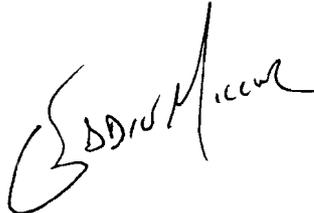




UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

February 16, 2010

MEMORANDUM TO: Lois M. James, Chief
Probabilistic Risk Assessment Op Support Branch
Division of Risk Assessment
Office of Nuclear Reactor Regulation

FROM: G. Edward Miller, Project Manager
Plant Licensing Branch I-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation 

SUBJECT: NOTICE OF PUBLIC MEETINGS OF THE DIGITAL
INSTRUMENTATION AND CONTROL (I&C) TASK WORKING GROUP
NO. 6 TO ADDRESS DEVELOPMENT OF DIGITAL I&C LICENSING
GUIDANCE

DATES & TIMES: Wednesday, March 24, 2010
10:00 a.m. - 4:00 p.m.

LOCATIONS: U.S. Nuclear Regulatory Commission
One White Flint North, Room 7-B4
11555 Rockville Pike
Rockville, MD 20852

PURPOSE: The Nuclear Regulatory Commission (NRC) staff is convening this meeting with the Nuclear Energy Institute (NEI) to discuss the development of interim staff guidance on the licensing of digital I&C safety systems for operating nuclear plants. A copy of this document is enclosed with this notice.

CATEGORY 2:* This is a Category 2 public meeting. The public is invited to participate in this meeting by providing comments and asking questions at a designated point during the meeting. There may be limited space at the meeting location, and interested members of the public are encouraged to participate in this meeting via a toll-free teleconference. For details, please email the NRC meeting contact by Monday, March 22, 2010.

CONTACT: G. Edward Miller, NRR
301-415-2481
Ed.Miller@nrc.gov

* Commission's Policy Statement on "Enhancing Public Participation in NRC Meetings" (67 FR 36920), May 28, 2002.

PARTICIPANTS: Participants from the NRC include members of the Office of Nuclear Reactor Regulation (NRR).

NRC

W. Kemper, NRR
L. James, NRR
E. Miller, NRR

Industry

G. Clefton, NEI

The NRC provides reasonable accommodation to individuals with disabilities where appropriate. If you need a reasonable accommodation to participate in a meeting, or need a meeting notice or a transcript or other information from a meeting in another format (e.g., Braille, large print), please notify the NRC's meeting contact. Determinations on requests for reasonable accommodation will be made on a case-by-case basis.

Project No. 689

Enclosures:

1. Agenda
2. Draft Interim Staff Guidance 6

cc w/encl: See next page

cc:

Mr. Anthony Pietrangelo, Vice President
Regulatory Affairs
Nuclear Energy Institute
1776 I Street, NW, Suite 400
Washington, DC 20006-3708
arp@nei.org

Mr. Alexander Marion, Executive Director
Nuclear Operations & Engineering
Nuclear Energy Institute
1776 I Street, NW, Suite 400
Washington, DC 20006-3708
am@nei.org

Mr. Jack Roe, Director
Operations Support
Nuclear Energy Institute
1776 I Street, NW, Suite 400
Washington, DC 20006-3708
jwr@nei.org

Mr. John Butler, Director
Safety-Focused Regulation
Nuclear Energy Institute
1776 I Street, NW, Suite 400
Washington, DC 20006-3708
jcb@nei.org

Mr. Charles B. Brinkman
Washington Operations
ABB-Combustion Engineering, Inc.
12300 Twinbrook Parkway, Suite 330
Rockville, MD 20852
brinkmcb@westinghouse.com

Mr. Gordon Clefton, Sr. Project Manager,
Nuclear Energy Institute
1776 I Street, NW, Suite 400
Washington, DC 20006-3708
gac@nei.org

Mr. Dave Modeen, Vice President,
Nuclear Power Sector
Electric Power Research Institute
2000 L Street, NW, Suite 805
Washington, DC 20036
gvine@epri.com

Mr. James Riley, Director, Engineering,
Nuclear Energy Institute
1776 I Street, NW, Suite 400
Washington, DC 20006-3708
jhr@nei.org

Mr. James Gresham, Manager
Regulatory Compliance and Plant Licensing
Westinghouse Electric Company
P.O. Box 355
Pittsburgh, PA 15230-0355
greshaja@westinghouse.com

Ms. Barbara Lewis
Assistant Editor
Platts, Principal Editorial Office
1200 G St., N.W., Suite 1100
Washington, DC 20005
Barbara_lewis@platts.com

AGENDA
FORTHCOMING PUBLIC MEETING
DIGITAL INSTRUMENTATION AND CONTROL (I&C) TASK WORKING GROUP NO. 6
DEVELOPMENT OF LICENSING PROCESS GUIDANCE
March 24, 2010, 10:00 a.m. - 4:00 p.m.

10:00 a.m. - 10:15 a.m.	Introduction of Participants and Opening Remarks
10:15 a.m. - 10:30 a.m.	Presentation of Status and Path Forward
10:30 a.m. - 11:00 a.m.	Opening Remarks From NEI and Presentation of Comments
11:00 a.m. - 12:00 p.m.	Discussion of Comments
12:00 p.m. - 1:00 p.m.	Break for Lunch
1:00 p.m. - 2:30 p.m.	Continuation of Discussion
2:30 p.m. - 2:45 p.m.	Break
2:45 p.m. - 3:30 p.m.	Continuation of Discussion
3:30 p.m. - 4:00 p.m.	Public Comments



DIGITAL INSTRUMENTATION AND CONTROLS
DI&C-ISG-06

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

Interim Staff Guidance

(Initial Issue for Use)

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 systems in accordance with current licensing processes. This ISG also informs licensees of the information and documentation the NRC staff will need for its review of LARs for digital I&C upgrades and when the information should be provided. Review of this document should allow licensees to prepare digital I&C upgrade applications that are complete with respect to the areas that are within the NRC staff's 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 upgrades against the design basis of the plant and the guidance in the Standard Review Plan (NUREG-0800), Chapter 7, and other associated guidance including ISGs. Licensees should provide a discussion of the licensing basis for the plant, focusing these efforts on areas where the licensing basis differs from current guidance. Additionally, licensees should clearly identify those parts of the licensing basis they are updating as a result of the proposed change.

B.1 Background

The NRC oversight includes two 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) Inspections¹ are most appropriate where critical characteristics can be verified.
- (2) Reviews are most appropriate where an evaluation (by an evaluator that has specific technical expertise) is required.

The SRP (NUREG-0800) 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. 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 process's which describes 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 actually used during the design of the software under review, with the intent of determining that the process described is the process that was used, and that the process was used 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. 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 High Quality Process is a Critical Characteristic of Software

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.

This bimodal approach is 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.

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

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."

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.”

It is generally accepted in the software industry that no non-trivial software can be completely tested (or be bug free), which means that (by strict interpretation) the critical characteristics of software cannot be verified. The result would be that no commercially developed software could be used in any safety related application, but that software developed under a quality assurance program could be. To reconcile this apparent contradiction, the NRC staff 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 a quality assurance program.

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 and early site permit (ESP), design certification (DC), combined license (COL), standard design approval (SDA), or manufacturing license (ML) applications under 10 CFR Part 52 (including requests for amendments).

The principal purpose of the SRP is to assure the quality and uniformity of staff safety 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 SRP was originally written for 10 CFR Part 50 license applications. For DC and COL applications submitted under 10 CFR Part 52, the level of design information reviewed should be consistent with that of a final safety analysis report (FSAR) submitted in an OL application. However, verification that the as-built facility conforms to the approved design is performed through the inspections, tests, analyses, and acceptance criteria (ITACC) verification 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 to be submitted in a License Amendment Request (LAR) that seeks to install a digital I&C safety system.

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.

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 are contained in Enclosure B, column 1. This list would not include those documents already reviewed and approved by the NRC staff.

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 tier two review are contained in Enclosure B, column 2, however it should be noted that for any particular submittal, the actual list of documents needed will be determined by the changes from the previously approved topical report.

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 are contained in Enclosure B, column 3.

It should be noted that the lists provided in Enclosure B provide a high-level concept of the documents that are typically needed for verifying regulatory compliance. 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. It should be noted that not all of the review areas directly address meeting regulatory requirements, instead,

some lay the groundwork for evaluating the criteria of others. As an example, the “Hardware description” and “Hardware Design Process and Quality Control” review areas do not have specific regulatory criteria to be met, nor do they come directly from a regulatory requirement (other than the basic requirement to adequately describe and justify a proposed change). Instead, they discuss the level of detail to which the licensee should describe the system and supporting development, maintenance, and operation programs. 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 operator 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.

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. It should be noted that 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:

- Hardware Architecture (Section D.1)
- Hardware Design Process (Section D.2)
- Software Architecture (Section D.3)
- Software Design Process (Section D.4)
- System 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 Compliance (Section D.10)
- Technical Specifications (Section D.11)
- System and Software Security (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 issue requests for additional information (RAI) based on the initial LAR as necessary to continue the review. 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 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 licensee should be aware that some information needs may be best met by documentation available at site (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.

It should be noted that 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).

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 (e.g., of documents listed in Enclosure B, table of documents to be available for audit 12 months prior requested approval date), in accordance with LIC-111, "Regulatory Audits" (Note: This document is not publically available).

Any audits (e.g., of completed factory acceptance test procedure and results, configuration management reports, detailed system and hardware drawings, final circuit schematics, final software integration report, individual completed test procedures and reports, Individual V&V problem reports up to FAT, software code listings, and vendor build documentation) 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 (e.g., V&V and factory acceptance testing). 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.

It should be noted that some documentation (e.g., factory acceptance testing results) may not be available 12 months prior to the anticipated issuance of the amendment. Although the plans and other available information should be submitted as early as possible, it is acceptable to submit the results when available but prior to the SER.

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 SER 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, effecting associated procedural and technical specification changes, and completing startup testing.

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 Hardware Architecture

D.1.1 Scope of Review

Reviewing the hardware architecture of the digital I&C system allows the NRC staff to understand how the high-level functional units 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.

D.1.2 Information to be Provided

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:

Hardware Architecture Description²

It should be noted that Enclosure B is only an example list and an applicant may have different names for similar documents. The licensee's submittal should provide sufficient documentation and description to allow the NRC staff to identify what hardware is being used in this application, how the hardware items function, how the various hardware items are interconnected, and any software which runs on that hardware. The 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. Any deviations or revision changes should be identified and adequately justified.

² The Hardware Architecture Description is 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 (e.g., nineteen inch rack and associated sub-racks), 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.

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 also be reviewed in detail by Section D.7, "Communications."

The information the staff will need to understand the system hardware architecture should be contained in the system description, hardware architecture description, theory of operations description, systems requirements specification, and design analysis report.

These descriptions will allow the NRC staff to conceptualize and adequately document the hardware 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.1.3 Regulatory Evaluation

The licensee's description of the hardware and hardware architecture will be documented in the NRC staff's SE to explain system operation, demonstrate a high quality product, support a determination of channel or division independence, and as supporting information to other review areas.

D.1.4 Technical Evaluation

The NRC staff will provide a description of the hardware 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.1.5 Conclusion

The NRC staff will use the RAI process to fulfill informational needs related to understanding the hardware architecture of the digital I&C system. Additionally, the NRC staff will communicate, via the RAI process when these needs have been satisfied.

D.2 Hardware Design 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 design process used during the design 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

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:

Quality Assurance Plan for Digital Hardware³

It should be noted that Enclosure B is only an example list and an applicant may have different names for similar documents. 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.

This information would typically be in the quality assurance plans and reports, commercial grade dedication plans and reports (if commercial grade dedication is used), the system description, hardware architecture description, theory of operations description, detailed system and hardware drawings, final circuit schematics, vendor build documentation, and the systems and hardware requirements specification.

D.2.3 Regulatory Evaluation

The pertinent aspects of the licensee's description of the hardware design process and quality control will be documented in the NRC staff's safety evaluation as a demonstration of a high quality design process and as supporting information to other review areas.

D.2.4 Technical Evaluation

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 use the RAI process to fulfill informational needs related to understanding the hardware design process and quality control of the digital I&C system. Additionally, the NRC staff will communicate, via the RAI process when these needs have been satisfied.

³ 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.

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.

It is important to note that some digital technologies, such as a field-programmable gate array (FPGA), do not utilize software while the system is in operation. Instead, these systems use software to generate a hardware layout to be implemented in the FPGA. In these situations, the NRC staff's scope of review will include the software (including all aspects of the life-cycle) used to generate, implement, and maintain the hardware logical functions.

D.3.2 Information to be Provided

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:

Software Architecture Descriptions⁴

It should be noted that Enclosure B is only an example list and an applicant may have different names for similar documents. 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, "Hardware 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).

⁴ The Software Architecture Description is 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.

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

The licensee's description of the software and software architecture will be documented in the NRC staff's SE to explain system operation, demonstrate a high quality product, support a determination of channel or division independence, and as supporting information to other review areas.

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 use the RAI process to fulfill informational needs related to understanding the hardware architecture of the digital I&C system. Additionally, the NRC staff will communicate, via the RAI process when these needs have been satisfied.

D.4 Software Design Processes

There may be several design 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.

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 design process review area, the NRC staff reviews the failure modes and effects analysis (FMEA). The FMEA is a method of analysis of potential hardware or programming failure modes within a system for determination of the effect of failures on the system. This information can then be used to assess the potential for an undetectable failure or a common mode failure.

D.4.2 Information to be Provided

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example⁵:

- Software Management Plan
- Software Development Plan
- Software Quality Assurance Plan
- Software Integration Plan
- Software Installation Plan
- Software Maintenance Plan
- Software Training Plan
- Software Operations Plan
- Software Safety Plan
- Software Verification and Validation Plan
- Requirements Traceability Matrix
- Software Configuration Management Plan
- Software Test Plan
- System Requirements Specification
- Platform Software Requirements Specification
- Application Software Requirements Specification
- Software Design Specification
- System Build Documents
- Configuration Lists
- Configuration Tables
- FMEA

It should be noted that Enclosure B is only an example list and an applicant may have different names for similar documents. 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.

⁵ The documents listed below will be described in the individual sections where they are used for the first time.

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."

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 1012-1998, "IEEE Standard for Software Verification 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 Management Plan (SMP)

SRP BTP 7-14, in Section B.3.1.1, provides acceptance criteria for a software management plan⁶. 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, and retirement. These requirements are applied to both licensee and vendor programs.

⁶ 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 SPMP, 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.

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 (see SRP BTP 7-14, in Section B.3.1.1), 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 groups that check the quality of both the software development program and the software itself. Generally, these are the quality assurance organization, the software safety organization, and the software verification and validation organization. It is important that these groups maintain independence from the development organization, by both organization and function. The independence of the quality assurance organization, the software safety organization, and the software verification and validation organization should be described in terms of management, schedule, and finance. If these independence aspects are described in the planning documents of these organizations, such as the V&V Plan, Safety Plan or QA plan, the SMP should provide a pointer to the appropriate section of those plans.

The NRC staff may review the responsibilities of each position of the project's management and technical teams. The review 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 security requirements for the reviewer to determine that the methods used are consistent with Regulatory Guide 1.152 and that the methods are used effectively. This needs to be an actual description of the security requirements enumerated in RG 1.152, and not just a statement that all security 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.

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.4.4.2 Software Development Plan (SDP)

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

The acceptance criteria for a software development plan⁷ 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 (SCMP0, and so forth, and 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 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, compilers, 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

⁷ 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 SPM. The SPM 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 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.

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.

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.

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 be compared to the suggestions contained in NUREG/CR-6463, "Review Guidance for Software languages for Use in Nuclear Power Plant Safety Systems," and any deviations should be justified.

D.4.4.3 Software Quality Assurance Plan (SQAP)

Quality Assurance is required by 10 CFR Part 50, Appendix B, and the Software Quality Assurance Plan⁸ 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,"

⁸ 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 may not be mutually consistent, and that some aspects of software quality that are important to safety may be overlooked.

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 SQP 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.

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. IEEE Std 1028-1998 can be used as guidance.

D.4.4.4 Software Integration Plan (SIntP)

The acceptance criteria for a software integration plan⁹ 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.

⁹ 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.

While the Software Integration Plan is not as critical as some of the other plans, the staff may still review or audit (e.g., final software integration report) 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.4.4.5 Software Installation Plan (SInstP)

The acceptance criteria for a software installation plan¹⁰ are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.5, "Software Installation Plan." This section states that Regulatory Guide 1.173, endorses IEEE Std 1074-1995, and that Clause 6.1.3 of that standard, "Plan Installation," contains an acceptable approach relating to planning for installation. This clause states that an installation plan describe the tasks to be performed during installation, and shall include the required hardware and other constraints, detailed instructions for the installer, and any additional steps that are required prior to the operation of the system . Further guidance is provided in NUREG/CR-6101, Section 3.1.8, "Software Installation Plan," and Section 4.1.8, "Software Installation Plan," which contains a sample outline of an installation plan.

The critical part of the software installation is the system test (Note: Per IEEE Std 1012-1998, Final System testing is considered a V&V test and is the responsibility of the V&V group).

¹⁰ 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 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.

There should be written and approved procedures for software installation, for combined hardware/software installation, and systems installation. The SIP should include the method by which these errors are identified, corrected, and documented, and should confirm that these corrections are subject to the same quality and configuration control as the rest of the system.

D.4.4.6 Software Maintenance Plan (SMaintP)

The acceptance criteria for a software maintenance plan¹¹ are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.6, "Software Maintenance Plan." This section states that NUREG/CR-6101, Section 3.1.9, "Software Maintenance Plan," and Section 4.1.9, "Software Maintenance Plan," contain guidance on software maintenance plans. These sections break the maintenance into three activities, failure reporting, fault correction, and re-release.

The Software Maintenance Plan is important because software maintenance is often done after the system has been delivered, installed, accepted, and has been in use for a period of time. By this time, the software development team may have moved on to other projects or other jobs and the knowledge of how the software works and what it does may be limited to its documentation. In addition, software maintenance is often done when the software has failed for some reason. Thus, the Software Maintenance Plan should clearly document the same careful and deliberate methods that other plans require and which management controls are in place to implement them.

The Software Maintenance Plan, together with the Software Configuration Management Plan (SCMP), defines what records are kept and who controls those records. If the software is to be modified, it is critical to ensure that the right version of the software undergoes that modification. The methods for testing modifications are also critical. The plan should document what controls are in place to ensure that implementing a change does not inadvertently introduce other errors. The regression testing requirements should be described in sufficient detail for the staff to be able to determine that all the acceptance tests originally performed, or a carefully selected and justified subset, will be used to ensure that no new errors have been created. The SCMP should also describe the review process required to determine that the proposed software maintenance does not introduce new functions or other design changes.

The Software Maintenance Plan should also describe how it will be determined that the personnel performing the maintenance are fully qualified. This generally means that the personnel should be at least as qualified as the original design team. The SMP should also describe how the maintainer will determine that the software tools are qualified and identical to

¹¹ Software maintenance is the process of correcting faults in the software product that led to failures during operation. 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 failures that were detected during operation, correction of the faults that caused those failures, and release of new versions of the software product.

There may be a considerable delay between the completion of the development project and changing the product. An organization other than the development organization, termed the maintenance organization here, may actually do the maintenance. Without a Maintenance Plan, it is not easy to know how the product may be changed, and what procedures 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.

those used during the original design. The Software Maintenance Plan should have some provisions for qualifying a new revision of the tool if the original version of the tool is no longer available.

The process may be complicated due to vendor-licensee interactions. In many instances, the software maintenance will be done by the original system vendor. In this case, two maintenance plans are required. The first is that of the vendor to actually perform the maintenance, and the second is that of the licensee, showing how the licensee will review and approve the changes implemented by the maintenance. The licensee software maintenance plan should document which measures, consistent with its QA plan, are used to ensure that the required modification is appropriate and correct. This is needed because 10 CFR Part 50, Appendix B allows the licensee to delegate the work, but the licensee retains the responsibility for safety and quality.

D.4.4.7 Software Training Plan (STRngP)

The acceptance criteria for a software training plan¹² are contained in the Standard Review Plan, BTP 7-14, Section 7.4.3, "Software Training Plan." This section states that Regulatory Guide 1.173 endorses IEEE Std 1074-1995, and that Clause 7.4.3 of that standard, "Plan Training," contains an acceptable approach relating to planning for training. BTP 7-14, Section B.3.1.7 also states that NUREG/CR-6101, Section 3.1.10, "Software Training Plan," contains further guidance on Software Training Plans.

Clause A.1.2.6 of IEEE Std 1074 requires different types of training depending on the need. It states that training tools, techniques, and methodologies shall be specified, and that the planning shall include developing schedules, estimating resources, identifying special resources, staffing, and establishing acceptance criteria. This planning shall be documented in the Training Planned Information.

The Software Training Plan may be quite simple or very complex, depending on whether the original vendor or the licensee is performing the software maintenance. If the licensee has contracted with the vendor to perform the software maintenance, the licensee personnel need only to know how to operate the digital equipment. An intermediate step is that the licensee personnel perform first level maintenance, determining which sub-unit, such as an individual PC board has failed, replacing that sub-unit and sending it to the vendor for repair. The vendor may offer training in the operation of the equipment, and with some site specific additional training, this may be sufficient. Maintenance training is more complex, in particular software maintenance. Training provided by the vendor will typically show how to use the software tools used to generate original programs. The licensee may, however, have a qualified engineering staff to be able to do software maintenance themselves.

For these reasons, the training plan should show the organization responsible for performing the operation and maintenance of the system, and who will be performing the training when determining the adequacy of the Software Training Plan.

¹² The software training plan will describe the methods that will be used to train the operators of the software system. In this case, reactor operators 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).

It should be noted that the implementation of the training plan will not be reviewed or commented upon in the staff SER. 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.

D.4.4.8 Software Operations Plan (SOP)

The acceptance criteria for a software operations plan¹³ are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.8, "Software Operations Plan." This section states that the primary aspect is completeness, however it adds that the operations plan needs to address the security of the system, and in particular, the means used to ensure that there are no unauthorized changes to hardware, software and system parameters, and that there is monitoring to detect penetration or attempted penetration of the system.

The Software Operations Plan is not intended describe how the software is intended be used; the requirements for how the software is intended to be used should be included in the design documentation so that the software can be designed for its intended use. The Software Operations Plan will be reviewed for completeness, and therefore the plan needs to address all operations of the system and the plant after it is installed. The plan should discuss measures to ensure the security¹⁴ of the system, and in particular, the means used to ensure that there are no unauthorized changes to hardware, software, and system parameters. Additionally, the plan should show how the operators will be able to detect actual or attempted penetration of the system. There should also be provisions on how to respond to security problems. In general, the plan should show how the licensee has considered the problem and is prepared to respond.

It should be noted that the implementation of the Software Operations Plan will not be reviewed or commented upon in the staff SER. 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.

¹³ 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 operator 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 operator. The Operations Manual structure is dependent on the actual characteristics of the particular computer system.

¹⁴ System and software security is addressed in D.12.

D.4.4.9 Software Safety Plan (SSP)

The acceptance criteria for a software safety plan¹⁵ 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-6101 and Regulatory Guide 1.173, Section C.3, "Software Safety Analyses," contains guidance on safety analysis activities.

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 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 security 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.4.4.9.1 Safety Analysis

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

¹⁵ 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.

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.

The safety analysis activities also includes the cyber security risk, and the methods used to ensure that the standards and procedures 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.

D.4.4.10 Software Verification and Validation Plan (SVVP)

The acceptance criteria for software verification and validation plans¹⁶ 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 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. 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.

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, 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.

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.

¹⁶ 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.

One of the most critical items in the Software Verification & Validation Plan is the independence of the V&V organization. Per IEEE Std 1012-1995, 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 why 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 resolved effectively. The plan should also show how the V&V effort is sufficiently independent to adequately perform the tasks without undue influence to schedule and financial pressure.

A second important issue is the number and quality of the V&V personnel. There is no specific 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 procedures, and anomaly resolution procedures. 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 met, and for any IEEE 1012 requirement which is not being met, what compensatory actions are being used to demonstrate an equivalent level of verification and validation.

D.4.4.11 Software Configuration Management Plan (SCMP)

The acceptance criteria for a software configuration management plan¹⁷ 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.

¹⁷ 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.

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 should specify how modified software or documentation should be tested and verified, and who is to do this.

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.

D.4.4.12 Software Test Plan (STP)

The acceptance criterion for a software test plan¹⁸ 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

¹⁸ The STP describes how all of the individual testing activities (including unit testing, integration testing, factory acceptance testing, site acceptance testing and installation testing) complement and support each other. The plans for individual testing activities describe the methods used for testing and test case generation. The STP should describe how all of the minimum test program activities (identified in RG 1.170, regulatory Position 1; and RG 1.171 Regulatory Position 1) are performed and documented. The STP should describe all of the different types of testing documents used, and identify the procedures governing each. Lower Tier test plan should

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 points out that "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.

D.4.4.13 Software Requirements Specification (SRS)

The acceptance criteria for a software requirements specification¹⁹ is contained in the Standard Review Plan, BTP 7-14, Section B.3.3.1, "Requirements Activities - Software Requirements 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."

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 (e.g., of completed factory acceptance test procedure and results), each requirement should be traceable to one or more safety system requirements, and the requirements traceability matrix should show where in the software the

¹⁹ Software requirements are concerned with what the software must do in the context of the entire application, and how the software will interact with the remainder of the application. These requirements come from the overall application system design, and reflect the requirements placed on the software by the application 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. A hazard analysis of the safety system should be available.

required action is being performed. The key to an adequate SRS is its completeness and understandability.

It should be noted that the NRC staff will not be able to completely review the SRS, but will only 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.

D.4.4.14 Software Architecture Design (SAD)

The acceptance criteria for the software architecture description²⁰ 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 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."

D.4.4.15 Software Design Specification (SDS)

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.

It should be noted that the NRC staff will not be able to completely review the SDS, but will only sample a limited number of requirements during the thread audit (e.g., of software code listings). 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.

D.4.4.16 System Build Documents (SBDs)

The acceptance criteria for the system build documentation²¹ are contained in the SRP, BTP 7-14, Section B.3.3.5, "Integration Activities -System Build Documents." This section states that

²⁰ See footnote in Section D.3.2.

²¹ 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.

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 final configuration lists or tables, final logic diagrams, or in the system and software configuration documentation.

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.

It should be noted that the NRC staff will not be able to completely review the SBDs, but will only sample a limited number of requirements during the thread audit (e.g., of configuration management reports, final software integration report, and vendor build documentation). 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.

D.4.4.17 Installation Configuration Tables (ICT)

The acceptance criteria for the installation configuration tables²² 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, and the staff reviewer will sample these configuration items to verify that they are correct. The reviewer will also verify that the V&V team has already made this determination, and will then sample various items.

D.4.4.18 Requirements Traceability Matrix

The licensee should ensure that the Requirements Traceability Matrix²³ (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, and the actual code. Tracing backwards, it should be possible to take any portion of code and

²² 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.

²³ The definition of an RTM is contained in The Standard Review Plan, BTP 7-14, Section A.3, definitions, and says: "" 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, that 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.

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.4.4.19 Failure Modes and Effects Analysis (FMEA)

There is no specific regulatory guidance on the required format, complexity or conclusions concerning the FMEA²⁴, however IEEE Std 1228-1994 and MIL-Std-882B identify techniques which can be used for identifying hazards. 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.

The FMEA is a method of analysis of potential hardware or programming failure modes within a system for determination of the effect of failures on the system. This information can then be used to assess the potential for an undetectable failure or a common mode failure. The overall staff expectation is that each potential hardware and software failure will be identified, and the effect of that failure 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 hardware and software failures are identified, and accuracy, where the analysis reaches an understandable reason for what the failure effect is for each failure mode. The FMEA is also used as an input to the diversity and defense in depth analysis.

D.4.4.20 Operations Manual

The acceptance criteria for the operations manual²⁵ are contained in the SRP, BTP 7-14, Section B.3.3.7, "Installation Activities – Operations Manual (OM)."

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 sample the design process actually used during the design of the software under review, with the intent of determining that the process described is the process that was used, and that the process was used was used correctly, and in such a manner as to produce high quality software suitable for use in safety-related applications at nuclear power plants.

D.5 System Qualifications

D.5.1 Scope of Review

²⁴ An FMEA is a systematic method of identifying the affects of single failures.

²⁵ 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 operator 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 operator. The Operations Manual structure is dependent on the actual characteristics of the particular computer system.

The NRC staff will review the information provided to verify that the system has been demonstrated to be able to operate 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 including temperature, humidity, seismic, and electromagnetic.

D.5.2 Information to be Provided

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information for system qualifications, for example:

Equipment Qualification Testing Plans
Qualification Test Methodologies
Summaries of Final EMI, Temperature, Humidity, and Seismic Testing Results

It should be noted that Enclosure B is only an example list and an applicant may have different names for similar documents. 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 of final EMI, temperature, humidity, and seismic testing.

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

D.5.3 Regulatory Evaluation

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

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 1.89, Revision 1, that endorses and provides guidance for compliance with IEEE Std. 323-1974; IEEE Std 7-4.3.2-2003, that is endorsed by RG 1.152, Revision 2;

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 any potential aging mechanisms. An aging mechanism is significant if in the normal and abnormal service environment, it causes degradation during the installed life of the system 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.

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. It should be noted that 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

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

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 up removal of the stressor) radiation exposure equivalent to the total dose expected during the system's service life should be applied as an aging mechanism.

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

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

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 operator intervention 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 operators to make 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

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:

D3 analysis

It should be noted that Enclosure B is only an example list and an applicant may have different names for similar documents. The licensee's D3 analysis submittal should provide sufficient documentation to support the assertion that a proposed digital I&C system is diverse and sufficiently robust against CCF. Additional guidance is available in Interim Staff Guidance DI&C-IGS-02. As further discussed in Section D.6.3, the NRC staff will evaluate the licensee's

proposed amendment using Branch Technical Position 7-19, which contains four points to be addressed. To satisfy these four points, the NRC staff would expect a submittal to include:

- An analysis of the diversity 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.
- 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.
- 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.
- A list of all manual operator actions credited for diversity.
- Detailed justification for operator actions with limited margin.

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, "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, 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, 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.

Additionally, the NRC staff's review is guided by 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 ... not result in loss of the protection function ... Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

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

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

It should be noted that 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 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

ISG-2 provides guidance to the NRC staff on performing an evaluation of the defense-in-depth and diversity of a digital I&C system.

D.6.4.1 Adequate Diversity and Manual Operator Actions

Section 1 of ISG-2 provides guidance to the NRC staff for reviewing the defense-in-depth and diversity of a digital I&C upgrade with respect to adequate diversity and manual operator actions.

D.6.4.2 Branch Technical Position 7-19, Position 4

The NRC staff, in ISG-2, has recommended that BTP 7-19, Position 4 be re-written to state:

In addition to the above, a set of displays and controls (safety or non-safety) should be provided in the main control room 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, reactor coolant system integrity, and containment isolation and integrity. The displays and controls should be independent and diverse from the RPS discussed above. However, these displays and controls could be those used for manual operator action as described above. Where they serve as backup capabilities, the displays and controls should also be able to function downstream of the lowest-level software-based components subject to the same common cause failure (CCF) that necessitated the diverse backup system; one example would be the use of hardwired connections.

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 and ISG 2 to determine adequate diversity exists.

D.7 Communications

D.7.1 Scope of Review

Digital systems have the capability for individual channels of a control or protection function to be aware of the status of its redundant channels. While this ability can be utilized to provide additional capabilities, it also presents the potential that erroneous data from a malfunctioning channel or failure of a communications pathway could adversely impact system performance. Therefore, a digital I&C system 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 ISG #4.

D.7.2 Information to be Provided

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:

Design Analysis Report²⁶

It should be noted that Enclosure B is only an example list and an applicant may have different names for similar documents. 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 ISG-4 has been met, or what alternative is proposed when an individual clause is not meet. This documentation should also show where in the documentation of design details this compliance can be verified. Submission of this document is not absolutely required, but since the NRC staff will then have to do this verification themselves, submission of this document will have the effect of reducing the time and effort required for NRC staff review.

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,

²⁶ 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 ISG#6 compliance matrix.

“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 ISG-4, “Highly-Integrated Control Rooms – Communication Issues,” (ADAMS Accession No. ML072540138).

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 ISG-4.

The technical evaluation will address each applicable section of ISG-4, 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 ISG-4, the NRC staff will review the proposed alternative, and determine if the alternative still meets regulatory requirements.

Section 1 of ISG # 4 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 ISG #4 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 ISG #4 provides guidance concerning operator 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 ISG 4. 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.

D.8.2 Information to be Provided

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:

Design Analysis Report²⁷

It should be noted that Enclosure B is only an example list and an applicant may have different names for similar documents. 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; however, for topical reports (TRs), it is strongly encouraged that the updated TRs be submitted for approval before a LAR is submitted referencing the TR.

Where appropriate, the licensee and vendor should discuss each of the documents listed in Enclosure B of this ISG. For each document, the licensee and vendor should state whether this document has changed since the last review. If the document has not changed, the licensee and vendor should show the date when the document was previously submitted, and the ADAMS accession number where the document can currently be found. For documents, including system, hardware and software descriptions 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.

²⁷ A modifications design analysis report provides sufficient detail to support and justify the acceptability of system, hardware, software, and methodology modifications.

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. It should be noted that 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 603-1991, 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

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:

Design Analysis Report
Design Report on Computer Integrity, Test and Calibration, and Fault Detection
Theory of Operation Description
Software QA Plan
System Description
Quality Assurance Plan for Digital Hardware
Safety Analysis
System Test Plan
Final Design Description
Final Logic Diagrams
Reliability Analysis
Final Factory Acceptance Test Reports
Installation Test Plans and Methodologies
Operation Manuals
Summary of Test Results

It should be noted that Enclosure B is only an example list and an applicant may have different names for similar documents. The licensee's submittal should provide sufficient documentation to support the assertion that a proposed digital I&C system meets the requirements of IEEE Std. 603-1991. To assist the NRC staff in making the determination that the licensee submittal meets the requirements of IEEE 603, the licensee may 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.

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 603-1991, Clause 4, Design Basis

Clause 4 of IEEE Std. 603-1991 requires, in part, that a specific 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 the design basis would be needed. 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.

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 603-1991, 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).

D.9.4.1.2 IEEE 603-1991, 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.

D.9.4.1.3 IEEE 603-1991, 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.

D.9.4.1.4 IEEE 603-1991, 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 603-1991, 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 for the operator to 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, ISG-5 addresses this issue.

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 603-1991, 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 603-1991, 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 603-1991, 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 603-1991, 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 failures 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 603-1991, 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 603-1991, 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 603-1991, Clause 4.12, Special Design Basis

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

D.9.4.2 IEEE 603-1991, 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 603-1991, Clause 5.1, Single Failure Criterion

Clause 5.1 requires that any single failure within the safety system shall not prevent proper protective action at the system level when required. The analysis²⁸ 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, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," which endorses IEEE Std. 379-1988, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

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

²⁸ The analysis is sometimes documented in a Failure Modes and Effects Analysis (FMEA) report; see Section D.4.4.19.

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 criteria 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 databases and process equipment has the potential to propagate a common-cause failure of redundant equipment. ISG-4, 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 ISG-4.

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 provides guidance for addressing the potential of common-cause failures.

D.9.4.2.2 IEEE 603-1991, 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 operator 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 operator 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 603-1991, 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 and procedures will be audited by the NRC staff (e.g., completed factory acceptance test procedures and results, individual completed test procedures, individual V&V problem reports up to FAT).

D.9.4.2.4 IEEE 603-1991, Clause 5.4, Equipment Qualification

Clause 5.4 states that safety system equipment²⁹ shall be qualified 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. 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. Regulatory Guide 1.89 Revision 1, endorses guidance for compliance with IEEE Std 323-1974, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.”

²⁹ The information needed by the NRC staff to reach a determination of adequate system qualification is discussed in Section D.5.

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.

Mild environment qualification should conform with the guidance of IEEE Std. 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." The information provided should demonstrate how the equipment was tested, or what analysis was done. The resultant test data or analysis should also be provided to allow the NRC staff to make a determination that the testing or analysis was adequate and demonstrate that the environmental qualification envelopes the worst case accident conditions in the location where the equipment 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 addresses review of mild environment qualifications. The reviewer should also confirm that the environmental protection of instrument sensing lines is addressed.

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

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

Additional disciplines 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 NRC staff determination that the system adequately meets IEEE 603 Clause 5.4 will reference the environmental qualification section of the NRC staff SE.

D.9.4.2.5 IEEE 603-1991, Clause 5.5, System Integrity

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 SER.

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 operator has already placed the affected channel in a bypass mode (this would change a two-out-of-four logic to a two-out-of-three logic). Hardware or software failures 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 should not inhibit manual initiation of protective functions or the operator 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 under the control of the operator in accordance with appropriate plant procedures.

D.9.4.2.6 IEEE 603-1991, Clause 5.6, Independence

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.³⁰ 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 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 ISG-4 provide additional information on this topic.

D.9.4.2.6.1 IEEE 603-1991 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

³⁰ 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.4.4.19.

the independence between redundant portions of the safety system. Section D.7 and ISG-4 describes the requirements for demonstration of this independence.

D.9.4.2.6.2 IEEE 603-1991 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 603-1991 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 384-1981. 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.

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 603-1991, Clause 5.7, Capability for Test and Calibration

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 603-1991, Clause 5.8, Information Displays

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 and will meet the requirements of IEEE Std. 479-1981. The design should minimize the possibility of ambiguous indications that could confuse an operator.

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 that could confuse an operator. 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 603-1991, Clause 5.9, Control of Access

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 System and Software Security 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 603-1991, Clause 5.10, Repair

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 603-1991 Clause 5.11, Identification

Clause 5.11 requires that the safety system equipment be distinctly identified for each redundant portion of a safety system in accordance with IEEE Std. 384-1981 and IEEE Std. 420-1982. 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 hardware and software such that the NRC staff is able to determine that the Clause 5.11 has been met.

D.9.4.2.12 IEEE 603-1991 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 met is required. In addition, ISG-4, 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 603-1991 Clause 5.13, Multi-Unit Stations

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 IEEE Std. 308-1980, and guidance on application of the single-failure criterion to shared systems is contained in IEEE Std. 379-1988. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the Clause 5.13 has been met.

D.9.4.2.14 IEEE 603-1991 Clause 5.14, Human Factors Considerations

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 human operators and maintainers can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std. 1023-1988. The information provided should be sufficient to demonstrate that the guidance contained in ISG-5 has been met.

D.9.4.2.15 IEEE 603-1991 Clause 5.15, Reliability

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.³¹ IEEE Std. 352-1987 and IEEE Std. 577-1976 provide guidance for reliability analysis. The information provided should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed. For computer systems, both hardware and software should be included in this analysis. The NRC staff considers software that complies with the quality criteria of Clause 5.3, and that is used in safety systems that provide measures for defense against common-cause failures as described in 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 and software failures and the design features provided to prevent or limit the effects of these failures, 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 603-1991, 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 603-1991 Clause 6.1, Automatic Control

Clause 6.1 requires that for each design basis event, all protective actions should automatically initiate without operator action, 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 without operator action 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,

³¹ A reliability analysis provides sufficient detail to support and justify that the system meets the reliability requirements.

and the final test reports will be reviewed to verify that the testing showed these features were acceptable.

D.9.4.3.2 IEEE 603-1991 Clause 6.2, Manual Control

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 operator manipulations, and will depend on the operation of a minimum of equipment consistent with the constraints of Clause 5.6.1. RG 1.62 provides further guidance on this topic.

Clause 6.2 also requires implementation of manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 5.2 of IEEE 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.

It is important to note that the manual control required by Clause 6.2 is different from a manual action which may be used as an acceptable diverse actuation required by BTP 7-19 as defense against common cause software failure (CCSF). The manual initiation and indicators to tell the operator 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 not be the ones used in the event of CCSF, 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, 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.

D.9.4.3.3 IEEE 603-1991 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 603-1991 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 product the safety system inputs, 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 603-1991 Clause 6.5, Capability for Testing and Calibration

Clause 6.5 requires that is 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 operator will not take incorrect action if the two channel readouts differ.

D.9.4.3.6 IEEE 603-1991 Clause 6.6, Operating Bypass

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 603-1991 Clause 6.7, Maintenance Bypass

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 603-1991 Clause 6.8, 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 603-1991, Clause 7, Execute Features

Clause 7 of IEEE Std. 603-1991 provides the requirements for actuators and other executable features.

In addressing clauses 7.1 through 7.5, the additional considerations should be taken into account:

D.9.4.4.1 IEEE 603-1991 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 603-1991 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 603-1991 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 603-1991 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 603-1991 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 603-1991, Clause 8, Power Source Requirements

Clause 8 of IEEE Std. 603-1991 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 7-4.3.2-2003 Compliance

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

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:

- Commercial Grade Dedication Plan
- Commercial Grade Dedication Report
- Design Analysis Report
- Design Report on Computer Integrity, Test and Calibration, and Fault Detection
- Theory of Operation Description
- System Description
- Reliability Analysis
- Vendor Software Plan
- Software Development Plan
- Software Installation Plan
- Software Integration Plan
- Software Maintenance Plan
- Software Management Plan
- Software Operations Plan
- Software Project Risk Management Program
- Software Safety Plan
- Software Test Plan
- Software Tool Verification Program
- Software Training Plan
- Software V&V Plan
- Software Configuration Management Plan
- Commercial Grade Dedication Report
- Final System Configuration Documentation
- Software Project Risk Management Report
- System Test Procedures
- Software Test Procedures
- V&V Reports

It should be noted that Enclosure B is only an example list and an applicant may have different names for similar documents. The licensee's submittal should provide sufficient documentation to support the assertion that a proposed digital I&C system is consistent with IEEE Std. 7-4.3.2-2003. The information necessary to address the various clauses of the standard are elaborated in Section D.10.4.

D.10.3 Regulatory Evaluation

While compliance with IEEE Std. 7-4.3.2 is not required by regulation, it is a defacto standard used by the NRC staff in evaluating digital I&C upgrades and is endorsed by RG 1.152 Rev. 2 dated 2003. To demonstrate compliance with another standard in lieu of IEEE Std. 7-4.3.2, the

licensee must include an evaluation that allows the NRC staff to conclude that adherence provides reasonable assurance of a high quality system. This activity should be expected to require a significant amount of additional review time and effort.

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

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

- Inslection
- Installation, Checkout and Acceptance Testing
 - Operation
 - Maintenance
 - Retirement.

The NRC staff 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.

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. IEEE Std. 1061-1998 discusses software quality metrics methodology and methods by which various metrics systems can be evaluated. The metrics methodology should use diverse software measures that appropriately aggregate the measurement data to provide a quantitative assessment of the quality of the outputs.

This recommends 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.

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

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.

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.

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 than those specifically tested. The use of software tools should be evaluated in the overall context of the quality control and V&V process, and there should be a method of evaluating the output of the tool.

Operating experience may be used to provide confidence in the suitability of a tool, but may not be used to demonstrate that a tool is of sufficient quality to be the equivalent to safety-related software. If the first option is chosen, that the tool be developed in the same manner as safety-related software is developed, the NRC staff 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 (e.g., configuration management reports).

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

Clause 5.3.3 states that a V&V program shall exist throughout the system lifecycle and that the software V&V effort shall 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) shall be applied. The information provided should demonstrate that the V&V process provides an objective assessment of the software products and processes throughout the lifecycle and must address the computer hardware and software, integration of the digital system components, and the interaction of the resulting computer system with the plant.

As described in section D.4.4.10 of this ISG, the licensee will need to submit the V&V plan actually used during the development of the platform and the applications software. If the V&V effort used documents which are not included as part of the V&V plan, those documents must also be submitted for NRC staff review.

It should be noted that review of the V&V plan, and the determination that the V&V effort meets regulatory requirement is one of the most significant part of the NRC staff review of the design life cycle, and therefore will receive a through 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.

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

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

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.

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 (e.g., configuration management reports).
- 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 different software configuration management programs to evaluate, that being used by the software vendor during the design process, and that used by the licensee after the software has been delivered and installed in the nuclear power plant. Both 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.

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 sites, to ensure that the methods discussed in the plans are properly implemented.

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

Clause 5.3.6 defines the risk management activities required for a software project. 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 computer 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. 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. The scope of hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems. The software safety plan should include the safety analysis implementation tasks that are to be carried out by the applicant/licensee. The acceptance criterion for software safety analysis implementation is that the tasks in that plan have been carried out in their entirety. Documentation should exist that shows that the safety analysis activities have been successfully accomplished for each life cycle activity group. In particular, the documentation should show 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.

SRP BTP 7-14 Subsection B.3.1.9 has additional details on the management, implementation and resource characteristics of the software safety plan.

Another item for risk management is the security considerations in the life cycle processes of digital computer-based systems. Guidance for the treatment of security items in the life cycle process is provided in Regulatory Guide 1.152, Revision 2 which endorses IEEE Std 7-4.3.2-2003.

The reviewer, when analyzing the risk management program, should keep 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. The reviewer should look for alternative solutions, and analysis of those alternatives, 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.

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

Clause 5.4 defines the equipment qualification³² 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

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.

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

Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:

- Commercial Grade Dedication Plan
- Commercial Grade Dedication Report
- Commercial Grade Dedication Reports
- Final Report on Acceptance of Commercial Grade Dedication

³² The information needed by the NRC staff to reach a determination of adequate system qualification is discussed in Section D.5.

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 as 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 application.

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 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 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 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.

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

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 failures to the diagnostic software, and show the effect of those failures.

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

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.³³ 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

³³ 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.4.4.19.

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.

ISG #4 discussed communications independence, and if the licensee can demonstrate compliance with ISG #4, this demonstration should also suffice for compliance with this clause. The licensee should point to documentation on compliance with ISG #4.

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

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 reviewer should carefully examine the capability of the software to test itself. 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 reviewer should examine the portion of the analysis in the Factory Modes Effects Analysis (FMEA) on diagnostic code failure. Assertions that failure of the operation code is not credible because the system and software diagnostics will find every failure should be carefully examined.

The total amount of software code should be compared to the amount of operational code. Large amounts of test and diagnostic software increase the complexity of the total software, 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. The reviewer's judgment should be used.

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 reviewer should look for a hardware watchdog timer whose only software input is reset after the safety processor completes its function. Even then, the reviewer should look to ensure that there is no possibility of a software failure causing a jump to the reset function, thereby nullifying the effectiveness of the watchdog timer.

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 functions³⁴, 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 performed when necessary. This is the same issue as in subsection 5.6, "Independence," and similar methods are appropriate. If the

³⁴ See ISG#4, Section 3, "Multidivisional Control and Display Stations."

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.³⁵ 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.

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

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.

³⁵ See ISG#4, Section 1, "Interdivisional Communications."

Software error recording and trending may be used in combination with analysis, field experience, or testing.³⁶

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 failure 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.

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.

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

³⁶ A reliability analysis provides sufficient detail to support and justify that the system meets the reliability requirements.

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.

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

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 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 SER on whether or not the proposed digital I&C upgrade is acceptable with respect to technical specifications.

D.12 System and Software Security

System and software security will be addressed following the issuance of separate NRC guidance on this issue.

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

Documents to be Submitted in Support of a Digital I&C Upgrade License Amendment Request

Tier			Submitted with LAR (Phase 1)
1	2	3	
	X	X	Commercial Grade Dedication Plan (D.10.4.2.4.2)
		X	Commercial Grade Dedication Report (D.10.4.2.4.2)
X	X	X	D3 Analysis (D.6.2)
X	X	X	Design Analysis Reports (D.7.2, D.8.2, D.9.4.2.6, D.10.4.2.6)
	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)
	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)
	X	X	Equipment Qualification Testing Plans (Including EMI, Temperature, Humidity, and Seismic) (D.5.2)
	X	X	Software QA Plan (D.4.4.3)
X	X	X	System Description (To block diagram level) (D.9, D.10)
X	X	X	Hardware Architecture Descriptions (D.1.2)
X	X	X	Software Architecture Descriptions (D.3.2)
		X	Quality Assurance Plan for Digital Hardware (D.2.2)
X	X	X	Safety Analysis (D.4.4.9.1)
X	X	X	System Requirements Specification (D.4.4.13)
X	X	X	System Test Plan (D.10.4.2.3.1)
		X	Vendor Software Plan (D.10.4.2.3.1)
X	X	X	Software Design Specification (D.4.4.15)
	X	X	Software Development Plan (D.4.4.2)
X		X	Software Installation Plan (D.4.4.5)
		X	Software Integration Plan (D.4.4.4)
X	X		Software Maintenance Plan (D.4.4.6)
		X	Software Management Plan (D.4.4.1)
X	X		Software Operation Plan (D.4.4.8)
X		X	Software Project Risk Management Program (D.10.4.2.3.6)
		X	Platform Software Requirements Specification (Platform Specific) (D.4.4.13)
X	X	X	Application Software Requirements Specification (Plant Specific) (D.4.4.13)
X	X	X	Software Safety Plan (D.4.4.9)
X	X	X	Software Test Plan (D.4.4.12)
	X	X	Software Tool Verification Program (D.10.4.2.3.2)
X	X		Software Training Plan (D.4.4.7)
	X	X	Software V&V Plan (D.4.4.10, D.10.4.2.3.3, D.10.4.2.3.4)
X	X	X	Requirement Traceability Matrix (D.4.4.18)
X	X	X	Software Configuration Management Plan (D.4.4.11, D.10.4.2.3.5)

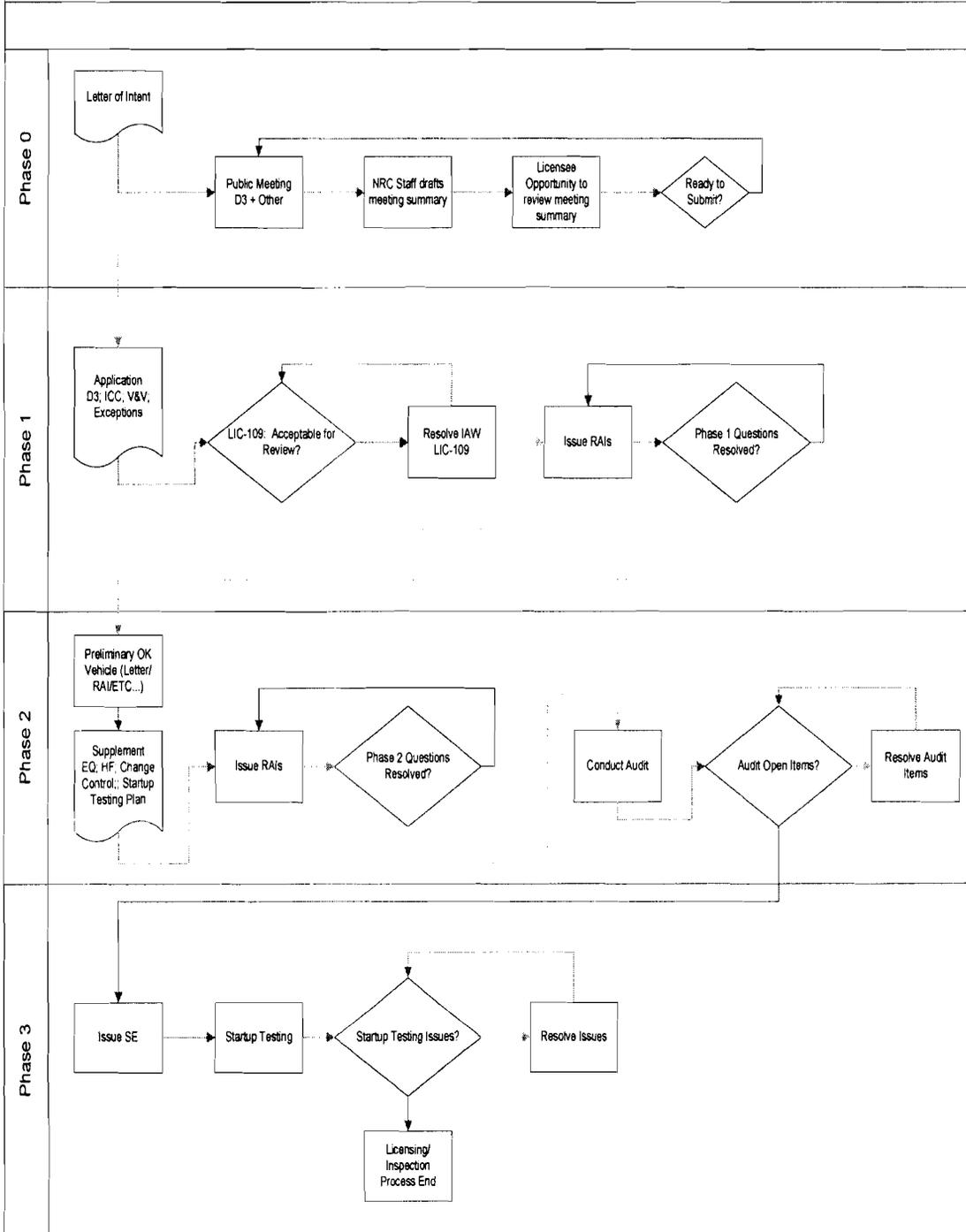
Note: The list of Tier 2 documents to be submitted is only a representation on one type of system modification. In this particular example, the microprocessor has been upgraded, and the printed circuit boards, support chip set, and memory have also been modified along with the new microprocessor. The 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.

Tier			Submitted 12 months prior to requested approval (PHase 2)
1	2	3	
	X		Commercial Grade Dedication Report (D.10.4.2.4.2)
		X	Final Configuration Lists (D.4.2)
		X	Final Configuration Tables (D.4.4.17)
X	X	X	Final Design Description (D.9.2)
	X	X	FMEA (D.4.4.19)
X	X	X	Final Logic Diagrams (D.9.2)
X	X	X	Reliability Analysis (D.9.4.2.15, D.10.4.2.15)
	X	X	Final Report on Acceptance of Commercial Grade Dedication (D.10.4.2.4.2)
X	X	X	Final System Configuration Documentation (D.10.4.2.3.5)
X	X	X	Final Factory Acceptance Test Reports (D.9.2)
X			Operation Manuals (D.4.4.20)
	X	X	Qualification Test Methodologies (D.5.2)
	X	X	Summary of Final EMI, Temp., Humidity, and Seismic Testing Results (D.5.2)
X	X	X	Summary of Test Results (Including FAT) (D.9.4.2.5, D.10.4.2.5)
X	X	X	System Test Procedures (D.10.4.2.4.1)
X	X	X	Software Project Risk Management Report (D.10.4.2.3.6)
X	X	X	Software Test Procedures (D.10.4.2.4.1)
	X	X	Software Tool Analysis Report (D.10.4.2.3.2)
X	X	X	V&V Reports (D.10.4.2.3.1, D.10.4.2.3.3, D.10.4.2.3.4)
X	X	X	System Build Documents (D.4.4.16)

Tier			Available for audit 12 months prior to requested approval (Phase 2)
1	2	3	
X	X	X	Completed Factory Acceptance Test Procedure and Results
X	X	X	Configuration Management Reports
X	X	X	Detailed System and Hardware Drawings
X	X	X	Final Circuit Schematics
X	X	X	Final Software Integration Report
X	X	X	Individual Completed Test Procedures and Reports
X	X	X	Individual V&V Problem Reports up to FAT
X	X	X	Software Code Listings
X	X	X	Vendor Build Documentation

Enclosure C
Digital I&C Licensing Process
Flow Chart

Digital I&C Licensing Process Flow Chart



Enclosure D

Sample Safety Evaluation for Digital I&C License Amendment

Note: This is only a sample of what the final Safety Evaluation Report may be. Since each digital system is somewhat different and each presents unique challenges to the review process, each SER will be unique and any particular SER will be different from the sample shown.

Table of Contents

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.....2

1.0	INTRODUCTION.....	2
2.0	REGULATORY EVALUATION.....	2
3.0	TECHNICAL EVALUATION.....	2
3.1	Hardware Architecture.....	2
3.2	Hardware Design Process and Quality Control.....	2
3.3	Software Architecture.....	2
3.4	Software Design Process.....	2
3.4.1	Software Planning Documentation.....	2
3.4.1.1	Software Management Plan (SMP).....	2
3.4.1.2	Software Development Plan (SDP). (RG 1.173 & IEEE 1074).....	2
3.4.1.3	Software Quality Assurance Plan (SQAP).....	2
3.4.1.4	Software Integration Plan (SIntP).....	2
3.4.1.5	Software Installation Plan (SInstP).....	2
3.4.1.6	Software Maintenance Plan (SMaintP).....	2
3.4.1.7	Software Training (STrngP).....	2
3.4.1.8	Software Operations Plan (SOP).....	2
3.4.1.9	Software Safety Plan (SSP).....	2
3.4.1.9.1	Review of Safety Analyses.....	2
3.4.1.10	Software V&V Plan (RG 1.168 & IEEE 1012).....	2
3.4.1.10.1	V&V Reports.....	2
3.4.1.11	Software Configuration Management Plan.....	2
3.4.1.12	Software Test Plan (STP).....	2
3.4.1.13	Software Requirements Specification.....	2
3.4.1.14	Software Architecture Description.....	2
3.4.1.15	Software Design Description (or Software Design Specification).....	2
3.4.1.15.1	Software Design Review.....	2
3.4.1.16	System Build Documents (SBD).....	2
3.4.1.17	Installation Configuration Tables.....	2
3.4.1.18	Traceability Matrix.....	2
3.4.1.18.1	Thread Audit of source Code Listings (CL).....	2
3.4.1.19	FMEA.....	2
3.5	System Qualifications.....	2
3.5.1	Environmental Qualification of System - IEEE Std 323-1974/1983.....	2
3.5.1.1	Atmospheric.....	2
3.5.1.2	Interference.....	2
3.5.1.3	Susceptibility.....	2
3.5.1.4	Radiation.....	2
3.5.1.5	Electromagnetic Interference/Radio Frequency Interference.....	2

3.5.1.6	Seismic Qualification - IEEE Std 344-1987	2
3.5.2	Power Quality requirements	2
3.5.3	Response time characteristics and testing requirements	2
3.6	Defense-in-Depth and Diversity.....	2
3.7	Communications.....	2
3.7.1	DI&C ISG 04 Compliance.....	2
3.7.1.1	DI&C ISG 04, Section 1 – Interdivisional Communications	2
3.7.1.2	DI&C ISG 04, Section 2 – Command Prioritization.....	2
3.7.1.3	DI&C ISG 04, Section 3 – Multidivisional Control and Display Stations	2
3.8	System, Hardware, Software and Methodology Modifications.....	2
3.9	Review of System and IEEE 603 requirements.....	2
3.9.1	Clause 4. Design Basis	2
3.9.1.1	Clause 4.1 identification of the design basis events	2
3.9.1.2	Clause 4.2 Identification Of Safety Functions And Protective Actions	2
3.9.1.3	Clause 4.3 Permissive Conditions for Operating Bypasses.....	2
3.9.1.4	Clause 4.4 identification of variables monitored	2
3.9.1.5	Clause 4.5 minimum criteria for manual protective actions	2
3.9.1.6	Clause 4.6 identification of the minimum number and location of sensors	2
3.9.1.7	Clause 4.7 Range of Transient and Steady-State Conditions	2
3.9.1.8	Clause 4.8 Conditions Causing Functional.....	2
3.9.1.9	Clause 4.9 methods used to determine	2
3.9.2	Clause 5. System	2
3.9.2.1	Clause 5.1 Single-Failure Criterion.....	2
3.9.2.2	Clause 5.2 Completion of Protective Action	2
3.9.2.3	Clause 5.3 Quality	2
3.9.2.4	Clause 5.4 Equipment Qualification	2
3.9.2.5	Clause 5.5 System Integrity.....	2
3.9.2.6	Clause 5.6 Independence.....	2
3.9.2.7	Clause 5.7 Capability for Test and Calibration	2
3.9.2.8	Clause 5.8 Information Displays.....	2
3.9.2.9	Clause 5.9 Control of Access	2
3.9.2.10	Clause 5.10 Repair.....	2
3.9.2.11	Clause 5.11 Identification	2
3.9.2.12	Clause 5.12 Auxiliary Features.....	2
3.9.2.13	Clause 5.13 Multi-Unit Stations	2
3.9.2.14	Clause 5.14 Human Factors Considerations	2
3.9.2.15	Clause 5.15 - Reliability.....	2
3.9.3	Clauses 6. - Sense and Command Features.....	2
3.9.3.1	Clause 6.1 - Automatic Control.....	2
3.9.3.2	Clause 6.2 - Manual Control.....	2
3.9.3.3	Clause 6.3 Interaction with Other Systems.....	2
3.9.3.4	Clause 6.4 Derivation of System Inputs.....	2
3.9.3.5	Clause 6.5 Capability for Testing and Calibration.....	2
3.9.3.6	Clauses 6.6 Operating Bypasses	2

3.9.3.7	Clases 6.7 Maintenance Bypass	2
3.9.3.8	Clause 6.8 Setpoints	2
3.9.4	Clause 7 - Execute Features	2
3.9.4.1	Clause 7.1- Automatic Control.....	2
3.9.4.2	Manual Control	2
3.9.4.3	Clause 7.3 Completion of Protective Action	2
3.9.4.4	Clause 7.4 Operating Bypasses	2
3.9.4.5	Clause 7.5 Maintenance Bypass	2
3.9.5	Clause 8 Power Source Requirements.....	2
3.10	Review IEEE 7-4.3.2 Requirements	2
3.10.1	Clause 5. System	2
3.10.1.1	Clause 5.3 Quality	2
3.10.1.1.1	Clause 5.3.1 Software Development	2
3.10.1.1.2	Clause 5.3.2 Software Tools	2
3.10.1.1.3	Clause 5.3.3 Verification and Validation.....	2
3.10.1.1.4	Clause 5.3.4 Independent V&V (IV&V) Requirements	2
3.10.1.1.5	Clause 5.3.5 Software Configuration Management.....	2
3.10.1.1.6	Clause 5.3.6 Software Project Risk Management	2
3.10.1.2	Clause 5.4 Equipment Qualification	2
3.10.1.2.1	Clause 5.4.1 Computer System Testing.....	2
3.10.1.2.2	Clause 5.4.2 Qualification of Existing Commercial Computers.....	2
3.10.1.3	Clause 5.5 System Integrity.....	2
3.10.1.3.1	Clause 5.5.1 Design for Computer Integrity.....	2
3.10.1.3.2	Clause 5.5.2 Design for Test and Calibration.....	2
3.10.1.4	Clause 5.6 Independence.....	2
3.10.1.5	Clause 5.7 Capability for Test and Calibration	2
3.10.1.6	Clause 5.8 Information Displays.....	2
3.10.1.7	Clause 5.11 Identification	2
3.10.1.8	Clause 5.15. Reliability	2
3.11	Technical Specification changes	2
3.12	System and Software Security	2
4.0	NRC FINDINGS	2
4.1	Summary of Regulatory Compliance.....	2
4.2	Limitations and Conditions	2
5.0	CONCLUSION	2
6.0	REFERENCES	2

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 ISG#6 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 ISG#6 Enclosure B).

3.1 Hardware Architecture

Read ISG#6 Section D.1, "Hardware Architecture"

3.2 Hardware Design Process and Quality Control

Read ISG#6 Section D.2, "Hardware Design Process and Quality Control"

3.3 Software Architecture

Read ISG#6 Section D.3, "Software Architecture"

3.4 Software Design Process

Read ISG#6 Section D.4, "Software Design 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 ISG#6 Section D.4.4.1, "Software Management Plan"

3.4.1.2 Software Development Plan (SDP). (RG 1.173 & IEEE 1074)

Read ISG#6 Section D.4.4.2, "Software Development Plan"

3.4.1.3 Software Quality Assurance Plan (SQAP)

Read ISG#6 Section D.4.4.3, "Software Quality Assurance Plan"

3.4.1.4 Software Integration Plan (SIntP)

Read ISG#6 Section D.4.4.4, "Software Integration Plan"

3.4.1.5 Software Installation Plan (SInstP)

Read ISG#6 Section D.4.4.5, "Software Installation Plan"

3.4.1.6 Software Maintenance Plan (SMaintP)

Read ISG#6 Section D.4.4.6, "Software Maintenance Plan"

3.4.1.7 Software Training (STrngP)

Read ISG#6 Section D.4.4.7, "Software Training Plan"

3.4.1.8 Software Operations Plan (SOP)

Read ISG#6 Section D.4.4.8, "Software Operation Plan"

3.4.1.9 Software Safety Plan (SSP)

Read ISG#6 Section D.4.4.9, "Software Safety Plan"

3.4.1.9.1 Review of Safety Analyses

See SRP Chapter 7 BTP 7-14 Section B.3.2.1 for SRP acceptance criteria and references to applicable guidance.

3.4.1.10 Software V&V Plan (RG 1.168 & IEEE 1012)

Read ISG#6 Section D.4.4.10, "Software Verification and Validation Plan"

3.4.1.10.1 V&V Reports

Providing the results of the verification reviews, inspections, tests, and analyses, and the validation test.

3.4.1.11 Software Configuration Management Plan

Read ISG#6 Section D.4.4.11, "Software Configuration Management Plan"

3.4.1.12 Software Test Plan (STP)

Read ISG#6 Section D.4.4.12, "Software Test Plan"

3.4.1.13 Software Requirements Specification

Read ISG#6 Section D.4.4.13, "Software Requirements Specification"

3.4.1.14 Software Architecture Description

Read ISG#6 Section D.4.4.14, "Software Architecture Design"

3.4.1.15 Software Design Description (or Software Design Specification)

Read ISG#6 Section D.4.4.15, "Software Design Specification"

3.4.1.15.1 Software Design Review

See SRP Chapter 7 BTP 7-14 Section B.3.3.4 for SRP acceptance criteria and references to applicable guidance.

3.4.1.16 System Build Documents (SBD)

Read ISG#6 Section D.4.4.16, "System Build Documents"

3.4.1.17 Installation Configuration Tables

Read ISG#6 Section D.4.4.17, "Installation Configuration Tables"

3.4.1.18 Traceability Matrix

Read ISG#6 Section D.4.4.18, "Requirements Traceability Matrix"

3.4.1.18.1 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.

3.4.1.19 FMEA

Read ISG#6 Section D.4.4.19, "Failure Modes and Effects Analysis"

3.5 System Qualifications

Read ISG#6 Section D.5, "System Qualifications"

3.5.1 Environmental Qualification of System - IEEE Std 323-1974/1983

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 ISG#6 Section D.5.4.1, "Atmospheric"

3.5.1.2 Interference

Read ISG#6 Section D.5.4.3.2, "Interference"

3.5.1.3 Susceptibility

Read ISG#6 Section D.5.4.3.1, "Susceptibility"

3.5.1.4 Radiation

Read ISG#6 Section D.5.4.2, "Radiation"

3.5.1.5 Electromagnetic Interference/Radio Frequency Interference

Read ISG#6 Section D.5.4.3, "Electromagnetic Interference/Radio Frequency Interference"

3.5.1.6 Seismic Qualification - IEEE Std 344-1987

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 ISG#6 Section D.6, "Defense-in-Depth and Diversity"

3.7 Communications

Read ISG#6 Section D.7, "Communication"

3.7.1 DI&C ISG 04 Compliance

The NRC Task Working Group # 4, "Highly Integrated Control Rooms—Communications Issues," has provided interim NRC Staff Guidance on the review of communications issues. DI&C ISG 04 contains three sections, (1) Interdivisional Communications, (2) Command Prioritization, and (3) Multidivisional Control and Display Stations.

3.7.1.1 DI&C ISG 04, Section 1 – Interdivisional Communications

Section 1 of DI&C ISG 04 provides guidance on the review of communications, includes transmission of data and information, among components in different electrical safety divisions and communications between a safety division and equipment that is not safety related. This ISG does not apply to communications within a single division. This NRC staff position states that bidirectional communications among safety divisions and between safety- and nonsafety equipment may be acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems. It goes on to say that systems which include communications among safety divisions and/or bidirectional communications between a safety division and nonsafety equipment should adhere to the 20 points described.

3.7.1.2 DI&C ISG 04, Section 2 – Command Prioritization

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

Existing D3 guidance indicates that diverse actuation signals should be applied to plant equipment control circuits downstream of the digital system to which they are diverse, in order to ensure that the diverse actuation will be unaffected by digital system failures and

malfunctions. Accordingly, the priority modules that combine the diverse actuation signals with the actuation signals generated by the digital system should not be executed in digital system software that may be subject to common cause failure (CCF).

3.7.1.3 DI&C ISG 04, Section 3 – Multidivisional Control and Display Stations

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

3.8 System, Hardware, Software and Methodology Modifications

Read ISG#6 Section D.8, "System, Hardware, Software and Methodology Modifications"

3.9 Review of System and IEEE 603 requirements

Read ISG#6 Section D.9, "IEEE 603-1991, Compliance"

3.9.1 Clause 4. Design Basis

Read ISG#6 Section D.9.4.1, "IEEE 603-1991, Clause 4..."

3.9.1.1 Clause 4.1 identification of the design basis events

Read ISG#6 Section D.9.4.1.1, "IEEE 603-1991, Clause 4.1..."

3.9.1.2 Clause 4.2 Identification Of Safety Functions And Protective Actions

Read ISG#6 Section D.9.4.1.2, "IEEE 603-1991, Clause 4.2..."

3.9.1.3 Clause 4.3 Permissive Conditions for Operating Bypasses

Read ISG#6 Section D.9.4.1.3, "IEEE 603-1991, Clause 4.3..."

3.9.1.4 Clause 4.4 identification of variables monitored

Read ISG#6 Section D.9.4.1.4, "IEEE 603-1991, Clause 4.4..."

3.9.1.5 Clause 4.5 minimum criteria for manual protective actions

Read ISG#6 Section D.9.4.1.5, "IEEE 603-1991, Clause 4.5..."

3.9.1.6 Clause 4.6 identification of the minimum number and location of sensors

Read ISG#6 Section D.9.4.1.6, "IEEE 603-1991, Clause 4.6..."

3.9.1.7 Clause 4.7 Range of Transient and Steady-State Conditions

Read ISG#6 Section D.9.4.1.7, "IEEE 603-1991, Clause 4.7..."

- 3.9.1.8 Clause 4.8 Conditions Causing Functional
Read ISG#6 Section D.9.4.1.8, "IEEE 603-1991, Clause 4.8..."
- 3.9.1.9 Clause 4.9 methods used to determine
Read ISG#6 Section D.9.4.1.9, "IEEE 603-1991, Clause 4.9..."
- 3.9.2 Clause 5. System
Read ISG#6 Section D.9.4.2, "IEEE 603-1991, Clause 5..."
- 3.9.2.1 Clause 5.1 Single-Failure Criterion
Read ISG#6 Section D.9.4.2.1, "IEEE 603-1991, Clause 5.1..."
- 3.9.2.2 Clause 5.2 Completion of Protective Action
Read ISG#6 Section D.9.4.2.2, "IEEE 603-1991, Clause 5.2..."
- 3.9.2.3 Clause 5.3 Quality
Read ISG#6 Section D.9.4.2.3, "IEEE 603-1991, Clause 5.3..."
- 3.9.2.4 Clause 5.4 Equipment Qualification
Read ISG#6 Section D.9.4.2.4, "IEEE 603-1991, Clause 5.4..."
- 3.9.2.5 Clause 5.5 System Integrity
Read ISG#6 Section D.9.4.2.5, "IEEE 603-1991, Clause 5.5..."
- 3.9.2.6 Clause 5.6 Independence
Read ISG#6 Section D.9.4.2.6, "IEEE 603-1991, Clause 5.6..."
- 3.9.2.7 Clause 5.7 Capability for Test and Calibration
Read ISG#6 Section D.9.4.2.7, "IEEE 603-1991, Clause 5.7"
- 3.9.2.8 Clause 5.8 Information Displays
Read ISG#6 Section D.9.4.2.8, "IEEE 603-1991, Clause 5.8..."
- 3.9.2.9 Clause 5.9 Control of Access
Read ISG#6 Section D.9.4.2.9, "IEEE 603-1991, Clause 5.9..."
- 3.9.2.10 Clause 5.10 Repair
Read ISG#6 Section D.9.4.2.10, "IEEE 603-1991, Clause 5.10"

- 3.9.2.11 Clause 5.11 Identification
Read ISG#6 Section D.9.4.2.11, "IEEE 603-1991, Clause 5.11..."
- 3.9.2.12 Clause 5.12 Auxiliary Features
Read ISG#6 Section D.9.4.2.12, "IEEE 603-1991, Clause 5.12..."
- 3.9.2.13 Clause 5.13 Multi-Unit Stations
Read ISG#6 Section D.9.4.2.13, "IEEE 603-1991, Clause 5.13..."
- 3.9.2.14 Clause 5.14 Human Factors Considerations
Read ISG#6 Section D.9.4.2.14, "IEEE 603-1991, Clause 5.14..."
- 3.9.2.15 Clause 5.15 - Reliability
Read ISG#6 Section D.9.4.2.15, "IEEE 603-1991, Clause 5.15..."
- 3.9.3 Clauses 6. - Sense and Command Features
Read ISG#6 Section D.9.4.3, "IEEE 603-1991, Clause 6..."
- 3.9.3.1 Clause 6.1 - Automatic Control
Read ISG#6 Section D.9.4.3.1, "IEEE 603-1991, Clause 6.1..."
- 3.9.3.2 Clause 6.2 - Manual Control
Read ISG#6 Section D.9.4.3.2, "IEEE 603-1991, Clause 6.2..."
- 3.9.3.3 Clause 6.3 Interaction with Other Systems
Read ISG#6 Section D.9.4.3.3, "IEEE 603-1991, Clause 6.3..."
- 3.9.3.4 Clause 6.4 Derivation of System Inputs
Read ISG#6 Section D.9.4.3.4, "IEEE 603-1991, Clause 6.4..."
- 3.9.3.5 Clause 6.5 Capability for Testing and Calibration
Read ISG#6 Section D.9.4.3.5, "IEEE 603-1991, Clause 6.5..."
- 3.9.3.6 Clauses 6.6 Operating Bypasses
Read ISG#6 Section D.9.4.3.6, "IEEE 603-1991, Clause 6.6..."
- 3.9.3.7 Clauses 6.7 Maintenance Bypass
Read ISG#6 Section D.9.4.3.7, "IEEE 603-1991, Clause 6.7..."

3.9.3.8 Clause 6.8 Setpoints

Read ISG#6 Section D.9.4.3.8, "IEEE 603-1991, Clause 6.8..."

3.9.4 Clause 7 - Execute Features

Read ISG#6 Section D.9.4.4, "IEEE 603-1991, Clause 7..."

3.9.4.1 Clause 7.1- Automatic Control

Read ISG#6 Section D.9.4.4.1, "IEEE 603-1991, Clause 7.1..."

3.9.4.2 Manual Control

Read ISG#6 Section D.9.4.4.2, "IEEE 603-1991, Clause 7.2..."

3.9.4.3 Clause 7.3 Completion of Protective Action

Read ISG#6 Section D.9.4.4.3, "IEEE 603-1991, Clause 7.3..."

3.9.4.4 Clause 7.4 Operating Bypasses

Read ISG#6 Section D.9.4.4.4, "IEEE 603-1991, Clause 7.4..."

3.9.4.5 Clause 7.5 Maintenance Bypass

Read ISG#6 Section D.9.4.4.5, "IEEE 603-1991, Clause 7.5..."

3.9.5 Clause 8 Power Source Requirements

Read ISG#6 Section D.9.4.5, "IEEE 603-1991, Clause 8"

3.10 Review IEEE 7-4.3.2 Requirements

Read ISG#6 Section D.10 "IEEE 7-4.3.2 Compliance"

3.10.1 Clause 5. System

Read ISG#6 Section D.10.4.2 "IEEE 7-4.3.2, Clause 5..."

3.10.1.1 Clause 5.3 Quality

Read ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 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 ISG#6 Section D.10.4.2.7 "IEEE 7-4.3.2, Clause 5.7..."
- 3.10.1.6 Clause 5.8 Information Displays
Read ISG#6 Section D.10.4.2.8 "IEEE 7-4.3.2, Clause 5.8..."

3.10.1.7 Clause 5.11 Identification

Read ISG#6 Section D.10.4.2.11 "IEEE 7-4.3.2, Clause 5.11..."

3.10.1.8 Clause 5.15. Reliability

Read ISG#6 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 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 System and Software Security

Read ISG#6 Section D.12 "System and Software Security"

4.0 NRC FINDINGS

4.1 Summary of Regulatory Compliance

4.2 Limitations and Conditions

Limitations are defined as the boundaries of what is being approved by the safety evaluation both in the context of the plant specific approval and potential use as a precedent.

Any conditions of approval discussed in the safety evaluation should correspond to a license condition to be actual license.

5.0 CONCLUSION

Read and follow LIC-101 Rev. 3 Attachment 3 Section 6, "Conclusion"

6.0 REFERENCES

Read and follow LIC-101 Rev. 3 Attachment 3 Section 7, "References"

Enclosure E
Proposed Table of Contents for
License Amendment Request (LAR)

Proposed Table of Contents for LAR

- 1 Summary Description - *This should provide a high level description of what the system is, and what safety functions it 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 Technical Specifications (See Section D.11 of ISG #6)
- 4 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.*)
- 5 Detailed System Description
 - 5.1 System Architecture – *This should include reference to the system specification, and describe every safety function the system performs.*
 - 5.1.1 Hardware Description (See Section D.1 of ISG #6)
 - 5.1.1.1 Processor Subsystem
 - 5.1.1.2 Safety Function Processor – *The description should include the brand and model of the processor, speed, internal memories, bit width, and bus interface.*
 - 5.1.1.3 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.*
 - 5.1.1.4 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.*
 - 5.1.1.5 Voters - *If the voters contain processors, these should be described in the same manner as the safety function processor.*
 - 5.1.1.6 Manual Channel Trip and Reset
 - 5.1.1.7 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.*

- 5.1.1.8 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.*
- 5.1.1.9 Other Subsystems
- 5.1.1.10 Cabinets, Racks, and mounting hardware
- 5.1.1.11 Diverse Instrumentation & Control (I&C) Systems
- 5.1.1.12 Hardware Changes since topical report or previous use of system (See Section D.8 of ISG #6)
- 5.1.1.13 Hardware Design process and Quality Control (See Section D.2 of ISG #6)
- 5.1.1.14 Appendix B Compliance
- 5.1.1.15 System Qualification (See Section D.5 of ISG #6)
 - 5.1.1.15.1 Atmospheric (See Section D.5.4.1 of ISG #6)
 - 5.1.1.15.1.1 Temperature
 - 5.1.1.15.1.2 Humidity
 - 5.1.1.15.2 Radiation (See Section D.5.4.2. of ISG #6)
 - 5.1.1.15.3 Electromagnetic Interference/Radio Frequency Interference (See Section D.5.4.3 of ISG #6)
 - 5.1.1.15.3.1 EMI/RFI Susceptibility (See Section D.5.4.3.1 of ISG #6)
 - 5.1.1.15.3.2 EMI/RFI Interference (See Section D.5.4.3.2 of ISG #6)
 - 5.1.1.15.4 Sprays and Chemicals (See Section D.5.4.4 of ISG #6)
 - 5.1.1.15.5 Seismic (See Section D.5.4.5 of ISG #6)
- 5.1.2 System Response Time (See Section D.9.4.1.4 of ISG #6)
- 5.1.3 Communications (See Section D.7 of ISG #6) *This should include a description of how the proposed system complies with ISG #4, or reference a stand-alone documents describing the compliance. In any area where the proposed system does not comply with ISG #4, the licensee needs to describe in detail why the system still meets regulatory requirements.*
- 5.2 Software
 - 5.2.1 Software Architecture (See Section D.3 of ISG #6)
 - 5.2.1.1 Individual Software Modules (*software for each processor, whether on the main processor, I/O processors, or communications processors should be individually discussed*)
 - 5.2.2 Software Design Process (See Section D.4 of ISG #6)
 - 5.2.2.1 Software Management Plan (See Section D.4.4.1 of ISG #6)
 - 5.2.2.2 Software Development Plan (See Section D.4.4.2 of ISG #6)
 - 5.2.2.3 Software Quality Assurance Plan (See Section D.4.4.3 of ISG #6)
 - 5.2.2.4 Software Integration Plan (See Section D.4.4.4 of ISG #6)
 - 5.2.2.5 Software Installation Plan (See Section D.4.4.5 of ISG #6)
 - 5.2.2.6 Software Maintenance Plan (See Section D.4.4.6 of ISG #6)
 - 5.2.2.7 Software Training Plan (See Section D.4.4.7 of ISG #6)
 - 5.2.2.8 Software Operations Plan (See Section D.4.4.8 of ISG #6)
 - 5.2.2.9 Software Safety Plan (See Section D.4.4.9 of ISG #6)
 - 5.2.2.10 Software Verification and Validation Plan (See Section D.4.4.10 of ISG #6)
 - 5.2.2.11 Software Configuration Management Plan (See Section D.4.4.11 of ISG #6)

- 5.2.2.12 Software Test Plan (See Section D.4.4.12 of ISG #6)
- 5.2.2.13 Software Requirements Specification (See Section D.4.4.13 of ISG #6)
- 5.2.2.14 Software Architecture Design (See Section D.4.4.14 of ISG #6)
- 5.2.2.15 Software Design Specification (See Section D.4.4.15 of ISG #6)
- 5.2.2.16 System Build Documents (See Section D.4.4.16 of ISG #6)
- 5.2.2.17 Installation Configuration Tables (See Section D.4.4.17 of ISG #6)
- 5.2.2.18 Requirements Traceability Matrix (See Section D.4.4.18 of ISG #6)
- 5.2.2.19 Failure Modes and Effects Analysis (See Section D.4.4.19 of ISG #6)

- 5.2.3 Software Changes since topical report or previous use of system (See Section D.8 of ISG #6)

- 5.3 Conformance with IEEE Std 603 (See Section D.9 of ISG #6)

- 5.4 Conformance with IEEE Std 7-4.3.2 (See Section D.10 of ISG #6)

- 6 Defense-in-depth & Diversity (See Section D.6 of ISG #6)

- 7 System, Hardware, Software, and Methodology Modifications (See Section D.8 of ISG #6)

- 8 System and Software Security (See Section D.12 of ISG #6)

- 9 References

Enclosure F
Glossary for
License Amendment Request (LAR)

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.

Design: A description of components, systems, or modules and how they function in order to accomplish a requirement.

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 (e.g., nineteen inch rack and associated sub-racks), 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.

Layout Diagram: See "Pictorial Diagram"

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.

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.

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.

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.

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.

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).

PARTICIPANTS: Participants from the NRC include members of the Office of Nuclear Reactor Regulation (NRR).

<u>NRC</u>	<u>Industry</u>
W. Kemper, NRR	G. Clepton, NEI
L. James, NRR	
E. Miller, NRR	

The NRC provides reasonable accommodation to individuals with disabilities where appropriate. If you need a reasonable accommodation to participate in a meeting, or need a meeting notice or a transcript or other information from a meeting in another format (e.g., Braille, large print), please notify the NRC's meeting contact. Determinations on requests for reasonable accommodation will be made on a case-by-case basis.

Project No. 689

Enclosures:

1. Agenda
2. Draft Interim Staff Guidance 6

cc w/encl: See next page

DISTRIBUTION:

PUBLIC

RidsAcrsAcnw_MailCTR Resource
 RidsNrrDorl Resource
 RidsNrrDorlLpl1-2 Resource
 RidsNrrDorlLpl2-2 Resource
 RidsNrrDorlLpl3-2 Resource
 RidsNrrPMOysterCreek
 RidsOgcMailCenter Resource
 RidsRgn1MailCenter Resource
 RidsRgn3MailCenter Resource
 L. Trocine, EDO R-I & R III
 S. Williams, EDO R-IV
 R. Hannah, OPA R-II
 V. Dricks OPA RIV
 L. James, NRR
PMNS Resource
 TWFN Receptionist
 am@nei.org
 jhr@nei.org

LPL1-2 R/F
 RidsRgn4MailCenter Resource
 RidsNrrDorlLpl1-1 Resource
 RidsNrrDorlLpl2-1 Resource
 RidsNrrDorlLpl3-1 Resource
 RidsNrrDorlLpl4 Resource
 RidsNrrLAABaxter Resource
 RidsOpaMail Resource
 RidsRgn2MailCenter Resource
 S. Burnell, OPA
 J. Adams EDO R-II
 D. Screnci, OPA R-I
 V. Mitlyng, OPA R-III
 K. Scales, NRR
 D. Santos, RES
 OWFN Receptionist
 C. Steger, NRR
 gac@nei.org
 W. Kemper, NRR

ADAMS Accession Number: ML093491083 * via email

OFFICE	LPLI-2/PM	LPLI-2/LA	LPLIII-1/BC
NAME	GEMiller	ABaxter *	LJames
DATE	2/16/10	02/05/10	2/16/10

OFFICIAL RECORD COPY