Std 603, Clause 6.6..."*

3.9.3.7 Clauses 6.7 Maintenance Bypass  
*Read DI&C-ISG-06 Section D.9.4.3.7, "IEEE Std 603, Clause 6.7..."*

3.9.3.8 Clause 6.8 Setpoints  
*Read DI&C-ISG-06 Section D.9.4.3.8, "IEEE Std 603, Clause 6.8..."*

3.9.4 Clause 7 - Execute Features  
*Read DI&C-ISG-06 Section D.9.4.4, "IEEE Std 603, Clause 7..."*

3.9.4.1 Clause 7.1- Automatic Control  
*Read DI&C-ISG-06 Section D.9.4.4.1, "IEEE Std 603, Clause 7.1..."*

3.9.4.2 Manual Control  
*Read DI&C-ISG-06 Section D.9.4.4.2, "IEEE Std 603, Clause 7.2..."*

3.9.4.3 Clause 7.3 Completion of Protective Action  
*Read DI&C-ISG-06 Section D.9.4.4.3, "IEEE Std 603, Clause 7.3..."*

3.9.4.4 Clause 7.4 Operating Bypasses  
*Read DI&C-ISG-06 Section D.9.4.4.4, "IEEE Std 603, Clause 7.4..."*

3.9.4.5 Clause 7.5 Maintenance Bypass  
*Read DI&C-ISG-06 Section D.9.4.4.5, "IEEE Std 603, Clause 7.5..."*

3.9.5 Clause 8 Power Source  
*Read DI&C-ISG-06 Section D.9.4.5, "IEEE Std 603, Clause 8"*

3.10 Review IEEE Std 7-4.3.2  
*Read DI&C-ISG-06 Section D.10 "IEEE Std 7-4.3.2 Guidance"*

3.10.1 Clause 5. System  
*Read DI&C-ISG-06 Section D.10.4.2 "IEEE Std 7-4.3.2, Clause 5..."*

3.10.1.1 Clause 5.3 Quality  
*Read DI&C-ISG-06 Section D.10.4.2.3 "IEEE Std 7-4.3.2, Clause 5.3..."*

3.10.1.1.1 Clause 5.3.1 Software Development

*Read DI&C-ISG-06 Section D.10.4.2.3.1 "IEEE Std 7-4.3.2, Clause 5.3.1..."*

3.10.1.1.2 Clause 5.3.2 Software Tools

*Read DI&C-ISG-06 Section D.10.4.2.3.2 "IEEE Std 7-4.3.2, Clause 5.3.2..."*

3.10.1.1.3 Clause 5.3.3 Verification and Validation

*Read DI&C-ISG-06 Section D.10.4.2.3.3 "IEEE Std 7-4.3.2, Clause 5.3.3..."*

3.10.1.1.4 Clause 5.3.4 Independent V&V (IV&V)

*Read DI&C-ISG-06 Section D.10.4.2.3.4 "IEEE Std 7-4.3.2, Clause 5.3.4..."*

3.10.1.1.5 Clause 5.3.5 Software Configuration Management

*Read DI&C-ISG-06 Section D.10.4.2.3.5 "IEEE Std 7-4.3.2, Clause 5.3.5..."*

3.10.1.1.6 Clause 5.3.6 Software Project Risk Management

*Read DI&C-ISG-06 Section D.10.4.2.3.6, "IEEE Std 7-4.3.2, Clause 5.3.6..."*

3.10.1.2 Clause 5.4 Equipment Qualification

*Read DI&C-ISG-06 Section D.10.4.2.4 "IEEE Std 7-4.3.2, Clause 5.4, Equipment Qualification"*

3.10.1.2.1 Clause 5.4.1 Computer System Testing

*Read DI&C-ISG-06 Section D.10.4.2.4.1 "IEEE Std 7-4.3.2, Clause 5.4.1..."*

3.10.1.2.2 Clause 5.4.2 Qualification of Existing Commercial Computers

*Read DI&C-ISG-06 Section D.10.4.2.4.2 "IEEE Std 7-4.3.2, Clause 5.4.2, Qualification of Existing Commercial Computers"*

3.10.1.2.3 Deterministic System Behavior

*Explicitly address deterministic system behavior in this section.*

3.10.1.2.4 Performance – Response Time

*Explicitly address system response time in this section.*

3.10.1.3 Clause 5.5 System Integrity

*Read DI&C-ISG-06 Section D.10.4.2.5 "IEEE Std 7-4.3.2, Clause 5.5..."*

3.10.1.3.1 Clause 5.5.1 Design for Computer Integrity

*Read DI&C-ISG-06 Section D.10.4.2.5.1 "IEEE Std 7-4.3.2, Clause 5.5.1..."*

3.10.1.3.2 Clause 5.5.2 Design for Test and Calibration

*Read DI&C-ISG-06 Section D.10.4.2.5.2 "IEEE Std 7-4.3.2, Clause 5.5.2..."*

3.10.1.4 Clause 5.6 Independence

*Read DI&C-ISG-06 Section D.10.4.2.6 "IEEE Std 7-4.3.2, Clause 5.6..."*

3.10.1.5 Clause 5.7 Capability for Test and Calibration

*Read DI&C-ISG-06 Section D.10.4.2.7 "IEEE Std 7-4.3.2, Clause 5.7..."*

3.10.1.6 Clause 5.8 Information Displays

*Read DI&C-ISG-06 Section D.10.4.2.8 "IEEE Std 7-4.3.2, Clause 5.8..."*

3.10.1.7 Clause 5.11 Identification

*Read DI&C-ISG-06 Section D.10.4.2.11 "IEEE Std 7-4.3.2, Clause 5.11..."*

3.10.1.8 Clause 5.15. Reliability

*Read DI&C-ISG-06 Section D.10.4.2.15 "IEEE Std 7-4.3.2, Clause 5.15..."*

3.11 Technical Specification changes

*This section should list exactly what is TS changes are being approved. The details should be such that this is a stand-alone document, and the reader should not have to go back to the LAR to know what was approved. The suggested format would be to show the old TS section, the new section, and then why this is being approved, i.e.:*

*TS section [list the exact section] will be modified. The section currently says:*

*[Quote the old section exactly]*

*The new section will read:*

*[Quote the new section exactly]*

*This change is acceptable because [go into some detail as to why this is an acceptable change].*

*Use for this format should allow the reader to understand exactly what is being changed, and why that change is acceptable. It is not a good practice to just say that the change listed in the LAR is acceptable. This forces the reader to go back to the LAR to see what the changes are.*

3.12 Secure Development and Operational Environment

*Read DI&C-ISG-06 Section D.12 "Secure Development and Operational Environment"*

4.0 NRC FINDINGS

4.1 Summary of Regulatory Compliance

4.2 Limitations and Conditions

*Limitations are defined as the boundaries of what is being approved by the safety evaluation both in the context of the plant specific approval and potential use as a precedent.*

*Any conditions of approval discussed in the safety evaluation should correspond to a license condition to be actual license.*

## 5.0 CONCLUSION

*Read and follow LIC-101 Rev. 3 Attachment 3 Section 6, "Conclusion"*

## 6.0 REFERENCES

*Read and follow LIC-101 Rev. 3 Attachment 3 Section 7, "References"*

**Enclosure E**  
**Proposed Table of Contents for**  
**License Amendment Request (LAR)**

## Proposed Table of Contents for LAR

- 1 Summary Description - *This should provide a high level description of what the system is, and what safety functions it should perform. This should include discussions on the content of the current license condition or technical specification, the proposed change and why the change is being requested, how it relates to plant equipment and/or operation, whether it is a temporary or permanent change, and the effect of the change on the purpose of the technical specification or license condition involved.)*
- 2 No significant hazards consideration determination in accordance with 10 CFR 50.92.
- 3 Licensee's safety analysis/justification for the proposed change (*including the current licensing basis that is pertinent to the change (e.g., codes, standards, regulatory guides, or Standard Review Plan (SRP) sections). The safety analysis that supports the change requested should include technical information in sufficient detail to enable the NRC staff to make an independent assessment regarding the acceptability of the proposal in terms of regulatory requirements and the protection of public health and safety. It should contain a discussion of the analytical methods used, including the key input parameters used in support of the proposed change. The discussion also should state whether the methods are different from those previously used and whether the methods have been previously reviewed and approved by the staff.*)
- 4 Detailed System Description
  - 4.1 System Description (Section D.1 of DI&C-ISG-06)
    - 4.1.1 Processor Subsystem
    - 4.1.2 Safety Function Processor – *The description should include the brand and model of the processor, speed, internal memories, bit width, and bus interface.*
    - 4.1.3 Input/Output (I/O) Modules – *Each I/O module should be described. If the I/O modules contain processors, these should be described in the same manner as the safety function processor.*
    - 4.1.4 Communication Modules or Means - *Each communications module should be described. If the communications modules contain processors, these should be described in the same manner as the safety function processor.*
    - 4.1.5 Voters - *If the voters contain processors, these should be described in the same manner as the safety function processor.*
    - 4.1.6 Manual Channel Trip and Reset
    - 4.1.7 Power Supply – *specifically describe the portion of the system powered by each power supply, any redundancy within the power supplies, and where the power supply itself gets power.*
    - 4.1.8 Test Subsystem – *Specifically discuss the interface between the test system and the safety system. Discuss if and how the safety system will be taken out of service when the test system is attached.*
    - 4.1.9 Other Subsystems
      - 4.1.10 Cabinets, Racks, and mounting hardware
      - 4.1.11 Appendix B Compliance

- 4.1.12 System Response Time
- 4.1.13 Communications
- 4.2 Hardware Development Process (Section D.2 of DI&C-ISG-06)
- 4.3 Software Architecture (Section D.3 of DI&C-ISG-06)  
*The individual software modules for each processor, whether on the main processor, I/O processors, or communications processors should be individually described.*
- 4.4 Software Development Process (Section D.4 of DI&C-ISG-06)
- 4.5 Environmental Equipment Qualification (Section D.5 of DI&C-ISG-06)
- 4.6 Defense-in-depth & Diversity (Section D.6 of DI&C-ISG-06)
- 4.6.1 Diverse Instrumentation & Control Systems (Section D.6 of DI&C-ISG-06)
- 4.7 Communications (Section D.7 of DI&C-ISG-06)  
*This should include a description of how the proposed system complies with DI&C-ISG-04, or reference a stand-alone documents describing the compliance. In any area where the proposed system does not comply with DI&C-ISG-04, the licensee needs to describe in detail why the system still meets regulatory requirements.*
- 4.8 System, Hardware, Software, and Methodology Modifications (Section D.8 of DI&C-ISG-06)
- 4.9 Compliance with IEEE Std 603 (Section D.9 of DI&C-ISG-06)  
*This section should include a detailed explanation of how the equipment, described in detail above, meets each regulatory requirement.*
- 4.10 Conformance with IEEE Std 7-4.3.2 (Section D.10 of DI&C-ISG-06)  
*This section should include a detailed explanation of how the equipment, described in detail above, meets each of these SRP acceptance criteria.*
- 4.11 Technical Specifications (Section D.11 of DI&C-ISG-06)
- 4.12 Secure Development and Operational Environment (Section D.12 of DI&C-ISG-06)
- 5 References



**Enclosure F**  
**Glossary for**  
**License Amendment Request (LAR)**

The only accepted definitions of terms defined in the federal regulations (i.e., 10 CFR) are the definitions in the federal regulations. Any application that includes an attempt to redefine a term defined in the federal regulations should be rejected as soon as the re-definition is found (unless an exemption request is filed under 10 CFR 50.12). NRC guidance documents can only clarify these definitions but cannot change them.

Terms that are defined or used in NRC regulatory guidance documents are assumed to be used in the manner defined or implied in the NRC guidance document, unless a licensee explicitly redefines a term, and explicitly states that the licensee-defined definition supersedes that in the guidance document.

**Applicant:** The author (that does not hold a license) of an application.

**Application (plant specific):** A use to which something is put, for example: a Reactor Trip System (RTP) or an Engineered Safety Features Actuation System (ESFAS).

**Application Framework (e.g., digital I&C platform topical report):** A set of hardware, software, tools, and methodologies used to develop applications.

**Application Software Requirements Specification (plant specific):** Application software criteria are concerned with what the application software must do in the context of the NPP application, and how the software should interact with the remainder of the application. These criteria come from the system criteria, and reflect the criteria placed on the software by the system. In a safety system, this means that the system design must be known and documented, and the demands that the system makes on the computer system must be known.

See SRP Chapter 7 BTP 7-14 Section B.3.3.1

**Application-System Architecture Description:** A description of the manner in which the application components are organized and integrated. These descriptions should include a description of all assemblies (e.g., cabinet, channel, train) and sub-assemblies down to the field replaceable units (e.g., power supply, display, circuit board), the necessary behavior of each, and how they work together to accomplish the various application functions. It is expected that this architecture description include both text and diagrams.

**As-Built:** The state of the system after installation and associated testing.

**As-Manufactured:** The state of the system after successful completion of factory acceptance testing.

**Block Diagram:** A block diagram gives a basic overview of how the main components within a module or assembly interact. Block diagrams describe how a module or assembly functions rather than depicting components.

**Code Listings:** See SRP Chapter 7 BTP 7-14 Section B.3.3.4

**Commercial Grade Dedication Plan:** The safety evaluation of EPRI TR-106439, "Guideline on Evaluation and acceptance of Commercial Grade Equipment for Nuclear Safety Applications," states (Section 5.0, "Conclusion"): "Licensees referencing TR-106439 in...a license amendment...for a proposed digital modification should document the dedication process such that there are descriptions and justifications for the alternatives selected which

should support the use of the commercial product in a safety application.” The commercial grade dedication plan is the documentation of the dedication process.

**Commercial Grade Dedication Report:** A report that documents the acceptable dedication of a commercial grade item. This report should identify the critical characteristics and describe the methods used to determine the acceptability of the commercial grade item.

**Completed Procedures and Reports:** The documentation of the testing.

**Computer:** A system that includes computer hardware, software, firmware, and interfaces.

**Configuration Management Reports:** A report that documents the configuration.

**Configuration Tables:** Real-time systems frequently need tables of information that tailor the system to the operational environment. These tables indicate I/O channel numbers, sensor and actuator connections and names, and other installation-specific quantities. The Installation Configuration Tables describes all the configuration information that must be provided and how the system is to be informed of the configuration information. The actual configuration tables are created as part of the installation activity.

See SRP Chapter 7 BTP 7-14 Section B.3.3.6

**Cyber Security:** Those aspects that are addressed by 10 CFR 73.54 and Regulatory Guide 5.71 (e.g., NSIR review scope).

**Design:** The specification of components, systems, or modules and how they function in order to accomplish a requirement.

A description of the function of a component, system, or module without a description of the implement of the function is not considered to be a description of a design of that item.

**Example (not a design):** The safety system is designed so that once initiated automatically or manual, the intended sequence of protective actions of the execute features continue until completion.

**Design Analysis Reports:** A design analysis report documents the analysis of a design. There may be many types of design analysis reports, for example:

**Communications Analysis Report:** A communications design analysis report provides sufficient detail to support and justify the ability of the digital I&C system limit the effect of communications from one channel from adversely impacting other channels or divisions. This report may include a DI&C-ISG-04 compliance matrix.

**Independence Analysis Report:** An independence design analysis report provides sufficient detail to support and justify independence: (1) between redundant portions of a safety systems, (2) from the effects of design basis events, and (3) from other systems. Some of the supporting analysis is sometimes documented in a Failure Modes and Effects Analysis (FMEA) report; see Section D.9.4.2.1.1.

**Reliability Analysis Report:** A reliability analysis provides sufficient detail to support and justify that the system meets the reliability criteria.

**Design output:** Documents, such as drawings and specifications, that define technical aspects of structures, systems, and components. For software, design outputs include the products of the development process that describe the end product that should be installed in the plant. The design outputs of a software development process include software requirements specifications, software design specifications, hardware and software architecture designs, code listings, system build documents, installation configuration tables, operations manuals, maintenance manuals, and training manuals.

**Detailed System and Hardware Drawings:** The detailed design drawings of the system.

**Deterministic timing:** Timing is deterministic if the time delay between stimulus and response has a guaranteed maximum and minimum.

**Electronic Block Diagram:** An electronic block diagram gives a basic overview of how the main circuits within a device interact. Each block is presumed to represent all the schematic symbols related to that part of the circuit. Block diagrams describe how a circuit functions rather than depicting components.

**Equipment Qualification:** The activities and documentation associated with addressing IEEE Std 603-1991 Clause 5.4, "Equipment Qualification," IEEE 279-1971 Clause 4.4, "Equipment Qualification," or various GDCs associated with equipment qualification.

**Equipment Qualification Testing:** The testing associated with equipment qualification.

**Failure Modes and Effects Analysis (FMEA):** An FMEA is a systematic method of identifying the affects of single failures. Regulatory Guide 1.53 Revision 2, "Application of the Single-Failure Criterion to Safety Systems," endorses IEEE Std 379-2000, "Application of the single-Failure Criterion to Nuclear Power Generating Stations Safety Systems," which states: "A systematic analysis of the design shall be performed to determine whether any violations of the single-failure criterion exist." An FMEA is one way that the staff has accepted of documenting this systematic analysis. The single failure criterion is generally applicable to plant safety systems; therefore, and FMEA is generally not required for a topical report that does not propose an application specific architecture, except to demonstrate that components do not have any undetectable failure modes.

**FMEA:** See Failure Modes and Effects Analysis

**GDC:** General Design Criterion (e.g., 10 CFR 50 Appendix A)

**Hardware Architecture Description:** A description of the manner in which the hardware components of a digital I&C system are organized and integrated. These descriptions should include a description of all assemblies (e.g., Cabinet, Channel, Train) and sub-assemblies down to the field replaceable units (e.g., power supply, display, circuit board), the specified behavior of each, and how they work together to accomplish the various system functions. It is expected that this architecture description include both text and diagrams.

**Hazard:** A condition that is a prerequisite to an accident. (see also Software Hazard)

**Hazard Analysis:** A systematic qualitative or quantitative evaluation of software for undesirable outcomes resulting from the development or operation of a system. These outcomes may include injury, illness, death, mission failure, economic loss, property loss, environmental loss, or adverse social impact. This evaluation may include screening or analysis methods to

categorize, eliminate, reduce, or mitigate hazards. (per IEEE Std 1012-1998 Clause 3.1.7, see also Software Hazard Analysis)

**Individual V&V Problem Reports up to FAT:** It is expected that V&V should identify some problems that must be addressed. The individual V&V problem reports are the documentation of the individual problems and associated resolutions.

**Inspection:** These activities are performed by regional staff (qualified inspectors) in support of the reactor oversight process.

**Interrupt:** Interrupts are changes in the flow of control caused, usually, not by the running program, but by something else. Processor, hardware and software interrupts are invoked differently.

**Asynchronous-Interrupt:** An asynchronous-interrupt is one whose cause is not associated with the currently executing instruction, for example, a hardware-interrupt or process-interrupt.

**Hardware-Interrupt:** Hardware interrupts are invoked by peripheral devices that set the respective interrupt request lines.

**Process-Interrupt:** When the process being controlled changes the flow of control as a direct result of some process state or action, for example, pushing a button results in a routine being initiated. Process interrupts generally result in process dependent CPU loading which may be incompatible with deterministic behavior.

**Processor-Interrupt:** Microprocessor or logical interrupts are invoked by the processor as a result of some unusual program result, such as an attempt to divide by zero.

**Software- Interrupt:** Software interrupts are invoked by an instruction.

**Synchronous-Interrupt:** A synchronous interrupt is one whose cause is associated with the currently executing instruction, for example, a software-interrupt or a Processor-Interrupt.

**Trap:** A trap is a kind of automatic procedure call initiated by some condition caused by the program, usually an important but rarely occurring condition. A good example is numeric overflow. On many computers, if the result of an arithmetic operation exceeds the largest number that can be represented, a trap occurs, meaning that the flow of control is switched to some fixed memory location instead of continuing in sequence. At that fixed location is a branch to a procedure called the trap handler, which performs some appropriate action.

**Layout Diagram:** See "Pictorial Diagram"

**Licensing Audit:** These activities are performed by headquarters staff (qualified technical reviewers) at the appropriate facilities, in support of a License Amendment Request (LAR). A licensing audit is a planned, licensing related activity that includes the examination and evaluation of primarily non-docketed information. LIC-111, "Regulatory Audits," (ADAMS Accession No. ML082900195), provides guidance to staff members who conduct regulatory audits. Digital upgrades generally include a thread audit to conclude that certain implementation activities are in accordance with the high quality development process.

**Licensing Review:** These activities are performed by headquarters staff (qualified technical reviewers) on docketed material, in support of a license amendment request (LAR). SRP Chapter 7 contains the associated evaluation criteria. LIC-101 (Non-Publically Available) provides a basic framework for processing license amendment applications.

**NPP:** Nuclear Power Plant

**Operation Manuals:** The Operations Manual provides all of the information necessary for the correct operation of the safety system. Start-up and shut-down of the computer system should be discussed. All communications between the computer system and the users should be described, including the time sequencing of any extended conversations. All error messages should be listed, together with their meaning and corrective action by the user. The Operations Manual structure is dependent on the actual characteristics of the particular computer system. An operations manual is generally not required for a topical report that does not propose an application specific architecture.

See SRP Chapter 7 BTP 7-14 Section B.3.3.7

**Pictorial Diagram:** An electronic pictorial diagram shows the physical relationships of how the components are arranged (i.e., actual proportional sizes of components).

**Plan:** A plan documents the results of planning. The essence of planning is to think through the consequences of certain activities to ensure that those activities will result in the desired goals. Plans are generally project specific documents that describe how certain activities are to be performed. Each activity is composed of three elements: (1) a condition element, (2) an action element, and (3) a result element.

**Platform Software Requirements Specification (platform specific):** Software criteria are concerned with what the platform software must do in support of the application, and how the platform software should interact with the application.

See SRP Chapter 7 BTP 7-14 Section B.3.3.1

**Precedent:** A precedent is an item that was reviewed and approved by the NRC. Changes made to one plant under 10CFR50.59 are not considered by the NRC to be a precedent for the same plant or any other.

**Quality Assurance Plan for Digital Hardware:** This plan should contain sufficient information for the staff to conclude that the regulatory requirements of: 10CCFR 50.55a(a)(1) and IEEE Std 603-1991 Clause 5.4, Quality," are met. NUREG-0800, Chapter 7, Appendix 7.1-C Section 5.3 contains SRP acceptance criteria for IEEE Std 603-1991 Clause 5.3.

**Qualification Test Methodologies:** The description of the methodologies used in qualification testing; typically this testing would address IEEE Std 603-1991 Clause 5.4, "Equipment Qualification," IEEE 279-1971 Clause 4.4, "Equipment Qualification," or various GDCs associated with equipment qualification.

**Redundant equipment or system:** A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the function, regardless of the state of operation or failure of the other (from IEEE Std 603-1991).

### **Explicit Regulatory Requirement:**

IEEE Std 603-1991

Clause 2.0, "Definitions" states, "**safety group**. A given minimal set of interconnected components, modules and equipment that can accomplish a safety function."

Clause 5.0, "Safety System Criteria" states, "The power, instrumentation, and control portions of each safety system shall be composed of more than one safety group of which any one safety group can accomplish the safety function. (See Appendix A for an illustrative example."

### **Implicit Regulatory Requirement:**

IEEE Std 603-1991

Clause 5.1, "Single-Failure Criterion" states the criteria that a safety system must meet to satisfy the single failure criterion. This criterion is generally satisfied by using redundancy.

General Design Criteria (GDC)

*"Criterion 22--Protection system independence.* The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

**Reference Design, Change Analysis:** A modifications design analysis report provides sufficient detail to support and justify the acceptability of system, hardware, software, and methodology modifications.

**Regulatory Evaluation:** A description of how the system meets regulatory requirements. This description should include the necessary coordination with or reliance on other systems and equipment.

**Reliability Analysis:** A documented analysis that provides sufficient detail to support and justify that the system meets its reliability criteria.

**Requirement:** A statement of what must be done or achieved without a description of how it is done. A requirement may be implemented by several different designs.

Sometimes a document (e.g., IEEE Std 603-1991) contains both descriptive text (e.g., informative text) and requirements (e.g., normative text). The descriptive text is to describe the context of the requirement statement. In these instances a documented convention normally exists to distinguish between normative and informative text (e.g., the IEEE Standards Style Manual dated July 2005 states: "The word *shall* is used to indicate mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted...").

**Example:** IEEE Std 603-1991 Clause 5.2, “Completion of Protective Action” states, “The safety system shall be designed so that once initiated automatically or manual, the intended sequence of protective actions of the execute features shall continue until completion.”

The NRC prefers to use the term “requirement” to refer to requirements in the regulations. The NRC sometimes endorses an industry standard as an acceptable way of meeting regulatory requirements. In casual conversation, many people refer to the normative material of an NRC endorsed standard as “requirements”. This use of the term “requirement” should be replaced with the term “normative material,” “mandatory material,” or some other term to avoid confusion.

**Requirement Traceability Matrix:** The definition of an RTM is contained in The Standard Review Plan, BTP 7-14, Section A.3, definitions, and says: “An RTM shows every [criteria], broken down in to sub-[criteria] as necessary, and what portion of the software requirement, software design description, actual code, and test requirement addresses that system requirement.” This is further clarified in Section B.3.3, “Acceptance Criteria for Design Outputs,” in the subsection on Process Characteristics. This section states that a requirements traceability matrix needs to show every criteria, should be broken down in to sub-criteria as necessary. The RTM should show what portion of the software requirement, software design description, actual code, and test requirement addresses each system criteria.

**Safety Analysis Activities:** See SRP Chapter 7 BTP 7-14 Section B.3.2.1

**Secure Environment:** Certain aspects of reliability and access control that are addressed by the organization responsible for the review of I&C through Regulatory Guide 1.152.

**Software Architecture Descriptions:** A description of the manner in which the software components of a digital I&C system are organized and integrated. These descriptions should include a description of all programs (e.g., operating system, application), the specified behavior of each, and how they work together to accomplish the various system functions. It is expected that this architecture description include both text and diagrams.

See SRP Chapter 7 BTP 7-14 Section B.3.3.2

**Software Code Listings:** Software code can take many forms. Software can be considered to be machine code files (all “1s” and “0s”). Software can be compiled and executed, or interpreted. The listing of each of these forms could be considered to be a “software code listing.” The software code listings that are of regulatory interest are the forms as entered into the computer by a human. Tools are sometimes used to translate the form entered into the computer (by a human) into various intermediate forms before the machine code is produced. Code reviews are generally of the human entered form against the specification for that form (e.g., Software Code Listing vs. Software Design Description) and any associated coding guidelines. Tools that are used to translate or manipulate the human entered form into other forms should be evaluated for suitability for use (e.g., IEEE Std 7-4.3.2-2003 Clause 5.3.2). Scripts that are used during testing are considered to be software tools and should be controlled as software.

See SRP Chapter 7 BTP 7-14 Section B.3.3.4

**Software CM Activities:** See SRP Chapter 7 BTP 7-14 Section B.3.2.3



**Software Configuration Management Plan (SCMP):** Software configuration management (SCM) is the process by which changes to the products of the software development effort are controlled. SCM consists of four major parts: the SCM plan (SCMP), the SCM baseline, the configuration control board and the configuration manager. The configuration baseline identifies the development products (termed configuration items) that should be under configuration control. The configuration control board (CCB) approves all changes to the baseline. The configuration manager makes sure the changes are documented and oversees the process of making changes to the baseline.

Without a SCMP it is difficult or impossible to manage configuration baseline change, or for software developers to know which versions of the various configuration items are current. Software modules that call other modules may be created using an incorrect version of the latter; in the worst case, this might not be discovered until operation under circumstances when correct operation is absolutely necessary to prevent an accident. This can occur if some functions are rarely needed, so are inadequately tested or linked into the software product. It is also possible that several people will have different understandings as to what changes have been approved or implemented, resulting in an incorrect product.

See SRP Chapter 7 BTP 7-14 Section B.3.1.11

**Software Design Description (SDD):** See Software Design Specification

**Software Design Specification (SDS):** See SRP Chapter 7 BTP 7-14 Section B.3.3.3

**Software Development Plan (SDP):** The Software Development Plan (SDP) provides necessary information on the technical aspects of the development project, that are used by the development team in order to carry out the project. Some of the topics that should be discussed in this plan were also listed for the SMP. The SMP document is directed at the project management personnel, so emphasizes the management aspects of the development effort. The SDP emphasizes the technical aspects of the development effort, and is directed at the technical personnel. The SDP should specify the life cycle model that will be used, and the various technical activities that take place during that life cycle. Methods, tools, and techniques that are necessary in order to perform the technical activities should be identified.

Without a development plan, there is likely to be confusion about when the various technical development activities should take place and how they should be connected to other development activities. The probability is high that the different team members will make different assumptions about the life cycle that is being used, about what is needed for each life cycle phase, and about what methods, tools, and techniques are permitted, required, or forbidden. The differences among the members of the project technical team can result in a confused, inconsistent, and incomplete software product whose safety cannot be assured, and may not be determinable.

See SRP Chapter 7 BTP 7-14 Section B.3.1.2

**Software Hazard:** A software condition that is prerequisite to an unplanned event or series of events that result in death, injury, environmental damage, or damage to or loss of equipment or property; this definition was derived from IEEE Std 1228-1998 (R2002).

**Software Hazard Analysis:** eliminates or controls software hazards and hazards related to interfaces between the software and the system (including hardware and human components). It includes analyzing the requirements, design, code, user interfaces and changes.

**Software Installation Plan (SInstP):** Software installation is the process of installing the finished software products in the production environment (e.g., at the NPP). The SInstP should describe the process for installing the software product. For any particular installation, modifications, or additions may be needed to account for local conditions (e.g., fuel cycle). There may be a considerable delay between the time the software product is finished and the time it is delivered to the utility for installation.

Without an Installation Plan, the installation may be performed incorrectly, which may remain undetected until an emergency is encountered. If there is a long delay between the completion of the development and the delivery of the software to the utility, the development people who know how to install the software may no longer be available.

See SRP Chapter 7 BTP 7-14 Section B.3.1.5

**Software Integration Plan (SIntP):** Software integration consists of three major phases: (1) integrating the various software modules together to form single programs, (2) integrating the result of this with the hardware and instrumentation, and (3) testing the resulting integrated product. During the first phase, the various object modules are combined to produce executable programs. These programs are then loaded in the second phase into test systems that are constructed to be as nearly identical as possible to the ultimate target systems, including computers, communications systems and instrumentation. The third phase consists of testing. Multiple levels of integration may be necessary, depending on the complexity of the software system that is being developed. Several integration steps may be needed at some levels.

Without a Software Integration Plan, it is possible that the computer system will lack important elements, or that some integration steps will be omitted.

See SRP Chapter 7 BTP 7-14 Section B.3.1.4

**Software Maintenance Manuals:** See SRP Chapter 7 BTP 7-14 Section B.3.3.8

**Software Maintenance Plan (SMaintP):** Software maintenance is the process of correcting errors in the software product (after the product is licensed). There is a related activity, sometimes termed “enhancement,” which is the process of adding functionality to a software product; that is not considered here. Enhancement of a safety system should repeat all of the development steps. The software maintenance plan describes three primary activities: reporting of errors that were detected during operation, correction of the errors that caused failures, and release of new versions of the software product.

There may be a considerable delay between the completion of the development project and changing the product. An organization other than the development organization, termed the maintenance organization here, may actually do the maintenance. Without a Maintenance Plan, it is not easy to know how the product may be changed, and what processes are needed in order to make changes. Inconsistencies and faults may be inserted into the product during maintenance changes, and this may not become known until the software needs to react to an emergency. In the worst case, maintenance that is carried out in order to improve the reliability of the software product may actually lessen its reliability.

See SRP Chapter 7 BTP 7-14 Section B.3.1.1

**Software Management Plan (SMP):** The software management plan (SMP) is the basic governing document for the development effort. Project oversight, control, reporting, review, and assessment are all carried out within the scope of the SMP. The plan contents can be roughly divided into several categories: introduction and overview, project organization, managerial processes, technical processes, and budgets and schedules.

Without an SMP, the probability is high that some safety concerns will be overlooked at some point in the project development period, that inappropriate assignment of resources will cause safety concerns to be ignored as deadlines approach and funds expire, and that testing will be inadequate. Confusion among project development team members can lead to a confused, complex, inconsistent software product whose safety cannot be assured.

See SRP Chapter 7 BTP 7-14 Section B.3.1.1

**Software Operation Plan (SOP):** The software operations plan provides all of the information necessary for the correct operation of the safety system. Start-up and shut-down of the computer system should be discussed. All communications between the computer system and the user should be described, including the time sequencing of any extended conversations. All error messages should be listed, together with their meaning and corrective action by the user. The Operations Manual structure is dependent on the actual characteristics of the particular computer system.

See SRP Chapter 7 BTP 7-14 Section B.3.1.8

**Software Project Risk Management Program:** See SRP Chapter 7 BTP 7-14

Per Regulatory Guide 1.152 Revision 2, see IEEE-7.4.3.2-2003 Clause 5.3.6, "Software project risk management."

**Software Project Risk Management Report:** See SRP Chapter 7 BTP 7-14

Per Regulatory Guide 1.152 Revision 2, see IEEE-7.4.3.2-2003 Clause 5.3.6, "Software project risk management."

**Software QA Plan (SQAP):** The Software Quality Assurance Plan (SQAP) contains a description of the planned and systematic pattern of all actions necessary to provide adequate confidence that the item or product conforms to established technical criteria. Software quality assurance (SQA) is the portion of general quality assurance that applies to a software product. The SQAP describes how the quality of the software should be assured by the development organization. There should be considerable overlap between the SQAP and the other project plans. The SQAP should generally reference such documents, and limit the discussion in the SQAP itself to matters of particular concern to SQA activities. For example, the section on code control may reference the Software Configuration Management Plan (SCMP), and describe the methods by which the SQA organization should ensure that this plan is followed.

Many aspects of software quality are described in the various software development plans. This includes the Software Configuration Management Plan, the Software Safety Plan, the Software Verification and Validation Plan, and others. Without a single SQAP governing these various individual plans, it is possible that the various individual plans may not be mutually consistent, and that some aspects of software quality that are important to safety may be overlooked.

See SRP Chapter 7 BTP 7-14 Section B.3.1.3

**Software Requirements Specification:** Software requirements are concerned with what the software must do, not how the software should do it (design).

See SRP Chapter 7 BTP 7-14 Section B.3.3.1

**Software Safety Analysis:** See RG 1.173 dated September 1997, Regulatory Position C.3, "Software Safety Analysis"

**Software Safety Hazards Analysis:** See NUREG/CR-6463, "Software Safety Hazards Analysis"

**Software Safety Plan (SSP):** The Software Safety Plan (SSP) is necessary for safety related applications, such as reactor protection systems, to make sure that system safety concerns are properly considered during the software development.

The Software Safety Plan is the basic document used to make sure that system safety concerns are properly considered during the software development. Without a Software Safety Plan (SSP), it will be difficult or impossible to be sure that safety concerns have been sufficiently considered and resolved. Some matters are likely to be resolved by different people in different inconsistent ways. Other matters are likely to be overlooked, perhaps because people may assume that others have accepted those responsibilities.

See SRP Chapter 7 BTP 7-14 Section B.3.1.9

See also NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.1.5 "Software Safety Plan," and Section 4.1.5 "Software Safety Plan."

Per RG 1.173 dated September 1997, Regulatory Position 3.2, the SSP includes a description of how to perform the software safety analysis, which is documented in the Software Safety Analysis.

**Software Test Documentation:** See RG 1.170 and IEEE Std 829-1983

RG 1.170 states:

"IEEE Std 829-1983 does not mandate the use of all of its software test documentation in any given test phase. It directs the user to specify the documents needed for a particular test phase. If a subset of the IEEE Std 829-1983 documentation is chosen for a particular test phase, information necessary to meet regulatory requirements regarding software test documentation must not be omitted. As a minimum, this information includes:

- Qualifications, duties, responsibilities, and skills needed of persons and organizations assigned to testing activities,
- Environmental conditions and special controls, equipment, tools, and instrumentation needed for accomplishing the testing,
- Test instructions and procedures incorporating the criteria and acceptance limits in applicable design documents,
- Test prerequisites and the criteria for meeting them,
- Test items and the approach taken by the testing program,

- Test logs, test data, and test results,
- Acceptance criteria, and
- Test records indicating the identity of the tester, the type of observation, the results and acceptability, and the action taken in connection with any deficiencies.

Any of the above information items that are not present in the subset selected for a particular test phase must be incorporated into the appropriate documentation as an additional item.

**Software Test Plan (STP):** (see also Test Plan) The STP describes how all of the individual testing activities (including unit testing, integration testing, factory acceptance testing, site acceptance testing and installation testing) complement and support each other. The plans for individual testing activities describe the methods used for testing and test case generation. The STP should describe how all of the minimum test program activities (identified in RG 1.170, Regulatory Position 1; and RG 1.171 Regulatory Position 1) are performed and documented. The STP should describe all of the different types of testing documents used, and describe the procedures governing each.

See SRP Chapter 7 BTP 7-14 Section B.3.1.12

**Software Training Manuals:** See SRP Chapter 7 BTP 7-14 Section B.3.3.9

**Software Training Plan:** The software training plan should describe the methods that should be used to train the users of the software system. In this case, users should be trained in use of the safety system software. It is also possible that training should be specified for managers and for maintenance personnel. The actual training criteria depend to a great extent on the actual software product, development organization, maintenance organization, and customer (utility).

See SRP Chapter 7 BTP 7-14 Section B.3.1.7

**Software V&V Activities:** See SRP Chapter 7 BTP 7-14 Section B.3.2.2

**Software V&V Plan (SVVP):** Verification is the process that examines the products of each life cycle phase for compliance with the criteria and products of the previous phase. Validation is the process that compares the software product with the original system requirements and established standards to be sure that the customer's expectations are met. The combination of verification and validation (V&V) processes generally includes both inspections and tests of intermediate and products of the development effort. The SVVP is the plan for these activities.

Without a Software V&V Plan, it will be difficult or impossible to be sure that the products of each phase of the software life cycle have been adequately verified, and that the software system is a correct implementation of the criteria imposed upon it by the original system specifications.

See SRP Chapter 7 BTP 7-14 Section B.3.1.10

**System Build Documents:** A System Build Specification describes precisely how the system is assembled, including hardware and software component names and versions, the location of particular software components in particular hardware components, the method by which the

hardware components are connected together and to the sensors, actuators, and terminals, and the assignment of logical paths connecting software modules to hardware communication paths.

See SRP Chapter 7 BTP 7-14 Section B.3.3.5

**System Configuration Documentation:** The documentation that describes the configuration of the system that is to be installed at the NPP (application specific).

**Safety Analysis:** Chapter 7 BTP 7-14 Section B.3.1.9 & B.3.2.1

**Schematic Diagram:** An electronic schematic diagram contains every component that makes up a circuit, via various symbols (i.e., a symbolic representation of a circuit without regard to shape or size).

**Sneak Circuit Analysis:** NUREG-1412, "Foundation for the Adequacy of the Licensing Bases," describes the development and application of sneak circuit analysis in the regulatory review process for instrumentation and control systems. The NRC has accepted sneak circuit analysis as an acceptable way of demonstrating that the regulations have been met, for example in NUREG-0717 Supplement 4, "Safety Evaluation Report related to the operation of Virgil C. Summer Nuclear Station, Unit 1":

"In Supplement No. 3 to the Safety Evaluation Report we stated that the applicant's commitment to perform a sneak circuit analysis on the engineered safety feature load sequencer is acceptable for granting a full power license and that any required modifications to the sequencer resulting from the sneak circuit analysis must be completed prior to startup after the first refueling outage. By letter dated March 25, 1982, the applicant submitted a final report on the sneak circuit analysis of the engineered safety features load sequencer. The staff has reviewed this report which documents the results of the sneak circuit analysis and concludes that the engineered safety features load sequencer is free of sneak circuits. As a result, no hardware modifications are required. The staff concludes that all sneak circuit analysis findings are reported and have been resolved in an acceptable manner, leaving no residual concerns. Therefore, the staff finds this matter resolved."

**System Build Documents:** See SRP Chapter 7 BTP 7-14 Section B.3.3.5

**System Requirements Specification:** The specification of the functions that the system must perform and the associated interfaces.

**Testing Activities:** See SRP Chapter 7 BTP 7-14 Section B.3.2.4

**Test-Case Specification:** Per RG 1.170 see IEEE Std 829-1983 Section 5, "Test-Case Specification": A document Specifying inputs, predicted results, and a set of execution conditions for a test item.

**Test-Design Specification:** Per RG 1.170 see IEEE Std 829-1983 Section 4, "Test-Design Specification": A document Specifying the details of the test approach for a software feature or combination of software features and identifying the associated tests.

**Test-Incident Report:** Per RG 1.170 see IEEE Std 829-1983 Section 9, "Test-Incident Report": A document reporting on any event that occurs during the testing process which needs to be investigated.

**Test-Item Transmittal Report:** Per RG 1.170 see IEEE Std 829-1983 Section 7, “Test-Item Transmittal Report”: A document identifying test items. It contains the current status and location information.

**Test Log:** Per RG 1.170 see IEEE Std 829-1983 Section 8, “Test Log”: A chronological record of the relevant details about the execution of the tests.

**Test Plan:** Per RG 1.170 see IEEE Std 829-1983 Section 3, “Test Plan”: A document describing the scope, approach, resources, and schedule of intended testing activities. It identifies test items, the features to be tested, the testing tasks, who should do each task, and any risks requiring contingency planning.

**Test-Procedure Specification:** Per RG 1.170 see IEEE Std 829-1983 Section 6, “Test-Procedure Specification”: A document specifying a sequence of actions for the execution of a test.

**Test-Summary Report:** Per RG 1.170 see IEEE Std 829-1983 Section 10, “Test-Summary Report”: A document summarizing testing activities and results. It also contains an evaluation of the corresponding test items.

**Theory of Operation Description:** Description of how systems and components work together to accomplish the specified functions.

**V&V Reports:** Reports documenting the V&V activities.

**Vendor Build Documentation:** See SRP Chapter 7 BTP 7-14 Section B.3.3.5