U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-06

Licensing Process

Interim Staff Guidance
Revision 2

December 2018

DI&C-ISG-06, Revision 2

DIGITAL INSTRUMENTATION AND CONTROLS
Licensing Process

Interim Staff Guidance
Revision 2

ADAMS Accession No.: ML18269A259 *concurrence via e-mail

OFFICE	NRR/DE/EICB*	NRR/DE/EICB*	NRO/DEI/ICE*	RES/DE/ICEEB*	QTE*
NAME	SDarbali	RStattel	DZhang	BDittman	
DATE	9/26/2018	10/3/2018	9/27/2018	9/27/2018	10/5/2018
OFFICE	NRR/DLP/PLPB/PM	NRR/DIRS/IRGB/LA*	NRR/DLP/PLPB/BC*	NRR/DE/EICB/BC*	RES/DE/ICEEB/BC*
NAME	JGolla	ELee	DMorey	MWaters	RJenkins
DATE	10/1/2018	9/27/2018	9/26/2018	10/5/2018	9/27/2018
OFFICE	NRO/DEI/ICE/BC*	NRO/DCIP/D*	NRR/DIRS/D*	NRR/DRA/D*	RES/DE/D*
NAME	DTaneja	TMcGinty (WJones for)	CMiller	MFranovich	BThomas
DATE	10/3/2018	10/3/2018	9/27/2018	10/2/2018	10/4/2018
OFFICE	NRO/DEI/DD*	NRR/DORL/D*	NRR/DE/D*	OGC – NLO*	NRR/DE/D*
NAME	RCaldwell	CErlanger	EBenner	RWeisman	EBenner
DATE	10/3/2018	10/9/2018	10/5/2018	12/21/2018	12/21/2018

OFFICIAL RECORD COPY

Paperwork Reduction Act

This Interim Staff Guidance provides voluntary guidance for implementing the mandatory information collections in 10 CFR Part 50 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). These information collections were approved by the Office of Management and Budget, approval numbers 3150-0011. Send comments regarding this information collection to the Information Services Branch (O-1F13), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the OMB reviewer at: OMB Office of Information and Regulatory Affairs (3150-0011), Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC 20503; e- mail: oira_submission@omb.eop.gov.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

Contents

A Introduction 1
B Purpose 1
B.1 Background 2
B.1.1 Scope of Digital Instrumentation and Control Modification 3
B.1.2 Documentation Reviewed 3
B.1.3 Digital Instrumentation and Control Review Scope 3
B.2 Description of This Revision to DI&C-ISG-06 4
C Digital Instrumentation and Control License Amendment Request Review Processes 6
C.1 Tier 1, 2, and 3 Review Process Overview 7
C.2 Alternate Review Process Overview 10
C.2.1 Details of License Amendment Request Content 11
C.2.2 Licensee Prerequisites for the Alternate Review Process 13
C.3 Review Process 14
C.3.1 Pre-Application (Phase 0) Coordination Meeting(s) 14
C.3.2 Application, Review and Audit 15
C.3.2.1 Tier 1, 2, and 3 Review Process 16
C.3.2.2 Alternate Review Process 17
C.3.3 Post-License Amendment Issuance 18
D Review Areas for the License Amendment Process 18
D.1 Plant System Description 18
D.1.1 Information To Be Provided 19
D.1.2 Evaluation 19
D.2 System Architecture 20
D.2.1 Existing Architecture 20
D.2.1.1 Information To Be Provided 20
D.2.1.2 Evaluation 20
D.2.2 New System Architecture 20
D.2.2.1 Information To Be Provided 20
D.2.2.2 Evaluation 23
D.2.3 New System Functions 25
D.2.3.1 Information To Be Provided 25
D.2.3.2 Evaluation 26
D.2.3.3 System Requirements Documentation 26
D.2.4 Functional Allocation 29
D.2.4.1 Information To Be Provided 29

D.2.4.2 Evaluation 29
D.2.5 System Interfaces 30
D.2.5.1 Information To Be Provided 30
D.2.5.2 Evaluation 31
D.2.6 Fundamental Design Principles in the New Architecture 34
D.2.6.1 Information To Be Provided 34
D.2.6.2 Evaluation 34
D.3 Hardware Equipment Qualification 39
D.3.1 Information To Be Provided 39
D.3.2 Evaluation 39
D.4 Digital Instrumentation and Control System Development Processes 41
D.4.1 Information To Be Provided 41
D.4.2 Evaluation 42
D.4.2.1 System and Software Development Activities 42
D.4.2.2 Project Management Processes 49
D.4.2.3 Software Quality Assurance Processes 50
D.4.2.4 Software Verification and Validation Processes 51
D.4.2.5 Configuration Management Processes 52
D.5 Applying a Referenced Topical Report Safety Evaluation 52
D.5.1 Information To Be Provided 53
D.5.1.1 Addressing Platform Changes after Approval of a Topical Report 53
D.5.1.2 Resolution of Topical Report Plant-Specific Action Items 53
D.5.2 Evaluation 54
D.6 Compliance/Conformance Matrix for IEEE Standards 603-1991 and 7-4.3.2-2003 54
D.7 Technical Specifications 57
D.7.1 Information To Be Provided 57
D.7.2 Evaluation 58
D.7.2.1 Technical Specifications 58
D.7.2.2 Setpoint Changes 58
D.8 Secure Development and Operational Environment 59
D.8.1 Information To Be Provided 59
D.8.2 Evaluation 59
D.9 Other Review Guidance for Tier 1, 2, and 3 Reviews 60
D.9.1 Software Requirements Specification 60
D.9.1.1 Information To Be Provided 60
D.9.1.2 Evaluation 61

D.9.2 Software Design Specification....61
D.9.2.1 Information To Be Provided....61
D.9.2.2 Evaluation....61
D.9.3 Changes to Referenced Platform Design....61
D.9.3.1 Information To Be Provided....61
D.9.3.2 Evaluation....62
D.9.4 Software Safety Analysis....62
D.9.4.1 Information To Be Provided....62
D.9.4.2 Evaluation....62
D.9.5 Configuration Management Activities....62
D.9.5.1 Information To Be Provided....62
D.9.5.2 Evaluation....62
D.9.6 Testing Activities....63
D.9.6.1 Information To Be Provided....63
D.9.6.2 Evaluation....63
D.9.7 System Integrity—Time Response/Deterministic Performance....63
D.9.7.1 Information To Be Provided....63
D.9.7.2 Evaluation....63
D.9.8 Platform- and System-Level Failure Modes....64
D.9.8.1 Information To Be Provided....64
D.9.8.2 Evaluation....64
D.9.9 Commercial-Grade Dedication of Digital Equipment....64
D.9.9.1 Information To Be Provided....64
D.9.9.2 Evaluation....65
D.9.10 Hardware Development Process....66
D.9.10.1 Information To Be Provided....66
D.9.10.2 Evaluation....66
Enclosure A—Sample Summary of Initial Public Meeting To Discuss Plans To Request NRC Approval in Support of a Digital Instrumentation and Control Modification License Amendment Request....1
Enclosure B—Information Provided in Support of a License Amendment Request for a Digital Instrumentation and Control Modification....1
Enclosure C—Sample Safety Evaluation Table of Contents for a Digital Instrumentation and Control License Amendment....1

List of Figures

Figure B-1 Structure of DI&C-ISG-06 5

Figure C-1 DI&C Licensing Process and Post-License Amendment Issuance Process for Tiers 1, 2, and 3 8

Figure C-2 DI&C Licensing Process and Post-License Amendment Issuance Process for Alternate Review 13

List of Tables

Table D-1 IEEE Standards 603-1991 and 7-4.3.2-2003 Compliance/Conformance Table..... 55

A Introduction

This interim staff guidance (ISG) defines the licensing process used to support the review of license amendment requests (LARs) associated with safety-related digital instrumentation and control (DI&C) equipment modifications in operating plants and in new plants once they become operational. This guidance is consistent with the U.S. Nuclear Regulatory Commission's (NRC's) policy on DI&C equipment and is not intended to be a substitute for NRC regulations.

This ISG provides guidance for activities performed before LAR submittal and during LAR review. The NRC staff uses the process described in this ISG to evaluate compliance[1] with NRC regulations.

The purpose of the NRC's review activities is to evaluate the following for compliance with Federal regulations:

- facility and equipment
- proposed use of the equipment, including human factors engineering considerations
- processes performed for development life cycle phases

NRC staff reviews are not intended to include the evaluation of all aspects of instrumentation and control (I&C) system design and implementation. The review scope should be of sufficient detail to allow the reviewer to conclude that the proposed equipment modification complies with applicable regulations.

This ISG describes how the staff reviews an LAR to determine whether the LAR meets the requirements of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," which is incorporated by reference into NRC regulations in 10 CFR 50.55a(h). In addition, this ISG invokes the criteria of IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," which is endorsed by Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," for performing the review of the proposed DI&C equipment modification. The staff should use these criteria to review the proposed DI&C equipment design in accordance with applicable regulatory requirements and the plant's licensing basis.

The review of DI&C equipment modifications should include an assessment of the acceptability of system development life cycle activities, including the expected level of licensee involvement and oversight of the plant modification. Although process is important, it is not a substitute for a review of the design of the system architecture, the human-system interfaces, and hardware and software architectures to determine whether the four fundamental design principles of redundancy, independence, deterministic behavior (i.e., predictability and repeatability), and defense-in-depth and diversity are met to ensure that the design satisfies NRC regulations.

B Purpose

This ISG provides guidance for the NRC staff's review of LARs for the installation of DI&C equipment in accordance with the licensing processes defined in Office of Nuclear Reactor

---

[1] This ISG uses the term "compliance" when referring to regulations, and the term "conformance" when referring to regulatory guidance or industry standards.

Regulation (NRR) Office Instruction LIC-101, "License Amendment Review Procedures," Revision 5, dated January 9, 2017 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16061A451). This ISG identifies information the NRC staff should review for DI&C equipment.

This ISG should also be used in conjunction with NRR Office Instruction LIC-109, "Acceptance Review Procedures," Revision 2, dated January 9, 2017 (ADAMS Accession No. ML16144A521), to determine whether the application contains sufficient information for NRC staff review. Finally, the staff has designed this ISG to be used with the NRC's review and approval process for topical reports, defined in NRR Office Instruction LIC-500, "Topical Report Process," Revision 7, dated October 22, 2018 (ADAMS Accession No. ML18227A063). In those areas for which a licensee's modification design references (i.e., is based on) an NRC-approved platform topical report, the NRC staff should be able, where appropriate, to limit its review to assessing whether the application of the DI&C modification conforms to the topical report approval. Because the staff developed this ISG on the basis of established guidance, the ISG is designed to work in concert with that guidance. As a result, this ISG references other guidance documents for review criteria.

The staff should ensure that the review is conducted according to the latest revision of these NRR Office Instructions. In the event that the guidance in this ISG conflicts with the guidance found in one of the NRR Office Instructions, the guidance in the latest revision of the Office Instructions should be used, except where this ISG explicitly states otherwise.

B.1 Background

In Section C, this ISG describes two processes for licensee submission and staff review of a DI&C LAR: (1) the Tier 1, 2, and 3 Review Process,[2] and (2) the Alternate Review Process. The NRC staff evaluates proposed DI&C equipment to ensure that equipment meets regulatory requirements. These evaluations use the guidance in NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP), Chapter 7, "Instrumentation and Controls," and other associated guidance. When a licensee submits an LAR under Title 10 of the *Code of Federal Regulations* (10 CFR) 50.90, "Application for Amendment of License, Construction Permit, or Early Site Permit," the licensee must fully describe the changes desired. Thus, the licensee is obligated to describe the functions of I&C equipment identified in the Final Safety Analysis Report (FSAR), as updated, and the equipment that implements the functions. Additionally, the licensee must identify those parts of the licensing basis being updated as a result of the proposed change.

The NRC staff review includes evaluating documentation of plans and processes that support system development activities and their outcomes (e.g., life cycle phase products, test results) to support a staff conclusion on whether system operation is acceptable. SRP Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," and Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," guide the NRC staff in reviewing digital systems. For reviews using the Alternate Review Process, this ISG provides additional guidance for performing early-stage reviews of digital safety-related systems. The NRC staff reviews the

[2] The Tier 1, 2, and 3 terminology used in this ISG is unique to DI&C-ISG-06. The terminology in this ISG does not involve the categories of information in a Design Control Document as defined in 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," and is not otherwise connected to the 10 CFR Part 52 terms "Tier 1" and "Tier 2" used for those 10 CFR Part 52 categories.

system design and development process to support a determination that the design meets regulatory requirements and that, in safety-related applications for nuclear power plants, the process is of sufficiently high quality to produce systems and software suitable for use.

B.1.1 Scope of Digital Instrumentation and Control Modification

The licensee, with feedback from the NRC staff through one or more pre-application (Phase 0) coordination meetings, will develop and submit on the docket the information necessary to support the staff evaluation of the modification or new installation. This process applies to a range of modifications, from one or more components through partial, complete, or multiple systems.

Additionally, the NRC staff recognizes that licensees may use NRC-approved DI&C platform topical reports in different ways. NRC-approved topical reports can be applied within the envelope of their generic approval or with deviations to suit the plant-specific application, provided that the licensee justifies the deviation as proposed for implementation at its facility. Licensees may also propose to use a platform for which there is no generic approval.

B.1.2 Documentation Reviewed

The NRC staff should review the information necessary to make a safety determination using the review criteria in SRP Chapter 7. The licensee is responsible for ensuring that the documentation provided demonstrates regulatory compliance for the safety-related system. The design information submitted to the NRC for review by the licensee should have passed the licensee's design control process before submission.

Documentation to support NRC safety evaluation activities should be submitted to the NRC on the licensee's docket. Confirmatory information for docketed material and other background information should be made available to the NRC staff for review and audit activities.

Enclosure B of this ISG includes a template that may be used to determine the information to be provided in support of an LAR. The NRC staff is expected to determine the document submittal status, submittal timing, and document audit availability for each applicable item in Enclosure B during the acceptance review period.

Some documents associated with software development will be revised as system development activities progress. These are sometimes referred to as "living documents." During the acceptance review period, the staff should decide whether a specific version of the document should be submitted to the NRC and when (i.e., in what phase) it should be submitted. Licensees do not normally need to submit each version of these living documents to support the safety evaluation. Each living document should include sufficient information to demonstrate compliance with applicable regulatory requirements. In some cases, licensees may also need to provide access to current versions of a living document to support audit activities.

B.1.3 Digital Instrumentation and Control Review Scope

The NRC staff's review of an LAR will be limited to the scope of the DI&C modification. During the review, the staff will create a draft safety evaluation with open items that identifies additional information needed to support the evaluation. Requests for additional information (RAIs) should have a clear nexus to the information needed to make a safety determination regarding the DI&C modification. The NRC staff reviews the information necessary to make this safety

determination using the review criteria in SRP Chapter 7 and either the Tier 1, 2, and 3 Review Process or the Alternate Review Process described in Section C of this ISG. The review will include any impact on other systems that have an interface with the system under review.

The NRC I&C staff does not review the DI&C modification for compliance with 10 CFR 73.54, "Protection of digital computer and communication systems and networks." However, the I&C staff should review any cyber security design features included as part of a safety-related system for the purposes of complying with 10 CFR 73.54 to ensure that their inclusion does not adversely affect the reliable performance of the safety function. If the licensee identifies a decrease in the effectiveness of the cyber security plan prepared under 10 CFR Part 73 resulting from the DI&C modification, the staff in the Office of Nuclear Security and Incident Response should review the proposed decrease in effectiveness associated with the modification.

With regard to industry standards endorsed by NRC guidance, the staff should review the design for conformance with the changes and exceptions documented in the endorsing RGs to determine whether the applicable regulatory criteria are met.

B.1.4 Review Areas Outside the Scope of this Interim Staff Guidance

A modification described in an LAR may also impact other review areas. The NRC staff should review the information necessary to make a safety determination using the review criteria found in the SRP for all relevant review areas.

For example, some DI&C equipment modifications may involve human factors engineering (HFE) considerations (e.g., HFE analyses and design processes). In these cases, an HFE safety evaluation should be performed in accordance with SRP Chapter 18, "Human Factors Engineering"; NUREG-0711, "Human Factors Engineering Program Review Model"; and NUREG-1764, "Guidance for the Review of Changes to Human Actions," with close coordination with the DI&C evaluation under SRP Chapter 7.

B.2 Description of This Revision to DI&C-ISG-06

This revision to DI&C-ISG-06 incorporates lessons learned from DI&C LAR reviews that used the previous revision of this ISG. The staff reorganized the ISG to enhance clarity and streamlined the Tier 1, 2, and 3 Review Process to reduce the amount of docketed material, while increasing the focus on the information needed to reach a safety determination. This revision also introduces the Alternate Review Process, which the NRC staff may use to make an earlier safety determination (i.e., before completion of detailed design, implementation, and testing).

Figure B-1 illustrates the structure of this ISG in relation to these review processes. Figure B-1 includes placeholders to maintain alignment as a visual aid to show which sections are common to both the Tier 1, 2, and 3 Review Process and the Alternate Review Process, and which sections are unique to one or the other.

Revision 2 of this ISG is intended to supersede Revision 1; however, ongoing reviews may continue to use Revision 1.

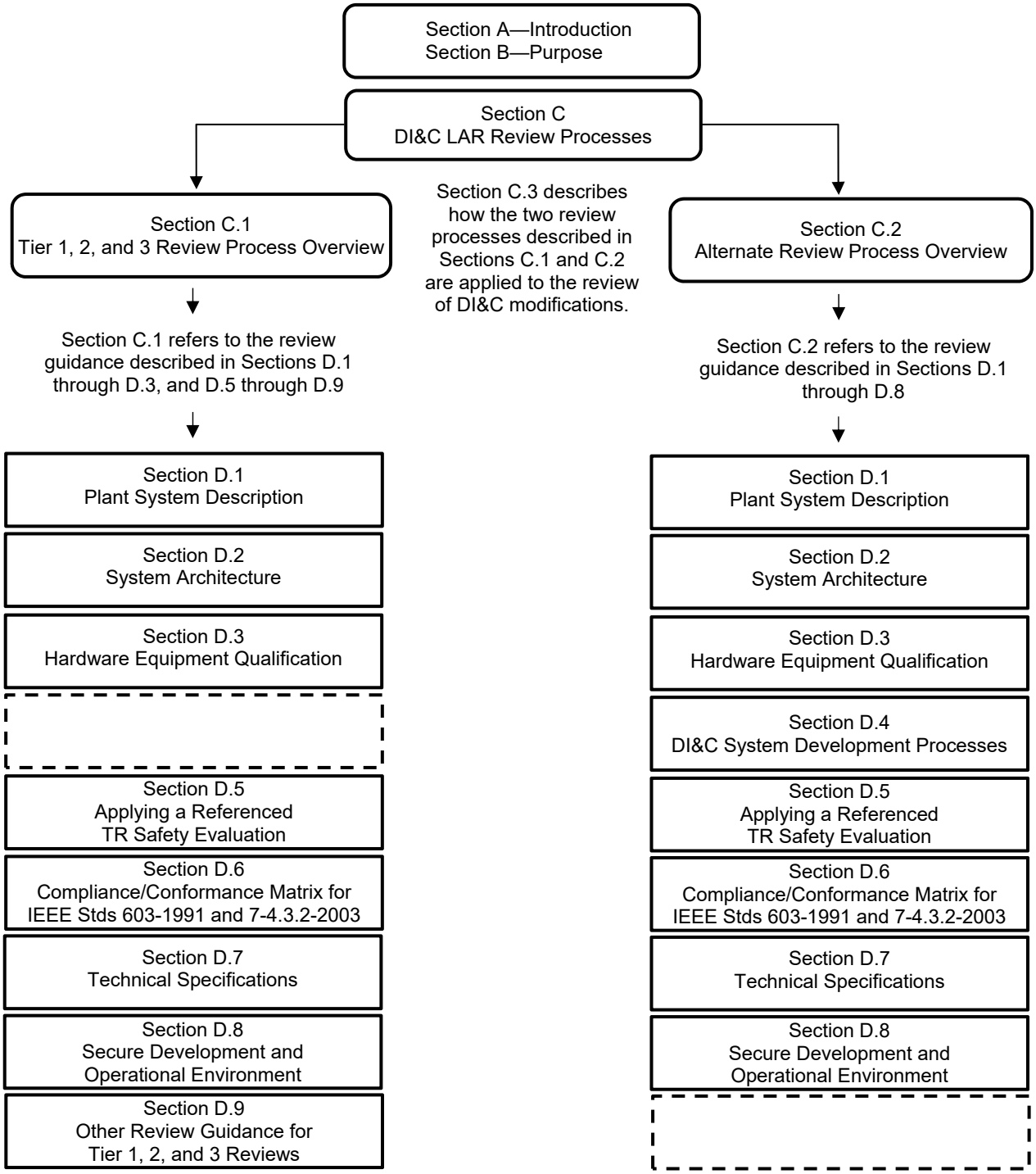

Figure B-1 Structure of DI&C-ISG-06

C Digital Instrumentation and Control License Amendment Request Review Processes

The SRP provides guidance to the NRC staff for performing safety reviews of LARs submitted under 10 CFR 50.90. This ISG presumes the use of the RGs and industry standards in SRP Table 7-1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety." The staff should use the most current revision of these guidance documents and the most recently endorsed edition of these standards, or the revisions and editions agreed upon during the pre-application (Phase 0 for the Tier 1, 2, and 3 Review Process) coordination meeting(s).

Previous licensing actions are those with a similar change and regulatory basis. Searching for, identifying, and using previous reviews in the review process maximizes staff efficiency, minimizes RAIs, and ensures the consistency of licensing actions. However, approval of a digital system or component at one plant does not necessarily serve as the basis for approving the same system or component at another plant. Each LAR is a plant-specific licensing action.

Based on proposed system changes, the reviewer should determine whether any regulatory criteria documented in SRP Section 7.1, "Instrumentation and Controls—Introduction," and SRP Table 7-1 should apply, in addition to those identified in the LAR. The criteria should be used as appropriate based on the scope of the modification.

As noted above, this ISG describes two processes for evaluating DI&C LARs: (1) the Tier 1, 2, and 3 Review Process and (2) the Alternate Review Process. Section C.1 provides the review process for Tiers 1, 2, and 3. Under the Tier 1, 2, and 3 Review Process, the NRC staff decides whether to issue or deny the license amendment after the factory acceptance testing (FAT) is completed and the results have been evaluated.

For the Tier 1, 2, and 3 Review Process, the acceptability of the DI&C platform and application software[3] for safety-related system functions is based on the following:

1.a. a determination that acceptable plans were prepared to control software development activities

1.b. information showing that the plans were followed in an acceptable software life cycle

1.c. information showing that the process produced acceptable design outputs

In Enclosure B of this ISG, columns 1, 2, and 3 of the table (for the Tier 1, 2, and 3 processes, respectively) provide a template that may be used when the NRC staff decides whether to issue or deny the license amendment in the late stages of design and development, after the completion of FAT. This method involves a two-phase submittal to allow the performance of licensing review activities in parallel with the design implementation and test activities of the software development process.

Section C.2 describes the Alternate Review Process by which the NRC staff decides whether to issue or deny the license amendment after the system design is completed and evaluated (see Section C.2.1) but before the system has been built and FAT completed. Acceptability of the Alternate Review Process is predicated upon the licensee using a previously approved DI&C

[3] Based on IEEE Std 7-4.3.2-2016, "software" refers to the programs used to direct operations of a programmable digital device. Examples include computer programs and logic for programmable hardware devices and data pertaining to its operation. This includes logic developed using hardware description languages.

platform, as documented in the applicable topical report safety evaluation. Under the Alternate Review Process, the following will take place:

2.a. the LAR references (i.e., is based on) an NRC-approved DI&C platform topical report.

2.b. the LAR provides detailed system design information (see Section C.2.1 of this ISG) and plant application planning and processes (see Section D.4)

2.c. system development activities will continue during LAR review and after the NRC staff decides whether to issue or deny the license amendment.

The acceptability of the application-specific DI&C platform system is based on the following:

3.a. the framework for the DI&C system development processes, in accordance with Section D.4 of this ISG

3.b. the licensee's oversight and evaluation of the vendor's DI&C system development process activities, and

3.c. the regulatory commitments the licensee makes to confirm that the vendor produces life cycle outputs that meet the associated life cycle design requirements (e.g. System Requirement Specification).[4]

In Enclosure B, column AR (for the Alternate Review Process) may be used if the NRC staff will decide whether to issue or deny the license amendment before completion of the detailed design, implementation, and/or testing activities. The information considered to make a safety determination under the Alternate Review Process is obtained from the licensee's docketed documents, which include conceptual design, system requirements, hardware requirements, software requirements, and human-system interface requirements.

For both the Tier 1, 2, and 3 Review Process and the Alternate Review Process, the staff reviews information related to the development of the system and the application software. For the Alternate Review Process, Section D.4 of this ISG focuses on the processes for system and application software development, as the NRC staff decides whether to issue or deny the license amendment before the completion of system development. For the Tier 1, 2, and 3 Review Process, Section D.9 focuses on the evaluation of design outputs and system validation test results, which should be available during later stages of system and application software development. The NRC staff audits the documentation and development products that are referenced in the LAR. Enclosure B provides guidance on the content of the LAR.

C.1 Tier 1, 2, and 3 Review Process Overview

Because DI&C plant modifications represent a significant licensee resource commitment, a phased approach is appropriate. In this approach, the NRC staff initially reviews critical, fundamental system information before reviewing subsequent DI&C system development and testing information. Therefore, the NRC staff should hold public meetings before the submittal of the LAR to discuss issues regarding system development. The purpose of this activity is to reduce regulatory uncertainty through the early resolution of issues that may challenge the staff's ability to assess the system's compliance with NRC regulations. The NRC staff

[4] As used here, the term "design requirements" and the like do not refer to NRC regulatory requirements, but to system or component design or operating characteristics upon which the licensee relies to accomplish the stated system or component safety functions. Throughout this ISG, context will indicate whether requirements are NRC regulatory requirements or "design requirements" as explained in this footnote.

recognizes that, for some projects, certain information may not be available upon initial submittal of the LAR; thus, information sufficient to address all review topics is not expected to be submitted until later in the evaluation period. During the Phase 0 meetings, the NRC staff should discuss with the licensee the timing of specific information availability. During the acceptance review period, the NRC staff should verify the licensee's proposed timing of specific information availability.

Figure C-1 provides a flowchart of the overall review process. This figure illustrates the various review phases, discussed in Section C.3.

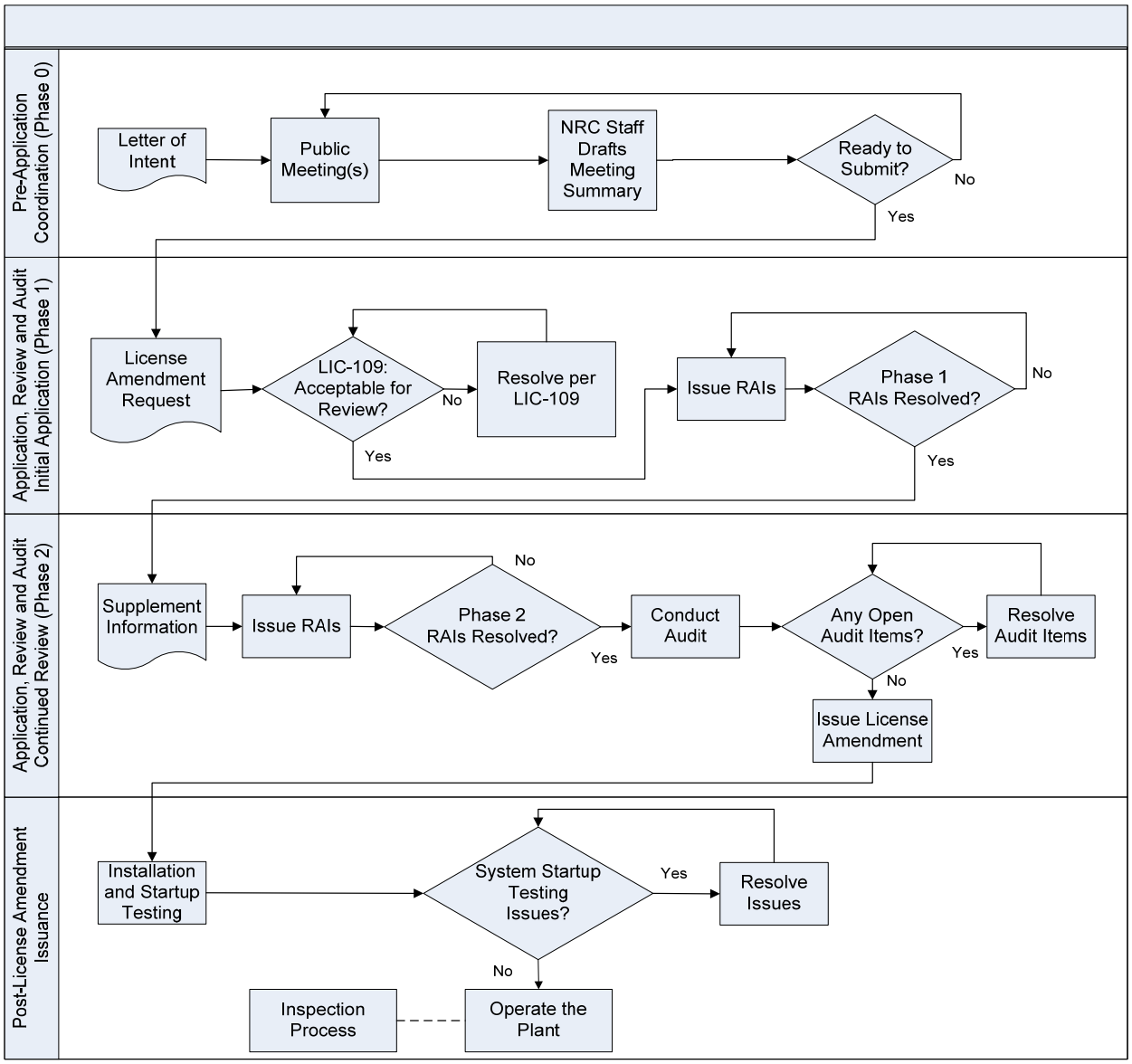

Figure C-1 DI&C Licensing Process and Post-License Amendment Issuance Process for Tiers 1, 2, and 3

The NRC staff recognizes that licensees may use and apply an NRC-approved topical report for a DI&C platform in different ways. Therefore, the NRC staff should consider applications to be within one of the following three tiers of review:

Tier 1

Tier 1 applies to license amendments proposing to reference an NRC-approved topical report (on a DI&C platform or component(s), including hardware, software, and developmental tools) in full conformance with its approval. A Tier 1 review would rely on the previous review of the referenced DI&C platform topical report. In Enclosure B, the Tier 1 column (1) shows an example of the information to be provided in support of a Tier 1 review. This list would not include those documents already reviewed and approved by the NRC staff. Section D.5 discusses applying an NRC-approved topical report safety evaluation.

Tier 2

Tier 2 applies to license amendments proposing to reference an NRC-approved topical report (on a DI&C platform or component(s), including hardware, software, and developmental tools), with deviations. Deviations could include, for example, a revised software development process or new hardware. A licensee assessment of deviations from the approved topical report should be part of the LAR. Typically, an application citing licensing experience from another plant's previous approval would also be considered a Tier 2 review. However, this determination depends on the similarities of the application. In Enclosure B, the Tier 2 column (2) shows an example of the information to be provided in support of a Tier 2 review. However, the changes from the previously approved topical report, as identified in the Phase 0 meetings, should determine the information provided. Tier 2 safety evaluations generally include Tier 1 review scope and a review of any deviations from the approved safety evaluation or topical report.

Tier 3

Tier 3 applies to license amendments proposing to use a new DI&C platform or component(s) that the NRC has not previously approved via a DI&C platform topical report. A Tier 3 review will necessitate a complete review of the DI&C platform concurrent with the LAR. In Enclosure B, the Tier 3 column (3) shows an example of the information to be provided in support of a Tier 3 review. NRC staff Tier 3 evaluations generally combine the scope of both a Tier 1 review and a topical report review. The typical review of a topical report includes hardware, software, developmental tools, and associated developmental methods (e.g., application restrictions and integration methods).

These tier labels are a general guide for defining the scope or complexity of a review. The tables in Enclosure B are examples of "information to be provided for review," as explained throughout this ISG. A licensee may have different names for similar documents. Regardless of the titles of the documents submitted, the LAR should contain sufficient information to address the criteria discussed in Sections D.1 through D.3 and D.5 through D.9, as applicable to Tiers 1, 2, and 3. It is possible that the plant-specific application of a digital system may eliminate the need for the review of certain listed documents and necessitate the inclusion of other unlisted documents.

C.2 Alternate Review Process Overview

The NRC staff recognizes that different approaches are available to licensees with regard to the use and application of NRC-approved topical reports. In addition to the Tier 1, 2, and 3 Review Process, this ISG provides an alternate approach that facilitates review and approval at an earlier stage in the overall system life cycle.

The Alternate Review Process provides an alternative to the Tier 1, 2, and 3 Review Process for reaching a safety determination for a proposed plant modification. Whereas the Tier 1, 2, and 3 Review Process includes NRC evaluation of software design, implementation, and testing, the Alternate Review Process focuses on detailed system design information (see Section C.2.1 of this ISG), additional design information (see Section D.2), and application planning and processes (see Section D.4). For the NRC staff to reach a safety determination using the Alternate Review Process, the application should include the necessary information at the time of LAR submission.

As in the process described in Section C.1 of this ISG, the NRC staff should hold public meetings before LAR submittal to discuss issues with regard to system development. One potentially significant topic that should be discussed includes potential design changes that the licensee may elect to make during detailed implementation of the design after NRC approval of the LAR using the Alternate Review Process. If the NRC approves a system design proposed in an LAR, implementation challenges may arise during system development that could necessitate a design change. Depending on its scope and impact, the design change could require NRC review and approval of a subsequent LAR. Such a design change could also be implemented without prior NRC approval through the process in 10 CFR 50.59, “Changes, Tests and Experiments,” which is subject to NRC inspection.

The Alternate Review Process provides a single-step license amendment submittal process for licensee use. Like Tiers 1 and 2, the Alternate Review Process is applicable to license amendments proposing to reference an NRC-approved topical report. In Enclosure B, the Alternate Review Process column (labeled AR) shows an example of the information to be provided in support of an Alternate Review Process review. Section D.5 discusses applying a topical report safety evaluation previously approved by the NRC.

Unlike the Tier 1, 2, and 3 Review Process, the Alternate Review Process does not provide for Phase 2 document submittals. Accordingly, the reviewer should verify that the application includes the information identified in Enclosure B, as applicable. A safety evaluation conducted for an Alternate Review Process submittal will base its safety conclusions on information provided in accordance with Enclosure B and any supplemental information.

Under the Alternate Review Process, it may be appropriate to convert a licensee’s regulatory commitment (see Section C.2.2) to a legally binding regulatory requirement in the form of a license condition based on the NRC staff’s determination that the issue is of high safety or regulatory significance. Therefore, the staff should evaluate licensee regulatory commitments related to design, implementation, and testing activities as potential license conditions, to address issues of high safety or regulatory significance, in accordance with NRR Office Instruction LIC-101, Section 4.4, “Regulatory Commitments and License Conditions.” NRR Office Instruction LIC-101, Section 4.4, also provides guidance on regulatory commitments that do not warrant conversion to a license condition but are relied on by the staff as an element of the staff’s approval of the proposed amendment. As part of the NRC oversight process, the

NRC staff may perform one or more inspections to evaluate compliance with the license conditions associated with the license amendment.

C.2.1 Details of License Amendment Request Content

When the licensee elects to use the Alternate Review Process and the NRC accepts the LAR for review, the NRC staff will review the application planning and processes related to the detailed hardware and/or software design, implementation, and testing activities. The Alternate Review Process is based on the use of a topical report previously approved by the NRC, and the topical report vendor is expected to develop the system.

The NRC staff will review design information related to the site-specific configuration at a level that is sufficient to demonstrate compliance with the applicable regulations, which can be done by demonstrating conformance with the associated guidance described in the SRP. When reviewing the information described in Figure B-1 (e.g., system architecture, equipment qualification), the NRC staff should credit, to the extent practicable, the results of previous topical evaluations and previously granted amendments that are similar and reference the same approved topical report(s). The NRC staff should examine plant-specific action items (PSAIs) in a referenced topical report's safety evaluation to identify information that will be needed to demonstrate that the topical report can be applied at the licensee's plant. The NRC staff should confirm that the licensee has addressed plant-specific items in the topical report, including items that the licensee identifies as regulatory commitments (e.g., detailed design, implementation, and integration activities) as described above.

The docketed LAR should contain information sufficient to demonstrate regulatory compliance. The Alternate Review Process provides guidance for information to be included in an LAR. This information is obtained from a variety of licensee documents that include conceptual design, system requirements, hardware requirements, software requirements, and human-system interface requirements, each of which may include part of the sufficient "system design" information in the context of the Alternate Review Process. The level of information and detail in the LAR needed for demonstrating compliance with regulatory requirements may vary by design, configuration, and operational features that are unique to the proposed digital modification.

The NRC staff should verify that the life cycle development process, as described in the LAR, will result in outputs that meet the requirements of each life cycle phase. The licensee verifies the vendor's adherence to the life cycle development process. As such, the LAR should describe the licensee's Vendor Oversight Plan. The plan, when executed, can be used to ensure that the vendor executes the project consistent with the LAR. The Vendor Oversight Plan, when executed, can also be used to ensure that the vendor uses an adequate software QA program; for example, the NRC-endorsed 2015 version of the American Society of Mechanical Engineers Nuclear Quality Assurance (NQA)-1, Part II, "Quality Assurance Requirements for Nuclear Facility Applications," Subpart 2.7, "Quality Assurance Requirements for Computer Software for Nuclear Facility Applications."

The staff should use additional review guidance from relevant portions of SRP Chapter 7 to determine the level of design detail needed to address specific acceptance criteria in conjunction with the guidance in these sections. For example, Section D.2.2.1 of this ISG states, in part, "The LAR should demonstrate how any self-test portions of the service/test functions provide fault detection capabilities…." Although this section of this ISG does not reference SRP Chapter 7, the reviewer may use additional review guidance related to self-test

and self-diagnostics from SRP BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions.”

For the Alternate Review Process, Enclosure B provides examples of “information to be provided for review,” as explained throughout this ISG. A licensee may have different names for similar documents. Regardless of the titles of the documents submitted, the LAR should contain sufficient information to address the criteria discussed in the applicable technical evaluation in Sections D.1 through D.8 of this ISG. It is possible that the plant-specific application of a digital system may depend on information that has not been identified in Enclosure B. The licensee and NRC staff should identify and discuss these differences during the pre-application coordination meeting(s).

Figure C-2 is a flowchart of the overall Alternate Review Process. This figure illustrates the various stages of the review, discussed further in Section C.3.

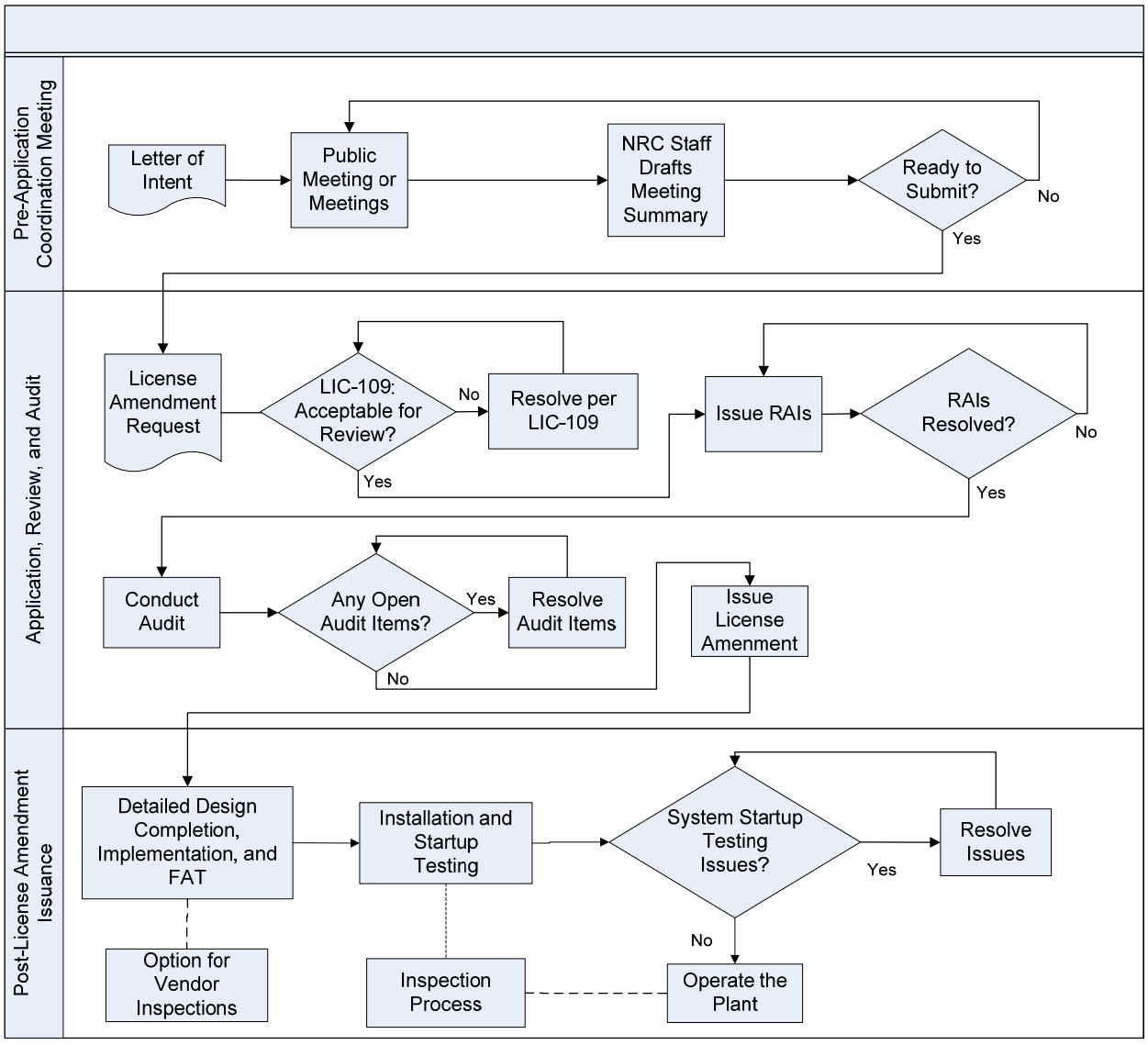

Figure C-2 DI&C Licensing Process and Post-License Amendment Issuance Process for Alternate Review[5]

C.2.2 Licensee Prerequisites for the Alternate Review Process

To use the Alternate Review Process, the staff should verify that the LAR addresses the following items:

1. A description of the licensee's Vendor Oversight Plan. The plan, when executed, can be used to ensure that the vendor: (1) executes the project consistent with the LAR, and (2) uses an adequate software QA program. The Vendor Oversight Plan, when executed, helps ensure that the vendor will meet both the process and the technical regulatory requirements. Vendor oversight is a series of licensee interactions with the vendor and progresses throughout the entire system development life cycle. The plan should address the intended interactions among the vendor's design, test, verification and validation (V&V), and QA organizations.

2. A reference to an NRC-approved DI&C topical report. The proposed DI&C modification should reference (i.e., be based on) an NRC-approved DI&C topical report. The NRC-approved DI&C topical report is also referred to as the "-A version." This reference should address the following:

   a. The proposed DI&C modification should be within the scope of the referenced topical report's applicability.

   b. The extent to which the vendor of the NRC-approved topical report, or a supplier with an approved 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," quality assurance (QA) program, commits to performing detailed software design, implementation, and testing in accordance with the approved topical report.

3. The Licensee's regulatory commitments:

   a. The LAR should include regulatory commitments to complete plant-specific actions that are identified in the referenced topical report.

   b. The LAR should include regulatory commitments to complete life cycle activities under the licensee's QA program (see Section C.2.2 of this ISG). Note that a licensee would complete these activities under a Tier 1, 2, and 3 licensing review before the staff makes a determination on the amendment, but under the Alternate Review Process, the licensee would undertake these activities after the NRC staff decides whether to issue or deny the license amendment, and accordingly, regulatory commitments regarding these activities are warranted.

[5] The dotted connector lines indicate these activities may be optional.

C.3 Review Process

C.3.1 Pre-Application (Phase 0) Coordination Meeting(s)

Before submittal of an LAR for a DI&C modification, it is beneficial to have an overall design concept that adequately addresses NRC regulatory requirements and policy on key issues. The NRC staff intends to use the pre-application coordination meeting process (Phase 0 for the Tier 1, 2, and 3 Review Process) to help ensure that the licensee will meet regulatory requirements early in the process. During pre-application coordination meetings, the licensee and the NRC staff discuss any design features that may raise challenges in the NRC staff's review of the system's compliance with NRC regulations. The NRC staff should discuss with the licensee how the proposed DI&C modification LAR will address the following:

a. selection of the appropriate review process, namely the Tier 1, Tier 2, Tier 3 Review Process or the Alternate Review Process (see Sections C.1 and C.2)
b. key design concepts, including the four fundamental design principles (see Section D.2.6)
c. significant deviations from current guidance
d. significant deviations from a referenced NRC-approved topical report (if applicable)
e. application of the selected system (platform) to the plant system (see Section D.5)
f. definition of the portion of the plant system to be replaced, changes to the FSAR necessary to reflect the replacement, and impact of the replacement on the plant, calibration, and surveillance testing,
g. identification of the level of licensee involvement in the modification project, including the anticipated level of participation by licensee personnel who are assigned responsibilities for oversight of vendor activities
h. establishment of an appropriate licensee living document schedule (see Section B.1.2 regarding description of a living document)
i. any other unique or complex topics associated with the proposed design

These pre-application meetings are intended to allow the licensee the opportunity to present the design concept and the NRC staff to provide feedback on the critical aspects of the proposed design that are likely to affect the NRC staff's evaluation. Before the licensee submits an LAR, the staff should understand the licensee's overall design concept and how it addresses NRC regulatory requirements and policy on each of the key issues.

Further, these discussions should include whether the licensee is proposing the use of an NRC-approved topical report. If an NRC-approved topical report will be used, these discussions should include any changes the vendor has made (or will make as part of this project) to the platform after the NRC has reviewed it and issued a safety evaluation on the NRC-approved topical report. These discussions should also include any planned deviations from the approved platform. The pre-application discussions should also include any planned deviations from NRC guidance, including guidance on software development processes. The staff encourages licensees to discuss topics from other review areas (e.g., how to use best estimate evaluations with realistic assumptions or models and the impact on the uncertainties associated with the results).

These discussions should also address the level of licensee involvement in the plant modification project. Having this discussion before an LAR is prepared enables the licensee to account for impacts on the project schedule, translation and traceability of system requirements, current plant processes, technical specification (TS) surveillance, operating procedures, and maintenance and training activities. These meetings should also address the schedule and scope of audits and potential inspections, which may be updated as the NRC staff's review progresses.

All proposed deviations from the submittal information guidance in Enclosure B should be discussed in the pre-application (Phase 0) coordination meeting(s). The pre-application (Phase 0) coordination meeting summary should document any associated common understandings.

Following each public meeting, the NRC staff should document the topics discussed in a meeting summary. This summary should include a preliminary NRC staff understanding of the licensee's concept (or those subparts of the overall concept discussed) and identify the areas significant to this preliminary understanding. The staff should discuss the applicability of the review process selected (i.e., Tier 1, 2, and 3 Review Process or Alternate Review Process) for the proposed modification. If the Tier 1, 2, and 3 Review Process is selected, the staff should include a discussion of the tier applicability for the proposed modification. Enclosure A to this document presents an example of a meeting summary.

C.3.2 Application, Review and Audit

The NRC staff should perform an acceptance review of the application in accordance with NRR Office Instruction LIC-109 to determine whether the application contains sufficient information for NRC staff review (see Enclosure B for an example of the information to be provided with the LAR). The staff should verify that the licensee has identified any design features and concepts that may affect the staff's preliminary understanding of the design obtained during the pre-application (Phase 0) coordination meeting process. The NRC should document the acceptability of the application for docketing in a letter to the licensee, in accordance with LIC-109.

As determined during both the Phase 0 meeting(s) and the review, the staff should verify that additional documents can be made available for NRC staff audit. This will allow the NRC to audit the documents and to determine whether these documents need to be submitted on the docket. Because the NRC staff may only rely on information submitted on the docket in making a determination on the LAR, as documented in its safety evaluation, it may determine that certain documents or portions of documents need to be submitted on the docket under oath or affirmation.

It is important that the NRC staff and the licensee communicate closely so that both parties remain cognizant of deliverables and due dates. During the review, the staff should have publicly noticed periodic conference calls with the licensee to discuss staff questions. Following each call, the NRC staff should document the topics discussed in a meeting summary. Questions raised by the staff can be kept in an "open items" list, along with the responses from the licensee. The open items list can contain information to track issues to closure. The staff may determine that some items and responses should be formalized into RAIs.

Sections C.3.2.1 and C.3.2.2 further describe the LAR review process for the Tier 1, 2, and 3 Review Process and the Alternate Review process, respectively.

C.3.2.1 Tier 1, 2, and 3 Review Process

C.3.2.1.1 Initial Application (Phase 1)

To the extent possible, the LAR should address the criteria associated with the areas defined in Sections D.1 through D.3 and D.5 through D.9.

Some information may not be available at the time of the initial application, and the review process may be more efficiently administered by beginning before that information is available. Therefore, the NRC staff may find a DI&C modification application to be sufficient for review if it includes a clear schedule for the submission of omitted information. As an exception to the guidance for timing of public notification indicated in Section 3.0, "Public Notification," of LIC-101, Revision 5, the staff will issue a notice of the amendment and provide an opportunity to request a hearing on it when the licensee has submitted complete information in Phase 2. All other guidance regarding public notification and opportunity to request a hearing in LIC-101, Revision 5, will apply without exceptions. Delays in Phase 2 information receipt could potentially impact timely public notification and issuance of the amendment. Proposed changes to the schedule in advance of any document due date should be discussed with the NRC staff, and the staff should document its agreement to such a change in a public meeting summary, email, standalone letter to the licensee, or routine licensee interactions.

During Phase 1, the NRC staff should draft the safety evaluation and issue RAIs for the information or clarifications necessary to finish the review of the docketed material. These activities should be conducted in accordance with NRR Office Instruction LIC-101. The NRC staff should also communicate those areas of review that, based on the available information, appear to be acceptable.

The staff should verify that the licensee has responded to the RAIs before the Phase 2 information is submitted. Although the NRC staff may have additional questions based on the responses to the Phase 1 RAIs, the staff should make sure that the licensee does not delay submission of the Phase 2 information.

If necessary, the NRC staff should conduct one or more audits in accordance with NRR Office Instruction LIC-111, "Regulatory Audits," dated December 16, 2008 (ADAMS Accession No. ML082900195). The NRC staff should be aware that some information may be in documentation available only at the licensee's or vendor's facility. The information examined in this manner should be documented in the audit report. The NRC project manager, in consultation with the licensee and NRC technical staff, should schedule the audit. If any of the audited information is relied upon to complete the safety evaluation, the NRC staff should request the licensee to submit the information on the docket under oath or affirmation.

C.3.2.1.2 Continued Review (Phase 2)

After the NRC has received a response to the Phase 1 RAIs, and with sufficient lead time to support the requested approval date, the licensee should submit the Phase 2 information. The staff should verify that the supplement contains sufficient information to address aspects of the review areas not included in the initial LAR or subsequent responses to RAIs (see Enclosure B for an example of the information to be submitted before the requested approval date). If the licensee does not adhere to previously established schedules for submitting information, e.g., RAI responses and Phase 2 information, the NRC staff may not be able to maintain the schedule for completing the review.

During Phase 2, the NRC staff should continue the RAI process until the licensee has provided sufficient information for the staff to make a decision on the acceptability of the proposed digital modification. If necessary during the Phase 2 process, the NRC staff should conduct one or more audits in accordance with NRR Office Instruction LIC-111. Audits may cover information from both Phase 1 and Phase 2. Audits may result in more requests for information to be docketed. The NRC staff intends to perform the audits as early in the process as is reasonable. However, an effective and efficient audit process can only occur if the LAR and supplements provide sufficiently detailed information about the later phases of the system development life cycle.

Although the plans and other available information should be submitted as early as possible, certain documentation may be deferred based on the Phase 0 meeting discussions. All information needed to make a determination on the application must be submitted before the staff can complete the safety evaluation.

Phase 2 should conclude with the issuance of a safety evaluation documenting the approval or denial of the licensee's proposed DI&C modification. Although Figure C-1 contains post-license amendment issuance activities, the licensing process covered by this ISG ends when the NRC staff decides whether to issue or deny the license amendment.

Consistent with licensing review guidance, the staff should develop a safety evaluation that documents the basis for the decision. The safety evaluation should document applicable regulatory requirements; the information provided by the licensee, including regulatory commitments; a summary of the staff evaluation; and the basis for the determination of whether or not the application meets applicable regulatory requirements.

In addition, the staff should separately identify in the safety evaluation "potential items for inspection" as recommendations to help inform the focus of post-license amendment inspections. However, the "potential items for inspection" cannot be relied upon or used as a safety basis for LAR approval. NRC Headquarters staff should keep the NRC inspection staff aware of the LAR review scope, activities, and milestones.

C.3.2.2 Alternate Review Process

The LAR should address the criteria associated with Sections D.1 through D.8. Along with the LAR, the submission should include the information necessary to support the NRC's review and be submitted on the docket under oath and affirmation. The documents will contain materials necessary to reference in the safety evaluation.

The NRC staff should draft the safety evaluation and issue RAIs for the information or clarifications necessary to finish the review of the docketed material. It should conduct these activities in accordance with NRR Office Instruction LIC-101. The NRC staff should also communicate those areas of review that, based on the available information, appear to be acceptable.

If necessary, the NRC staff should conduct one or more audits in accordance with NRR Office Instruction LIC-111. The NRC staff should be aware that some information may be in documentation available only at the licensee's or vendor's facility. The information examined in this manner should be documented in the audit report. The NRC project manager, in consultation with the licensee and NRC technical staff, should schedule the audit. If any of the

audited information is relied upon to complete the safety evaluation, the NRC staff should request the licensee to submit the information on the docket under oath or affirmation.

During the review of an LAR, certain items may be identified that apply to system configuration, testing, or operation that will be completed after the NRC issues the license amendment. The NRC staff should identify such items separately in the safety evaluation as "potential items for inspection" to inform the focus of post-license amendment vendor and site inspections. However, the "potential items for inspection" cannot be relied upon or used as a safety basis for LAR approval. NRC Headquarters staff should keep the NRC inspection staff aware of the LAR review scope, activities, and milestones.

Although Figure C-2 contains post-license amendment issuance activities, the licensing process covered by this ISG ends when the NRC staff decides whether to issue or deny the license amendment.

C.3.3 Post-License Amendment Issuance

If the NRC staff decides to approve an LAR for a DI&C system, the licensee may complete the design (for an LAR evaluated under the Alternate Review Process) and install the system. In doing so, the licensee will implement associated procedural and TS changes and complete startup testing. SRP Section 7.0, "Instrumentation and Controls—Overview of the Review Process," Section V, "Application-Specific Review Plan," contains guidance for establishing inspections.

For the Alternate Review Process, the NRC quality assurance and/or vendor inspection staff may inspect the software design and implementation activities before the transfer of the equipment to the site, in accordance with applicable inspection procedures. Section D.4.2.1.9 describes I&C system testing. The NRC staff may inspect the system testing, startup testing, and other documents in accordance with applicable inspection guidance (e.g., Inspection Procedure 52003, "Digital Instrumentation and Control Modification Inspection"). NRC technical staff may need to advise and assist NRC inspection staff as appropriate to verify the adequacy of the development, implementation, and/or installation phases of the approved digital modification.

Upon approval of an LAR, changes are controlled and implemented by licensee programs which, in turn, are governed by 10 CFR Part 50, Appendix B, and other regulatory requirements. The regulation in 10 CFR 50.59 governs the need for prior NRC review and approval of changes to the facility and procedures as described in the FSAR.

D Review Areas for the License Amendment Process

As noted in Figure B-1 and Enclosure B, Sections D.1 through D.3 and D.5 through D.9 of this ISG are applicable to the Tier 1, 2, and 3 Review Process, whereas Sections D.1 through D.8 are applicable to the Alternate Review Process.

D.1 Plant System Description

Reviewing the existing plant system description allows the reviewer to understand how the components of the existing plant system interact to accomplish the design function. The plant system description should include all affected plant equipment and the interfaces with operations and maintenance. Depending on the plant modification, the plant system description

could consist of one or more systems, one or more subsystems, or one or more components. This description should come from an integrated hardware and software perspective to develop a clear understanding of the overall system. Understanding the existing plant system provides a solid foundation for the subsequent reviews and evaluations against the acceptance criteria.

D.1.1 Information To Be Provided

The licensee's submittal should provide documentation (through text and drawings) to describe the affected plant equipment. The documentation should describe the design basis and operational, maintenance, calibration, surveillance, and engineering functions implemented.

The licensee's submittal should provide documentation and descriptions to allow the reviewer to identify the digital equipment being used, how the digital equipment functions, how the various digital equipment items are interconnected, and any software in the system. The digital equipment should be identified to the revision level for both hardware and platform software (see Section D.5 of this ISG). If the NRC has previously evaluated the digital equipment proposed, the NRC staff should verify that the LAR refers to that description and evaluation, including any available ADAMS accession numbers. The staff should verify that the licensee has identified all changes or deviations from the previously evaluated digital equipment. The staff should evaluate all changes to previously approved aspects (see Section D.5).

The documentation and description should be on two levels. First, the LAR should describe the individual channels or divisions, including the signal flows between the various digital equipment items. Second, it should describe the overall system, with particular emphasis on additional hardware items not included in the description of the channels or divisions, such as voters, equipment to support communications with workstations or non-safety-related systems, bypass functions/switches, and diverse actuation systems (DASs).

The acceptability of a safety-related system is based on the system's ability to perform design basis functions (e.g., trip on high level, display of proper indications) and the system's compliance to regulatory requirements (e.g., independence). The system design description and safety analysis reports should contain this information to demonstrate that the design meets regulatory and design requirements.

D.1.2 Evaluation

The reviewer should determine whether the LAR information presents a comprehensive explanation of the system. From this, the reviewer should determine the scope of the review and identify any constraints on system approval. The safety evaluation should document the NRC's understanding of the plant system and digital equipment in order to explain system operation and to support the technical evaluations of other sections of the LAR.

D.2 System Architecture

D.2.1 Existing Architecture

D.2.1.1 Information To Be Provided

The licensee's submittal should provide documentation to describe the physical and functional architecture of the existing system through text and diagrams (e.g., functional/architecture block diagrams and functional logic diagrams). This description should include the following:

a. system design functions
b. service/test functions
c. provisions for separation and independence within the system (e.g., channels, trains, isolation)
d. connections and internal interfaces within the safety-related system, including cross-divisional interfaces and interfaces between components
e. connections to human-system interfaces
f. connections between safety-related systems
g. connections between safety-related and non-safety-related systems and identification of signal and data isolation devices
h. temporary connections (e.g., for maintenance workstations)
i. interface with supporting systems (e.g., electrical power supply)
j. physical location(s) of system equipment in the plant

This description should also identify which portion(s) of the system are being replaced. (Although this list includes system design functions, Section D.2.3.1 of this ISG describes their design bases.)

D.2.1.2 Evaluation

The reviewer should understand that the changes to the replacement system may result in changes to existing input and output I&C interfaces with the plant and I&C interfaces with control room displays, indicators, and controls. This understanding should include a review of the system's role in meeting post-accident monitoring requirements.

The safety evaluation should document the NRC's understanding of the existing system architecture to support the technical evaluations of other sections of the LAR.

D.2.2 New System Architecture

D.2.2.1 Information To Be Provided

The LAR should describe and illustrate the new plant system architecture. It should clearly designate and describe changes to the existing architecture, including the reason for the changes. This description provides a basis for the discussion of the fundamental design principles in Section D.2.6 of this ISG.

The LAR should provide documentation to describe the physical and functional architecture of the replacement digital equipment through text and diagrams (e.g., functional/architecture block diagrams and functional logic diagrams). It should provide sufficient information to enable the staff to understand the changes needed for installation of this new digital equipment. The information should reflect the new plant system architecture and design. The information should define how the changes affect the existing plant (e.g., architectural restrictions on size, location, cooling, or power supplies).

The LAR should describe the new digital equipment and reflect the final plant system to be installed in the plant. The LAR should also clearly describe any changes made to items (a) through (j) listed in Section D.2.1.1. The description should include changes resulting from the use of the new digital equipment and any other changes made under other processes that have the potential to affect the safety function of the new digital equipment (e.g., eliminating single-point vulnerabilities within divisions, adding redundant power supplies). The LAR should document any restrictions on the new system architecture based on physical plant location, such as size, cooling, or power supply.

If the LAR references an NRC-approved topical report, the LAR should identify the digital equipment vendor and the topical report and revision cited in the NRC safety evaluation on the report. A referenced NRC-approved topical report may address the matters described below, in which case they need not be re-evaluated. Nonetheless, the below matters need to be addressed, either in a referenced NRC-approved topical or in the application.

The LAR should describe all design functions and service/test functions. Sections D.2.3.1 and D.2.3.2 of this ISG describe how the staff should evaluate these functions. The licensee's submittal should describe each design function that is performed by the portion(s) of the system being replaced. It should also describe all new design functions proposed in the LAR. These design functions are safety functions implemented in the application-specific software, programmable logic, hardware (e.g., hardware voters and relays), credited manual operator actions (MOAs), or some combination of these.

The LAR should describe service/test functions together with the design functions. Service/test functions are digital equipment features to support the design functions. Unlike the design functions, the service/test functions are not directly related to the performance of safety functions but relate to specific activities of the digital equipment, including the functions necessary for configuration, validation, operation, periodic testing, maintenance, incorporation of design modifications, self-test, self-diagnostics, and maintenance of a secure operational environment (SOE). A referenced topical report may describe the service/test functions. These functions may also be implemented in application software, which the topical report may not describe. Although any portions of the service/test functions that remain unchanged from the topical report should not warrant repeating a prior evaluation, the LAR should identify these portions.

The LAR should demonstrate how any self-test portions of the service/test functions provide fault detection capabilities and thus conform with IEEE Std 7-4.3.2-2003, Clauses 5.5.2 and 5.5.3, consistent with IEEE Std 603-1991, Clause 5.7. The discussion of self-tests and self-diagnostics should demonstrate compliance with existing applicable TS and any proposed change to the TS.

The LAR should demonstrate how the design detects malfunctions. The following are examples of issues that could be applicable to the replacement design:

1.a. If the application references an NRC-approved topical report, how the application interfaces with and uses the self-test and self-diagnostic features defined in the topical report and evaluated in the safety evaluation on the report. For an application that does not reference an NRC-approved topical report, see §§ D.2.2.2 and D.7.2.1 of this ISG. In either circumstance, the evaluation should include a discussion of the malfunction detection coverage considering the combination of TS surveillances and the automated features.

1.b. How the design implements communications messages. This should include a description of the types and purposes of each message, the format of each message, the response of the receiver to invalid data, methods used to detect repeated messages, alarming on malfunctions, and the use of each message (e.g., voting, bypass). Error detection means provided in communications messaging and processing (see Section 1, Item 12, of DI&C-ISG-04, "Highly Integrated Control Rooms—Communications Issues (HICRc)," Revision 1, dated March 6, 2009 (ADAMS Accession No. ML083310185)) apply to communications messages used by safety functions. This section of the LAR should demonstrate conformance to the DI&C-ISG-04 assessment containing these data.

1.c. How the design prevents failures from affecting watchdog timer timing and timeout. This should address hardware and software malfunction coverage for the watchdog timers, including a description of the annunciation and the effects on the plant during and after any reset function initiated by an expiring watchdog timer.

1.d. Treatment and detection of malfunctions: in the system inputs, including sensors and transmitters; in the system logic, including internal voters within the safety-related system or voters external to the safety-related system; and in the system outputs, including discrete output switches, analog modulating outputs, and the actuated devices, as well as feedback of actual position or condition where employed. This should include the expected failure state(s) of each input, the response of the system to each failure, the expected failure state(s) of each output, and the response of the plant to each failure. These should be based on the platform failure modes and effects analysis (FMEA) and consider the FMEA for the plant application.

1.e. Use of an external safety-related system to perform continuous channel cross-checks, as well as logic cross-checks between divisions, to provide a means to detect drift and other malfunctions in external devices and system inputs.

For review efficiency, the LAR should provide a markup of the plant's FSAR, showing how the FSAR will reflect the new design. The content of the FSAR may be based on RG 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)," or RG 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)," as applicable. Any TS markups should be included based on the guidance in Section D.7 of this ISG.

If the design includes a DAS, then the architecture section of the LAR should contain information, which could include diagrams, to describe the interconnections and interactions between the DAS and the following:

2.a. the primary protection system

2.b. any portions of the existing system that remain

2.c. the priority logic (if applicable)

2.d. credited manual operator actions

2.e. maintenance, test, surveillance, and other similar actions

2.f. detection of DAS and DAS interface malfunctions

If the design interfaces with instruments that are used for other purposes, such as post-accident monitoring, the LAR should describe methods (e.g., isolation devices) used to ensure that the new digital equipment does not adversely affect the function of those instruments. If the design affects indications used by the operator for manual control, the LAR should describe how those modifications affect the ability of the operator to implement manual actions, in accordance with IEEE Std 603-1991, Clause 5.8.1. The LAR should describe the interface and controls associated with status indication and bypass indication in accordance with IEEE Std 603-1991, Clauses 5.8.2, 5.8.3, 5.8.3.1, 5.8.3.2, and 5.8.3.3. If the design affects indications used by the operator for manual control, status indications, or bypass indication, the LAR should describe how the modifications support the ability of the operator to use the indications in accordance with IEEE Std 603-1991, Clause 5.8.4.

D.2.2.2 Evaluation

The safety evaluation should describe the new architecture. The reviewer should evaluate whether the LAR describes the architecture of the replacement system through text and diagrams, with emphasis on changes from the existing system. The reviewer should evaluate whether the drawings in the LAR explain the modification, including block diagrams showing channels and divisions and drawings showing changes to human-system interfaces. The reviewer should evaluate whether the LAR text describes what is being changed and how the change meets regulations and general or licensed plant design criteria (see Section D.2.6 of this ISG).

The reviewer should evaluate whether the LAR defines the extent to which the replacement system architecture is constrained by the existing plant architecture (including electrical divisions and mechanical trains), sensor and actuator physical arrangement, capabilities of the sensors and actuators, existing plant wiring, and functions performed by the existing system.

The reviewer should evaluate whether the LAR defines the mapping of logic channels and logic divisions to electrical divisions, as well as any mapping to engineered safety features mechanical trains.

The reviewer should evaluate whether added, deleted, or modified connections (including temporary connections for maintenance) between the following are described and meet regulatory criteria:

1.a. between safety-related systems

1.b. between safety-related and non-safety-related systems

The reviewer should evaluate whether the LAR justifies changes (including modifications, additions, and deletions) and demonstrates that the changes do not adversely affect plant safety for each of the following:

2.a. plant system design functions

2.b. connections within the safety-related system, including cross-divisional interfaces and connections to human-system interfaces

2.c. connections between safety-related systems

2.d. connections between safety-related and non-safety-related systems and the identification of signal and data isolation devices

2.e. indications used for manual control

2.f. temporary connections (e.g., for maintenance workstations)

The reviewer should evaluate whether changes to the system design functions are identified, documented, and justified to meet the revised licensing basis. The reviewer should confirm that the service/test functions described in the LAR meet the requirements of IEEE Std 603-1991, Clause 5.7. Section D.2.3.2 discusses the evaluation of the service/test functions. The reviewer should evaluate whether the self-test and self-diagnostic portions of the service/test functions provide adequate fault detection capabilities to conform to the guidance in IEEE Std 7-4.3.2-2003, Clauses 5.5.2 and 5.5.3 (thereby meeting the requirements of IEEE Std 603-1991, Clause 5.7). The reviewer should evaluate the level of detail included in the LAR for the malfunctions detected by the service/test functions to ensure that these malfunctions are annunciated.

If the design includes a DAS, then the reviewer should evaluate whether the LAR describes how the integration of the system and the DAS meets regulatory requirements. Section D.2.5 discusses the evaluation of DAS interfaces. Sections D.2.6.2.2 and D.2.6.2.4 describe how the staff should evaluate the implementation of independence, defense-in-depth, and diversity between the DAS and the proposed system.

If the LAR discusses any interfaces with post-accident monitoring instrumentation, the reviewer should evaluate whether the replacement design adversely affects the required capabilities and data display functions.

If the design affects indications used by the operator for manual control, status indications, or bypass indication, the reviewer should evaluate those changes in accordance with IEEE Std 603-1991, Clauses 5.8.1, 5.8.2, 5.8.3, 5.8.3.1, 5.8.3.2, 5.8.3.3, and 5.8.4.

SRP Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std 603,” provides acceptance criteria for IEEE Std 603 for those clauses applicable to this section. SRP

Appendix 7.1-D, “Guidance for Evaluation of the Application of IEEE Std 7-4.3.2,” provides acceptance criteria for IEEE Std 7-4.3.2 for those clauses applicable to this section.

D.2.3 New System Functions

D.2.3.1 Information To Be Provided

The LAR should describe the existing functions (i.e., design functions and service/test functions) performed by the portion(s) of the system being replaced. The LAR should also describe new functions.

Each design function’s description should include equipment from sensor to actuated device(s), including logical operation, manual versus automatic, and any interdependencies (e.g., signal split and used in a safety function as well as in a display in the control room).

Each design function’s description should include the following:

1.a. identification of the safety functions, including the trip/actuation functions credited for each anticipated operational occurrence and postulated accident

1.b. all monitored variables used to control each protective action

1.c. minimum number and location of sensors and equipment relied upon for protective purposes

1.d. functionality—if there are TS setpoint changes, include input/output ranges and setpoints (for trip functions, the documentation defines the margins between setpoints and allowable values (including all applicable uncertainties))

1.e. performance, including accuracy and response times (where appropriate, performance requirements are defined for different initial plant conditions and design-basis events)

1.f. appropriate signal filtering, signal validation, and interlocks to minimize the potential of spurious actions

1.g. the safety classification of each safety function and whether there are independence constraints from other functions based on safety classifications

1.h. the range of transient and steady-state conditions throughout which the safety-related systems should perform, including conditions (e.g., environmental, plant process) with the potential to degrade the functions of safety-related system performance

The LAR should address each IEEE Std 603-1991 requirement in Clause 4 for each design function. Although most IEEE Std 603-1991 requirements in Clause 4 may be addressed for each design function, some may be addressed for the system. For example, IEEE Std 603-1991, Clause 4.9, may identify reliability methods used for all design functions.

The LAR should address each of the listed IEEE Std 603-1991 requirements for each service/test function. As with design functions, some service/test functions may be addressed for the system. These service/test functions should conform to the guidance in Clause 5.5 guidance in IEEE Std 7-4.3.2-2003, Clauses 5.5.2, “Test and Calibration,” and 5.5.3, “Fault Detection and Self-Diagnostics,” to meet the requirements in IEEE Std 603-1991, Clause 5.7 for digital equipment. Regarding service/test functions, the LAR should demonstrate compliance with the following:

2.a. Clauses 5.2 and 7.3, “Completion of Protective Action”

2.b. Clause 5.5, “System Integrity”

2.c. Clauses 5.7, 6.5, 6.5.1, and 6.5.2, “Capability for Testing and Calibration”

2.d. Clause 5.8, “Information Displays”

2.e. Clause 5.9, “Control of Access”

2.f. Clause 5.10, “Repair”

2.g. Clauses 6.6 and 7.4, “Operating Bypasses”

2.h. Clauses 6.7 and 7.5, “Maintenance Bypass”

2.i. Clause 6.8, “Setpoints” (partial compliance, for variables with multiple setpoints depending on plant condition)

The discussion of self-tests and self-diagnostics should demonstrate compliance with any proposed TS for new system functions.

The LAR should state how the quality requirements of IEEE Std 603-1991, Clause 5.3, are being (or will be) met.

D.2.3.2 Evaluation

Through an evaluation of system design information, the reviewer should confirm that the design-basis information provided in the LAR satisfies Clause 4 of IEEE Std 603-1991. The system design information includes design function descriptions, functional block diagrams, descriptions of operation, architectural descriptions, and other submitted design details.

The reviewer should evaluate whether the test and calibration portions of the service/test functions meet the needs for those features to support the design functions of applicable modes of plant and system operation. The reviewer should evaluate whether the platform-specific service/test functions meet the IEEE Std 603-1991 clauses listed in Section D.2.3.1 of this ISG. The NRC may have previously reviewed the service/test functions (e.g., internal diagnostics, calibration, and surveillance test support) as part of a topical report safety evaluation on the digital equipment. The reviewer should evaluate whether the LAR addresses any application-specific implementation of service/test functions and any changes to the service/test functions since topical report approval.

Section D.7.2.1 addresses the evaluation of TS and the self-tests and self-diagnostics that are implemented for new system functions.

SRP Appendix 7.1-C provides acceptance criteria for IEEE Std 603-1991 for those clauses applicable to this section. SRP Appendix 7.1-D provides acceptance criteria for IEEE Std 7-4.3.2-2003 for those clauses applicable to this section.

D.2.3.3 System Requirements Documentation

D.2.3.3.1 Information To Be Provided

The NRC staff should verify that the application includes a System Requirements Specification (SyRS) or other document with equivalent content. Although the document may have a different

title, the content should be consistent with the descriptions below. The staff uses the SyRS to confirm that what is being designed is consistent with what is being reviewed in the LAR. The SyRS is a product of the modification life cycle development process and bounds the design.

This section uses the definitions from the International Electrotechnical Commission Std 61513, "Nuclear Plants—Instrumentation and Control Important to Safety—General Requirements for Systems," paraphrased below to fit modifying and replacing existing systems, rather than designing new systems.

The SyRS provided should address the overall architecture of the I&C systems, including but not limited to the following:

1.a. defining system requirements for the I&C functions in the modification's scope and the modification's effects on associated systems and equipment within the plant's safety analysis

1.b. defining the plant layout for the modification scope

1.c. defining the operational context for the modification scope and changes resulting from the modification

1.d. structuring the overall I&C architecture and assigning I&C functions to the modification scope

1.e. identifying the design criteria for the modification scope, including ensuring that features providing defense-in-depth in the existing system are not compromised and minimizing the potential for common-cause failure (CCF)

1.f. describing how the modification fits within the overall architecture of the plant's I&C systems and any changes to the architecture

1.g. defining system interfaces and the reasons for the interfaces (see Section D.2.5.1 of this ISG)

The SyRS should address the requirements that are specific to digital implementations. The licensee will ensure the implementation of requirements and processes needed to ensure that the modification can be integrated, commissioned, operated, and maintained.

The SyRS should describe the system-level design, hardware and software design requirements, and the arrangement of equipment to assess the allocation of design functions described in Section D.2.4. The I&C architecture, plant design bases, and functional assignments are inputs to the SyRS.

The SyRS should contain provisions for digital equipment quality to comply with IEEE Std 603-1991, Clause 5.3.

The SyRS should contain functional and performance requirements that are consistent with the replacement system functions in Section D.2.3.1.

The SyRS should establish the following for each design function:

2.a. functionality—if there are TS setpoint changes, include input/output ranges and setpoints (for trip functions, the documentation defines the margins between setpoints and allowable values (including all applicable uncertainties))

2.b. performance, including accuracy and response times; where appropriate, performance requirements are defined for different initial plant conditions and design basis events

2.c. appropriate signal filtering, signal validation, and interlocks to minimize the potential for spurious actions

The SyRS should specify boundaries and interfaces with other systems, including independence requirements per IEEE Std 603-1991, Clause 5.6. Other boundary and interface information specified should include the following:

3.a. intended location and the physical constraints relevant to the installation of the system in the plant

3.b. physical and functional interfaces of the system with the supporting systems and equipment

3.c. physical and functional interfaces of the system with other systems and equipment with which it exchanges information

3.d. interfaces with the operator or maintenance technician

The SyRS should specify environmental conditions applicable to the system (see Section D.3 of this ISG). The normal and extreme ranges of environmental conditions that the system is required to withstand should be specified in accordance with the constraints imposed from the plant design framework. Environmental conditions specified should include the following:

4.a. temperature, humidity, pressure, and radiation during normal operation and accident conditions

4.b. conditions imposed by potential hazards external to the system, including seismic conditions, electromagnetic interference, and flooding

4.c. power supply and heating and ventilation conditions

4.d. conditions specified for environmental qualification of hardware based on design bases functions (For computer-based systems, this qualification addresses the hardware (including its ability to perform its safety functions under the applicable environmental conditions), the operating system software (if applicable), and representative application software, both integrated in the hardware, based on IEEE Std 7-4.3.2-2003, Clause 5.4, and IEEE Std 603-1991, Clause 5.4)

The SyRS should establish the requirements for any service/test functions available in the system's NRC-approved platform. The requirements for these functions are determined on a case-by-case basis depending on equipment complexity. These functions could include self-diagnostics/testing, maintenance, etc.

D.2.3.3.2 Evaluation

The reviewer should evaluate the SyRS to confirm:

a. that the SyRS contains the Section D.2.3.3.1 information, and
b. that the Section D.2.3.3.1 information is consistent with the design information contained in the LAR.

D.2.4 Functional Allocation

D.2.4.1 Information To Be Provided

The LAR should describe the allocation of design and service/test functions (see Section D.2.2.1 of this ISG for the description of these functions) to the various elements of the proposed architecture (e.g., hardware, software, and operators using human-system interfaces).

The LAR should use text and drawings to describe how functions (e.g., logic functions) are distributed into physical hardware.

The LAR should demonstrate how the range of response times in the new design falls within the range of response times credited in the accident analysis for the applicable modes of replacement system operation.

The LAR should include a mapping of logic drawings (i.e., functions) to logic elements in the system. The LAR should describe the mapping of design functions and auxiliary features to software, hardware, MOAs, or some combination of the software, hardware, and MOAs.

D.2.4.2 Evaluation

The reviewer should evaluate whether the range of system response times given in the LAR includes all interlock and monitoring functions identified in the system architecture and SyRS. The reviewer should evaluate whether the response time range falls within the range of response times credited in the accident analysis for the applicable modes of replacement system operation.

SRP BTP 7-21, “Guidance on Digital Computer Real-Time Performance,” provides regulatory guidance for reviewing digital system real-time system architectures in DI&C systems.

The reviewer should evaluate whether the rationale provided by the LAR for each interface justifies the presence of each interface or logical group of interfaces defined in the LAR. The reviewer should evaluate whether the list of interfaces is complete.

The reviewer should evaluate whether the LAR defines and justifies any changes to the existing logic drawings, as well as changes to the existing plant interfaces and their effect on plant safety and licensing basis.

For this evaluation, the reviewer should consider IEEE Std 603-1991, Clauses 5.1 and 5.6. SRP Appendix 7.1-C provides acceptance criteria for IEEE Std 603-1991 for those clauses applicable to this section. SRP Appendix 7.1-D provides acceptance criteria for IEEE Std 7-4.3.2-2003 for those clauses applicable to this section.

D.2.5 System Interfaces

D.2.5.1 Information To Be Provided

The LAR should provide documentation and drawings as necessary to illustrate, explain, and justify data distribution within and external to the system, including all interfaces, whether these interfaces are hardwired or use data communications and whether they are point-to-point, multiplexed, or networked. This discussion should include those aspects of the design that maintain independence between channels and divisions.

The LAR should identify and describe each of the following, whether existing, modified, deleted, or added:

1.a. input and output interfaces with other plant equipment (e.g. mechanical components) and plant sensor or actuators, whether hardwired or using some form of data communication, including provisions for isolation

1.b. interfaces with control room displays, indicators, controls, and alarm systems, including the system's role and interfaces with post-accident monitoring and any reference by emergency plan implementing procedures, including provisions for isolation (including credited manual operator actions)

1.c. human-system interfaces for the licensee's maintenance and engineering workstations used for test and maintenance, whether considered internal or external to the new plant system, including provisions for isolation

The LAR should identify and describe each of the following:

2.a. support and auxiliary systems, normal power sources, emergency power sources, and heating, ventilation, and air conditioning (HVAC), including the impact of single failure in a supporting system, the diverse means of annunciating such failures, and the means of repair and restoration; this includes the HVAC and the diverse means of annunciation of HVAC failure, along with a coping procedure

2.b. if a NRC-approved topical report is referenced, the communication features from this topical report that are proposed for the replacement system

2.c. how identified hazards are controlled in communication features

2.d. how hazards are handled in the design, demonstrating elimination or at least mitigation of the hazards in each interface or logical group of interfaces

2.e. how malfunctions are detected by the self-test and self-diagnostics for each interface or logical group of interfaces

2.f. features that affect the SOE (see Section D.8.1 of this ISG)

2.g. if multidivisional controls and displays are applied, how the controls and displays are applied in accordance with DI&C-ISG-04

The LAR should describe methods applied in the hardware and in the logic that are intended to minimize the potential for spurious actuation caused by malfunctions in the interfaces or the connected equipment.

For each data communication interface, the LAR should demonstrate how the SOE is maintained when using that interface and reference the secure development and operational environment (SDOE) discussion in the LAR.

The LAR should demonstrate that any interface requiring electrical isolation is provided with sufficient electrical isolation, based on the electrical hazards present and the electrical isolation criteria in SRP BTP 7-11, “Guidance on Application and Qualification of Isolation Devices.”

The LAR should describe the use of power sources, electric and non-electric, and should state how the system continues to perform its credited safety functions while power sources are bypassed for maintenance as required by IEEE Std 603-1991, Clauses 8.1, 8.2, and 8.3.

The LAR should demonstrate how the communication features meet the criteria of IEEE Std 603-1991, Clauses 5.6.1, 5.6.2, 5.6.3, 5.6.3.1, 5.6.3.2, 5.6.3.3, and 5.6.4, and IEEE Std 7-4.3.2-2003, Clause 5.6.

The LAR should demonstrate how each clause in DI&C-ISG-04 is being met or justify the proposed alternatives when an individual clause is not met. If priority logic modules are provided or priority logic is embedded in a digital system, the LAR should demonstrate conformance with the applicable guidance of DI&C-ISG-04.

The LAR should define interfaces between the different elements of the proposed architecture that are within the scope of the modified portion(s) of the system. Interfaces should include all communication interfaces with permanently installed and temporary workstations.

The LAR should describe and justify the use of redundancy in interfaces internal to a division for satisfying existing reliability goals or otherwise meeting or exceeding the reliability of the existing system. The description of redundancy should include methods to detect malfunctions in redundant links, to inform maintenance staff, and to support troubleshooting, repair, and restoration.

The LAR should describe use of systems in multi-unit stations and demonstrate how malfunctions in one station will not affect the other station or stations, addressing IEEE Std 603-1991, Clause 5.13.

The LAR should describe the human-system interfaces to be provided, and address changes from the existing human-system interfaces. The LAR should describe or reference the human factors engineering processes and results used for compliance with IEEE Std 603-1991, Clause 5.14.

The discussion of self-tests and self-diagnostics should demonstrate conformance to any proposed TS associated with system interfaces.

D.2.5.2 Evaluation

The reviewer should consider that DI&C-ISG-04, Section 3, applies to workstations without regard to the following:

1.a. whether the workstations are permanently installed or portable

1.b. whether the workstations provide direct or indirect control of safety equipment (e.g., non-safety-related workstations that interface with safety-related workstations to control safety equipment)

1.c. whether the workstations control safety equipment through means other than direct data communications (e.g., translation of data communication signals to hardwired signals through the use of associated circuits to the safety-related system)

With regard to the guidance in DI&C-ISG-04 that addresses communications features in safety-related systems to cope with "any operation, malfunction, design error, communication error or software error or corruption," the NRC reviewer should determine whether the LAR submittals address the following:

2.a. information that identifies communications hazards for the plant-specific system, hardware and/or application software in addition to those reviewed in a referenced NRC-approved topical report and an explanation of how these hazards are controlled

2.b. information on the elimination, or at least mitigation, of the plant-specific design communication hazards that the referenced NRC-approved topical report does not address

The NRC reviewer should evaluate the following:

3.a. the description of the interfaces between the portions of the system being replaced and the portions of the system and the plant that are unchanged

3.b. whether the LAR defines the connections between this system and other safety-related systems with a rationale and set of requirements for each connection

3.c. whether the LAR defines the connections between this system and any non-safety-related systems with a rationale and set of requirements for each connection

3.d. whether the LAR documents the functionality and purpose of sensors and actuators and how the sensors and actuators interface with the logic

3.e. whether the LAR defines any connection allowing communication from a non-safety-related system to a safety-related system with a demonstrated and justified purpose and whether the safety-related system is designed with protection from any adverse action by the non-safety-related system

3.f. whether the safety function and the SOE for the safety-related system are compromised by any connection

3.g. whether the LAR demonstrates electrical isolation for any signal crossing electrical or classification boundaries

3.h. whether the LAR defines the hardwired interfaces, including any manual actuation means provided for operator use

3.i. whether the defined use of the hardwired interfaces is consistent with the previous system and with any changes, including the rationale for the changes

3.j. whether the information or controls associated with MOA are subject to a digital CCF that would adversely affect the ability to perform the credited safety function manually

Although this list mentions features that affect the SOE, Section D.8 of this ISG presents guidance for their review.

The reviewer should evaluate how the communication features meet the criteria of IEEE Std 7-4.3.2-2003, Clause 5.6, and the requirements of IEEE Std 603-1991, Clauses 5.6.1, 5.6.2, 5.6.3, 5.6.3.1, 5.6.3.2, 5.6.3.3, and 5.6.4, and how the communication features address the electrical isolation criteria in SRP BTP 7-11. The reviewer should evaluate each hardwired connection, or logical group of similar hardwired connections, for electrical isolation and data independence.

The reviewer should evaluate whether the LAR describes the function of each hardwired connection, including whether the hardwired connection provides a discrete or an analog signal and the use of that signal in the receiving equipment. The reviewer should evaluate whether the LAR describes the function of each data communication connection, including the content of the data packet and methods used to minimize data corruption, as well as the use of that signal in the receiving equipment.

Section D.7.2.1 of this ISG addresses the evaluation of TS and the self-tests and self-diagnostics that are implemented for system interfaces.

The reviewer should evaluate whether the LAR describes adequate isolation by describing the electrical connections between safety divisions in sufficient detail to define the electrical division assigned to each connection, how divisional (or equipment location) isolation is maintained, and how isolation is provided between electrical divisions or equipment locations. This is especially critical for connections such as anticipatory trips, where non-safety-related systems provide anticipatory trip signals to safety-related systems.

The reviewer should evaluate whether those portions of the design associated with multi-unit stations comply with IEEE Std 603-1991, Clause 5.13.

The reviewer should evaluate whether the human-system interfaces and human factors engineering portions of the LAR comply with IEEE Std 603-1991, Clause 5.14.

The reviewer should evaluate whether the LAR has addressed each applicable clause in DI&C-ISG-04 in sufficient detail, or whether the proposed alternatives address the underlying hazard. To enable the reviewer to forego review of the LAR in regard to a particular clause of ISG-04, the LAR should provide an explanation, but not a detailed evaluation, for why that particular clause does not apply to the proposed design. The reviewer should assess the proposed alternative against the following regulatory requirements and guidance:

4.a. IEEE Std 603-1991, Clause 5.6, provides requirements for independence.

4.b. IEEE Std 7-4.3.2-2003 provides guidance on how digital systems can meet the independence requirement in IEEE Std 603-1991, Clause 5.6.

4.c. SRP BTP 7-11 provides guidance for the application and qualification of isolation devices. BTP 7-11 applies to the use of electrical isolation devices for connections between redundant portions of safety-related systems or between safety-related and non-safety-related systems.

4.d. SRP Section 7.9, “Data Communications Systems,” also contains guidance for data communication systems.

The reviewer should evaluate whether the LAR addresses conformance with the independence guidance in DI&C-ISG-04 for any digital multidivisional safety-related controls and displays and any digital multidivisional non-safety-related controls and displays.

The reviewer should evaluate whether the LAR addresses conformance with the guidance in IEEE Std 7-4.3.2-2003 and the requirements of IEEE Std 603-1991, Clause 5.12, "Auxiliary Features," for traditional auxiliary features (e.g., HVAC, emergency power).

The reviewer should evaluate whether the use of electric and non-electric power sources complies with the requirements in IEEE Std 603-1991, Clauses 8.1, 8.2, and 8.3.

If the design provides separate priority logic modules, the reviewer should evaluate whether the LAR describes how the design conforms to the guidance in Section 2 of DI&C-ISG-04 and in Sections 1 and 3 of that ISG as appropriate for the design. If priority logic is embedded in a digital system, the reviewer should evaluate whether the LAR identifies, describes, and demonstrates how the design conforms to the guidance in DI&C-ISG-04, Section 2.

SRP Appendix 7.1-C provides acceptance criteria for IEEE Std 603-1991 for those clauses applicable to this section. SRP Appendix 7.1-D provides acceptance criteria for IEEE Std 7-4.3.2-2003 for those clauses applicable to this section.

D.2.6 Fundamental Design Principles in the New Architecture

This section explains the new architecture in terms of the fundamental design principles.

D.2.6.1 Information To Be Provided

In accordance with Section D.2.2.1, the LAR should describe the replacement system architecture that is intended to provide a basis for discussion of the fundamental design principles. This information supports the discussions in all five of the sections below (i.e., redundancy, independence, deterministic behavior, defense-in-depth and diversity, and simplicity). Each section describes additional information needed to support its particular area.

D.2.6.2 Evaluation

SRP Appendix 7.1-C provides acceptance criteria for IEEE Std 603-1991 for those clauses applicable to these sections. SRP Appendix 7.1-D provides acceptance criteria for IEEE Std 7-4.3.2-2003 for those clauses applicable to these sections.

D.2.6.2.1 Redundancy

Redundancy helps ensure that a single failure will not cause the loss of a safety-related system's ability to perform safety functions.

D.2.6.2.1.1 Information To Be Provided

The NRC staff should verify that the licensee has demonstrated the use and application of redundancy in the new architecture.

The NRC staff should verify that the licensee has demonstrated, by implementing an FMEA, that the use and application of redundancy in the new architecture ensures that the safety functions can be achieved in the event of a postulated single failure. The FMEA should document the postulated failures and the effects of the failures on the plant, as well as on the system. The FMEA should provide sufficient detail on the evaluation of failures, such as failure

of an individual input, an input module, a processing module, a voter, an output module, and an individual output.

The NRC staff should verify that the licensee has demonstrated that the use and application of redundancy in the new architecture support the associated TS (e.g., limiting conditions for operation (LCOs), action statements, and surveillance requirements (SRs)). If the LAR includes changes to the associated TS, then this demonstration should address the proposed TS.

D.2.6.2.1.2 Evaluation

The reviewer should evaluate whether the scope and level of detail are sufficient to demonstrate that the new architecture meets the following clauses of IEEE Std 603-1991 when applying the associated guidance of IEEE Std 7-4.3.2-2003:

1.a. Clause 5.1, “Single-Failure Criterion”

1.b. Clause 5.15, “Reliability”

1.c. Clause 6.7, “Maintenance Bypass”

1.d. Clause 7.5, “Maintenance Bypass”

For the single-failure criterion, the reviewer should evaluate whether the use and application of redundancy in the new architecture conform to the guidance in RG 1.53, “Application of the Single-Failure Criterion to Safety Systems,” which endorses IEEE Std 379, “IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.”

The reviewer should evaluate whether the use and application of redundancy in the new architecture meet the following general design criteria (GDC) of Appendix A, “General Design Criteria for Nuclear Power Plants,” to 10 CFR Part 50:

2.a. GDC 21, “Protection System Reliability and Testability”

2.b. GDC 24, “Separation of Protection and Control Systems”

Section D.7.2.1 of this ISG addresses the evaluation of TS and redundancy.

D.2.6.2.2 Independence

Independence ensures that failures are not propagated across independent domains.

D.2.6.2.2.1 Information To Be Provided

The NRC staff should verify that the licensee has demonstrated the use and application of physical, electrical, and functional independence in the new architecture. Section D.2.5 of this ISG addresses data communications independence.

D.2.6.2.2.2 Evaluation

The reviewer should evaluate whether the scope and level of detail are sufficient to demonstrate that the new architecture meets the following clauses of IEEE Std 603-1991 when applying the associated guidance of IEEE Std 7-4.3.2-2003:

1.a. Clause 5.6, “Independence”

1.b. Clause 5.11, “Identification”

1.c. Clause 6.3, “Interaction with Other Systems”

The reviewer should evaluate whether the use and application of physical and electrical independence in the new architecture conform to the guidance in RG 1.75, “Criteria for Independence of Electrical Safety Systems,” which endorses IEEE Std 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.”

The reviewer should evaluate whether the use and application of functional independence in the new architecture ensure that physically and electrically independent portions of safety-related systems do not depend on information from other independent portions of the safety-related system. Note that coincidence voting is permitted to depend on information from other independent portions of the safety-related system. The reviewer should evaluate whether the use and application of independence in the new architecture meet the following GDC:

2.a. GDC 13, “Instrumentation and Control”

2.b. GDC 21, “Protection System Reliability and Testability”

2.c. GDC 22, “Protection System Independence”

2.d. GDC 23, “Protection System Failure Modes”

2.e. GDC 24, “Separation of Protection and Control Systems”

D.2.6.2.3 Deterministic Behavior

Deterministic behavior ensures predictable and repeatable behavior of systems performing safety functions.

D.2.6.2.3.1 Information To Be Provided

The NRC staff should verify that the licensee has demonstrated the use and application of deterministic behavior in the new architecture.

D.2.6.2.3.2 Evaluation

The reviewer should evaluate whether the scope and level of detail are sufficient to demonstrate that the new architecture meets the following clauses of IEEE Std 603-1991 and the associated guidance of IEEE Std 7-4.3.2-2003 (as applicable):

1.a. Clause 5.2, “Completion of Protective Action”

1.b. Clause 5.5, “System Integrity”

1.c. Clause 6.1, “Automatic Control”

1.d. Clause 6.2, “Manual Control”

1.e. Clause 7.1, “Automatic Control”

1.f. Clause 7.2, “Manual Control”

The reviewer should evaluate whether the use and application of deterministic behavior in the new architecture meet the following GDC:

2.a. GDC 13, “Instrumentation and Control”

2.b. GDC 21, “Protection System Reliability and Testability”

2.c. GDC 23, “Protection System Failure Modes”

2.d. GDC 29, “Protection Against Anticipated Operational Occurrences”

The reviewer should evaluate whether the deterministic behavior of the new architecture ensures the following:

3.a. Input signals and system characteristics result in output signals through known relationships among system states and responses to those states.

3.b. The system produces the same outputs for a given set of input signals (and the sequence of inputs) within well-defined response time limits to allow the timely completion of credited actions.

The reviewer should evaluate whether the deterministic behavior of digital data communication outputs ensures the following:

4.a. The replacement system architecture satisfies the system timing derived from the analyses of design-basis events.

4.b. The replacement system architecture and communication protocols provide features to ensure that the system produces the correct response to inputs within the time credited to produce a response.

4.c. The design adequately identifies and accounts for hazards that could challenge predicted behavior.

If an NRC-approved platform (described in a topical report) is used and the following two conditions are met, then the review should focus on the acceptable use of the communications in the system design and architecture:

(1) The system design and architecture information specify the use of the platform’s standard data communications.

(2) The NRC has already reviewed and approved the deterministic behavior of these communications as part of the topical report.

The NRC should review compliance with any restrictions on the DI&C platform communications to confirm compliance with the conditions identified in the NRC-approved topical report safety evaluation. The review should evaluate whether the credited response time can be met using the standard communication methods provided by the platform.

D.2.6.2.4 Defense-in-Depth and Diversity

Defense-in-depth and diversity are (D3) methods can be used to protect against CCFs.

D.2.6.2.4.1 Information To Be Provided

The NRC staff should verify that the licensee has demonstrated, via a D3 evaluation, that the use and application of D3 in the new architecture ensure that safety functions are accomplished in the event of a postulated CCF.

D.2.6.2.4.2 Evaluation

The reviewer should evaluate whether the scope and level of detail are sufficient to demonstrate that the new architecture meets the following GDC:

a. GDC 13, “Instrumentation and Control”
b. GDC 22, “Protection System Independence”
c. GDC 24, “Separation of Protection and Control Systems”

The reviewer should evaluate whether the licensee’s D3 assessment conforms to the guidance in SRP BTP 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” including use of an analysis as described in NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” issued December 1994.

The reviewer should evaluate whether the use and application of D3 in the new architecture meets 10 CFR 50.62, “Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants.”

D.2.6.2.5 Simplicity of Design

Evaluation of this principle relies more heavily on engineering judgment than the other fundamental design principles; therefore, rather than attempting to evaluate the adequacy of the modified system design’s simplicity solely using a set of defined criteria, the reviewer should evaluate the rationale for those design decisions that result in the replacement system architecture being more complex than it might be otherwise.

D.2.6.2.5.1 Information To Be Provided

The NRC staff should verify that the licensee has demonstrated the use and application of simplicity in the new architecture, focusing on the simplicity (or lack thereof) resulting from design decisions that affect redundancy, independence, deterministic behavior, and D3.

For design decisions resulting in more complex approaches than might otherwise have been chosen, the NRC staff should verify that the licensee has demonstrated that the benefit(s) obtained, particularly with respect to the other fundamental design principles, justify the reduction in simplicity. Design decisions involving such tradeoffs may be driven by the need to satisfy a regulatory requirement (e.g., surveillance testing, improved maintainability or operability for faulted conditions).

D.2.6.2.5.2 Evaluation

The reviewer should evaluate, for design decisions resulting in more complex approaches than might otherwise have been chosen, whether the benefit(s) obtained, particularly with respect to the other fundamental design principles, justifies the reduction in simplicity.

The reviewer should evaluate whether the new architecture meets IEEE Std 603-1991, Clause 6.4, “Derivation of System Inputs.”

D.3 Hardware Equipment Qualification

D.3.1 Information To Be Provided

The NRC staff should verify that the licensee has demonstrated that the system will perform its safety functions under the design-basis conditions at the location in which the equipment will be installed. This information should be found in equipment qualification test plans, methodologies, and test reports. The NRC staff should verify that the licensee has included a summary of documents referencing detailed test reports to support this conclusion (e.g., seismic test reports or analysis, electromagnetic compatibility reports, environmental test reports). The summary should document the results of the qualification testing. The summary should compare the standards and test limits to which the equipment has been qualified and should compare the equipment qualification test limits to the licensee-established plant environmental conditions. The LAR should describe and justify any discrepancies between equipment qualification test limits and expected plant environmental conditions.

In the Tier 1, 2, and 3 Review Process, the information should be provided as follows:

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

Phase 2: (1) Qualification Test Methodologies

(2) Summary of EMI, Temperature, Humidity, and Seismic Test Results

The NRC staff should verify that, in those cases for which the hardware qualification has previously been demonstrated by the vendor and evaluated by the NRC staff, the licensee has referenced that evaluation. The LAR should identify and justify any deviations or revision changes.

D.3.2 Evaluation

The reviewer should evaluate whether the information demonstrates that the hardware is designed to operate in the specified environment. This includes both the normal operating conditions and the worst conditions expected during the abnormal and accident conditions in which the equipment is expected to perform its safety functions.

The following are the regulatory requirements for the design of safety-related equipment to withstand environmental conditions:

a. 10 CFR Part 50, Appendix A, GDC 2, "Design Bases for Protection Against Natural Phenomena," and GDC 4, "Environmental and Dynamic Effects Design Bases"

b. 10 CFR 50.55a(h), which incorporates, based on the date the construction permit was issued, either IEEE Std 279, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," Clause 4.4, or IEEE Std 603-1991, Clause 5.4

c. 10 CFR Part 50, Appendix B, Criterion III, "Design Control"[6]

The following guidance provide criteria for the design of safety-related equipment to withstand environmental conditions:

a. RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2-2003, Clause 5.4

b. RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," which endorses IEEE Std 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," including five enhancements and exceptions

c. RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems"

To comply with the regulatory requirements, the information provided should demonstrate through environmental qualification that I&C systems meet design-basis and performance criteria when the equipment is exposed to normal and adverse environments. The testing should include exposure to the most severe conditions expected at the location of the equipment, including temperature, humidity, radiation, electromagnetic and radio interference, and seismic input, depending on the requirement. While testing against all of these stressors, the system should be functioning with software and diagnostics representative of those used in actual operation. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces. For digital systems located in mild environments, Regulatory Position 1 in RG 1.209 states that the NRC does not consider the age conditioning in IEEE Std 323, Section 6.2.1.2, to apply because of the absence of significant aging mechanisms.

The NRC staff should evaluate the various test plans to ensure that the plans are rigorous enough to support the conclusion that the environment should not have a negative effect on the ability of the system to perform its safety function in the worst case environment in which it needs to operate. The NRC staff should evaluate the comparison that shows that the equipment qualification envelopes the worst case plant conditions for each environmental stressor at the location where the equipment is proposed to be installed.

If any portions of this equipment will be subject to a harsh environment, then additional disciplines should participate in the review of equipment qualification for meeting GDC 4 and 10 CFR 50.49, "Environmental qualification of electric equipment important to safety for nuclear

[6] In accordance with 10 CFR Part 50, Appendix B, Criterion III, if a test program is used to verify the adequacy of the design, suitable qualification testing should be performed.

power plants," to ensure that the requirements for equipment qualification to harsh environments are met.

D.4 Digital Instrumentation and Control System Development Processes

D.4.1 Information To Be Provided

The NRC staff should verify that the licensee has described the proposed framework being used to design and develop DI&C safety-related systems under the Alternate Review Process. This framework should supplement the licensee's overall QA program descriptions with specific system, hardware, and software development activities, including a description of the proposed development life cycles, development documents to be produced, and management activities that will be implemented in the design and development of DI&C safety-related systems. In the pre-application (Phase 0) coordination meeting(s), the development documents expected to be available during the LAR review should be identified.

The framework should describe the following system development process activities:

1.a. Create the concepts on which the system design will be based.

1.b. Translate these concepts into system requirements.

1.c. Allocate system requirements to system elements (e.g., software, hardware, and human-system interfaces).

1.d. Implement the design into hardware and software functions.

1.e. Integrate system elements such as software and hardware.

1.f. Test the unit functions and the completed system to confirm that system requirements have been implemented correctly.

1.g. Perform appropriate human factors engineering for the human-system interfaces throughout the development process.

1.h. Analyze hazards and incorporate requirements that eliminate or mitigate identified hazards throughout the development process.

1.i. Perform V&V activities on work products throughout the development process.

The NRC staff should verify that the licensee has demonstrated that the software life cycle process follows the guidance in RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," or, alternatively, has described how the regulatory requirements referenced in RG 1.173 are satisfied. To demonstrate that the software life cycle process follows the guidance, the LAR should include the following:

2.a. description of the software life cycle processes to be used

2.b. identification of any planned exceptions and clarifications

2.c. description of how these planned exceptions and clarifications meet the underlying regulations

The NRC staff should verify that, for any RGs referenced, the licensee has demonstrated how the RG-specific activity follows the guidance of the RG or, alternatively, has described how the

underlying regulatory requirements referenced in the RG are satisfied. To demonstrate that the RG-specific activity follows the guidance, the LAR should include the following:

3.a. description of the RG-specific activity

3.b. identification of any planned exceptions and clarifications

3.c. description of how these planned exceptions and clarifications meet the underlying regulations

The NRC staff should verify that the licensee has identified those development activities addressed as part of the development process defined for an NRC-approved topical report and those activities that are part of the application-specific software development process (i.e., development processes that will be used but that the NRC has not previously reviewed and approved). The NRC staff should also verify that the licensee has addressed the applicable PSAIs defined in the referenced topical reports (see Section D.5 of this ISG).

D.4.2 Evaluation

Using the criteria in this section, the reviewer will evaluate whether the proposed framework described in the LAR is adequate to deliver a high-quality DI&C safety-related system.

The activities that are part of the development process defined for NRC-approved topical report DI&C platform activities, including relevant PSAIs, should be credited to the degree allowed by the platform safety evaluation. The LAR review should focus on the application-specific software development activities that the NRC has not previously reviewed and approved. If the licensee is using an NRC-approved development process for application development (e.g., software program manual), then the LAR should credit these processes to the degree allowed by the applicable safety evaluation of the software program manual, including relevant PSAIs. The reviewer should evaluate whether the software life cycle process description demonstrates that the software life cycle process meets the guidance of RG 1.173 or how the underlying regulatory requirements referenced in RG 1.173 are satisfied.

Sections D.4.2.1 of this ISG describe the criteria against which the NRC reviewer should evaluate the DI&C life cycle process described in the LAR. Sections D.4.2.1.1 through D.4.2.1.4 address life cycle activities that are part of the NRC review scope. Sections D.4.2.1.5 through D.4.2.1.9 describe process evaluations that are part of the NRC review scope. The evaluation of the design outputs using the process described in Sections D.4.2.1.5 through D.4.2.1.9 are not within the scope of the LAR review. The licensee is responsible for ensuring vendor use of procedures and the acceptability of all vendor work products discussed in Sections D.4.2.1.1 through D.4.2.1.9.

D.4.2.1 System and Software Development Activities

To evaluate whether a licensee has described measures that satisfy Criterion III, “Design Control,” of 10 CFR Part 50, Appendix B, the reviewer should determine whether the LAR describes input information, life cycle activities, and output information necessary to develop DI&C safety-related systems, in accordance with applicable regulatory guidance and the design bases. In addition, the LAR should describe the use of industry standards, including any international standards.

The development of DI&C safety-related systems should progress according to a defined life cycle, which is part of the overall system development framework. Although the staff has not recommended a particular life cycle model, the reviewer should evaluate whether the LAR describes life cycle activities and tasks, including inputs and outputs that will be implemented in the development of the proposed DI&C safety-related system. The LAR should also describe the analysis, review, and test activities that will be implemented. The licensee may choose among many different life cycle models for system, hardware, software, and human factors engineering development. Generally, these models differ in the timing of the various activities and tasks used to produce a high-quality product.

The reviewer should evaluate whether the licensee has described a life cycle model that includes processes tailored and relevant to its particular development project and digital technology to implement the activities listed in Sections D.4.2.1.1 through D.4.2.1.9 of this ISG. Based on the common understanding reached during the pre-application (Phase 0) meeting(s), the staff may evaluate a sample of referenced system development process documents to be made available for audit during the LAR review to confirm that the life cycle activities are being (or will be) effectively implemented. The reviewer should apply the review procedure in SRP BTP 7-14, Section B.4, to the extent the design documents are available during the LAR review.

D.4.2.1.1 Plant and Instrumentation and Control System Safety Analysis

The reviewer should evaluate whether the plant and DI&C system safety analysis process description addresses the following:

a. To meet Clause 4 of IEEE Std 603-1991, this information should be consistent with the plant safety analysis provided in the plant's updated FSAR. The LAR should describe changes to the plant safety analysis associated with the DI&C system modification and justify the acceptability of the changes to the plant design basis (see Section D.2 of this ISG).

b. The reviewer should evaluate whether the software safety analysis defines a software integrity level (SIL) scheme to classify software criticality, as specified in IEEE Std 1012, "IEEE Standard for System and Software Verification and Validation," and as endorsed by RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." A software criticality analysis should be performed to determine the SIL of the software necessary to accomplish each safety function. Software that implements auxiliary features or self-diagnostic functions that may be of a lower safety classification should have a SIL consistent with the highest SIL in the hardware module.

D.4.2.1.2 Instrumentation and Control System Requirements

The reviewer should evaluate whether the DI&C system requirements process description addresses the following:

a. DI&C system requirements process development should describe the identification, development, documentation, review, approval, and maintenance of DI&C system requirements. It should include the technical elements described in Section D.2 of this ISG.

b. All identified system requirements, including software and hardware as applicable, should be analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management (CM).

c. A means for requirements traceability should be developed, documented, tracked, and maintained. The requirements traceability documentation should provide bidirectional traceability (from plant system requirements to system validation testing and from plant system requirements to DI&C system requirements).

d. The DI&C system requirements should be used as input to the ongoing life cycle activities.

D.4.2.1.3 Instrumentation and Control System Architecture

The reviewer should evaluate whether the DI&C system architecture process description addresses the following:

a. The DI&C system architecture should be developed on the basis of a defined methodology that provides all necessary I&C functions needed to ensure compliance with applicable NRC requirements. It should include the technical elements described in Section D.2 of this ISG.

b. The DI&C system architecture should be documented, analyzed, reviewed, approved, baselined, updated as necessary, and placed under CM.

c. The DI&C system architecture should be used as input to the ongoing life cycle activities.

D.4.2.1.4 Instrumentation and Control System Design

The reviewer should evaluate whether the DI&C system design process description addresses the following:

a. The design process description should cover how the detailed design of the DI&C system is developed to conform to the plant licensing and design basis described in the LAR, based on the architectural design and encompassing the technical elements described in Section D.2 of this ISG.

b. The DI&C system design should demonstrate bidirectional traceability of the system requirements to the DI&C system design (including the architecture and functional logic designs).

c. DI&C system safety analyses should be reviewed to identify hardware, software, or human-system interfaces that have the potential to cause a hazard or are credited to eliminate or mitigate hazards. The review principles in SRP BTP 7-14,

Section B.3.1.9.4, should be applied to the review of the DI&C system safety analyses. DI&C system safety analyses may be performed by one or more organizations (e.g., design group or V&V team) rather than a single safety organization.

d. The DI&C system design should be analyzed, reviewed, approved, baselined, updated as necessary, and placed under CM.

e. The DI&C system-level design should be used as input to the ongoing life cycle activities.

D.4.2.1.5 Software Requirements

The reviewer should evaluate whether the DI&C software requirements process description addresses the following:

a. Software requirements should be developed to document the functions to be performed by the software. RG 1.172, "Software Requirement Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants," provides an acceptable approach for preparing software requirements and should be applied to the extent practicable when reviewing the software development process description in the LAR. The LAR should identify the system requirements allocated to software. The reviewer should evaluate whether the process for developing the software requirement specifications described in the LAR follows the guidance of RG 1.172 or how the underlying regulatory requirements referenced in RG 1.172 are satisfied.

   To demonstrate the software requirement specification development will conform to the guidance in RG 1.172, the LAR should address the following:

   - Functionality—Describe what the software is supposed to do.
   - External interfaces—Describe how the software interacts with people, the system's hardware, other hardware, and other software.
   - Performance—Describe the speed, availability, response time, and recovery time of various software functions.
   - Attributes—Describe portability, correctness, maintainability, security, and other attributes.
   - Design constraints imposed on implementation—Describe any applicable standards in effect, implementation language, policies for database integrity, resource limits, operating environment(s), etc.

   Ranking requirements for importance or stability for safety-related systems are not mandatory. The reviews of the software requirements development process should focus on activities that the NRC has not previously reviewed and approved unless the NRC acceptance criteria have changed.

b. The reviewer should evaluate whether the software requirements process description addresses the following:

- The software requirements should be analyzed, reviewed, approved, baselined, updated as necessary, and placed under CM. Software requirements should be baselined before initiating software design.

- The software requirements should be derived from and traceable to the system design, DI&C system architecture, and system requirements.

- An independent V&V team should develop the system V&V test plans. SRP BTP 7-14, Section B.3.1.12.4, contains the applicable review guidance for the system V&V test plans.

- The most recently baselined software requirements should be used as input to the ongoing life cycle activities.

D.4.2.1.6 Software Design

The reviewer should evaluate whether the DI&C software design process description addresses the following:

a. The software design decomposes the software requirements to document the design and implementation of software components, modules, and units used to implement the DI&C system. A software unit is the highest element in the software hierarchy. Software units are composed hierarchically of software components and software modules. SRP BTP 7-14 does not endorse any RGs for the technical review of software designs. The reviewer should use the review guidance in items (b) through (j) below to evaluate the process for developing a software design; the guidance should be applied to the extent practicable for the Alternate Review Process LAR review.

b. The software design should include the detailed design for each software element of the system and how the software components, modules, and units are to be constructed.

c. The software design should document, at a minimum, the methods by which software will be refined into lower levels. The methods should allow coding, compiling, and testing, and the division of the software into a set of interacting components, modules, and units. The software design should describe the software components, modules, and units, and define their interfaces and dependencies in a structured fashion.

d. The software design and implementation should fulfill applicable software requirements.

e. The software design should establish the relationship between component(s), software module(s), and software unit(s).

f. The software design should describe how adequate coverage of software requirements is achieved. There should be no unnecessary functions. Predeveloped digital platforms and preexisting software (e.g., operating system software) may contain features that are not used (or not configured for use) in a specific DI&C system. In those cases, the NRC staff should verify that, unless otherwise demonstrated as part of a platform topical report approval, the licensee has identified those unused capabilities. The staff should evaluate whether those functions may affect the performance of the safety function and identify any compensatory measures taken.

g. The documented acceptance and use of support software and tools (e.g., code generating tools, compilers, assemblers, operating systems, coverage analyzers, automated test tools, traceability tools, simulators, and emulators) should be consistent with the guidance in IEEE Std 7-4.3.2-2003, Clause 5.3.2, as endorsed in RG 1.152.

h. The software design should be analyzed, reviewed, approved, baselined, updated as necessary, and placed under CM.

i. An independent V&V team should develop the system V&V test designs.

j. The most recently baselined software design should be used as input to the ongoing life cycle activities.

D.4.2.1.7 Software Implementation

The reviewer should evaluate whether the software implementation process description addresses the following:

a. The software implementation process should define the criteria, test procedures, and data for testing software components, modules, and units.

b. The software implementation process should describe the translation of the detailed design into code in the selected programming language.

c. The code should be capable of executing the safety design features and methods developed during the software design process.

d. The use of documented coding rules, guidelines, methods, standards, and other applicable criteria should be defined and enforced. The coding rules and standards should facilitate understanding, analysis, review, testing, and readability of the implemented code.

e. The correct implementation of software requirements in each software component, module, and unit should be verified to ensure accuracy and conformance with design requirements.

f. Software unit (or component) testing should be performed as software is developed to ensure that it satisfies design requirements. The primary testing methods and standards, test cases used, test coverage, and test results should be documented, controlled, and the documentation maintained. SRP BTP 7-14, Section B.3.2.4, contains the applicable review principles for software unit testing activities, which should be applied to the description of the test process and controls for the Alternate Review Process LAR review. The software implementation process should describe the following:

   - The general approach, resources, and schedule for software unit testing
   - The features to be tested
   - The design of the set of tests
   - The test execution and evaluation controls

   Reviews of the software unit testing process should focus on activities that the NRC has not previously reviewed and approved unless the NRC acceptance criteria have changed.

   The reviewer should evaluate whether the software implementation process description demonstrates that the software life cycle process meets the guidance in RG 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” or how the underlying regulatory requirements referenced in RG 1.171 are satisfied.

g. The development of software test documentation should consist of a description of the software test documentation structure and content.

   It is acceptable for a licensee to adapt test documentation to reflect important process differences, technology differences, and exceptions related to the use of integrated design environment tools. IEEE Std 829, "IEEE Standard for Software and System Test Documentation," allows test documents to be combined or eliminated.

   The reviews of the software test documentation process should focus on activities that the NRC has not previously reviewed and approved, unless the NRC acceptance criteria have changed.

   The reviewer should evaluate whether the software implementation process meets the guidance of RG 1.170, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," or how the underlying regulatory requirements referenced in RG 1.170 are satisfied.

h. The software implementation should be analyzed, reviewed, approved, baselined, updated as necessary, and placed under CM.

i. The software implementation activities should be traceable to the software design, DI&C system architecture, and system requirements.

j. An independent V&V team should develop the system V&V test procedures.

k. The most recently baselined software implementation should be used as input to the ongoing life cycle activities.

l. The software implementation process should ensure that software items conform to the design documentation guidance. SRP BTP 7-14, Section B.3.3.4.3, contains applicable review guidance for code listings which should be applied to the extent practicable for the Alternate Review Process LAR review.

D.4.2.1.8 Software Integration

The reviewer should evaluate whether the software integration process description addresses the following:

a. A software integration process should be developed to describe the methods for integrating software components and modules into software units. Aggregates of components and modules tested during implementation should be integrated into a software unit, in accordance with the integration process. SRP BTP 7-14, Section B.3.1.4.4, contains the review principles for the software integration process, which may need to be adapted to the tool-based methods of modern DI&C platforms.

b. Critical elements of the software integration process should include, but are not limited to, identifying software components, modules, and units for integration; defining and implementing the integration environment; managing interfaces; and identifying item integration sequences. SRP BTP 7-14, Section B.3.3.5.3, contains applicable review guidance for documenting these activities and can be used to inform the review of the software integration process description to the extent practicable for the Alternate Review Process LAR review.

c. Software integration testing should be conducted to verify that software requirements have been adequately implemented for this stage of the software development. SRP BTP 7-14, Section B.3.2.4, contains the applicable review guidance for this activity and

can be used to inform the review of the description of the software integration testing process to the extent practicable for the Alternate Review Process LAR review.

d. The software integration results should be documented, analyzed, reviewed, approved, updated as necessary, and placed under CM.

e. The software integration results should be derived from and traceable to the software design, DI&C system architecture, and DI&C system requirements.

f. The most recently baselined software integration should be used as input to the ongoing life cycle activities.

D.4.2.1.9 Instrumentation and Control System Testing

The reviewer should evaluate whether the description of the DI&C system testing process addresses the following:

a. A system test plan should document the integration and testing of all software items, hardware, manual processes, and other system interfaces that constitute the DI&C system, consistent with the architectural design. An independent V&V team should develop the V&V test plans. SRP BTP 7-14, Section B.3.1.12.4, contains the applicable review guidance for the system V&V test plans.

b. System testing should consider all of the integrated software components, modules, and units that have successfully passed integration testing, as well as the software system itself, integrated with any applicable hardware systems and human-system interfaces.

c. System testing should be conducted on a complete, integrated system, using a baselined version of the hardware and system software, to evaluate the system's performance of the DI&C system requirements.

d. The test plan should include tasks to integrate and test all software, hardware, and human-system interfaces; to prepare the test environment; to write test cases (inputs, outputs, and test criteria); and to test interfaces with other systems.

e. System test results should be documented. Not everything can be tested, and some items are verified and validated by analysis or review. For those items verified by test, test results should be analyzed to verify that DI&C system requirements have been satisfied. SRP BTP 7-14, Section B.3.2.4, contains applicable review guidance for documenting test results and should be applied to the extent practicable for the Alternate Review Process LAR review.

f. Testing should validate the control, mitigation, or elimination of hazards in the DI&C system design.

g. The system test results should be documented, analyzed, reviewed, approved, updated as necessary, and placed under CM.

h. The system test results should be used as input to the ongoing plant system design, installation, and test activities.

D.4.2.2 Project Management Processes

The reviewer should evaluate the LAR description of the project management or organizational processes that will be employed by the QA program and used to define the project's organization, planning, execution, monitoring, control, and closure activities of the entire DI&C safety-related system development effort. The project management concepts listed in SRP

BTP 7-14, Sections B.3.1.1.4 and B.3.1.2.4, can inform the review of the software management process description.

NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," issued June 1996, as cited in SRP BTP 7-14, Section B.3.1.2.4, is not relevant if the licensee is using the tool-based methods of modern DI&C platforms and will apply only to the software coding languages used in the system development.

The reviewer's evaluation of the LAR description of the organizational and project management processes should focus on the following:

a. measures for the creation of plans to control the system development environment, including hardware and software in accordance with Criterion V, "Instructions, Procedures, and Drawings," of Appendix B to 10 CFR Part 50, with the planning process resulting in a set of documents that will be used to control and oversee the development of system elements, including hardware and software
b. controls for identifying the project scope, determination of deliverables, lines of communication, formal and informal reviews, and interfaces with other internal and external organizations
c. provisions for the establishment, documentation, and maintenance of a schedule that considers the overall project, as well as interactions of milestones
d. provisions for risk management, including problem identification, impact assessment, and development of risk-mitigation plans for risks that have the potential to significantly affect system quality goals, with appropriate metrics for tracking resolution progress, in keeping with the additional guidance on software-related project risk activities in IEEE Std 7-4.3.2-2003, Clause 5.3.6
e. establishment of quality metrics throughout the life cycle to assess whether the quality requirements of IEEE Std 603-1991, Clause 5.3, are being met, in keeping with the additional guidance from IEEE Std 7-4.3.2-2003, Clause 5.3
f. adequate control of software tools to support system development and software V&V processes, in keeping with the additional guidance in IEEE Std 7-4.3.2-2003, Clause 5.3.2
g. provisions for the documentation and resolution of problems and nonconformances found in the system elements
h. provisions for effective oversight of life cycle activities

The NRC review of software project management should focus on the application-specific software development activities rather than the platform development process defined in an NRC-approved DI&C platform, unless the NRC acceptance criteria have changed.

Through all aspects of this design, all changes and modifications should be documented and controlled. The project management function should incorporate the impacts of change in the project risks, schedule, and budget.

D.4.2.3 Software Quality Assurance Processes

The reviewer should evaluate the LAR description of the software QA processes. SRP BTP 7-14, Section B.3.1.3.4, can inform the review of the software QA process description to

the extent practicable for an Alternate Review Process LAR review. The process used to develop the DI&C safety-related system should conform to the licensee's approved QA program.

Clauses 5.3.3 and 5.3.4 of IEEE Std 7-4.3.2-2003 provide guidance on V&V activities and independent V&V, respectively.

The reviewer should evaluate whether the software life cycle process description demonstrates that the software life cycle process meets the guidance of RG 1.168 or how the underlying regulatory requirements referenced in RG 1.168 are satisfied. IEEE Std 1028, "IEEE Standard for Software Reviews and Audits," provides guidance acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits, subject to certain provisions. Although IEEE Std 1028 describes how to perform systematic software reviews, it does not establish the need to conduct specific reviews. Software review and audit activities should define which reviews in the software development process are systematic software reviews.

The NRC review of software QA should focus on the application-specific software development activities rather than the platform development process defined in an NRC-approved DI&C platform, unless the NRC acceptance criteria have changed.

D.4.2.4 Software Verification and Validation Processes

The reviewer should evaluate the LAR description of the software V&V processes. IEEE Std 1012, as endorsed by RG 1.168 and referenced in SRP BTP 7-14, Sections B.3.1.10 and B.3.2.2, contains the applicable review guidance for software V&V processes. To the extent practicable, IEEE Std 1012 and RG 1.168 should be used to inform the review of the software V&V process description for the Alternate Review Process LAR review.

The reviewer should evaluate whether the software V&V processes follow the guidance of RG 1.168 or, alternatively, describe how the regulatory requirements referenced in RG 1.168 are satisfied. The description of the software V&V processes should address the following:

a. V&V organization responsibilities
b. V&V processes, activities, and tasks
c. V&V reporting
d. V&V administrative controls for anomaly resolution and reporting, task iteration policy, and deviation policy
e. V&V test documentation

It is acceptable for a licensee to adapt software V&V programs activities and tasks to reflect important process differences, technology differences, and exceptions related to the use of integrated design environment tools. Secure development and operating environment vulnerability assessments performed in accordance with the guidance in RG 1.152 can replace security analyses described in IEEE Std 1012, Clause 5 and Tables 1 and 2.

The NRC review of software V&V should focus on the application-specific software development activities rather than the platform development process defined in an NRC-approved DI&C platform, unless the NRC acceptance criteria have changed.

D.4.2.5 Configuration Management Processes

The reviewer should evaluate the LAR description of the CM processes. Although vendors perform some CM activities, responsibility for the system design modification and oversight of vendor activities rests with the licensee. This responsibility includes ensuring that as the design proceeds through to completion, the licensee is ensuring that the final vendor design and implementation will support the performance of periodic surveillance and maintenance in accordance with plant TS requirements, and will support specific plant operating procedures. Unless the licensee takes responsibility for oversight of the vendor's product development and CM activities at the outset of the development process, the gap can begin to widen between what the functional performance requirements document specifies, what the vendor is going to provide, and the impact on current processes and practices.

IEEE Std 828, "IEEE Standard for Configuration Management in Systems and Software Engineering," as endorsed by RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," contains the applicable review guidance for CM processes. SRP BTP 7-14, Sections B.3.1.11.4 and B.3.2.3, reference IEEE Std 828 and RG 1.169. To the extent practicable, a reviewer should use IEEE Std 828 and RG 1.169 to inform his or her review of the CM process description for the Alternate Review Process LAR review. RG 1.152 endorses IEEE Std 7-4.3.2-2003, subject to the positions and modifications identified in the RG. IEEE Std 7-4.3.2-2003, Clause 5.3.5, provides guidance on CM.

The reviewer should evaluate whether the CM processes follow the guidance in RG 1.169 or, alternatively, describe how the regulatory requirements referenced in RG 1.169 are satisfied. The description of the CM processes should address the following:

a. the responsibilities and authorities for managing and accomplishing the planned CM activities
b. the activities to be performed in applying CM to the project
c. coordination of CM activities with the other activities in the project
d. tools used for CM activities

The LAR should describe the organizational responsibilities for CM and for any designated configuration control board. The licensee may specify how modified software, hardware, or documentation should be tested and verified. These controls do not have to be defined within the CM process; instead, these controls are typically defined as part of the V&V process. The description of the CM process should include information on documenting and managing system-build documents, as called for in SRP BTP 7-14, Section B.3.3.5.3.

The NRC review of CM process controls should focus on the application-specific software and hardware development activities rather than the platform development process defined in an NRC-approved DI&C platform, unless the NRC acceptance criteria have changed.

D.5 Applying a Referenced Topical Report Safety Evaluation

NRR Office Instruction LIC-101, Appendix B, "Guide for Processing License Amendments," Section 4.2, "Use of Precedent and References to Topical Reports," states the following:

> If a licensee in its application or the NRC staff during its review identifies a deviation from the process or limitations associated with a topical report, the staff should address the deviation in its safety evaluation for the plant-specific license amendment application....

This section of the ISG describes how the NRC staff should assess a referenced NRC-approved DI&C topical report. This review would include evaluating how the licensee addressed plant-specific (or application-specific) action items in the cited NRC-approved topical report and the review of deviations from previously approved systems, hardware, software, or methodologies. This section is not applicable if the LAR does not reference a topical report previously approved by the NRC.

D.5.1 Information To Be Provided

D.5.1.1 Addressing Platform Changes after Approval of a Topical Report

The LAR should identify changes to the system, hardware, software, or design life cycle methodology from a topical report previously approved by the NRC. The goal is to leverage prior NRC approvals and allow the NRC staff to evaluate any changes to ensure that safety conclusions reached by a previous review are not invalidated.

When changes affect the conclusions of the original NRC-approved topical report safety evaluation, the LAR should provide information that supports the review of these changes in connection with the LAR. Where appropriate, the LAR should cross-reference any NRC-approved documents to the applicable items listed in Enclosure B to this ISG. The LAR should state whether the cited document has changed since the last NRC review. For documents that have changes affecting the conclusions of the associated safety evaluation, including system, hardware, and software descriptions, the NRC staff should verify that the licensee has submitted information on the docket describing the changes. The information provided should include adequate justification to allow the NRC staff to evaluate the acceptability of the change.

D.5.1.2 Resolution of Topical Report Plant-Specific Action Items

A safety evaluation for an NRC-approved topical report may have a section with a title such as “Plant-Specific Action Items” or “Application-Specific Action Items.” These are open items that the application should address in the LAR when using the NRC-approved topical report for a plant modification. The LAR should describe how each PSAI item is or will be resolved.

In the case of the Alternate Review Process for an LAR, the NRC staff should verify that the licensee has described the process for addressing those plant-specific items related to detailed design, implementation, testing, and ongoing life cycle activities (including associated V&V activities). Based on a topical report review in accordance with SRP BTP 7-14, some topical reports include plant-specific items stating that the NRC staff should review detailed design, implementation, testing, and ongoing life cycle activities. For the Alternate Review Process, the licensee will provide oversight of the performance of these activities, in accordance with the licensee’s QA program and Vendor Oversight Plan. The NRC staff will review the description of the processes used for these activities.

The LAR should evaluate PSAIs involving planning documents against the regulatory guidance in Section D.4 of this ISG or describe applicable licensee processes or programs used to address the PSAIs.

D.5.2 Evaluation

The reviewer should evaluate whether the plant-specific application is bounded by the applicability of the platform as described in the NRC-approved topical report. If there are plant-specific deviations from the NRC-approved topical report's PSAIs, the reviewer should evaluate each deviation against appropriate regulatory criteria.

The reviewer should evaluate changes to the system, hardware, software, or design life cycle methodology from the referenced NRC-approved topical report. The NRC staff should review changes that have affected safety evaluation conclusions to determine whether the changes continue to comply with regulatory requirements.

The reviewer should evaluate the resolutions for PSAIs. For the Alternate Review Process, the reviewer should evaluate the resolutions for PSAIs specific to detailed design, implementation, and testing against the regulatory guidance in Section D.4 of this ISG. Any PSAI that involves planning documents should be reviewed against the regulatory guidance in Section D.4 or covered by licensee processes or programs. For PSAIs that are addressed in the LAR and implemented by the licensee subsequent to issuance of the license amendment, a license condition may be established to verify that these PSAIs have been implemented in accordance with the design described in the application before system operation or at a time established in the license condition.

D.6 Compliance/Conformance Matrix for IEEE Standards 603-1991 and 7-4.3.2-2003

The reviewer should evaluate whether the DI&C modification complies with IEEE Std 603-1991 and conforms to the guidance in IEEE Std 7-4.3.2-2003. The staff can develop a compliance/conformance matrix to perform this evaluation, if the LAR did not provide one. Table D-1 of this ISG is an example of such a compliance/conformance matrix. It provides a row for each clause in IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003. Extended clauses are included if needed to point to different LAR sections. The table also provides titles from the standards, defining the clause.

In the appropriate "Compliance/Conformance" column cell, each row states whether the LAR submittal complies with (C), partially complies with (PC), takes an exception (E), or does not apply (N/A) to each clause and extended clause (row). Rather than documenting methods of compliance with each IEEE standard clause in this matrix, the table indicates each clause and extended clause (row) in all the LAR sections (at the lowest subdivision of LAR section numbering) where the LAR, for each clause or extended clause, demonstrates one of the following:

a. how full compliance/conformance is achieved

b. why partial compliance/conformance is acceptable and why full compliance to IEEE Std 603-1991 is not required in accordance with § 50.55a(z) or deviations from IEEE Std 7-4.3.2 are acceptable.

c. why the alternative exception proposed is acceptable

d. why the clause does not apply

For the example given in Table D-1, IEEE Std 7-4.3.2-2003 does not provide any additional guidance for Clause 4 requirements in IEEE Std 603-1991. However, IEEE Std 7-4.3.2-2003

defines several extended clauses under Clause 5.3. For both examples, each cell in the "Compliance/Conformance" and "LAR Section" would be completed, and the LAR should discuss the methods to be used to meet IEEE Std 603-1991 when applying the associated guidance of IEEE Std 7-4.3.2-2003.

The "DI&C-ISG-06 Section" column refers to the potential sections of this ISG that discuss the subject clause, depending on the review process (i.e., Alternate Review Process or Tier 1, 2, and 3 Review Process).

IEEE Std 7-4.3.2-2003 clauses that are marked with an asterisk (*) do not add any guidance for complying with the requirements of IEEE Std 603-1991.

Table D-1 IEEE Standards 603-1991 and 7-4.3.2-2003 Compliance/Conformance Table

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/ Conformance	LAR Section	DI&C-ISG-06 Section
4.1	4*	Safety System Design Basis			D.2.3.1, D.9.1, D.9.2, D.3
4.2					D.2.3.1
4.3					D.2.3.1
4.4					D.2.3.1
4.5					D.2.3.1, D.3
4.6					D.2.3.1
4.7					D.2.3.1, D.3
4.8					D.2.3.1, D.9.8
4.9					D.2.3.1, D.9.8
4.10					D.2.3.1
4.11					D.2.3.1
4.12					D.2.3.1
5.1	5.1*	Single-Failure Criterion			D.2.6.2.1.1, D.9.8
5.2	5.2*	Completion of Protective Action			D.2.3.1, D.2.6.2.3.1, D.9.1, D.9.2, D.9.8
5.3	5.3	Quality			D.2.3.1, D2.3.3.1, D.3, D.4
	5.3.1	Software Development			D.4
	5.3.1.1	Software Quality Metrics			D.4
	5.3.2	Software Tools			D.4
	5.3.3	Verification and Validation			D.4, D.9.6

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/ Conformance	LAR Section	DI&C-ISG-06 Section
	5.3.4	Independent V&V Requirements			D.4 D.9.6
	5.3.5	Software Configuration Management			D.4, D.9.5
	5.3.6	Software Project Risk Management			D.4
5.4	5.4	Equipment Qualification			D.2.3.3.1, D.3.1
	5.4.1	Computer System Testing			D.3.1
	5.4.2	Qualification of Existing Commercial Computers			D.3, D.9.9
5.5	5.5	System Integrity			D.2.3.1, D.2.6.2.3.1, D.9.7
	5.5.1	Design for Computer Integrity			D.2.6.2.3.1, D.9.7
	5.5.2	Design for Test and Calibration			D.2.3.1
	5.5.3	Fault Detection and Self-Diagnostics			D.2.2.1, D.9.8
5.6	5.6	Independence			D.2.6.2.2.1, D.9.1, D.9.2
5.6.1		Between Redundant Portions of a Safety System			D.2.5.1
5.6.2		Between Safety Systems and Effects of Design-Basis Event			D.2.5.1
5.6.3		Between Safety Systems and Other Systems			D.2.5.1
5.6.4		Detailed Criteria			D.2.5.1
5.7	5.7*	Capability for Testing and Calibration			D.2.3.1, D.9.1, D.9.2
5.8	5.8*	Information Displays			D.2.3.1, D.9.1, D.9.2
5.8.1		Displays for Manually Controlled Actions			D.2.2.1
5.8.2		System Status Indication			D.2.2.1
5.8.3		Indication of Bypasses			D.2.2.1
5.8.4		Location			D.2.2.1
5.9	5.9*	Control of Access			D.2.3.1 D.8
5.10	5.10*	Repair			D.2.3.1, D.9.1, D.9.2
5.11	5.11	Identification			D.2.6.2.2.1, D.9.5
5.12	5.12*	Auxiliary Features			D.2.5.1
5.13	5.13*	Multi-Unit Stations			D.2.5.1
5.14	5.14*	Human Factors Considerations			D.2.5.1

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/ Conformance	LAR Section	DI&C-ISG-06 Section
5.15	5.15	Reliability			D.2.6.2.1.1, D.9.8
6.1	6*	Automatic Control			D.2.6.2.3.1
6.2		Manual Control			D.2.6.2.3.1
6.3		Interaction between the Sense and Command Features and Other Systems			D.2.6.2.2.1
6.3.1		Requirements			D.2.6.2.2.1
6.3.2		Provisions			D.2.6.2.2.1
6.4		Derivation of System Inputs			D.2.3.1 D.2.6.2.5.1
6.5		Capability for Testing and Calibration			D.2.3.1, D.9.1, D.9.2
6.5.1		Checking the Operational Availability			D.2.3.1
6.5.2		Assuring the Operational Availability			D.2.3.1
6.6		Operating Bypasses			D.2.3.1
6.7		Maintenance Bypass			D.2.3.1, D.2.6.2.1.1
6.8		Setpoints			D.2.3.1, D.7.1
7.1	7*	Automatic Control			D.2.6.2.3.1
7.2		Manual Control			D.2.6.2.3.1
7.3		Completion of Protective Action			D.2.3.1, D.9.1, D.9.2
7.4		Operating Bypass			D.2.3.1
7.5		Maintenance Bypass			D.2.3.1, D.2.6.2.1.1
8.1	8*	Electrical Power Sources			D.2.5.1
8.2		Non-electrical Power Sources			D.2.5.1
8.3		Maintenance Bypass			D.2.5.1

* The standard does not add anything beyond IEEE Std 603-1991.

D.7 Technical Specifications

D.7.1 Information To Be Provided

The LAR should provide any proposed TS changes needed to demonstrate compliance with 10 CFR 50.36, “Technical specifications.” This includes proposed changes to instrument setpoints included in the TS. If the TS includes a setpoint control program, the LAR should identify any changes to that program.

Self-diagnostics in digital equipment can be used in some cases as an alternate means of accomplishing some SRs or of justifying less frequent manual surveillance and calibration. Performance of channel checks, channel calibrations, and other surveillance may no longer be necessary if the digital equipment’s internal self-test and self-diagnostic functions can be

credited. The proposed TS should reflect the SRs necessary to ensure the operability of the system and its components. Any extension, modification, or deletion of a TS should be documented and justified by the licensee.

In addition to reviewing a markup copy of the TS, the NRC staff should verify that the licensee has justified each change. This includes providing a detailed basis for how the digital equipment is used to support each added, modified, or deleted SR. These justifications, taken together, should demonstrate that the proposed TS reflect the equipment functions and response times credited in the FSAR and satisfy the requirements of 10 CFR 50.36.

D.7.2 Evaluation

D.7.2.1 Technical Specifications

The reviewer should evaluate the proposed TS in accordance with 10 CFR 50.36.

The reviewer should evaluate how the LAR allocates self-test and self-diagnostic features to system elements for those features used to support TS. The reviewer should evaluate whether the combination of self-test and self-diagnostic capabilities defined in the LAR, together with manual testing and external cross-checks, is sufficient to support existing TS and any proposed TS changes. This evaluation should include checking for consistency between the TS and the self-tests and self-diagnostics implemented in the architecture (see Section D.2.2.1 of this ISG) for new system functions (see Section D.2.3.1) and to address system interfaces (Section D.2.5.1). This evaluation should also check for consistency between the TS and the TS assumptions regarding redundancy (Section D.2.6.2.1.1).

Reviewers should evaluate TS LCOs being proposed for deletion against the four criteria in 10 CFR 50.36(c)(2)(ii) that require establishment of an LCO for a system function. If none of the criteria apply to the system or function addressed by an existing LCO, the LCO may be deleted. Additionally, LCOs proposed for addition should adequately define the lowest functional capability or performance levels of the system required for safe operation of the facility. This review considers the adequacy of the proposed LCOs and the potential need for additional LCOs that have not been proposed for addition to the TS.

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 operability aspects of the system are ensured and the LCOs are met. As with the review of the LCOs, the staff should evaluate proposed SRs and the need for additional SRs.

SRP BTP 7-17 provides review guidance in this area.

D.7.2.2 Setpoint Changes

Setpoints should meet IEEE Std 603-1991, Clause 6.8, in consideration of the uncertainties in the process analytical limit documented in Clause 4.4. Setpoints should be determined using a documented methodology.

The NRC provides additional guidance on the establishment of instrument setpoints in RG 1.105, “Setpoints for Safety-Related Instrumentation,” and Regulatory Issue Summary 2006-17, “NRC Staff Position on the Requirements of 10 CFR 50.36, ‘Technical Specifications,’ Regarding Limiting Safety System Settings During Periodic Testing and

Calibration of Instrument Channels," dated August 24, 2006 (ADAMS Accession No. ML051810077). SRP BTP 7-3, "Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service," contains additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

The reviewer should verify that the information provided describes the hardware and software in detail sufficient for the NRC staff to conclude that IEEE Std 603-1991, Clause 6.8, has been met.

D.8 Secure Development and Operational Environment

D.8.1 Information To Be Provided

The LAR should demonstrate that the proposed DI&C system is adequately robust to perform its safety function by establishing a secure development and operational environment. The LAR should provide information describing a secure environment, including any issues that may affect the secure environment and the DI&C equipment.

For the Tier 1, 2, and 3 Review Process, the LAR should provide information describing the vulnerability assessment and the SDOE controls that address Regulatory Position 2.1, "Concepts Phase," through Regulatory Position 2.5, "Test Phase," of RG 1.152.

For the Alternate Review Process, the LAR should provide the following information to address RG 1.152:

a. a description of the vulnerability assessment
b. a description of the secure development environment controls
c. the System Requirements Specification (see Section D.2.2.2 of this ISG) for the SOE controls

All SDOE and software information identified in RG 1.152, Regulatory Position 2, including the test phase specifications and results validating the requirements for the SOE, should be available for NRC staff review. The need to submit any of this information should be determined during the licensing review.

Documentation detailing how the licensee implemented (or will implement, in the case of the Alternate Review Process) SDOE controls should be available for NRC staff review.

D.8.2 Evaluation

The reviewer should determine whether the LAR conforms to the guidance of RG 1.152, Regulatory Position 2, for the SDOE of the system under review, and complies with the requirements of Clause 5.9 of IEEE Std 603-1991, Control of Access. For Tier 1 and the Alternate Review Process, the review is limited to the application software and hardware.

The NRC staff should review the licensee's vendor- and system-specific vulnerability assessment description and verify that the assessment identifies those vulnerabilities that could affect the secure development and reliable and secure operation of the digital safety-related system. RG 1.152, Section B, page 5, discusses vulnerabilities that could affect the reliability of

the system. RG 1.152, Section C, Regulatory Position 2.1, contains guidance for performing the vulnerability assessment.

The NRC staff should review the information provided to determine that the digital safety-related system:

a. was designed in a secure development environment, and was (or will be, in the case of the Alternate Review Process) developed, and tested in a secure development environment
b. will be protected from inadvertent actions in an SOE as defined in RG 1.152

The I&C staff in NRR reviews the safety aspects of the LAR while the Office of Nuclear Security and Incident Response (NSIR) staff evaluates the adequacy of cyber security features for compliance with 10 CFR 73.54. The I&C staff should communicate with NSIR any cyber security concerns or design features identified during the review of the DI&C modification (e.g., the use of one-way data flows using hardware mechanisms).

D.9 Other Review Guidance for Tier 1, 2, and 3 Reviews

The guidance in this section focuses on the evaluation of design outputs and system validation test results, which should be available during later stages of DI&C system development. The reviewer should apply this guidance to Tier 1, 2, and 3 reviews as needed. Because Alternate Review Process evaluations need not rely upon completed late-stage product development activities, the NRC does not expect the documentation necessary to perform the evaluations covered in this section to be available to the NRC reviewer before the NRC staff decides whether to issue or deny the license amendment.

D.9.1 Software Requirements Specification

D.9.1.1 Information To Be Provided

Review (Phase 1): Software Requirements Specification

SRP BTP 7-14, Section B.3.3.1, “Requirements Activities—Software Requirements Specification,” contains the review guidance for a Software Requirements Specification (SRS). The SRP references the following applicable guidance:

a. RG 1.172, “Software Requirement Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants”
b. IEEE Std 830, “IEEE Recommended Practice for Software Requirements Specifications,” which describes an acceptable approach for preparing an SRS for safety-related system software
c. NUREG/CR-6101, “Software Reliability and Safety in Nuclear Reactor Protection Systems,” issued November 1993 (ADAMS Accession No. ML072750055), Section 3.2.1, “Software Requirements Specification,” and Section 4.2.1, “Software Requirements Specifications”

The SRS documents the results of the requirements phase activities by the design team and identifies the aspects of the safety-related system to be addressed in the software design.

D.9.1.2 Evaluation

Errors in the specification of criteria or misunderstanding of their purpose can be a significant source of software errors. The reviewer should examine the SRS carefully to ensure that criteria are consistent, correct, understandable, traceable, unambiguous, and verifiable. The complexity of the SRS depends on the complexity of the proposed system, and the level of detail should reflect that level of complexity.

The staff may need to review two SRSs, one for the platform software and another for the applications software. Each of these may be reviewed separately.

Each SRS should be traceable to one or more safety-related system criteria, and the requirements traceability matrix should show where in the software the requirement is performed. The key to an adequate SRS is its understandability.

The NRC staff should review the SRS using the review guidance in SRP BTP 7-14, Section B.3.3.1.3, and should review a limited number of criteria during a thread audit, as described in SRP BTP 7-14, Section B.3.2.2. The NRC staff should expect to find sufficient V&V documentation to show that the V&V organization performed 100-percent V&V of the software criteria.

D.9.2 Software Design Specification

D.9.2.1 Information To Be Provided

Review (Phase 1): Software Design Specification

SRP BTP 7-14, Section B.3.3.3, “Design Activities—Software Design Specification,” contains the review guidance for the Software Design Specification (SDS) and cites NUREG/CR-6101, Section 3.3.2, “Software Design Specification,” and Section 4.3.2, “Software Design Specifications.”

The person who implements the software design is the primary user of the SDS. The V&V team ensures that the software accurately reflects the software requirements. The SDS should be detailed enough to enable the V&V team to determine how to implement software specifications. The SDS should also be traceable to software implementation code or function block diagrams.

D.9.2.2 Evaluation

The NRC staff should evaluate the SDS using the review guidance in SRP BTP 7-14, Section B.3.3.3.3, and should perform a sample review of specifications using a thread audit technique. The NRC staff should expect to find sufficient V&V documentation to show that the V&V organization performed a 100-percent V&V of the SDS.

D.9.3 Changes to Referenced Platform Design

D.9.3.1 Information To Be Provided

Review (Phase 1): Design Analysis Report (System, Hardware, Software, and Methodology Modifications)

The LAR should identify all changes made to hardware, software, or design life cycle methodology of a referenced NRC-approved topical report.

D.9.3.2 Evaluation

The NRC staff should review the changes from the NRC-approved topical report and determine whether the safety conclusions reached by a previous review remain valid. If the platform vendor has a platform change review process, the NRC staff should review the results of that process and determine whether the staff concurs with the conclusions relative to the impact on the NRC-approved topical report.

If the changes affect the conclusions of the safety evaluation for the platform topical report, the NRC may need to undertake an effort separate from the LAR review to update the platform topical report safety evaluation.

D.9.4 Software Safety Analysis

D.9.4.1 Information To Be Provided

Review (Phase 2): Safety Analysis

SRP BTP 7-14, Section B.3.2.1, “Acceptance Criteria for Safety Analysis Activities,” presents the review guidance for the implementation of a Software Safety Analysis (SSA). The acceptance criterion for SSA implementation is that the tasks in that plan have been carried out.

D.9.4.2 Evaluation

The reviewer should verify that the LAR presents documentation showing that the SSA tasks have been accomplished successfully.

D.9.5 Configuration Management Activities

D.9.5.1 Information To Be Provided

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

SRP BTP 7-14, Section B.3.2.3, refers to the applicable guidance for carrying out CM in RG 1.169, which endorses IEEE Std 828, subject to specific provisions identified in the RG. Although the vendor(s) performs some CM activities, responsibility for knowledge and control of the plant configuration, licensing basis, system design, plant modification, and system acceptance rests with the licensee. The licensee is responsible for oversight and acceptance of vendor activities that affect all configuration items (see Section D.4.2.5 of this ISG).

D.9.5.2 Evaluation

The reviewer should verify that the LAR presents documentation showing that the CM tasks for associated activity groups have been successfully accomplished.

D.9.6 Testing Activities

D.9.6.1 Information To Be Provided

Review (Phase 2): Summary Test Reports (Including FAT)

SRP BTP 7-14, Section B.3.2.4, refers to the following applicable guidance:

a. RG 1.168, Sections 7.b, "Regression Analysis and Testing," and 7.d, "Test Evaluation," contain guidance related to testing activities.
b. RG 1.170 endorses IEEE Std 829, with a few noted exceptions, and identifies an acceptable method for addressing test documentation.
c. RG 1.171 endorses IEEE Std 1008, "IEEE Standard for Software Unit Testing," with a few noted exceptions, and identifies an acceptable method for addressing software unit testing.

D.9.6.2 Evaluation

The software validation activities should demonstrate that all validation tests specified by the Software V&V plan were successful. FAT is one of those activities.

D.9.7 System Integrity—Time Response/Deterministic Performance

D.9.7.1 Information To Be Provided

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

(2) Design Report on Computer Integrity, Test and Calibration, and Fault Detection

Review (Phase 2): (1) System Response Time Confirmation Report

(2) Hardware Reliability Analysis

Clause 5.5 of IEEE Std 603-1991 requires that the safety-related systems be designed such that the system can accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," provides the review criteria for system integrity.

A special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure the completion of protective action within the critical points of time identified as required by Clause 4.10 of IEEE Std 603-1991.

D.9.7.2 Evaluation

The reviewer should evaluate computer system hardware integrity against IEEE Std 603-1991. The licensee's software safety analysis activities should demonstrate computer system software integrity (including the effects of hardware-software interaction).

The NRC staff should assess whether tests have been conducted on safety-related system equipment components and the system racks and panels as a whole to demonstrate that safety-

related system performance is adequate to ensure the completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment. The tests 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.

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. The information provided should be sufficient for the NRC staff to determine whether adequate testing and analysis have been performed on the system as a whole and its components. The review of system integrity should determine whether the design provides for safety-related 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. The reviewer typically evaluates this aspect through evaluation of the licensee's FMEA.

D.9.8 Platform- and System-Level Failure Modes

D.9.8.1 Information To Be Provided

Review (Phase 2): (1) System-Level Failure Modes and Effects Analysis

(2) Platform-Level Failure Modes and Effects Analysis

The FMEA should justify the acceptability of each failure effect. Reactor trip system functions should typically fail in the tripped state. Engineered safety feature actuation system (ESFAS) functions should fail to a predefined safe state. For many ESFAS functions, this predefined safe state should be that the actuated component remains as-is.

D.9.8.2 Evaluation

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

D.9.9 Commercial-Grade Dedication of Digital Equipment

D.9.9.1 Information To Be Provided

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

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

Clause 5.4.2 of IEEE Std 7-4.3.2-2003 presents the fundamental criteria for demonstrating that a commercial computer will perform its intended safety functions. Additional guidance appears in Electric Power Research Institute (EPRI) TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," issued October 1996, as endorsed by the NRC safety evaluation dated July 17, 1997 (ADAMS Accession No. ML12205A284), and EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC [Programmable Logic Controller] for Safety-Related Applications in Nuclear Power Plants," issued December 1996, as endorsed by the NRC safety evaluation dated July 30, 1998 (ADAMS Accession No. ML12205A265).

For commercial-grade software intended for use in safety-related systems, one of the critical characteristics is implementation of a high-quality development process. In essence, the NRC staff should verify that the licensee has demonstrated that the process used to develop the commercial software was as rigorous as that for software used in safety-related applications. If this cannot be demonstrated, then compensatory measures should be taken, such as extensive operating experience and, if necessary, additional analyses, tests, or inspections.

EPRI TR-106439 provides guidance for the evaluation of existing commercial computers and software to determine conformance with the criteria of Clause 5.4.2 of IEEE Std 7-4.3.2-2003. The review may apply the guidance of SRP BTP 7-14 to the evaluation of vendor processes described in EPRI TR-106439. EPRI TR-107330 provides more specific guidance for the evaluation of existing programmable logic controllers.

D.9.9.2 Evaluation

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

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

The dedication process for the digital safety-related system (e.g., as described in the Commercial-Grade Dedication Plan) should entail the identification of the physical, performance, and dependability (see EPRI TR-106439) critical characteristics necessary to demonstrate that the proposed digital system or component can achieve the safety function. The dedication process should apply to the computer hardware, software, and firmware that are necessary to accomplish the safety function. The dedication process for software should include an evaluation of the development process and the implementation of the development process.

In IEEE Std 7-4.3.2-2003, Clauses 5.4.2.1 through 5.4.2.2 describe the preliminary and detailed phase activities for commercial-grade item dedication.

D.9.10 Hardware Development Process

D.9.10.1 Information To Be Provided

Review (Phase 1): Hardware Development Process

The NRC staff should verify that the licensee has demonstrated that the hardware development process and the quality control methods used during system development will meet regulatory criteria by providing information that governs the process and methods. The LAR should include information that covers both the development methods employed during the design of individual hardware modules and the design of the application-specific system to be used in implementing the safety function. The quality control methods used for system development should be consistent with a 10 CFR Part 50, Appendix B, QA program and the criteria of IEEE Std 603-1991, Clause 5.3 “Quality.”

D.9.10.2 Evaluation

The reviewer should evaluate whether the application followed the guidance of RG 1.164, “Dedication of Commercial-Grade Items for Use in Nuclear Power Plants” regarding the hardware development process and should evaluate the information in the application on this subject to determine whether the licensee satisfied the following requirements:

a. 10 CFR 50.54(jj) and 10 CFR 50.55(i), which require that structures, systems, and components subject to the codes and standards in § 50.55a be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed

b. 10 CFR 50.55a(h), which incorporates, based on the date the construction permit was issued, either IEEE Std 279, Clause 4.3, or IEEE Std 603-1991, Clause 5.3

c. 10 CFR Part 50, Appendix A, GDC 1, “Quality Standards and Records”

As mentioned in Section B of this ISG, if a licensee references (i.e., bases its design on) an NRC-approved platform topical report, the NRC staff should be able, where appropriate, to limit its review to assessing whether the application of the DI&C modification conforms to the topical report approval. If the hardware development process and quality control methods used have previously been described by the vendor and evaluated by the NRC staff, the NRC staff should verify that the licensee has referred to that description and the safety evaluation on the topical report applies to the plant-specific DI&C modification. The NRC staff should verify that the licensee has identified and justified deviations from previously reviewed and approved processes or methods and revision changes since NRC approval.

Enclosure A—Sample Summary of Initial Public Meeting To Discuss Plans To Request NRC Approval in Support of a Digital Instrumentation and Control Modification 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 INSTRUMENTATION AND CONTROL PLANT MODIFICATION OF [SYSTEM] USING [PLATFORM]

On [DATE], the U.S. Nuclear Regulatory Commission (NRC) staff conducted a Category 1 public meeting to discuss [LICENSEE]'s plans for modifying the [PLANT] [SYSTEM] to the [PLATFORM] digital instrumentation and control (DI&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 how [LICENSEE] should address the review area of [REVIEW AREA].

In these discussions, the licensee identified the following characteristics and design specifications that contribute to the [PLATFORM]'s compliance with the criteria in [REVIEW AREA]:

- Item 1
- Item 2…

The NRC staff provided feedback to [LICENSEE], noting that the following aspects of the design, based on the available high-level information, seemed consistent with the NRC staff's position on [REVIEW AREA]:

- Item 1
- Item 2…

The following review areas were discussed:

- relevant precedents for similar systems in other plants
- communications interfaces

- secure development and operating environment
- plant-specific action items for [PLATFORM]
- regulations and general design criteria to be addressed
- applicable guidance to be considered
- development process planning and implementation
- unique requirements for existing system design
- defense-in-depth and diversity

The NRC discussed guidance criteria for determining the appropriate review process and tier level in relation to the proposed [PLANT][SYSTEM] based on current project status and the design and implementation schedules for the [PLANT][SYSTEM]. The NRC made a preliminary determination that this evaluation can be performed under the [Tier 1, 2, and 3 Review Process or Alternate Review Process] guidance. Based on this determination, the licensee committed to prepare its license amendment request (LAR) in accordance with the [REVIEW PROCESS AND/OR TIER LEVEL] guidance provided in DI&C-ISG-06, "Licensing Process," Revision 2 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML18269A259).

[For Tier 1, 2, or 3 submittals for Phases 1 and 2] The NRC discussed guidance criteria for phased submittals in relation to the proposed [PLANT][SYSTEM] based on planned development activities. The NRC made a preliminary determination that Phase 1 submittal documentation will be provided with the LAR and that Phase 2 documentation will be provided by [an agreed-upon date, before issuance of the safety evaluation.] The NRC indicated that the licensee's schedule should include sufficient margin for public notification and administrative tasks associated with the amendment after the Phase 2 submittal. [For Alternate Review Process submittals only] The NRC discussed guidance criteria for submittals in relation to the proposed [PLANT][SYSTEM] based on planned development activities. A preliminary determination was made about the documentation submittal schedule.]

The NRC staff identified the following aspects of the design for which additional information is needed before the staff can evaluate whether the proposed modification is fully consistent with the NRC staff's position on [REGULATORY POSITION]:

- 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. Concurrence may also include division-level management, as appropriate.

Enclosure B—Information Provided in Support of a License Amendment Request for a Digital Instrumentation and Control Modification

This enclosure can be used as a cross-reference or checklist for addressing the descriptive material identified in the body of this interim staff guidance. It is intended to be used in conjunction with the referenced sections of this interim staff guidance provided in parentheses for each row.

The list of information in this enclosure represents a typical system modification. Different information may be provided, depending on the scope and complexity of the system modification, to support the U.S. Nuclear Regulatory Commission's evaluation against the applicable acceptance criteria. Note that the Alternate Review Process column is labeled 'AR'.

		Tier			Plant-Specific Information Submitted with License Amendment Request (Phase 1 for Tier 1, Tier 2, and Tier 3)
	AR	1	2	3	
1.1	X				**(Summary of) Application Software Planning and Processes** (see D.4)
1.2	X				**(Summary of) Vendor Oversight Plan** (see C.2.2)
1.3	X	X	X		**Approved Topical Report Safety Evaluation** (see D.5)
1.4	X	X	X	X	**System Description** (see D.1)
1.5	X	X	X	X	**System Architecture** (see D.2)
1.6	X	X	X	X	**(Summary of) Hardware Equipment Qualification** (see D.3)
1.7	X	X	X	X	**(Unified Compliance/Conformance Matrix for) IEEE Stds 603-1991 and 7-4.3.2-2003** (see D.6)
1.8	X	X	X	X	**(Changes to) Technical Specifications** (see D.7)
1.9	X	X	X	X	**Setpoint Methodology and Calculations** (see D.7) Provided when technical specification setpoint methodology changes or calculations deviate from or are not addressed in an applicable referenced NRC-approved topical report
1.10	X	X	X	X	**Secure Development and Operational Environment** (see D.8)
1.11		X	X	X	**Software Requirements Specification** (see D.9.1)
1.12		X	X	X	**Software Design Specification** (see D.9.2)
1.13		X	X	X	**Design Analysis Reports for Platform Changes** (see D.9.3)
1.14		X	X	X	**System Response Time Analysis Report** (see D.9.7)
1.15			X	X	**Design Report on Computer Integrity, Test and Calibration, and Fault Detection** (see D.9.7)
1.16				X	**Commercial-Grade Dedication Plan** (see D.9.9)
1.17				X	**Quality Assurance Plan for Hardware** (see D.9.10)
1.18				X	**(Summary of) Hardware Development Process** (see D.9.10)

	Tier			Plant-Specific Information Submitted before Requested Approval (Phase 2 for Tier 1, Tier 2, and Tier 3 only) Note: This table does not apply to Alternate Review Process applications.
	1	2	3	
2.1	X	X	X	**Safety Analysis** (see D.9.4)
2.2	X	X	X	**As-Manufactured, System Configuration Documentation** (see D.9.5)
2.3	X	X	X	**Summary Test Reports** (Including Test Results up to and including FAT) (see D.9.6)
2.4	X	X	X	**System Response Time Confirmation Report** (see D.9.7)
2.5	X	X	X	**Reliability Analysis** (see D.9.7)
2.6	X	X	X	**System-Level Failure Modes and Effects Analysis** (see D.9.8)
2.7	X	X	X	**Qualification Test Methodologies** (see D.3)
2.8		X	X	**Platform-Level Failure Modes and Effects Analysis** (see D.9.8)
2.9		X	X	**(Summary of) Electromagnetic Interference, Temperature, Humidity, and Seismic Testing Results** (see D.3)
2.10			X	**Commercial-Grade Dedication Report(s)** (see D.9.9)

Enclosure C—Sample Safety Evaluation Input Table of Contents for a Digital Instrumentation and Control License Amendment[7]

1.0 Introduction .....
2.0 Regulatory Evaluation .....
3.0 Technical Evaluation .....
3.1 System Description and Configuration .....
3.2 Proposed Technical Specification Changes .....
3.3 System Interfaces Including Digital Instrumentation Communications .....
3.4 Defense-in-Depth and Diversity .....
3.5 Setpoint Methodology and Calculations .....
3.6 Response Time Performance .....
3.7 System Development Process .....
3.7.1 Software Planning Documents .....
3.7.2 Software Process Implementation .....
3.7.3 Software Design Outputs .....
3.8 Equipment Qualification .....
3.8.1 Environmental Qualification .....
3.8.1.1 Temperature and Humidity Qualification .....
3.8.1.2 Seismic Qualification .....
3.8.2 Electromagnetic Compatibility Qualification .....
3.8.3 Radiation Qualification .....
3.9 Deviations from Prior Licensing Topical Reports .....
3.10 Confirmation of Licensing Topical Reports Safety Evaluation Plant-Specific Actions .....
3.12 Tests and Self-Test Diagnostics .....
3.13 System Failure Analysis .....
3.14 Determinism .....
3.15 Compliance with IEEE Std 603-1991 Requirements .....
3.16 Conformance to IEEE Std 7-4.3.2-2003 .....
3.17 Secure Development and Operational Environment .....
3.18 Inspection Follow-up Items .....
4.0 Conclusion .....
5.0 References .....
6.0 Acronyms .....

[7] This Enclosure provides the template for the safety evaluation input developed by the I&C staff to the project management staff for issuance, per NRR Office Instruction LIC-101.