DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-06

Task Working Group #6: Licensing Process

Interim Staff Guidance

(Initial Issue for Use)

ISG-6 Draft (44).docx
Total Number of Pages: 134

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) provides the licensing process to be used in the review of license amendment requests associated with digital I&C (I&C) system modifications in operating plants. 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 how a licensee or applicant may efficiently request NRC approval to install a digital I&C system upgrade.

This ISG covers the entire life cycle for the review process including activities prior to submittal of the license amendment request (LAR). Except in those cases in which a licensee or applicant proposes or has previously established an acceptable alternative approach for complying with specified portions of NRC regulations, the NRC staff will use the process described in this ISG to evaluate compliance with NRC requirements.

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. This ISG also informs licensees of the information the NRC staff will need for its review of digital I&C equipment and when the information should be provided. Review of this documentation should allow licensees to prepare digital I&C upgrade applications that are complete with respect to the areas that are within the I&C scope of review.

Use of this ISG is designed to be complementary to the NRC's longstanding topical report review and approval process. Where a licensee references an NRC-approved topical report, the NRC staff will be able to, where appropriate, limit its review to confirming 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 licensing process for operating reactors.

The NRC staff will review proposed digital I&C equipment to ensure that there is reasonable assurance that the equipment will perform the required functions; this review will use the guidance in the Standard Review Plan (NUREG-0800), 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.

Comment [A1]: Comment No. 7.

B.1 Background

The NRC oversight includes different types of activities performed by the NRC staff in the oversight of design, construction and operation of a nuclear power plant (NPP). The determination of which type of activity is most appropriate is based on certain aspects:

(1) Inspections[1] are most appropriate where characteristics can be objectively verified.

(2) Reviews are most appropriate where an evaluation (requiring specific technical expertise) is required.

The SRP (NUREG-0800 Chapter 7) has been established to guide NRC staff in performing reviews of digital safety systems (DSS). The NRC staff does not perform an independent design review of the DSS. Instead, the staff reviews the design process and design outputs to determine 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") to verify 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 design process to produce acceptable systems and software. Therefore, a major 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 will sample the design process 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. For this reason, the DSS design must be complete and the system tested to demonstrate that it will perform its safety function.

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 21.2:

> "*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.

Comment [A2]: Comment No. 8.

Comment [A3]: Comment No. 9.

Comment [A4]: Comment No. 10.

Comment [A5]: Comment No. 11.

Comment [A6]: Comment No. 12.

[1] The NRC Inspection Manual Chapter 2503 defines inspections as: "An NRC activity consisting of examination, observation or measurements to determine applicant/contractor conformance with requirements and/or standards."

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, will provide reasonable assurance that 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 determined 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 (SE) 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."

Comment [A7]: Comment No. 13.

B.1.2 Documentation Reviewed

Comment [A8]: This section was added to the draft that was made available to the public in the March 24, 2010, ISG6 meeting announcement (ML093491083).

Comment Nos. 4 & 34.

Comment [A9]: Each instance of the use of the word "procedure" was carefully reviewed to ensure it is consistent with NRC practices.

The organization responsible for the review of I&C, generally does not review procedures; however, the organization responsible for the review of I&C must 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 will request and review those procedures. As a general rule, the organization responsible for the review of I&C reviews only the information required to make an evaluation against the review criteria in the SRP; the organization responsible for the review of I&C will require that information to be docketed. If the information required is contained in proprietary or larger documents, then the organization responsible for the review of I&C will 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 design process; an applicant is allowed to determine their own design process (e.g., per RG 1.73 and IEEE Std 1074). However, this ISG makes certain assumptions (consistent with 10 CFR 50 Appendix B), about that design process. For example, if there exists a regulatory requirement that a safety-system has a certain property (e.g., IEEE 603-1991 Clause 5.1, "Single-Failure Criterion"), then it is assumed that there is a documented design analysis that demonstrates that the safety system meets this regulatory requirement. It is also assumed that the V&V team evaluates this design documentation and documents their evaluation. In order to minimize regulatory burden, 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. A statement made under oath and affirmation that the regulatory

requirement is met is necessary but 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 there is reasonable assurance that 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

Comment [A10]: This section was added to the draft that was made available to the public in the March 24, 2010, ISG6 meeting announcement (ML093491083).

The organization responsible for the review of I&C must review sufficient information to make an evaluation that the equipment will perform the required safety functions. The organization responsible for the review of I&C does not, in general, review the adequacy of the required functions.

Licensee's 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).

The organization responsible for review of I&C will coordinate with other NRC technical organizations in the review of the following I&C system design features:

> The adequacy of the monitored variables, for example, the suitability of parameters, such as pressure, for initiating operation of reactor trip or a given ESF or auxiliary supporting features and other auxiliary features included in Chapter 15 of the SAR.
>
> The acceptability of the proposed setpoints, time delays, accuracy requirements, and actuated equipment response, and consistency with the safety analysis included in Chapter 15 of the SAR.
>
> The acceptability of the human-machine interface as described in Chapter 18 of the SAR.

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 confirms that they are consistent with the accident analysis, the operating requirements 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 requirements for the auxiliary supporting features and other auxiliary features to assure that they satisfy the applicable acceptance criteria. These features include, for

example, compressed (instrument) air, cooling water, boration, lighting, heating, and air conditioning. This review confirms that (1) the design of the auxiliary supporting features and other auxiliary features is compatible with the single-failure requirements of the I&C systems, and (2) the auxiliary supporting features and other auxiliary features will maintain the required 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 confirms that they are consistent with the operating requirements 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 required 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 confirms they are consistent with the accident analysis, operating requirements, 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) confirms 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 ~~and procedures~~ 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 ~~and procedures~~.

The organization responsible for the review of human-machine interface evaluates the adequacy of the arrangement and location of instrumentation and controls, and confirms 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 confirm that 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

Comment [A11]: This section was added to the draft that was made available to the public in the March 24, 2010, ISG6 meeting announcement (ML093491083).

NUREG-1412 (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 603-1991, "," 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 …"

Therefore, 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, Each has its own Perspective

Comment [A12]: This section was added to the draft that was made available to the public in the March 24, 2010, ISG6 meeting announcement (ML093491083).

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. 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 or confirmed by the V&V team).

Chapter 7 of the SRP includes pointers to the various guidance documents and allows the applicant the design freedom to develop a set of development processes. The result being that an applicant should understand SRP Chapter 7 and all associated guidance in order to address any particular topical area. Industry has requested that this ISG integrate into one place all of the associated guidance associated with particular topical areas; however, without making this guidance document significantly thicker it is not possible for this guidance document to replace SRP Chapter 7 and all associated 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 1012-1998, "IEEE Standard for Software Verification and Validation," subject to exceptions listed in the Regulatory Positions in the RG. IEEE 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 7-4.3.2 Sections 5.3.3 and 5.3.4 contain normative clauses 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 282 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 282 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 7-4.3.2 Sections 5.3.5 contains normative clauses 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 1012-1998, “IEEE Standard for Software Verification and Validation,” subject to exceptions listed in the Regulatory Positions in the RG. IEEE 1012 contains normative clauses regarding a Installation Configuration Audit and Change Assessment.

C. DIGITAL I&C REVIEW PROCESS

The Standard Review Plan (SRP) provides guidance to US Nuclear Regulatory Commission (NRC) staff in performing safety reviews of construction permit (CP) or operating license (OL) applications (including requests for amendments) under 10 CFR Part 50. The SRP sometimes references standards as sources of information for NRC staff. As such, a regulatory guide is not required for the staff to refer to the standards provided in the SRP. The caveat is that, since the standards have not been endorsed, the standards normative material does not provide a method acceptable to the NRC for meeting NRC regulations. However, the information is suitable for guiding a review.

Comment [A13]: Comment No. 14.

Comment [A14]: Comment No. 152.

The principal purpose of the SRP is to assure the quality and uniformity of staff reviews. It is also 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 Office of Nuclear Reactor Regulation (NRR) in performing reviews of requests for amendments to operating licenses. Specifically, Enclosure B identifies the documents and information to be submitted in

a typical License Amendment Request (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 the need to issue 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.

Comment [A15]: Comment No. 17.

The staff's acceptance of software for safety system functions is based upon (1) confirmation that acceptable plans were prepared to control software development activities, (2) evidence that the plans were followed in an acceptable software life cycle, and (3) evidence that the process produced acceptable design outputs. 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 is organized in the same manner as BTP 7-14, that the major and minor sub-sections below are the same as in BTP 7-14. In some cases, the staff does not review docketed material, but rather performs audits or inspections of the associated documentation. The subsections below clearly indicate they type (e.g., licensing review, licensing audit, & regional inspection) and timing (e.g., Phase 1, 2, & 3 – See Enclosure C) of regulatroy oversight activities.

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 provides a basic framework for processing license amendment (and other licensing actions, where applicable) applications.

Licensing Audit: These activities are performed by headquarters staff (qualified technical reviewers) at the applicant or vendors 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," provides guidance to staff members who conduct regulatory audits. Digital upgrades generally include a thread audit to verify that the implementation activities are in accordance with the high quality design process.

Regional Inspection: These activities a performed by regional staff (qualified inspectors) in support of the reactor oversight process.

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 design 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 design scope and development. 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 demonstrate the systems compliance with the 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 process is included in Enclosure C and the various 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 systems. Therefore, the NRC staff will consider applications to be within one of three tiers of review.

Tier one is applicable to license amendments proposing to reference a previously approved topical report completely within the envelope of its generic approval as described in the topical report. A tier one review would be able to rely heavily upon the previous review efforts, with large parts of the review being confirmatory. The list of documents that would typically need to be submitted by the licensee in support of a tier one review is contained in Enclosure B, column 1. This list would not include those documents already reviewed and approved by the NRC staff. Tier one generally address: (1) Application Specific Action Items (ASAI) identified in the safety evaluation of the digital I&C platform, (2) post-SE regulatory changes, (3) post-SE regulatory guidance changes (e.g., DI&C-ISG-04), and (4) evaluation of the equipment for performing application or plant specific requirements.

Comment [A16]: Comment No. 6.

Tier two is applicable to license amendments proposing to reference a previously approved topical report with deviations to suit the plant-specific situation. Deviations could include, for example, a revised software development process or new hardware. The aspects of a tier two review that are within the envelope of the generic approval would be confirmatory, while the deviations should be expected to require a more significant review effort. Typically, an application citing licensing experience from another plant's previous approval would be considered a tier two review. This, however, is dependent upon the similarities of the application. The list of documents that would typically need to be submitted by the licensee in support of a typical tier two review is contained in Enclosure B, column 2, however for any particular submittal, the actual list of documents needed will be determined by the changes from the previously approved topical report as determined in the Phase 0 meetings. Tier two evaluations generally include Tier 1 review scope and any deviations from the approved SE or Topical Report.

Comment [A17]: Comment No. 18.

Comment [A18]: Comment No. 6.

Tier three is applicable to license amendments proposing to use a completely new system with no generic approval. Licensees should expect that a tier three review will require a significant review effort within all review areas. The list of documents, that would typically need to be submitted by the licensee in support of a tier three review, is contained in Enclosure B, column 3. Tier three evaluations generally include Tier 1 review scope and Topical Report review scope.

Comment [A19]: Comment No. 6.

Enclosure B is only an example list of "information to be provided" which has been explained throughout this ISG and is needed to review a DSS. An applicant 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 will obviate the need for 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 which fosters better tracking of outstanding information needs and communication of those needs to the licensee. Additionally, this method supports knowledge transfer by allowing new reviewers to better

conceptualize what needs to be reviewed versus a single large list of requirements. 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 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 requirements and policy with regard to key issues such as defense-in-depth and diversity. 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 will address defense-in-depth and diversity, significant variances from current guidance, and 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, these discussions should include whether the system will have built-in diversity for all applicable events or whether the licensee will rely on diverse manual actions or diverse actuation systems. 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. If able, licensees should be encouraged to discuss topics from other review areas as well as how any best-estimate evaluations utilize realistic assumptions and 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 an applicant in honoring these commitments can result in an application being denied (see 10 CFR 2.108, "Denial of application for failure to supply information") or delaying the final evaluation completion date.

The NRC is currently considering development of office level procedures for the use of data portals (e.g., electronic reading rooms) to verify information within various documents referenced by the submittal and to determine if the documentation (or some portion thereof) should be submitted on the docket. When this procedure is available, it is expected that its use will enhance the efficiency of digital I&C reviews as well.

Following each meeting the NRC staff will capture the topics discussed via a meeting summary. This summary will 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 will include a preliminary assessment of which review tier would be applicable for the proposed upgrade. The licensee will 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 acceptance criteria, including defense-in-depth and diversity, variances to existing guidance, and any unique or

complex design features, it should prepare and submit a LAR (e.g., see Enclosure B, table of documents to be submitted with the LAR). It is incumbent upon the licensee to identify any deviations in design and concept that may impact the NRC staff's preliminary assessment made during Phase 0. These changes 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)
- IEEE 603 Compliance (Section D.9)
- IEEE 7-4.3.2 Guidance (Section D.10)
- Technical Specifications (Section D.11)
- Secure Development and Operational Environment (Section D.12)

Initially, the NRC staff will review the application in accordance with the NRR Office Instruction, LIC-109, "Acceptance Review Procedures," to determine if the application is sufficient for NRC staff review. 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 will rigorously 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 will draft the SE and issue requests for additional information (RAI) for the information that is necessary to complete the review of the docketed material. These activities will be conducted in accordance with LIC-101, "License Amendment Review Procedures" (Note: This document is not publically available). The NRC staff will 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

Comment [A20]: This section name was changed from that in the draft that was made available to the public in the March 24, 2010, ISG6 meeting announcement (ML093491083). This change has been made throughout.

Comment [A21]: This section name was changed from that in the draft that was made available to the public in the March 24, 2010, ISG6 meeting announcement (ML093491083). This change has been made throughout.

Comment [A22]: This section name was changed from that in the draft that was made available to the public in the March 24, 2010, ISG6 meeting announcement (ML093491083). This change has been made throughout.

Comment [A23]: This section name was changed from that in the draft that was made available to the public in the March 24, 2010, ISG6 meeting announcement (ML093491083). This change has been made throughout.

Basically qualifications are performed in two steps: (1) Equipment is qualified to some envelope, and (2) The equipment qualification is determined to be adequate for a particular application. Section D.5 was adapted to address the qualification of equipment, and Section D.9.4.2.4 addresses the suitability of equipment for an application.

Comment [A24]: This section name was changed from that in the draft that was made available to the public in the March 24, 2010, ISG6 meeting announcement (ML093491083). This change has been made throughout.

Comment [A25]: Comment No. 2.

the Phase 1 RAI response, the licensee should not delay submission of the Phase 2 information. It is important to maintain close communications with 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 needs may be best met by documentation available at licensee's facility (e.g., Enclosure B, table of documents to be available for audit 12 months prior requested approval date). Those information needs to be resolved in this manner should be documented and the Project Manager, in consultation with the licensee and technical staff, should schedule the audit. While the documentation needs discussed in Section D.1 through D.12 indicate which process will likely be used (i.e., RAI or Audit), individual circumstances will dictate the appropriate vehicle for the NRC staff to obtain needed information.

Comment [A26]: Comment No. 19.

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., containing proprietary information does not make an entire document proprietary).

It is recognized that it is a burden to licensees and vendors to maintain proprietary and non-proprietary versions of DSS documents; therefore, the staff will make every effort to minimize the use of proprietary information in safety evaluations. Conversely licensees and vendors are encouraged to exercise discipline in marking documents as proprietary.

Comment [A27]: Comment No. 20.

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 will 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 will conduct an audit in accordance with LIC-111, “Regulatory Audits” (Note: This document is not publically available).

Any audits will likely 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 requires that the LAR and supplements to 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.

Comment [A28]: Wording inside parentheses removed per Comment No. 22.

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 at early as

possible, it is acceptable to submit the results as mutually agreed in the Phase 0 meetings, but prior to the SE.

Comment [A29]: Editorial changes. No changed identified in Comment no. 23.

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

Phase 2 will conclude with the issuance of a safety evaluation (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 associated amendment.

C.5 Implementation and Inspection (Phase 3)

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

Comment [A30]: Comment No. 24.

The startup testing is conducted in accordance with the plan submitted during Phase 2. The 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."

D. Review Areas

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. 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

Comment [A31]: Comment Nos. 25, 26, & 27 addressed this section.

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

Comment [A32]: Many blocks like this were added because the 'Information to be provided" sections did not in general describe whether the information would be reviewed, audited, or inspected. The only place that contained this information was Enclosure B.

This block of information also addresses Comment No. 34.

Basically there are three types of NRC staff activities: Review, Audit, and inspect. And three different phases in which these activities occur: Phase 1, 2, & 3.

The licensee's submittal should provide sufficient documentation and description to allow the NRC staff to identify what hardware is being used, how the hardware items function, how the various hardware items are interconnected, and any software which runs on that hardware. The digital hardware items should be identified to the revision level. In those cases where the hardware 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. LIC-101 Revision 3, "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." As stated previously, electronic access

Comment [A33]: Comment No 25.

portals may be used for the staff to evaluate these changes and request information for significant changes to be docketed.

Comment [A34]: Inserted text to address Comment No. 26, 126.

The documentation and description should be on two levels. First, the individual channels or divisions should be described, along with 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 any 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 any data communication pathways will be reviewed in detail by Section D.7, "Communications."

D.1.3 Regulatory Evaluation

Comment [A35]: No change to this section as a result of Comment No. 28.

The licensee's description of the system will 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.

The ~~acceptance criteria~~ regulatory guidance applicable to ~~for the~~ architectural descriptions ~~are~~ is contained in the Standard Review Plan, BTP 7-14 Section B.3.3.2, "Design Activities - Software Architecture Description." This section states that the Architecture Description should support the understanding of all of the functional and performance ~~and development process~~ characteristics ~~listed~~credited, and that NUREG/CR-6101, Section 3.3.1 "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance.

Comment [A36]: Words added to address section heading.

D.1.4 Technical Evaluation

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

D.1.5 Conclusion

The NRC staff will need to find that the information provides a comprehensive explanation of the system. From this the NRC staff will determine the scope of review, confirm portion of the system already approved by previous licensing actions, and identify any other constraints on the approval of the system.~~The NRC staff will use the RAI process to fulfill informational needs related to understanding the hardware architecture of the digital I&C 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 high quality 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 design process and the quality control methods used during that design process. This documentation should cover both the design 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 design 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 an existing system 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.

For LARs that include safety-related components, the review by the technical review branch responsible for I&C is predicated on the application being by an Appendix B compliant organization; therefore, the hardware should be developed in accordance with the associated programmatic documentation. This information would typically be in the 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 ~~software~~ hardware design process:

10 CFR, Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."

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 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…"

Comment [A37]: No change as a result of Comment No. 30.

Comment [A38]: This block of information addresses Comment No. 29.

Comment [A39]: Words added to address section heading.

D.2.4 Technical Evaluation

Comment [A40]: No change as a result of Comment No. 31.

The NRC staff will provide a description of the design process and the quality control which governed that design process. This description will cover both design 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 will be contained in a publically available safety evaluation, portions of the licensee's description will need to be non-proprietary.

D.2.5 Conclusion

The NRC staff will need to find that the information provides a comprehensive explanation of the hardware development process. From this the NRC staff will determine the scope of review, confirm portion of the system already approved by previous licensing actions, and identify any other constraints on the approval of the system.~~The NRC staff will use the RAI process to fulfill informational needs related to understanding the hardware design process and quality control of the digital I&C 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 design function. Evaluation of the system at a high-level provides a solid foundation for the subsequent detailed reviews and evaluation against the acceptance criteria. The architecture of the platform software (i.e., application independent software) should also be described.

Some digital technologies, such as a field-programmable gate array (FPGA), do not utilize software while the system is in operation (BTP 7-14 will 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 will 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 must 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).

Please see also NUREG/CR-7006, "Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems."

Comment [A41]: Words added per comment No. 32.

D.3.2 Information to be Provided

Comment [A42]: No change as a result of Comment No. 33.

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

The licensee's submittal should provide sufficient documentation and description to allow the NRC staff to identify what software is being 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 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.

Similar to the information provided for Section D.1, "System Architecture," the documentation and description should be on two levels. First, the individual software operating within individual channels or divisions should be described, along with 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, communications with workstations or non-safety systems. The description of any data communication pathways will be reviewed in detail by Section D.7, "Communications."

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

Comment [A43]: Wording from Version 33 was added back.

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

D.3.3 Regulatory Evaluation

These descriptions will allow the NRC staff to conceptualize and adequately document the software used in this safety-related application and to understand the functional interactions within the system. This will subsequently be used in support of addressing the criteria of subsequent sections.~~The licensee's description of the software architecture will be documented in the NRC staff's SE to explain system operation and to support the technical evaluations of other sections.~~

Comment [A44]: Went back to wording of version 33.

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, 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).

Comment [A45]: Words added to address section heading.

D.3.4 Technical Evaluation

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

D.3.5 Conclusion

The NRC staff will need to find that the information provides a comprehensive explanation of the software architecture. From this the NRC staff will determine the scope of review, confirm portion of the system already approved by previous licensing actions, and identify any other

constraints on the approval of the system.~~The NRC staff will use the RAI process to fulfill informational needs related to understanding the software architecture of the digital I&C system.~~

D.4 Software Development Processes

There may be several development processes to consider (e.g., platform vendor, application vendor, 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 will have its own software configuration management processes. However, not all twelve plans identified in BTP 7-14 need to be docketed from each entity. In some cases an applicant 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 will generally contain application specific action items to address project specific aspects.

Comment [A46]: Comment Nos. 35 & 51.

D.4.1 Scope of Review

The software design 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 development project demonstrate that high quality programming will be the result of a deliberate, careful and high quality development process. The NRC staff review of the design process should confirm, by evaluation against applicable standards and criteria that the licensee and vendor plans and software development activities are sufficiently robust to accomplish this goal.

Parallel to the design process, a verification and validation program is implemented to monitor, evaluate, and document the design process. Verification is defined as the process of determining whether the products of a given phase of the development cycle fulfill the requirements 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 requirements. Combined, verification and validation is the process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill (i.e., implements) the requirements to meet the criteria imposed by the previous phase, and the final system or component complies with specified requirements. This determination may include analysis, evaluation, review, inspection, assessment, and testing of products and processes.

Additionally, within the software development process review area, the NRC staff reviews the failure modes and effects analysis (FMEA). The FMEA is a method of analysis of potential hardware failure modes or programming errors 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.

Comment [A47]: “failure modes” changed to “errors” in accordance with Comment No 5.

Per comment No. 5: "failures" replaced by "errors" were appropriate.

D.4.2 Information to be Provided

The licensee’s submittal should provide sufficient documentation to support and justify the robustness of the software life-cycle associated with the digital I&C system. The documentation should provide sufficient justification to allow the conclusion that the plan meets 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 design process:

10 CFR, Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.”

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 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, “Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants,” Revision 1.

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

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. These products, when found to be acceptable, provide the reviewer with additional criteria for reviewing the processes 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 requirements are applied to both licensee and vendor programs.

The purpose of the NRC staff review of the SMP is to verify that the management aspects of the software development project are such that high quality software will result. 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 done 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 will be evaluated by the licensee is critical. It is important that licensee oversight of the vendors software development program exists and is effective. Software or system vendors may not be familiar with nuclear requirements or with specific plant requirements, 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, what checks and audits the licensee will perform, and the standard by which the success of the audit will 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 should be described in terms of technical, managerial, schedule, and financial aspects. If these independence aspects are described in the planning documents of

Comment [A48]: The sub-section numbering was changed to more closely parallel BTP 7-14 and the SE for the Oconee RPS/ESPS LAR.

Comment [A49]: This sub-section heading was added.

Comment [A50]: These two characters were added to the section numbers of the following 12 sections.

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.

Comment [A51]: Comment Nos. 38, 41, 48, 50, 64.

The NRC staff may review the responsibilities of each position of the project's management and technical teams. The review will verify (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 environment (see Section D.12) for the reviewer to determine that the methods used are consistent with Regulatory Guide 1.152 (See also RG 1.152 Draft Rev. 3 – DG 1249, ML100490539) and that the methods are used effectively. This needs to be an actual description of the secure environment described in RG 1.152, and not just a statement that all secure environment requirements will be met. The review of how those requirements are being met will be addressed in separate NRC guidance on this issue, as indicated in Section D.12.

Comment [A52]: Comment No. 37.

Comment [A53]: Comment No. 40.

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 design effort. This will require some judgment, and it may require 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 design 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 determine that use of the SDP results in a careful and deliberate process which will result in high quality software, suitable for use in safety-related systems in nuclear power plants. The details on how this will be done may be found in other plans, such as the Software Verification and Validation Plan (SVVP), 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 determine that the software development plan allows the licensee

Comment [A54]: Comment No. 42.

or vendor to adequately monitor the software development process, and that any deviations from the software development process will 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 addressed. The reviewer will need to determine 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 will 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.

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, compliers, assemblers, or testers, etc., will be 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 will be detected by V&V activities. If this is not possible, the tool itself should be designed as safety-related.

Comment [A55]: Comment No. 46.

The SDP should list the international, national, industry, and company standards and guidelines, including regulatory guides, which will be followed, and whether or not these standards and guidelines have previously been approved by the NRC staff. If the standards have not been reviewed and approved, the staff will need to do so to ensure that adherence to the standard will result in meeting NRC 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." Any deviations from NUREG/CR-6463 should be identified in the LAR; all significant deviations should be explained.

Comment [A56]: Comment No. 43.

Comment [A57]: Comment No. 47.

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, and the Software Quality Assurance Plan 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 programming processes, and identify particular methods chosen to implement QA procedural requirements. There are several Regulatory Guides and Standards that offer guidance.

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 7-4.3.2, "Software Development," provides guidance.

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, 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 which will be reviewed by the staff. The staff reviewer will need to determine not only that the SQAP exhibits the appropriate management, implementation and resource characteristics discussed above, but also that following the SQAP will result in high quality software that will perform the intended safety function. The NRC staff will sample the design process and products to evaluate the effectiveness of the licensee or vendor QA and V&V efforts, and to determine that 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.

Comment [A58]: Comment No. 49.

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): Final 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 Requirements and the Software Detailed Design should be analyzed to determine 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 needed to perform the software (code) integrations. The planning shall include developing schedules, estimating resources, identifying special resources, staffing, and establishing exit or acceptance criteria.

The 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 final phase consists of testing the results. Multiple levels of integration may be necessary, depending on the complexity of the software system that is being developed. Several integration steps may be required at some levels. Without a Software Integration Plan, it is possible that the complete computer system will lack important elements, or that some integration steps will be omitted.

While the Software Integration Plan is not as critical as some of the other plans, the staff may still review or audit it to determine 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 determine 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 determine 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 will be used to accomplish the integration function. The plan should require 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)

Comment [A59]: The text of this section was reduced since this document will not be reviewed.

Comment No. 53. This comment was made irrelevant since text was removed.

Inspect (Phase 3): Software Installation Plan

The Software Installation Plan will not be reviewed in the staff SE. Application installation is not a part of the licensing process, and therefore may be inspected by the regional inspectors. 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)

Comment [A60]: The text of this section was reduced since this document will not be reviewed.

Comment No. 54, 57, 58. These comments were made irrelevant since text was removed.

Inspect (Phase 3): Software Maintenance Plan

The Software Maintenance Plan will not be reviewed in the staff SE. Licensee maintenance are not a part of the licensing process, and therefore may be inspected by the regional inspectors. 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 will 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 will not be reviewed in the staff SE. Licensee operations are not a part of the licensing process, and therefore may be inspected by the regional inspectors. 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." ~~and Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities."~~ These sections state 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, 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 ~~NUREG/CR-6430, "Software Safety Hazard Analysis," and~~ 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 company organizations. It should show how the software safety activities are integrated 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 determine the success or failure of the software safety effort and analyze its effectiveness.

A critical characteristic of the Software Safety Plan is its completeness. The plan needs to show how the licensee will 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 addresses, either approach is acceptable, however if the

Comment [A61]: The text of this section was reduced since this document will not be reviewed.

Comment [A62]: Comment No. 59.

Comment [A63]: The text of this section was reduced since this document will not be reviewed.

Comment No. 61, 62, 63. These comments were made irrelevant since text was removed.

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 determine the acceptability of the system, and the software safety plan should define that group. The safety organization should consider the secure environment risk as well as the risk to the plant if the digital system malfunctions. Since the NRC staff will assess whether the proper risks were considered, 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, "Verification, Validation, Reviews, And Audits for Digital Computer Software Used in Safety Systems Of Nuclear Power Plants," 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 in these Regulatory Positions. This section also 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, Section 3.1.4 and 4.1.4.

Comment [A64]: Comment No. 69.

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

Comment [A65]: Comment No. 66.

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 needs to demonstrate a V&V effort that is sufficiently disciplined and rigorous to provide a high quality software development process. The V&V plan needs to demonstrate to the staff that the V&V effort will identify and solve the problems which could detract from a high quality design effort. The NRC staff will 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 will report to a high enough level of management within the company to ensure that deficiencies discovered by the V&V organization will be

Comment [A66]: Comment No 67.

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.

Comment [A67]: Comment No. 68.

A second important issue is the number and quality of the V&V personnel. There is no specific requirement for the number of V&V personnel, but generally, equal effort is required 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 will fall behind, or the V&V effort will not be able to perform all the items required. The plan should illustrate how the vendor or licensee management will determine 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 final 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 requirements for discrepancy fixes, including the verification that the regression testing used was adequate.

The Software Verification & Validation Plan should describe reporting requirements. It should require 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 requirements, 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 needs to document how the requirements of IEEE 1012 will be meet, and for any IEEE 1012 requirement which is not being meet, 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)

Comment [A68]: Comment Nos. 70, 71, & 72.

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." NUREG/CR-6101, 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 needs to include an overview description of the development project and identify the configuration items that are governed by the plan. The plan will 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 will control 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 require 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 requirements, designs, or code 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 final product if a wrong version is used during the software development process.

The Software Configuration Management Plan may be two different plans, one used by the software vendor during the development of the software, and one used by the licensee during the operational phase of the project. 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 plant specific SCMP will not be reviewed and approved with the LAR, but may be subject to regional inspection of the system.

Comment [A69]: Comment No. 72.

Comment [A70]: Comment No. 71.

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 requirements.

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 require the full set of tests be run after any modification to the software.

It should also be noted that a significant portion of the testing is considered a part of the V&V activities. Section 5.4.5 of IEEE 1012, the IEEE Standard for Software Verification and Validation, endorsed by RG 1.168, discusses V&V test. This section states, "the V&V effort shall 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 requirements." 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 will specifically be reviewing the test plan to ensure that the required V&V test is actually generated and performed by the V&V group, and not done by a design or test group, and merely checked by V&V personnel.

Comment [A71]: Comment No. 73.

D.4.4.2 Software Implementation Documentation

Comment [A72]: This sub-section heading was added.

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 confirms that 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 Safety Analysis

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 describes the safety analysis 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 out in their entirety. ~~The SSP describes the safety analysis (SA) implementation tasks.~~ 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 requirements have been adequately addressed for each activity group; that no new hazards have been introduced; that the software requirements, design elements, and code elements that can affect safety have been identified; and that all other software requirements, design, and code elements will not adversely affect safety.

Regulatory Guide 1.168, "Verification, Validation, Reviews, And Audits for Digital Computer Software Used in Safety Systems Of Nuclear Power Plants," 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 in these Regulatory Positions. IEEE 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 requirements. 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 shall be documented in the organizational responsibility section of the SVVP."

~~The safety analysis activities also includes the secure environment risk, and the methods used to ensure that the processes used ensure that the design products do not contain undocumented code, malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted or undocumented functions or applications.~~

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

D.4.4.2.2 V&V Analysis and Reports

Review (Phase 2): ~~(1)~~ V&V Reports
~~(2) Requirements Traceability Matrix~~

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

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

Comment [A73]: This section number was previously D.4.4.9.1.

Comment [A74]: Moved from Phase 1 to Phase 2 in order to address Industry comments.

Comment [A75]: Comment No. 65.

Comment [A76]: This section was added since there is associated SRP acceptance criteria and this material was reviewed as part of the Oconee RPS/ESPS LAR (See ML100130944 Section 3.2.2.2, "V&V Activity Summary Report Evaluation").

Regulatory Guide 1.168, Revision 1, endorses IEEE Std 1012-1998, "IEEE Standard for Software Versification 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, walkthoughs 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 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 in their entirety. 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, integration, and installation 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 required 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 requirement imposed on the software by the system requirements document and system design documents, and one or more requirements 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 final analysis documentation should permit tracing from the system requirements and design through the software requirements, design, implementation, integration, validation, and installation.

The integration V&V activities should demonstrate that all unit and subsystem tests required by the SVVP were successfully completed. Any anomalies or errors found during the tests should be resolved and documented. Final integration tests should be completed and documented. Reports should be written for each test run. These reports should include any anomalies found and actions recommended. The final 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 required by the SVVP were successfully completed. The testing process should contain one or more tests for each requirement in the SRS, as well as the acceptance criteria for each test. The result of each test should clearly show that the associated requirement has been met. Each test procedure should contain detailed information for the test setup, input data requirements, 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 final 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 requirements 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): ~~(1)~~ Configuration Management Reports
~~(2) Interim, Configuration Tables~~

~~**Inspect (Phase 3):** (1) As-Built System Build Documents~~
~~(2) As-Built, Configuration Tables~~

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.

Software configuration management can be partitioned into two types of activities. Management and control of the software and the associated development environment, as well as document control. 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 will be created and placed under configuration control. If the software and documents are controlled in different systems, then each should be described, as well as their relationship to each other. 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 have been carried out in their entirety.

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.

Comment [A77]: This section was added since there is associated SRP acceptance criteria and this material was reviewed as part of the Oconee RPS/ESPS LAR (See ML100130944 Section 3.2.2.3, "Software Configuration Management Reports (SCMR)").

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 require 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

Comment [A78]: This section was added since there is associated SRP acceptance criteria and this material was reviewed as part of the Oconee RPS/ESPS LAR (See ML100130944 Section 3.2.2.4, "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

Comment [A79]: Test documentation names were changed to address industry comments and to bring the terminology in line with RG 1.170.

SRP Chapter 7 BTP 7-14 Section B.3.4. contains SRP acceptance criteria and references to applicable guidance:

> 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 satisfying computer system qualification testing requirements (See: IEEE Std 7-4.3.2-2003 Clause 5.4.1, "Computer System Testing").
>
> 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 satisfying test documentation requirements.
>
> 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 satisfying software unit testing requirements.

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 finally 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 required by the SVVP were successfully completed;" FAT is one of those activities.

D.4.4.2.5 Requirements Traceability Matrix

Review (Phase 2): Requirements Traceability Matrix

The licensee should ensure that the Requirements Traceability Matrix (RTM) is written such that each requirement and sub-requirement is traceable through the entire design process. The traceability should be possible both forwards and backwards, that is, the staff and the V&V teams should be able to take any requirement, and trace it through the SRS, SDS, the actual code, and test documentation. Tracing backwards, it should be possible to take any portion of code and determine what requirement is responsible for that code. One of the things this will be used for is to determine that there is no unnecessary code contained in the final product. Any application code which is not traceable back to a system or plant requirement is unnecessary, and should be removed.

D.4.4.2.6 Failure Modes and Effects Analysis (FMEA)

Review (Phase 2): FMEA

There is no specific regulatory guidance on the required format, complexity or conclusions concerning the FMEA. Each system must be independently assessed to determine if 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 will be identified, and the effects will be determined. For a complex system, this is expected to be a complex analysis. The key attribute which the staff will be reviewing is completeness, where all failures are identified, and accuracy, where the analysis reaches an understandable reason for what the failure effect is for each failure mode.

D.4.4.3 Software Design Outputs

This subsection describes the criteria to be used to determine 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 is contained in the Standard Review Plan, BTP 7-14, Section B.3.3.1, "Requirements Activities - Software Requirements

Comment [A80]: Section Number was previously D.4.4.18.

Comment [A81]: Comment No. 80, 83, 84 – no change.

Comment [A82]: This item was moved from Phase 1 to Phase 2 in response to industry comments.

Comment [A83]: Comment No, 81, 82.

Comment [A84]: Section number was previously D.4.4.19.

Comment [A85]: Comment No. 85.

Comment [A86]: Comment No. 89.

Comment [A87]: Comment No. 87, 88.

Comment [A88]: Comment No. 86.

Comment [A89]: This sub-section heading was added.

Comment [A90]: Section number was previously D.4.4.13.

Specification." This sections 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. The section also states that additional guidance can be found in NUREG/CR-6101, Section 3.2.1 "Software Requirements Specification," and Section 4.2.1, "Software Requirements Specifications."

The SRS documents the results of all the requirements activities and documents the required aspects of the safety system. It is not appropriate to include planning information (e.g. see Section D.4.4.1) in an SRS.

Comment [N91]: In two recent licensing applications, the vendor relied on programmatic documents and apparently did not produce sufficient project specific planning documentation (in the opinion of the SRS author); the SRSs included planning information.

Errors in requirements or misunderstanding of their intent are a major source of software errors. The SRS should be carefully examined to ensure that each requirement is complete, 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 Requirement Specifications which will require review, one for the platform software and another for the applications software. Each of these will require a separate review and separate discussion in the NRC staff safety evaluation.

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

The NRC staff will not independently review the SRS, but will review the SRS against the acceptance criteria in BTP 7-14 and will sample a limited number of requirements during the thread audit. The NRC staff will expect to find sufficient V&V documentation to show that there was a 100% verification and validation of the software requirements by the V&V organization.

Comment [A92]: Comment No. 75.

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

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

IEEE 603-1991 Clause 5.2, "Completion of Protective Action"
IEEE 603-1991 Clause 5.6, "Independence"
IEEE 603-1991 Clause 5.7, "Capability for Test and Calibration"
IEEE 603-1991 Clause 5.8, "Information Displays"
IEEE 603-1991 Clause 5.10, "Repair"
IEEE 603-1991 Clause 6.5, "Capability for Test and Calibration"
IEEE 603-1991 Clause 7.3, "Completion of Protective Action"

D.4.4.3.2 Software Architecture Description (SAD)

Comment [A93]: Section number was previously D.4.4.14.

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, Section 3.3.1 "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance.

The SAD must 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.

Comment [A94]: Comment No. 76.

D.4.4.3.3 Software Design Specification)

Comment [A95]: Section was previously D.4.4.15.

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

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 code accurately reflects the software requirements, and that NUREG/CR-6101, 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 code accurately reflects the software requirements, and needs to be detailed enough for the V&V team to check the requirements and follow them through the final code. The Software Design Specification needs to be understandable, and contains sufficient information for the staff to make the determinations shown above.

The NRC staff will not independently review the SDS, but will review it using the criteria in BTP 7-14 and will sample a limited number of requirements during the thread audit. The NRC staff will 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.

Comment [A96]: Comment No. 77.

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

IEEE 603-1991 Clause 5.2, "Completion of Protective Action"
IEEE 603-1991 Clause 5.6, "Independence"
IEEE 603-1991 Clause 5.7, "Capability for Test and Calibration"
IEEE 603-1991 Clause 5.8, "Information Displays"
IEEE 603-1991 Clause 5.10, "Repair"
IEEE 603-1991 Clause 6.5, "Capability for Test and Calibration"
IEEE 603-1991 Clause 7.3, "Completion of Protective Action"

D.4.4.3.4 Code Listings

Comment [A97]: Section added to explicitly address BTP 7-14 review criteria.

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)

Comment [A98]: Section number was previously D.4.4.16.

Review (Phase 2) ~~As-Manufactured,~~ System Build Documents

~~**Inspect (Phase 3)** As-Built, 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, Section 3.5.1, "System Build Documents," and Section 4.5.1, "System Build Documents," contain relevant guidance.

The information needed to determine the ~~final~~ system build may be contained in the configuration tables, final 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 upto the completion of factory acceptance testing (and associated analysis activities).

The build documentation is generally needed to verify that the programs actually delivered and installed on the safety system is the programming that underwent the V&V process and was tested. Any future maintenance, modifications or updates will require 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 will not independently review the SBDs, but will review against the acceptance criteria in BTP 7-14 and will sample a limited number of requirements during the thread audit. The NRC staff will, however, expect to find sufficient V&V documentation to show that there was a 100% verification and validation of the software requirements by the V&V organization.

Comment [A99]: Comment No. 78.

D.4.4.3.6 ~~Installation~~ Configuration Tables ~~(ICT)~~

Review (Phase 2) ~~As-Manufactured,~~ Configuration Tables

~~**Audit (Phase 2):** Interim, Configuration Tables~~

~~**Inspect (Phase 3):** As-Built, Configuration Tables~~

The acceptance criteria for the ~~installation~~ configuration tables are contained in the SRP, BTP 7-14, Section B.3.3.6 Installation Activities - Installation Configuration Tables. This section states that in the event that if the programming has options for use, variable setpoints, or other data, or may operate in various methods, the programming needs to be configured for the particular plant requirements. Any item that is changeable should have the intended configuration recorded in the ~~Installation~~ Configuration Tables. The NRC staff will not independently review the ~~ICT~~configuration tables, but will review against the acceptance criteria in BTP 7-14 and will sample a limited number of requirements during the thread audit. The NRC staff will, however, expect to find sufficient V&V documentation to show that there was a 100% verification and validation of the software requirements by the V&V organization.

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

D.4.4.3.7 Operations Manual

Inspect (Phase 3): Operations Manuals

The Operations Manual will not be reviewed in the staff SE. Licensee operations are not a part of the licensing process, and therefore may be inspected by the regional inspectors. 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

See SRP Chapter 7 BTP 7-14 Section B.3.3.8 for SRP acceptance criteria and references to applicable guidance.

D.4.4.3.9 Software Training Manuals

Inspect (Phase 3): Software Training Manuals

See SRP Chapter 7 BTP 7-14 Section B.3.3.9 for SRP acceptance criteria and references to applicable guidance.

Comment [A100]: Section Number was previously D.4.4.17.

Comment [A101]: Comment No. 79.

Comment [A102]: Section number was previously D.4.4.20.

Comment [A103]: Comment No. 90.

Comment [A104]: Section added to explicitly address BTP 7-14 review criteria.

Comment [A105]: Section added to explicitly address BTP 7-14 review criteria.

D.4.5 Conclusion

The NRC staff will need to find that the information describes a well-defined, disciplined process which will produce a high quality product. The NRC staff will also need to find that the V&V process described will provide acceptable analysis, evaluation, review, inspection, assessment, and testing of the products and processes. The NRC staff will review the design process information/documents produced during the development of the DSS. The NRC staff will also perform thread audits of the software under review, with the intent of confirming 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.

Comment [A106]: Comment No. 91.

D.5 Equipment Environmental Qualifications

Comment [A107]: Comment No. 92- no change.

D.5.1 Scope of Review

The NRC staff will review the information provided to verify that the equipment has been demonstrated to be able to operate within the ~~expected~~ 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.

Comment [A108]: Comment No. 93.

D.5.2 Information to be Provided

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

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

Audit (Phase 2): (1) ~~Digital Qualification~~Completed Test Procedures and Reports
(2) Miscellaneous Equipment - Qualification Documentation

Comment [A109]: The change here addresses the fact that the NRC is primarily interested in reviewing the qualification of digital equipment, and that historically the NRC has accepted applicant programs to address the qualification of miscellaneous equipment.

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 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 licensee's submittal should provide sufficient documentation to support the assertion that a proposed digital I&C equipment is qualified to the specified environmental conditions. The results of the qualification testing should be documented in a summary report.~~

Comment [A110]: Changed back to Rev. 33 language.

Comment No. 94, 95, 96, 98.

The equipiment 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, and is not interested in the qualification of all equipment in mild environments. Therefore the terms "digital" and "miscellanious" are used above to distinguish digital equipment from everything else.

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.

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

Comment [A111]: Comment No. 97, 131.

Comment [A112]: Comment No. 97, 131.

Comment [A113]: RG 1.89 is applicable to harsh environments and RG 1.209 is applicable to mild environments. IF equipment is installed in a harsh environment, then RG 1.89 (as augmented and supplemented by RG 1.209) is applicable.

Comment [A114]: Reference to RG 1.209 added in several places per industry comment Nos. 181 & 182.

Comment [A115]: Reference to IEEE 323-2003 added in several places per industry comment Nos. 181 & 182.

Comment [A116]: Comment No. 97, 131.

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 will be located for any event where the equipment is credited for mitigation. Additionally, the applicant or licensee should show why a single failure within the environmental control system, for any area in which safety system equipment is located, will 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 assumed 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 applicant/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.

Comment [A117]: Comment No. 132.

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 may need to 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.

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 must demonstrate through environmental qualification that the I&C systems meet design-basis and performance requirements 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.

Prior to the performance of testing, the system shall be reviewed to identify significant aging mechanisms. An aging mechanism is significant if in the normal or abnormal service environments, cause degradation during the installed life of the system (e.g., aging mechanisms that progressively and appreciably renders the equipment vulnerable to failure). If the system has one or more significant aging mechanisms, preconditioning is required 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.

Comment [A118]: Comment No. 99.

The NRC staff will evaluate the various test plans to ensure that they are rigorous enough to support the conclusion that the environment will not have a negative effect on the ability of the system to perform its safety function in the worst case environment in which it is required to operate. Environmental requirements 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 low design basis earthquake requirement, 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 will be 125° F. The NRC staff will 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

Comment [A119]: Com.ent No. 100 – no change.

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 must be qualified in the most severe environment to which it will 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 must be qualified in the most severe environment to which it will be exposed and is relied upon to perform its safety function.

Comment [A120]: Comment No. 102, 103.

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.

Comment [A121]: Comment No. 101.

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.

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 must be below the thresholds defined in the standard to which the system is qualified.

D.5.4.4 Sprays and Chemicals

Although I&C systems are typically not installed in environments where exposure to sprays (e.g., fire sprinkler systems) and chemicals is possible, the information provided should describe this aspect of the environment.

If the equipment has the potential to be exposed to any sprays or chemicals, the qualification testing shall include this exposure. If there is the potential for exposure to chemicals (e.g., volatile solvents) that can cause corrosion, this exposure 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 shall 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 will review the information provided on the environmental qualification of the system proposed for use, and will compare this to the plant accident analysis environmental conditions in the location where the equipment will be installed. The staff will 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

Comment [A122]: Comment No 104 – no change.

The principle of defense-in-depth may be thought of as requiring a concentric arrangement of protective barriers or means that are sequentially challenged by the failure of a preceding system. 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. Finally, if these three levels fail, the monitoring and indicator echelon is available to allow informed decisions regarding response to the transient.

Diversity, in the context of digital I&C, is a principle of using different parameters, technologies, logic or algorithms, and actuation means to provide a similar function. Diversity complements defense-in-depth by increasing the chances that a particular echelon will function appropriately. The diversity of a system can be subdivided into six areas: human diversity, design diversity (hardware), software diversity, functional diversity, signal diversity, and equipment diversity.

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

D.6.2 Information to be Provided

Review (Phase 1): (1) LAR Section 4.6 - Diverse I&C Systems

~~(a) Description of diversity credited within the safety system or backup systems(s)~~

~~(b) For credited backup systems, description of compliance with BTP 7-19 and SRP Section 7.8 quality and design requirements~~

~~(c) Description 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)~~

~~(d) D3, AOO, and PA Coping Analysis, including identification of credited operator actions, and plans for HFE analysis and V&V~~

(2) D3 Analysis~~, including~~

~~(a) D3 HFE analysis and preliminary validation for credited operator actions~~

~~(b) D3 demonstration of no potential for CCF for credited components~~

~~**Audit (Phase 2):** D3 HFE integrated system validation for credited operator actions (for conventional control rooms – minor simulator modifications)~~

~~**Inspect (Phase 3):** D3 HFE integrated system validation for credited operator actions (for upgrades that require extensive simulator modifications)~~

The licensee's D3 analysis submittal should provide sufficient documentation for the NRC staff to independently reach a conclusion that the plants I&C systems are sufficiently robust against CCF. As further discussed in Section D.6.3, the NRC staff will evaluate the licensee's proposed amendment using Branch Technical Position 7-19 Rev. 6 (ML093490771), 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).~~of the system~~ with respect to the six areas (human diversity, design diversity (hardware), software diversity, functional diversity, signal diversity, and equipment 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 RTS and ESFAS provided for system interlocks and justification that functions required by 10 CFR 50.62 are not impaired by the interconnection.
  - 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)

Formatted: Indent: Left: 0", Hanging: 1.75", Space After: 12 pt

Comment [A123]: Comment No. 105.

Comment [A124]: Comment No. 106, 108, 109.

Formatted: Indent: Left: 0", Tab stops: Not at 0.5" + 1" + 1.5" + 2"

Comment [A125]: Comment No. 110, 111.

Formatted: Indent: Left: 0.25", Tab stops: Not at 1" + 1.5" + 2" + 3"

– For credited backup systems, description of compliance with BTP 7-19 and SRP Section 7.8 quality and design requirements

  - A best-estimate evaluation of each anticipated operational occurrence (AOO) in the design basis occurring in conjunction with each single postulated common-cause failure.
  - A best-estimate 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.
  - ~~D3, AOO, and PA Coping Analysis, including identification of credited operator actions, and plans for HFE analysis and V&V~~

– For credited operator actions

  - D3 HFE analysis and preliminary validation for credited operator actions
  - ~~D3 demonstration of no potential for CCF for credited components~~
  - D3 HFE integrated system validation for credited operator actions (see SRP Chapter 18 Appendix 18-A, ML092950353)

Licensees should be aware that the specific situations and applications of a system may require 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 used 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 in digital systems and defense-in-depth. This position was also documented in BTP 7-19 Rev. 6 (ML093490771), "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 required safety functions can be achieved in the event of a postulated CCF in the digital system. As discussed in BTP 7-19 Rev. 6 (ML093490771), the NRC staff's review considered the following regulatory requirements:

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with Institute of Electrical & Electronics Engineers (IEEE) Standard (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 before January 1, 1971, the applicant/licensee may elect to comply instead with their plant-specific licensing basis. For nuclear power plants with construction permits issued between January 1, 1971,

Formatted: Indent: Left: 0", Tab stops: Not at 0.5" + 1" + 1.5" + 2"

Formatted: Indent: Left: 0.25", Hanging: 0.25", Tab stops: Not at 3"

Comment [A126]: Comment No. 112.

Comment [A127]: Comment No. 113.

Comment [A128]: Comment No. 107.

Comment [A129]: Commen No. 115 – no change.

Comment [A130]: Comment No. 114.

Formatted: Indent: Left: 0.25"

and May 13, 1999, the applicant/licensee may elect to comply instead with the requirements stated in IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE Std. 603-1991, Clause 5.1, requires, in part, that "safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures." IEEE Std. 279-1971, Clause 4.2, requires, in part, that "any single failure within the protection system shall not prevent proper protective action at the system level when required."

10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram [ATWS]," requires, in part, various diverse methods of responding to ATWS.

10 CFR Part 50, Appendix A, General Design Criterion (GDC) 21, "Protection Systems Reliability and Testability," requires, in part, that "no single failure results in the loss of the protection system."

GDC 22, "Protection System Independence," requires, in part, "that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions Y not result in loss of the protection function Y 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 Y safety functions."

Formatted: Indent: Left: 0.25"

Formatted: Indent: Left: 0.25"

Comment [A131]: Wording from Rev. 33 reinserted.

The NRC staff intends to provide a preliminary determination on the acceptability of the approach to demonstration of a sufficient level of defense-in-depth and diversity as part of the Phase 0 meetings and acceptance review of the amendment request. This will 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 (ML093490771) 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 confirming that vulnerabilities to CCF have been addressed:

Comment [A132]: Comment No. 116, 117.

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

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

Verify 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.

Formatted: Indent: Left: 0.25", Tab stops: Not at 1" + 1.5" + 2"

D.6.4.1 Adequate Safety System Diversity and Manual Actions

Branch Technical Position 7-19 Rev. 6 (ML093490771) and SRP Chapter 18, "Human Factors," Section 18-A, "Guidance for Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses," provide~~s~~ 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 sufficient diversity exists in the protection system or an automate Diverse Actuation System (DAS) is provided (which may be non-safety-realted), then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

If sufficient diversity does not exists 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.

D.6.4.2 ~~Branch Technical Position 7-19 Rev. 6 (ML093490771), Position 4~~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, 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 requirements 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 (ML093490771), 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… ~~discussed above~~. However, 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.
>
> 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… ~~(see Section 1.5, "Safety-Related Manual Actuation")~~. 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 will review the proposed system and any proposed diverse system to determine 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 will specifically address the positions in BTP 7-19 Rev. 6 (ML093490771) to determine adequate diversity exists.

D.7 Communications

D.7.1 Scope of Review

Comment [A133]: Comment No. 119 – no change.

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 must 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 will review the overall design as discussed in the following subsections. As part of this review, the NRC staff will 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 will include a review to determine if 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 will include a review to determine if a logical or software malfunction of the non-safety system affects the functions of the safety system. These reviews will be done by examination of the communication methods used, and comparing them to each staff position within DI&C-ISG-04 Revision 1, "Interim Staff Guidance on Highly-Integrated Control Rooms – Communications Issues (HICRc)," March 2009.

Comment [A134]: Coment No. 118.

D.7.2 Information to be Provided

Comment [A135]: Comment No. 120 – Foootnote deleted and therefore comment is no longer applicable.

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 limit the effect of a failed channel from adversely impacting separate channels or divisions. The documentation should provide sufficient justification to allow the conclusion that the plan meets the standards of IEEE 603-1991 Clause 5.6, IEEE 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 the error.

The information needed by the NRC staff 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 final 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 is proposed when an individual clause is not meet.

Comment [A136]: Comment No 121.

D.7.3 Regulatory Evaluation

IEEE 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 must not be able to affect the functions of the safety system.

IEEE 7-4.3.2, endorsed by Regulatory Guide 1.152, Clause 5.6, "Independence," provided guidance on how IEEE 603 requirements can be met by digital systems. This clause of IEEE 7-4.3.2 states that, in addition to the requirements of IEEE Std 603-1991, data communication between safety channels or between safety and non-safety systems shall 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.

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

Comment [A137]: Comment No. 122.

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 other non-safety-related systems shall be evaluated to confirm that a failure or malfunction in one does not adversely impact successful completion of the design function. Confirmation that the system is sufficiently robust against improper operation due to these communications is further discussed in DI&C-ISG-04.

The technical evaluation will address each applicable section of DI&C-ISG-04, and will 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 will review the proposed alternative, and determine if the alternative still meets regulatory requirements.

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.

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 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, 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.

D.7.5 Conclusion

The NRC staff will review the design and implementation of the digital I&C system to determine that either it does not employ data communications between separate channels or meets the requirements of IEEE 603-1991, IEEE 7-4.3.2 and DI&C-ISG-04. The NRC staff will find that the proposed digital I&C upgrade either is acceptable with respect to data communications, or is not acceptable and requires revision to the data communications.

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

D.8.1 Scope of Review

Section D.8 does not have an inherent scope of review. This review area describes how the NRC staff determines 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.

Comment [A138]: Comment No. 123 – no change.

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 any and all deviations to the system, hardware, software, or design lifecycle methodology from a previous NRC approval of a digital I&C system or topical report. The intent is to not only eliminate the need for the NRC staff to review items which have already been reviewed and approved, but also to allow the NRC staff to reach a determination that any changes do not invalidate conclusions reached by the previous review. Completion of this review will essentially result in an update of the previous digital I&C system;

Comment [A139]: Comment No. 124 – no change.

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.

Comment [A140]: Comment No. 125 – no change.

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 which 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 needed will be proportional to the significance of the change.

D.8.3 Regulatory Evaluation

The basis on which the new system, hardware, software, or design lifecycle methodology will be evaluated is the same as the evaluation of the original version of that item. The various acceptance criteria are discussed throughout this ISG.

D.8.4 Technical Evaluation

The technical evaluation of the submittals is the same as for the original submittal. One item the NRC staff will be checking for is the adequacy of the description of 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 considers significant changes to hardware such as a new microprocessor requiring re-compiling of software, changes in software which would 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 will continue to comply with regulatory requirements to be major. The NRC staff assumes that if the licensee or vendor believes the change would result in the new system, hardware, software, or design lifecycle methodology would not meet regulatory requirements, the change would not have been made. In each of these instances discussed above, the new documentation should be submitted to the NRC staff 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 which have previously been reviewed and approved. This process allows the licensee and vendor to limit the documentation submitted for review to only those documents which will require new review, and eliminate a new review of documentation which has had only minor changes or modifications. If the NRC staff reviews the change description and determines the change is not minor, but will require a new review, the Request for Additional Information process will result in a longer review than if the document had been submitted originally. In order for the licensee and vendor to reduce the overall review time and effort, a conservative approach, it is

recommended to submit any 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 IEEE 603, Compliance

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 directly apply to the 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, the guidance of IEEE Std. 603-1991 is directly applicable to those parts of data communication systems that support safety system functions.

Additionally, the review may require 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 the need for coordination with other technical disciplines.

- The site characteristics, systems (both physical and administrative), and analyses described in other sections of the UFSAR may necessitate additional requirements of the digital I&C system.

- Digital I&C systems may necessitate additional requirements upon other plant systems and analyses.

- Other plant systems may necessitate additional requirements 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 needed to achieve a safety function.

D.9.2 Information to be Provided

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

The licensee's ~~submittal~~ LAR should provide sufficient ~~documentation~~ 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 LARdocumentation. To assist the NRC staff in making the determination that the licensee submittal meets the requirements of IEEE 603, the licensee may also submit a document showing where within the other documentation submitted the confirmatory information can be found. While this is not an absolute requirement, it will 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.

Comment [A141]: The LAR includes a regulatory evaluation, and a public meeting industry accepted the idea that this evaluation can mostly be included in the LAR with a few exceptions as identified in the sub-sections below.

Comment [A142]: Comment No. 127.

D.9.3 Regulatory Evaluation

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with Institute of Electrical & Electronics Engineers (IEEE) Standard (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 before January 1, 1971, the applicant/licensee may elect to comply instead with their plant-specific licensing basis. For nuclear power plants with construction permits issued between January 1, 1971, and May 13, 1999, the applicant/licensee may elect to comply instead with the requirements stated in IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE Std. 603-1991, Clause 5.1, requires in part that "safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures." IEEE Std. 279-1971, Clause 4.2, requires in part that "any single failure within the protection system shall not prevent proper protective action at the system level when required."

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 Std. 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 required to approve the alternative will depend on how different the alternate standard is from IEEE Std-1991.

D.9.4 Technical Evaluation

D.9.4.1 IEEE 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, ~~very little additional justification for~~a simple description of the design basis would be

needed (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 require 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 needs to be specifically addressed in the information provided.

Comment [A143]: I strongly feel that the NRC needs to know what the design basis is, and that the applicant should tell us. It is very difficult to state that they system meets its design basis, when you do not know what the design basis is. Basically many of the clause in IEEE 603 Sections 5, 6, 7, & 8 require that the design meet the design basis as documented in Section 4.

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 determine if 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 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 assumed 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 reactor systems evaluates the adequacy of protective, control, display, and interlock functions and confirms that they are consistent with the accident analysis, the operating requirements 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.

D.9.4.1.2 IEEE 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 other systems evaluates the adequacy of protective, control, display, and interlock functions and confirms that they are consistent with the accident analysis, the operating requirements of the I&C systems, and the requirements of 10 CFR Part 50, Appendix A, General Design Criteria (GDC).

The organization responsible for review of I&C evaluates the adequacy of the equipment to perform the specified functions.

D.9.4.1.3 IEEE 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 other systems evaluates the adequacy of protective, control, display, and interlock functions and confirms that they are consistent with the accident analysis, the operating requirements of the I&C systems, and the requirements of 10 CFR Part 50, Appendix A, General Design Criteria (GDC).

The organization responsible for review of I&C evaluates the adequacy of the equipment to perform the specified functions.

D.9.4.1.4 IEEE 603, Clause 4.4, Variables monitored

Clause 4.4 requires the identification of variables that are monitored in order to provide protective action. Performance requirements, 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 confirm that the system performance requirements 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 confirming that an adequate margin exists between analytical limits and setpoints are discussed in Clause 6.8.

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

Clause 4.5 describes 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 shall be performed, and the variables in clause 4.4 shall be displayed 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, DI&C-ISG-05 addresses this issue.

Comment [A144]: Comment No. 128.

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

D.9.4.1.6 IEEE 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. Clause 5.1 further addresses this issue.

D.9.4.1.7 IEEE 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. This information will feed into additional evaluations. If these have not changed, this should be clearly identified in the information provided.

D.9.4.1.8 IEEE 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 will feed into additional evaluations, including Clause 5.4.

D.9.4.1.9 IEEE 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 any qualitative 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, rather than on qualitative methods used to confirm that these deterministic criteria have been met.

The NRC staff does not endorse the concept of qualitative 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 need to be used to assess the unreliability introduced by hardware and software.

D.9.4.1.10 IEEE 603, Clause 4.10, Control after Protective Actions

Clause 4.10 requires the documentation of the points in time or plant conditions after the onset of a design basis event that allow the implementation of manual actions necessary to maintain safe conditions.

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

D.9.4.1.11 IEEE 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 603, Clause 4.12, Special Design Basis

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

D.9.4.2 IEEE 603, Clause 5, System

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. The analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met. The evaluation should confirm that the general functional

requirements have been appropriately allocated to the various system components. The review in this regard should confirm that the system design fulfils the system design basis requirements established.

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

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

Review (Phase 2): FMEA

Clause 5.1 requires that any single failure within the safety system shall not prevent proper protective action at the system level when required. The analysis[2] should confirm that the requirements of the single-failure criterion are 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."

Comment [A145]: Comment No. 129.

Where it is determined that the spatial dependence of a parameter requires several sensor channels to ensure plant protection, the redundancy requirements are determined for the individual case. In certain designs, for example, adequate monitoring of core power requires a minimum number of sensors arranged in a given configuration to provide adequate protection. This aspect of redundancy is dealt with in coordination with the organization responsible for reviewing reactor designs to establish redundancy requirements.

Components and systems not qualified for seismic events or accident environments and non-safety-grade components and systems are assumed to fail to function if failure adversely affects safety system performance. Conversely, these components and systems are assumed 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 assumed to occur if the failure adversely affects the safety system performance. In general, the lack of equipment qualification or a less than high quality design process may serve as a basis for the assumption of certain failures. After assuming 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 arbitrarily assumed. With these failures assumed, the safety system must be capable of performing the protective functions required to mitigate the consequences of the specific event. The information needed by the NRC staff 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 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

[2] The analysis is sometimes documented in a Failure Modes and Effects Analysis (FMEA) report; see Section D.4.4.2.6.

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 will 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 needed by the NRC staff 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 final 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 will not result in an undue risk to public safety. This is addressed further in Section D.6 and Branch Technical Position 7-19 Rev. 6 (ML093490771).

Comment [A146]: Comment No. 130 – ISG 2 replaced with BTP 7-19.

A detailed diversity and defense-in-depth study should address common-cause failures in digital computer-based systems. The NRC's position for providing defense against common-cause failures in digital I&C systems for future light-water reactors is given in the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," (specifically in point 18: II Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems"). SRP BTP 7-19 Rev. 6 (ML093490771), provides guidance for addressing the potential of common-cause failures.

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

Clause 5.2 requires that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion, and that deliberate action shall be required 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 should include functional and logic diagrams sufficient to demonstrate this feature. The information should clearly demonstrate that deliberate action is required 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 final circuit schematics and in the software code listings, and in detailed system and hardware drawings.

D.9.4.2.3 IEEE 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 confirm 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 will be audited by the NRC staff.

D.9.4.2.4 IEEE 603, Clause 5.4, Equipment Qualification

Review (Phase 1): System Response Time Analysis Report

Review (Phase 2): System Response Time Confirmation Report

IEEE 603 Clause 5.4 states that safety system equipment shall be qualified[3] by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting the performance requirements as specified in the design basis (See IEEE 603 Clause 4.7). Appendix 7.1-C, Section 5.4, of the SRP provides acceptance criteria for Clause 5.4. This acceptance criteria states that the licensee should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. The information provided should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal, abnormal, and accident conditions.

Typically an 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 performance standards in specified environmental conditions. See Section D.5, "Environmental Equipment Qualifications," for detailed guidance on environmental equipment qualifications.

(2) Ensuring that the qualification envelop of the equipment bounds the performance and the plant specific application requirements.

(3) Ensuring that the application specific functional and performance requirements are achieved by the specific equipment and configuration proposed.

[3] The information needed by the NRC staff to reach a determination of adequate system qualification is discussed in Section D.5.

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 (e.g., IEEE 603 Clause 5.4) within its design-basis normal and adverse environments (e.g., as required to be documented by IEEE 603 Clause 4.7). The results of the qualification testing should be documented in a summary report.

The NRC staff will review the information provided to verify that the plant specific application has been demonstrated to be able to meet functional and performance requirements 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 603, Clause 5.5, System Integrity

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

Clause 5.5 states that the safety systems shall 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 should confirm that 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 completes 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 603 Clause 5.5 will 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 applicant/licensee's software safety analysis activities.

The review of system integrity should confirm 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 applicant/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 will 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 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.[4] Each case should be addressed with respect to physical, electrical, and communications independence.

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

Comment [A147]: Comment No. 133.

[4] 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.4.4.2.6.

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 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 requirements for demonstration of this independence.

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

Clause 5.6.2 states that the safety systems required 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 this standard. 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 information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the degree of independence is sufficient.

D.9.4.2.6.3 IEEE 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 will not prevent the safety systems from meeting the requirements of this standard. This requirement is subdivided into requirements for interconnected equipment, equipment in proximity, and the effects of a single random failure. Each of the sub-clauses will be addressed in the following paragraphs.

Clause 5.6.3.1 of IEEE 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 requirements during and following any design basis event requiring 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 determine that the degree of independence is sufficient.

Clause 5.6.3.2 of IEEE 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. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Standard 384-1992. 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 determine that the degree of independence is sufficient.

Comment [A148]: Comment No. 133.

Clause 5.6.3.3 of IEEE 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 determine that the degree of independence is sufficient.

D.9.4.2.7 IEEE 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. It is expected that safety systems will 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 required 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 confirm 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 required by 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 surveillance requirements, or less frequent performance of existing surveillance requirements, 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 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 required 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.

Comment [A149]: Comment No. 134, 135.

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 confirmation that 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. 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 required 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 shall be located such that they are accessible to the operator and that if the information display is provided for manually controlled protective actions, it shall 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 determine that the four sub-clauses have been met. The NRC staff will review the factory acceptance testing to determine if these design features have been tested, and the summary reports to verify that the testing showed these features were acceptable.

D.9.4.2.9 IEEE 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 determine that Clause 5.9 has been met. The Secure Environment Review Area 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 also have to examine (audit) the actual circuitry as described in the final circuit schematics and in the software code listings, and in detailed system and hardware drawings. The NRC staff will also review the plant specific administrative control documentation to determine that the administrative controls are such that they will adequately limit access to qualified and authorized plant personnel.

D.9.4.2.10 IEEE 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 determine that this requirement has been meet.

D.9.4.2.11 IEEE 603, Clause 5.11, Identification

Comment [A150]: Comment No. 138, 139.

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 Guige 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 require the frequent use of reference materials (i.e., be "user friendly"), and that the associated documentation be distinctly identified ~~in accordance with IEEE Std. 494-1974 (R1990)~~. 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, require identification. The information provided should sufficiently describe the identification of hardware, software, and documentation such that the NRC staff is able to determine that the Clause 5.11 has been met.

Comment [A151]: Comment No. 136.

Comment [A152]: Comment No. 137.

D.9.4.2.12 IEEE 603, Clause 5.12, Auxiliary Features

Clause 5.12 requires that auxiliary supporting features meet all requirements of this standard. Those auxiliary features that perform functions that are not required 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 meet 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 can not show that the supporting feature is needed, a detailed description of the feature, how it is designed and how it functions will be needed for the NRC staff to determine that having this feature will not compromise the safety or functionality of the system. This detailed description may require the NRC staff to review actual schematics or software code to reach its conclusion.

D.9.4.2.13 IEEE 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 required 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 determine that the Clause 5.13 has been met.

Comment [A153]: Comment No. 140.

Comment [A154]: Comment No. 141.

D.9.4.2.14 IEEE 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 design 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 also be sufficient to demonstrate that the guidance contained in NUREG-0700, NUREG-0711, and DI&C-ISG-05 has been met.

Comment [A155]: Operator changed to User throughout per Comment No. 3.

Comment [A156]: Comment No. 142.

D.9.4.2.15 IEEE 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.[5] 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

Comment [A157]: Comment No. 143.

[5] A reliability analysis provides sufficient detail to support and justify that the system meets the reliability requirements.

failures as described in Clause 5.1, 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.

The information provided should include a detailed Failure Modes and Effects Analysis and a reliability analysis in accordance with IEEE Standard 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," and IEEE Standard 577-2004, "IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities."

D.9.4.3 IEEE 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 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 sufficiently describe the hardware and software such that the NRC staff is able to determine 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 requirements have been appropriately allocated into hardware and software requirements. The description should confirm that the system's real-time performance is deterministic and known. The information needed by the NRC staff to reach a determination 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 have been adequately tested should be contained in the factory acceptance test plan, and the final test reports will be reviewed to verify that the testing showed these features were acceptable.

D.9.4.3.2 IEEE 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.

Comment [A158]: Comment No. 144.

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 603, with the information provided to the operators, the actions required 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 should be contained in the system, hardware and software specifications, architecture, and descriptions. The information to show that these features have been adequately tested should be contained in the factory acceptance test plan. The final test reports will also be reviewed to verify that the testing showed these features were acceptable.

The manual control required by Clause 6.2 may be different from a manual action which may be used as an acceptable diverse actuation required by BTP 7-19 Rev. 6 (ML093490771), 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 (9due 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. The SRM to SECY 93-087, as reflected in BTP 7-19 Rev. 6 (ML093490771), has the requirement for 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 requirements, by making those controls safety-related, system level, and downstream of any digital portion of the safety system.

Comment [A159]: Comment No. 145.

D.9.4.3.3 IEEE 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 will be provided, or equipment not subject to failure caused by the same single credible event shall 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 sufficiently describe the hardware and software such that the NRC staff is able to determine that Clause 6.3 has been met. Additionally, the FMEA should contain information to address this clause.

D.9.4.3.4 IEEE 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,

Comment [A160]: Comment No. 146.

such as range, accuracy, resolution, response time, and sample rate. 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 determine that the Clause 6.4 has been met.

D.9.4.3.5 IEEE 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 sensor required for a safety function during reactor operation, including the availability of each sense and command feature required 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 the two channel readouts differ.

Comment [A161]: Comment No. 147.

D.9.4.3.6 IEEE 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 determine that the Clause 6.6 has been met.

D.9.4.3.7 IEEE 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 determine that the Clause 6.7 has been met.

D.9.4.3.8 IEEE 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 when required. 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, when required. 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 determine that the Clause 6.8 has been met.

D.9.4.4 IEEE 603, Clause 7, Execute Features

Review (Phase 1): Theory of Operation Description

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

Comment [A162]: Comment No. 148.

D.9.4.4.1 IEEE 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 determine that the Clause 7.1 been met.

D.9.4.4.2 IEEE 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 determine that the Clause 7.2 has been met. The review of manual controls should include confirmation 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 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 require 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 determine that the Clause 7.3 has been met.

D.9.4.4.4 IEEE 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 simply be referenced.

D.9.4.4.5 IEEE 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 determine that the Clause 7.5 has been met.

D.9.4.5 IEEE 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 required to provide the power to the many facets of the safety system are governed by the criteria of IEEE 603-1991 and are considered a portion of the safety systems. Clauses 8.1 and 8.2 apply the requirements of IEEE 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 determine that the Clauses 8.1, 8.2, and 8.3 have been met.

D.9.5 Conclusion

The NRC staff will review the licensee's submittal against the requirements of IEEE 603-1991 to determine if the proposed implementation of meets the standard, and therefore would be acceptable with respect to IEEE 603-1991 and 10 CFR 50.55a(h)(2).

D.10 IEEE 7-4.3.2, Guidance

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 7-4.3.2-1982. IEEE/ANS 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

D.10.2 Information to be Provided

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

The licensee's ~~submittal~~ LAR should provide sufficient ~~documentation~~ information to support the assertion that a proposed digital I&C system ~~is consistent with~~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 of IEEE 7-4.3.2, the licensee may also submit a document showing where within the other documentation submitted the confirmatory information can be found. While this is not an absolute requirement, it will 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.10.4.

Comment [A163]: The LAR includes a regulatory evaluation, and a public meeting industry accepted the idea that this evaluation can mostly be included in the LAR with a few exceptions as identified in the sub-sections below.

Comment [A164]: Comment No. 149.

D.10.3 Regulatory Evaluation

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 and is endorsed by RG 1.152 Rev. 2 dated 2003 (i.e., RG 1.152 & IEEE 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 reasonable assurance of a high quality system. This activity should be expected to take a significant amount of additional review time and effort.

Comment [A165]: Comment No. 150.

D.10.4 Technical Evaluation

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

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

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

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

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

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

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

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

D.10.4.2.3 IEEE 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 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 of the development process will 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 requirements

- Using the requirements to develop a detailed system design

- Implementing the design into hardware and software functions
- Testing the functions to assure the requirements have been correctly implemented

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

Comment [A166]: Comment No. 151.

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 requirement, the licensee needs to provide a 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 requirements 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 QA plan should describe the method used to determine that this software was evaluated and found suitable for the use required of that software. It should also be noted that if the QA plan requires the use of separate documents, those documents should also be provided.

Clause 5.3.1.1 states that the use of software quality metrics shall be considered throughout the software lifecycle to assess whether software quality requirements 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.

Comment [A167]: Comment No. 152.

This recommends but does not require the use of software quality metrics. If metrics are used to justify software quality, the licensee must demonstrate how those metrics actually measure software quality, and how use of the metrics will demonstrate that the quality requirements of 10 CFR Appendix B are being met.

Comment [A168]: Comment No. 153.

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 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 states that software tools used to support software development processes and V&V processes shall be controlled under the configuration management plan. The tools shall either be developed to a similar standard as the safety-related software or the tool shall be used in a manner such that defects not detected by the tool will be detected by V&V activities.

Comment [A169]: Comment No. 154.

A test tool validation program should be developed to provide confidence that the necessary features of the software tool function as required. This basically means that if the output can-not 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.

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

Comment [A170]: Comment No 155.

SRP BTP 7-14 states that the resource characteristics that the software development plan should exhibit include methods/tools and standards. Methods/tools require 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 require that tools 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 requirements should be prohibited, unless analysis shows that the alternative would be less safe.

Reviewers will thoroughly evaluate tool usage. 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 will perform as intended. Testing alone can only show that those items tested for operate as intended, and can not be relied upon to show that no unintended functions exist, or that the software will function in conditions other that 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 will have to review the tool design 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 will

assume that the output of that tool may contain errors, and therefore the output of the tools will need to undergo the full verification and validation process.

The information required 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. Actual use of the tools will be audited by the NRC staff.

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

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

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

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 ~~s~~Section D.4.4.1.10 of this ISG, the licensee will need to 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 which 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).

Comment [A171]: Comment No. 157.

Review of the V&V plan, and the determination that the V&V effort meets regulatory requirements is one of the most significant part of the NRC staff review of the design life cycle, and therefore will receive a thorough review. It should also be noted that the V&V testing should be described in the system and software test plans, and the results of this testing should be contained in the final test reports. The NRC staff will review these test plans and associated documentation to ensure that the testing done was adequate to support the V&V effort, and meets the requirement of RG 1.168 and IEEE Std. 1012.

Comment [A172]: Comment No. 156.

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

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

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

Clause 5.3.4 defines the levels of independence required for the V&V effort in terms of technical, managerial, and financial independence. Oversight of the effort should be vested in an organization separate from the development and program management organizations and whose resources are allocated independent of the development resources. The information provided should demonstrate that:

- The V&V organization is independent and given sufficient time and.

- The V&V personnel are as qualified as the design personnel.
- The V&V organization is effective. During a thread audit, performed by the NRC staff, errors not identified by the V&V organization may indicate a lack of effectiveness.
- Problems identified by the V&V organization are properly addressed.

The information required for the NRC staff to determine 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 will audit the independence of the V&V during the vendor V&V and thread audits to determine 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 can-not perform a review of every requirement and every line of code, the staff relies on the V&V completeness and rigor of the V&V effort to provide reasonable assurance of high quality software development. 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 a thread audit 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 requirements, 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 actually work. 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 required 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 the problem reports carefully, and determine that each problem was addressed and that correction did, in fact, correct the problem without introducing new errors.

The review of the V&V is an important step in the determination of high quality software and a high quality design 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 reviewer identifies concerns with quality or effectiveness, those issues should be raised to NRC management to determine the next steps up to and including non-acceptance of the V&V effort of the digital system for use in a safety-related application at nuclear power plants.

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

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

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

~~**Audit (Phase 2):** (1) Interim, Installation Configuration Tables~~
~~(2) Configuration Management Reports~~

Clause 5.3.1.5 states that software configuration management shall 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 will 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 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 others.

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 design 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. 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 determine if 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.

Comment [A173]: Comment No./ 159.

IEEE Std 828-1990 and IEEE Std 1042-1987, which are endorsed by Regulatory Guide 1.169, should 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 will 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 determine 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 design process and after acceptance of the software for use will be made to the appropriate version and revision of the software. This will 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.

Comment [A174]: Comment No. 158.

D.10.4.2.3.6 IEEE 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 required 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).

Comment [A175]: Comment No. 160.

Comment [A176]: Comment No. 161, 162, 163.

Comment [A177]: Comment No. 164.

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

Clause 5.4 defines the equipment qualification[6] required for a software project. These requirements, 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 7-4.3.2, Clause 5.4.1, Computer system testing

~~**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~~

Clause 5.4.1 requires 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 this requirement, and that the test reports show what software was running during the tests.

[6] The information needed by the NRC staff to reach a determination of adequate system qualification is discussed in Section D.5.

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

Review (Phase 1): ~~Digital~~ Commercial Grade Dedication Plan

Review (Phase 2): ~~(1) Digital~~ Commercial Grade Dedication Report
~~(2) Final Report on Acceptance of Digital Commercial Grade Dedication~~

~~**Audit (Phase 2):** Miscellaneous commercial grade dedication reports~~

Comment [A178]: Comment No. 165.

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 a high quality design process. In essence, the licensee will need to show that the design process used to develop the commercial software was a rigorous as that required for non-commercial software used in safety-related applications. If this can~~-~~not be demonstrated, the commercial grade software may not be suitable for ~~this~~ safety-related applications.

EPRI TR-106439, as accepted by the NRC safety evaluation dated July 17, 1997, 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 7-4.3.2-2003. 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, provides more specific guidance for the evaluation of existing programmable logic controllers (PLC).

The fundamental criteria for demonstrating reasonable assurance that the 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 decribed 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 required functions. 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 ~~computer~~ digital safety system (e.g., as described in the Commercial Grade Dedication Plan) should entail identification of the physical, performance, and development process requirements 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 required to accomplish the safety function. The dedication process for software and firmware should include an evaluation of the design 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.

It is preferable to docket each commercial grade dedication report as soon as it has been completed; however, the complete set of reports should be docketed by the start of Phase 2.

D.10.4.2.5 IEEE 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 states that in addition to the system integrity criteria provided by IEEE Std. 603-1991, the digital system shall 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 requirements.

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

Clause 5.5.1 states that the computer shall 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 will need to provide this demonstration, however this demonstration will generally credit the design, V&V, and test documentation. It is unlikely that any additional documentation, beyond a reference to processes already documented, will be needed.

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

Clause 5.5.2 states that test and calibration functions shall not adversely affect the ability of the system to perform its safety function, and that it shall 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 be required 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 required 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 will need to provide this demonstration, however this demonstration will generally credit the design, V&V, and test documentation. It is unlikely that any additional documentation, beyond a reference to processes already documented, will be needed.

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

Clause 5.5.3 states that if reliability requirements 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 shall 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 requirements for self-diagnostics are contained in the software requirements documentation, 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. In addition, the FMEA of the software should consider errors in the diagnostic software, and show the effect of those errors.

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

Review (Phase 1): Design Analysis Report

Clause 5.6 requires, in addition to the requirements of IEEE Std. 603-1991, data communication between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function.[7] 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 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 shall be limited so as to assure that safety is not significantly impaired.

Comment [A179]: Comment No. 166.

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 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 requirements beyond those in IEEE Std. 603-1991. Therefore, this clause will 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, the 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. The Failure Modes Effects Analysis (FMEA) should include diagnostic code failure.

Large amounts of test and diagnostic software increase the complexity of the system, and this increase in complexity should be balanced against the potential gain in confidence in the system provided by that 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 this application.

[7] A 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.4.4.2.6.

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

Comment [A180]: Comment No. 167.

Comment [A181]: Comment No. 168.

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

Clause 5.8 states that there are no requirements 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[8], 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 required no two-way communications. More modern display systems may also have included control functions, and therefore the reviewer should ensure that incorrect functioning of the information displays does not prevent the safety function from being preformed 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 communications with non-safety control systems have the same isolation issues as any other non-safety to safety communications.[9] In addition, however, the reviewer should ensure that inadvertent actions, such as an unintended touch on a touch sensitive display can not prevent the safety function.

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

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

D.10.4.2.10 IEEE 7-4.3.2, Clause 5.10, Repair

There are no requirements beyond those in IEEE Std. 603-1991. Therefore, this clause will be addressed by the review performed under Section D.9.4.2.10.

D.10.4.2.11 IEEE 7-4.3.2, Clause 5.11, Identification

Clause 5.11 requires that firmware and software identification be used to assure the correct software is installed in the correct hardware component. Means shall 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 be done 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 the requirements of this clause, and when discussing compliance with the clause, point to the sections of the configuration management plans where this is discussed. In general, no new documentation should be required.

[8] See DI&C-ISG-04, Section 3, "Multidivisional Control and Display Stations."
[9] See DI&C-ISG-04, Section 1, "Interdivisional Communications."

D.10.4.2.12 IEEE 7-4.3.2, Clause 5.12, Auxiliary Features

There are no requirements beyond those in IEEE Std. 603-1991. Therefore, this clause will be addressed by the review performed under Section D.9.4.2.12.

D.10.4.2.13 IEEE 7-4.3.2, Clause 5.13, Multi-unit Stations

There are no requirements beyond those in IEEE Std. 603-1991. Therefore, this clause will be addressed by the review performed under Section D.9.4.2.13.

D.10.4.2.14 IEEE 7-4.3.2, Clause 5.14, Human Factor Considerations

There are no requirements beyond those in IEEE Std. 603-1991. Therefore, this clause will be addressed by the review performed under Section D.9.4.2.14.

D.10.4.2.15 IEEE 7-4.3.2, Clause 5.15, Reliability

Review (Phase 2~~1~~): Reliability Analysis (Phase 2)

Clause 5.15 states that, in addition to the requirements of IEEE Std. 603-1991, when reliability goals are identified, the proof of meeting the goals shall 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.[10]

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 software reliability value, determining a 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 using 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 depend on the software being perfect.

D.10.4.3 IEEE 7-4.3.2, Clause 6, Sense and Command Features

There are no requirements beyond those in IEEE Std. 603-1991. Therefore, this clause will be addressed by the review performed under Section D.9.4.3.

D.10.4.4 IEEE 7-4.3.2, Clause 7, Execute Features

There are no requirements beyond those in IEEE Std. 603-1991. Therefore, this clause will be addressed by the review performed under Section D.9.4.4.

[10] A reliability analysis provides sufficient detail to support and justify that the system meets the reliability requirements.

D.10.4.5 IEEE 7-4.3.2, Clause 8, Power Source Requirements

There are no requirements beyond those in IEEE Std. 603-1991. Therefore, this clause will be addressed by the review performed under Section D.9.4.5.

D.10.5 Conclusion

The NRC staff will review the licensee's submittal against the requirements of IEEE 7-4.3.2-2003 and will determine whether or not the proposed implementation meets the requirements of that standard.

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," will 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 or proposed for addition to the TSs.

Comment [A182]: Coment No. 169.

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 developmental methodologies to be references 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 marked 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 what verification is accomplished 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 anything 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, or 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

The Technical Specification LCOs being proposed for deletion are evaluated against the four criterion of 10 CFR 50.36(d)(2)(ii). If none of the criterion are met, the LCO may be deleted. Additionally, the LCOs being proposed for addition should be to ensure that they 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 ones not 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, this should evaluate those SRs proposed and the need for additional ones.

Finally, the NRC staff should ensure that the licensee has proposed to include the appropriate references to methodologies in the Administrative section of the TSs.

D.11.5 Conclusion

The NRC staff will review the proposed TS changes associated with the implementation of the digital I&C system and will find whether or not that the LCOs and SRs that will govern the operations, test, and maintenance of the digital I&C system are adequate to reasonably assure that the system will perform its design function. Additionally, the NRC staff will review the methodologies that have been proposed for incorporation into the administrative section of the TSs and will determine whether or not those methodologies are acceptable. The NRC staff make a statement in the SE on whether or not the proposed digital I&C upgrade is acceptable with respect to technical specifications.

Comment [A183]: Comment NO. 170.

D.12 Secure Development and Operational Environment

Comment [A184]: The entire contents of this section is new.

Comment No. 171.

D.12.1 Scope of Review

Comment [A185]: Comment No. 172.

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 will be made as part of the licensing review regarding the feature's ability to perform its intended cyber security function.

D.12.2 Information to be Provided

Comment [A186]: Comment No. 173.

Review (Phase 1): (1) LAR Section 4.12, "Secure Environment"
(2) Vulnerability Assessment
(3) Secure Development and Operational Environment Controls

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 normal and adverse environments.

Formatted: Space After: 0 pt

Development of a vulnerability assessment is an applicant'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 ~~To~~ address regulatory positions 2.1, Concepts Phase through 2.5, Test Phase of regulatory guide 1.152. ~~the following documents should be provided:~~
~~Vulnerability Assessment~~
~~Secure Operational Environment Design Features~~
~~Requirements Phase Requirements and Controls~~
~~Design Phase Requirements and Controls~~
~~Implementation Phase Requirements and Controls~~
~~Test Phase Requirements and Controls~~

The information necessary to address the various aspects of secure environment are elaborated in Section D.12.4.

D.12.3 Regulatory Evaluation

Comment [A187]: Comment No. 174.

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."

Appendix B to Part 50, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants" delineates the requirements for a quality assurance program. Criterion III of Appendix B, "Design Control" further enumerates measures for control of design, documentation, interfaces, verification & validation, testing, and design changes to assure quality.

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~~-1998, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations."~~. This standard ~~evolved from IEEE Std. 7-4.3.2-1993 and~~ reflects advances in digital technology~~. It also~~ 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 requirements to supplement the criteria and requirements ~~of IEEE Std. 603-1998~~which are endorsed by RG 1.152.

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~~NRC staff will review the interconnected systems and equipment to determine 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~~NRC staff will review the control of access requirements to ensure reliable performance of the safety function.

D.12.4 Technical Evaluation

Comment [A188]: Comment No. 175.

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 ~~are~~ is the ~~documents~~information that should be provided in support of the secure environment. It is recognized that every applicant may have a different name for the same document. In addition, it is conceivable that some of the applicants may address some of the documentation needs in another software related document. While including the secure environment requirements within another document is acceptable, the applicants 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

Identify 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 (~~non-malicious~~unintended) inadvertent access to the system and to protect the reliable operation of the system from undesired behavior from connected systems.

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 ~~non-malicious~~unitended actions are to be considered as part of the vulnerability assessment. These actions may be caused by operator error, inadvertent operator access to the system, ~~unintended~~ 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 requirements identified during this phase. These secure operational environment requirements may be included with the platform and/or application software requirements document (with a specific section devoted to secure environment).

Activities involved with the development of requirements to preclude introduction of unwanted or unneeded requirements 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, requirements 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 requirements 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 design 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 requirements 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 will be determined during the licensing review.

D.12.5 Conclusion

Comment [A189]: Comment No. 176.

The NRC staff will review the requested information to determine that the system and software designed and tested are controlled against identified vulnerabilities and that the overall design, development controls, and testing provide a reasonable assurance that the system 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. The staff reserves the right to review and audit any of the documentation and/or testing to reach a conclusion of reasonable assurance that the digital safety system was developed in a secure environment and that it will be protected in 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] will 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 require 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 ~~Tier 2~~ 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 will obviously require 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~~, D.10.4.2.3.3, D.10.4.2.3.4~~)
1.10	X	X	X	Software Configuration Management Plan (D.4.4.1.11~~, D.10.4.2.3.5~~)
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	~~Digital~~ 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				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, D.10)
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	~~Digital~~ 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.12.4.2, D12.4.3, D12.4.4, D12.4.5)

Comment [A190]: The following changes were made to this section: Re-ordered to make in order of occurrence within this ISG.

Comment [A191]: Previously there were three requirements specifications listed: "System," "Platform Software," and "Application Software." Since all three specifications pointed to the same information to be provided, within the body of this ISG, they were combined into one reference.

Comment [A192]: Comment No. 177.

	Tier			Submitted 12 months prior to requested approval (Phase 2)
	1	2	3	
2.1	X	X	X	Safety Analysis~~ – Implementation & Test Phases~~ (D.4.4.2.1)
2.2	X	X	X	V&V Reports~~ – Implementation & Test Phases~~ (D.4.4.2.2~~, D.10.4.2.3.3, D.10.4.2.3.4~~)
2.3	X	X	X	Requirement Traceability Matrix (~~D.4.4.2.2,~~ D.4.4.2.5)
2.4	X	X	X	Test Design Specification (D.4.4.2.4~~, D.10.4.2.4.1~~)
2.5	X	X	X	Summary ~~Factory Acceptance~~ Test Reports (Including FAT) (D.4.4.2.4~~, D.10.4.2.4.1~~)
2.6	X	X	X	Summary of Test Results (Including FAT) (D.4.4.2.4~~, D.10.4.2.4.1~~)
2.7		X	X	FMEA (D.4.4.2.6, D.9.4.2.1)
2.8	X	X	X	~~As-Manufactured~~ System Build Documents (D.4.4.3.5)
2.9		X	X	~~As-Manufactured,~~ Configuration Tables (D.4.4.3.6)
2.10		X	X	Summary of Final Digital EMI, Temp., Humidity, and Seismic Testing Results (D.5.2)
2.11	X	X	X	As-Manufactured Logic Diagrams (D.9.2)
2.12	X	X	X	System Response Time Confirmation Report (D.9.4.2.4)
2.13	X	X	X	Reliability Analysis (D.9.4.2.15, D.10.4.2.15)
2.14	X	X	X	Setpoint Calculations (D.9.4.3.8)
2.15		X	X	Software Tool Analysis Report (D.10.4.2.3.2)
2.16	X	X	X	As-Manufactured, System Configuration Documentation (D.4.4.2.3~~D.10.4.2.3.5~~)
~~2.17~~	~~X~~	~~X~~	~~X~~	~~Final Report on Acceptance of Digital Commercial Grade Dedication (D.10.4.2.4.2)~~
2.17		X	X	~~Digital~~ Commercial Grade Dedication Report(s) ~~(If not completed at time of application)~~ (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	Configuration Management Reports (D.4.4.2.3~~, D.10.4.2.3.5~~)
3.2	X	X	X	Test Procedure Specification (D.4.4.2.4~~, D.10.4.2.4.1~~)
3.3	X	X	X	Completed Test Procedures and Reports (D.4.4.2.4, D.5.2~~, D.10.4.2.4.1~~)
3.4	X	X	X	Test Incident Reports (D.4.4.2.4~~, D.10.4.2.4.1~~)
3.5	X	X	X	Code Listings (D.4.4.3.4)
~~3.6~~	~~X~~	~~X~~	~~X~~	~~Miscellaneous Equipment – Qualification Documentation (D.5.2)~~
3.7	X	X	X	Software Project Risk Management Report (D.10.4.2.3.6)
3.8		X	X	Miscellaneous Commercial Grade Dedication Report (D.10.4.2.4.2)
3.9	X	X	X	Final Circuit Schematics
3.10	X	X	X	Final Software Integration Report (D.4.4.1.4, D.4.4.2.2)
3.11	X	X	X	Detailed System and Hardware Drawings
3.12	X	X	X	Individual V&V Problem Reports up to FAT (D.4.4.2.2)

Comment [A193]: This list went from 20 to 21 items.

Comment [A194]: Moved from Phase1 to Phase 2 in order to address industry comments.

Comment No 179.

Comment [A195]: The former item was "Final Factory Acceptance Test Reports (D.9.2)." This item was changed since other testing (besides FAT) may be credited for demonstrating criteria have been met.

Comment [A196]: The Item 'Configuration List" was combined with "Configuration Tables" since BTP 7-14 does not describe "Configuration Lists" and does describe configuration tables. Section D.4 primarily addresses the items in BTP7-14.

Comment [A197]: Comment No. 180.

Comment [A198]: Formally was "System Test Procedures (D.10.4.2.4.1)" and "Software Test Procedures (D.10.4.2.4.1)." The term "Specification" was added to address industry comment and align the terminology with the RG on software test documentation.

Comment [A199]: Was formally "Completed Factory Acceptance Test Procedure and Results," and "Individual Completed Test Procedures and Reports," which were combined.

	Tier			Available for Inspection After Approval (Phase 3)
	1	2	3	
4.1	X	X	X	Software Installation Plan (D.4.4.1.5)
4.2	X	X	X	Software Maintenance Plan (D.4.4.1.6)
4.3	X	X	X	Software Training Plan (D.4.4.1.7)
4.4	X	X	X	Software Operations Plan (D.4.4.1.8)
4.5	X	X	X	Site Test Documentation (D.4.4.2.4~~, D.10.4.2.4.1~~)
4.6	X	X	X	Operations Manual (D.4.4.3.7)
4.7	X	X	X	Software Maintenance Manuals (D.4.4.3.7)
4.8	X	X	X	Software Training Manuals (D.4.4.3.8)

Comment [A200]: Table added per industry comments.

Comment [A201]: Moved to a region inspection item per Oconee RPS/ESPS LAR precedent.

Comment [A202]: Moved to a region inspection item per Oconee RPS/ESPS LAR precedent.

Comment No. 178.

Comment [A203]: Moved to a region inspection item per Oconee RPS/ESPS LAR precedent.

Comment [A204]: Moved to a region inspection item per Oconee RPS/ESPS LAR precedent.

Comment [A205]: Moved to a region inspection item per Oconee RPS/ESPS LAR precedent.

Comment [A206]: Moved to a region inspection item per Oconee RPS/ESPS LAR precedent.

Comment [A207]: Moved to a region inspection item per Oconee RPS/ESPS LAR precedent.

Enclosure C

Digital I&C Licensing Process

Flow Chart

FIGURE 1, “Process Flow Chart”

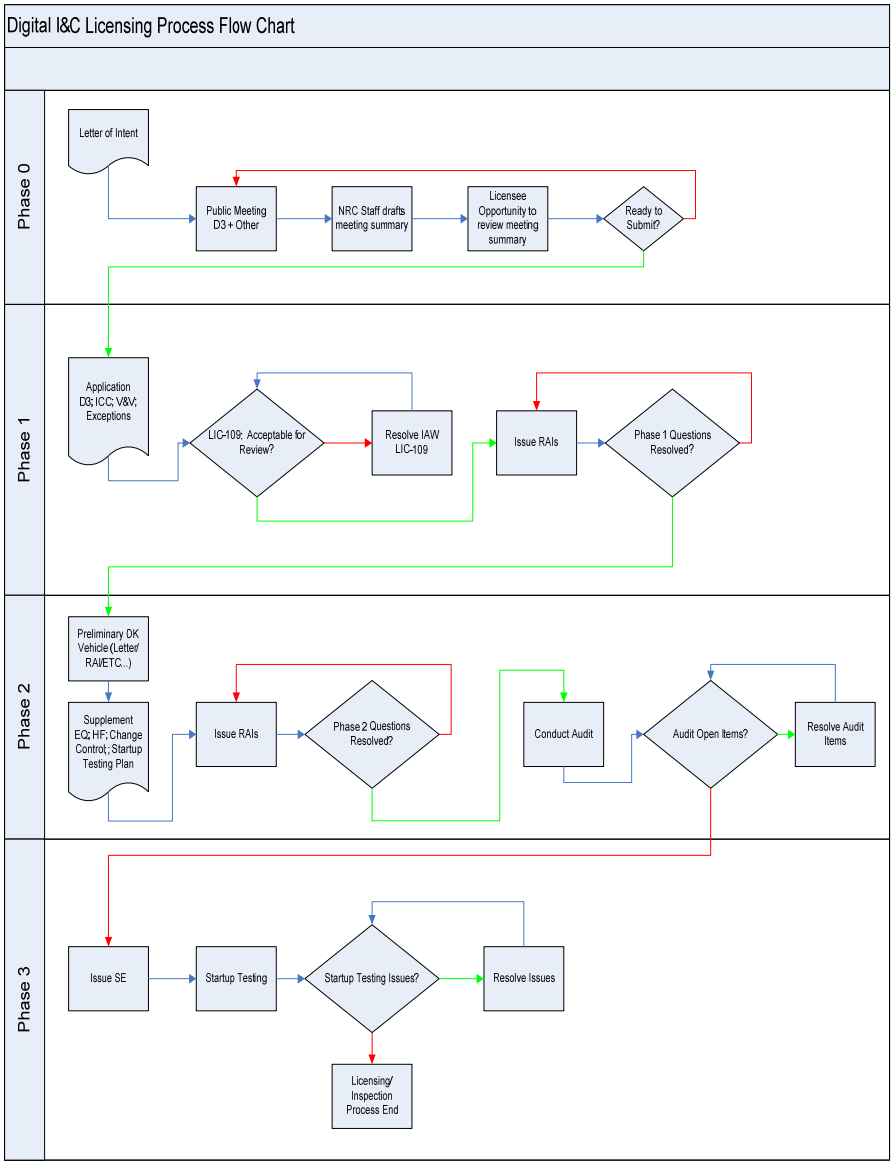

FIGURE 1, "Process Flow Chart"

Enclosure D

Sample Safety Evaluation for Digital I&C License Amendment

Comment [A208]: The sample SE was re-ordered to more closely align with the Oconee RPS/ESPS LAR.

Note: This is only a sample of what the final Safety Evaluation Report may be. Since each digital system is somewhat different and each presents unique challenges to the review process, each SE will be unique and any particular SE will 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
3.4.2.5 Traceability Matrix 7
3.4.2.5.1 Thread Audit of source Code Listings (CL) 7
3.4.2.6 FMEA 8
3.4.3 Software Design Outputs 8
3.4.3.1 Software Requirements Specification 8
3.4.3.2 Software Architecture Description 8
3.4.3.3 Software Design Description (or Software Design Specification) 8
3.4.3.4 Software Design Review 8
3.4.3.5 System Build Documents (SBD) 8
3.4.3.6 Configuration Tables 8
3.5 System Qualifications 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 9
3.5.1.5 Electromagnetic Interference/Radio Frequency Interference 9
3.5.1.6 Seismic Qualification 9
3.5.2 Power Quality requirements 9
3.5.3 Response time characteristics and testing requirements 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 ... 10
3.8 System, Hardware, Software and Methodology Modifications ... 10
3.9 Review of System and IEEE 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 ... 11
3.9.1.9 Clause 4.9 methods used to determine ... 11
3.9.2 Clause 5. System ... 11
3.9.2.1 Clause 5.1 Single-Failure Criterion ... 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 ... 11
3.9.2.10 Clause 5.10 Repair ... 11
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 ... 12
3.9.3.7 Clauses 6.7 Maintenance Bypass ... 12
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 Requirements 13
3.10 Review IEEE 7-4.3.2 Requirements 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 13
3.10.1.1.2 Clause 5.3.2 Software Tools 13
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) Requirements 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
3.10.1.3 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 14
3.10.1.4 Clause 5.6 Independence 14
3.10.1.5 Clause 5.7 Capability for Test and Calibration 14
3.10.1.6 Clause 5.8 Information Displays 14
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 Environment 15
4.0 NRC FINDINGS 15
4.1 Summary of Regulatory Compliance 15
4.2 Limitations and Conditions 15
5.0 CONCLUSION 15
6.0 REFERENCES 15

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 completed 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.

3.4.2.5 Traceability Matrix

Read DI&C-ISG-06 Section D.4.4.2.5, "Requirements Traceability Matrix"

3.4.2.5.1 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 require the assistance of other NRC personnel or independent contractor personnel to make this determination.

3.4.2.6 FMEA

Read DI&C-ISG-06 Section D.4.4.2.6, "Failure Modes and Effects Analysis"

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 System Build Documents (SBD)

Read DI&C-ISG-06 Section D.4.4.3.5, "System Build Documents"

3.4.3.6 ~~Installation~~ Configuration Tables

Read DI&C-ISG-06 Section D.4.4.3.6, "~~Installation~~ Configuration Tables"

3.5 System Qualifications

Read DI&C-ISG-06 Section D.5, "System Qualifications"

3.5.1 Environmental Qualification of System

Comment [A209]: Comment No. 181, 182.

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 required 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 requirements

3.5.3 Response time characteristics and testing requirements

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~~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 603 requirements

Read DI&C-ISG-06 Section D.9, "IEEE 603, Compliance"

3.9.1 Clause 4. Design Basis

Read DI&C-ISG-06 Section D.9.4.1, "IEEE 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 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 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 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 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 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 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 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 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 603, Clause 4.9…"

3.9.2 Clause 5. System

Read DI&C-ISG-06 Section D.9.4.2, "IEEE 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 603, Clause 5.1…"

3.9.2.2 Clause 5.2 Completion of Protective Action

Read DI&C-ISG-06 Section D.9.4.2.2, "IEEE 603, Clause 5.2…"

3.9.2.3 Clause 5.3 Quality

Read DI&C-ISG-06 Section D.9.4.2.3, "IEEE 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 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 603, Clause 5.5…"

3.9.2.6 Clause 5.6 Independence

Read DI&C-ISG-06 Section D.9.4.2.6, "IEEE 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 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 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 603, Clause 5.9…"

3.9.2.10 Clause 5.10 Repair

Read DI&C-ISG-06 Section D.9.4.2.10, "IEEE 603, Clause 5.10"

3.9.2.11 Clause 5.11 Identification

Read DI&C-ISG-06 Section D.9.4.2.11, "IEEE 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 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 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 603, Clause 5.14…"

3.9.2.15 Clause 5.15 - Reliability

Read DI&C-ISG-06 Section D.9.4.2.15, "IEEE 603, Clause 5.15…"

3.9.3 Clauses 6. - Sense and Command Features

Read DI&C-ISG-06 Section D.9.4.3, "IEEE 603, Clause 6…"

3.9.3.1 Clause 6.1 - Automatic Control

Read DI&C-ISG-06 Section D.9.4.3.1, "IEEE 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 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 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 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 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 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 603, Clause 6.7…"

3.9.3.8 Clause 6.8 Setpoints

Read DI&C-ISG-06 Section D.9.4.3.8, "IEEE 603, Clause 6.8…"

3.9.4 Clause 7 - Execute Features

Read DI&C-ISG-06 Section D.9.4.4, "IEEE 603, Clause 7…"

3.9.4.1 Clause 7.1- Automatic Control

Read DI&C-ISG-06 Section D.9.4.4.1, "IEEE 603, Clause 7.1…"

3.9.4.2 Manual Control

Read DI&C-ISG-06 Section D.9.4.4.2, "IEEE 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 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 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 603, Clause 7.5…"

3.9.5 Clause 8 Power Source Requirements

Read DI&C-ISG-06 Section D.9.4.5, "IEEE 603, Clause 8"

3.10 Review IEEE 7-4.3.2 Requirements

Read DI&C-ISG-06 Section D.10 "IEEE 7-4.3.2 Guidance"

3.10.1 Clause 5. System

Read DI&C-ISG-06 Section D.10.4.2 "IEEE 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 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 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 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 7-4.3.2, Clause 5.3.3…"

3.10.1.1.4 Clause 5.3.4 Independent V&V (IV&V) Requirements

Read DI&C-ISG-06 Section D.10.4.2.3.4 "IEEE 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 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 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 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 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 7-4.3.2, Clause 5.4.2, Qualification of Existing Commercial Computers"

3.10.1.3 Clause 5.5 System Integrity

Read DI&C-ISG-06 Section D.10.4.2.5 "IEEE 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 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 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 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 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 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 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 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 will 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 requirement currently says:

[Quote the old section exactly]

The new requirement 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 will 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 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)

Comment [A210]: The Sample LAR TOC was re-ordered to more closely align with the body of this ISG and the Oconee RPS/ESPS 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 will 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)

Comment [A211]: Comment No. 183.

4.5 System 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 Conformance 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 an applicant explicitly redefines a term, and explicitly states that the applicant-defined definition supersedes that in the guidance document.

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 requirements are concerned with what the application software must do in the context of the NPP application, and how the software will interact with the remainder of the application. These requirements come from the system requirements, and reflect the requirements 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-system 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 required behavior of each, and how they work together to accomplish the various application-system functions. It is expected that this architecture description include both text and diagrams.

As-Built: The state of the system after installation and any 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 will 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 ~~Factory Acceptance Test~~ Procedures and ~~Results~~Reports: The documentation of the ~~factory acceptance~~ testing.

Configuration Management Reports: A report that documents the configuration.

Configuration Tables: Real-time systems frequently require 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.

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 an DI&C-ISG-06 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.4.4.2.6.

Reliability Analysis Report: A reliability analysis provides sufficient detail to support and justify that the system meets the reliability requirements.

Design Report on Computer Integrity, Test and Calibration, and Fault Detection:

Detailed System and Hardware Drawings: The detailed design drawings of the system.

Electronic Block Diagram: An electronic block diagram gives a basic overview of how the main circuits within a device interact. Each block is assumed 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 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 exists." An FMEA is one way that the staff has excepted 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 propose an application specific architecture.

Final System Configuration Documentation: The documentation that describes the configuration of the system that is to be installed at the NPP (application specific).

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 required 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.

Formatted: Font: Not Bold

Comment [A212]: Comment No. 27.

Text moved here from Section D.1.2.

Formatted: Font: Not Bold

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. ~~A hazard is a condition that is prerequisite to an accident. Hazards include external events as well as conditions internal to computer hardware or software. The software and hardware safety plan addresses the identification, evaluation and resolution of hazards. Hazard analysis is the process that explores and identifies conditions that are not identified by the normal design review and testing process.~~ (per IEEE 1012-1998 Clause 3.1.7, See also Software Hazard Analysis)

~~**Individual Completed Test Procedures and Reports:** The documentation of the testing performed in accordance with each test procedure.~~

Individual V&V Problem Reports up to FAT: It is expected that V&V will identify some problems that must be addressed. The individual V&V problem reports are the documentation of the individual problems and associated resolutions.

Configuration Tables: Real-time systems frequently require 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

NPP: Nuclear Power Plant

Layout Diagram: See "Pictorial Diagram"

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 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 requirements are concerned with what the platform software must do in support of the application, and how the platform software will 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 to provide reasonable assurance that the regulatory requirements of : 10CCFR 50.55a(a)(1) and IEEE Std 603-1991 Clause 5.4, Quality," are met. NUREG-0800, dated March 2007, 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 603-1991 Clause 5.4, "Equipment Qualification," IEEE 279-1971 Clause 4.4, "Equipment Qualification," or various GDCs associated with equipment qualification.

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 required 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 requirements.

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 requirement, broken down in to sub-requirements 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 requirement, should be broken down in to sub-requirements as necessary. The RTM should show what portion of the software requirement, software design description, actual code, and test requirement addresses each system requirement.

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 required 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 final 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 (as described elsewhere). 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 will 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 final 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 final 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 will 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 required in order to perform the technical activities will be identified.

Comment [A213]: Per comment No. 44, SPM changed to SMP.

Comment [A214]: Comment No. 45.

Without a development plan, there is likely to be confusion about when the various technical development activities will take place and how they will 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 required 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.

Comment [A215]: Comment No. 74.

~~(NUREG/CR-6430, "Software Safety Hazard Analysis", describes a method for performing a software hazards analysis.)~~

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 will describe the ~~general procedures~~process for installing the software product. For any particular installation, modifications, or additions may be required to account for local conditions. 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 actually 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 final 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 required at some levels.

Without a Software Integration Plan, it is possible that the complete 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

Comment [A216]: Comment No. 52.

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. 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.

Comment [A217]: Comment No. 55.

Comment [A218]: Comment No. 56.

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 ~~procedures~~ processes are required 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 entire 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 misassignment 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.

Comment [A219]: Comment No. 39.

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 requirements. 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 will be assured by the development organization. There will be considerable overlap between the SQAP and the other project plans. The SQAP will 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 will 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 many 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 will 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 required 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, Section 3.1.5 “Software Safety Plan,” and Section 4.1.5 “Software Safety Plan.”

Per RG 1.73 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.

~~**Test:** Per RG 1.170 See IEEE Std 829-1983 Section 2, “Definitions”:~~
~~(1) a set of one or more test cases, or~~
~~(2) a set of one or more test procedures, or~~
~~(3) a set of one or more test cases and procedures.~~

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 required 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 required 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 requirements 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, R~~r~~egulatory 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 ~~identify~~ desscribe 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 will describe the methods that will be used to train the users of the software system. In this case, users will need to be trained in use of the safety system software. It is also possible that training will be required for managers and for maintenance personnel. The actual training requirements depend to a great extent on the actual software product, development organization, maintenance organization, and customer (utility).

Comment [A220]: Comment No. 60.

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 requirements and products of the previous phase. Validation is the process that compares the final 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 final 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 final software system is a correct implementation of the requirements 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

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 bet, 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 requires investigation.

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 will 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.

V&V Reports: Reports documenting the V&V activities.

Vendor Build Documentation: See SRP Chapter 7 BTP 7-14 Section B.3.3.5