U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

APRIL 12, 2018

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-06

Licensing Process

Interim Staff Guidance

(Revision 2 DRAFT)

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

Contents

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

List of Figures

List of Tables

ADAMS Accession No: ML18066A796 ***concurrence via e-mail**

OFFICE	NRR/DLP/PLPB/PM	QTE	NRR/DLP/PLPB/PM	NRR/DLP/PLPB/BC*	NRO/DEI/ICE/BC*
NAME	LWilkins		JGolla	DMorey	IJung
DATE					
OFFICE	NRO/DE/ICEEB/BC*	NRR/DE/EICB/BC*	NRR/DIRS/IRIB/BC	OGC	NRR/DIRS/IRGB/LA
NAME	RJenkins	MWaters	THipschman		ELee
DATE					
OFFICE	NRR/DIRS	RES/DE*	NRO/DEI*	NRR/DE*	
NAME	CMiller	BThomas	RCaldwell	EBenner	
DATE					

OFFICIAL RECORD COPY

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

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 with NRC regulations.

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

Review of DI&C equipment modifications should include an assessment of the acceptability of system development life-cycle activities. While 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 if the four fundamental design principles of redundancy, independence, deterministic behavior (i.e., predictability and repeatability), and defense in depth and diversity are met.

B Purpose

This ISG provides guidance for the NRC staff's review of LARs supporting installation of DI&C equipment in accordance with licensing processes defined in Office of Nuclear Reactor Regulation (NRR) Office Instruction LIC-101, "License Amendment Review Procedures." This ISG identifies information the NRC staff should review for DI&C equipment and provides guidance on the phases in which the information should be reviewed.

This ISG is also designed to be used with the NRC's review and approval process for topical reports, defined in NRR Office Instruction LIC-500, "Topical Report Process." Where a licensee references an NRC-approved topical report, the NRC staff should be able to, where appropriate, limit its review to assessing whether the application of the DI&C modification falls within the envelope of the topical report approval. Because this ISG was developed on the basis of established guidance, it is designed to work in concert with that guidance. As a result, this ISG references other guidance documents for review criteria.

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

B.1 Background

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 license amendment is required, licensees are 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, licensees 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.

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 in support of safety evaluations. For reviews using the Alternate Review Process (defined below), the ISG provides additional guidance for performing early-stage reviews of digital safety-related systems in support of safety evaluations. The NRC staff may review the system design and development process to support a determination that the design meets regulatory requirements and that, in safety-related applications in nuclear power plants, the process is of sufficiently high quality to produce systems and software suitable for use.

B.1.1 Effects of Modification Scope on the Content of the License Amendment Request

The licensee, with feedback from the NRC staff through the pre-application (Phase 0) meeting(s), will develop and docket the information necessary to support the safety evaluation of the modification or new installation. This process applies to a range of modifications—from component(s) through partial, complete, or multiple systems.

Additionally, the NRC staff recognizes there are different approaches available to licensees regarding use and application of an NRC-approved topical reports. 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 an applicant justifies the deviation as proposed for implementation at its facility. Licensees can also propose to use a platform for which there is no generic approval.

B.1.2 Documentation Reviewed

The NRC staff reviews the information necessary to make a safety determination using the review criteria found in SRP Chapter 7. It is the responsibility of the licensee or applicant to ensure that the documentation provided demonstrates regulatory compliance for the safety-related system. The licensee or applicant should perform design verification on design information.

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. Actual document submittals are expected to be unique for each I&C project.

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

Some documents associated with software development are expected to be revised as system development activities progress. These are sometimes referred to as “living documents.” During the acceptance review period, it should be decided whether a version of the document should be submitted to the NRC and when (i.e., in what phase) to submit it. It is normally not necessary for applicants to submit each version of these living documents to support the safety evaluation. Each living document should contain sufficient information to demonstrate conformance to applicable regulatory requirements. In some cases, it may also be necessary to provide access to current versions of a living document to support audit activities.

B.1.3 I&C Review Scope

Consistent with LIC-101, the staff’s review of LAR will be limited to the scope of the DI&C modification. Requests for additional information (RAIs) should have a clear nexus to information required 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 found in SRP Chapter 7, and using 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.

Some DI&C equipment modifications may credit manual operator actions and require 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, with close coordination with in the I&C evaluation under Chapter 7. The review of the modification described in the LAR may also impact other review areas. The NRC staff will review the information necessary to make a safety determination using the review criteria found in the SRP for all relevant review areas.

The staff reviews any cyber security design features included as part of a safety system for the purposes of complying with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, “Protection of Digital Computer and Communication Systems and Networks,” only to ensure that their inclusion does not adversely affect the reliable performance of the safety function.

For Institute of Electrical and Electronics Engineers (IEEE) standards endorsed by NRC guidance, the staff should review each standard for conformance with the changes and exceptions in the endorsing regulatory guide (RG) to determine if the plant revised licensing basis criteria are met.

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

As part of the Integrated Action Plan Modernization Plan #4A tactical efforts, dated March 31, 2017 (Agencywide Documents Access and Management System (ADAMS)

This draft is for presentation of the NRC staff’s current thinking. It has not been through the NRC’s review processes and remains subject to change.

Accession No. ML17102B307), the NRC staff coordinated with the Nuclear Energy Institute and industry representatives to identify key significant issues associated with the guidance for license amendments that include DI&C modifications.

This revision also incorporates lessons learned from DI&C LAR reviews that used the previous revision of this ISG.

C Digital I&C Review Process

NUREG-0800 provides guidance to the NRC staff for performing safety reviews of LARs under 10 CFR 50.90, "Application for Amendment of License, Construction Permit, or Early Site Permit." The SRP refers to some standards that are not endorsed by RGs as sources of information for the NRC staff. The SRP refers to these standards as sources of good practices for the NRC staff to consider. This ISG assumes 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 regulatory guidance should be the most current revision, and the standards should be the most recently endorsed edition, or the revisions and editions agreed upon during the pre-application (Phase 0) meeting.

The LAR description of the plant system includes all affected plant equipment and the interfaces with operations and maintenance. Depending on the extent of the plant modification, the plant system description may consist of a description of one or more systems; one or more subsystems, and/or; one or more components.

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 requests for additional information, and ensures 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 at another plant. Each LAR is a plant-specific licensing action.

The acceptability of a safety system is based on the system's ability to perform design-basis functions (e.g., trip on high level, display of proper indications) and the system's conformance to regulatory requirements (e.g., independence). This information should be contained in the system design description and, where applicable, in safety analysis reports to that demonstrate that the design meets the requirements.

Based on proposed system changes, the reviewer should determine if additional regulatory criteria from the SRP, documented in Chapter 7.1, "Instrumentation and Controls—Introduction," and Table 7.1, should be applied. The criteria should be used as appropriate, based on the scope of the modification.

This ISG describes processes for evaluating DI&C LARs: Tier 1, Tier 2, Tier 3, and Alternate Review Process. Section C.1 provides the process for Tiers 1, 2, and 3. Under the Tier 1, 2, and 3 processes, the license amendment is issued after the factory acceptance testing (FAT) is completed and the results have been evaluated. Section C.2 describes the Alternate Review Process. Under the Alternate Review Process:

a. the license amendment is issued after the system design (see Section C.2.1) is completed and evaluated

b. system development activities will continue during LAR review and after license amendment issuance in compliance with specific license conditions

c. the LAR references an NRC-approved topical report

For Tiers 1, 2, and 3, acceptability of platform and application software[1] for safety system functions is based on the following:

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

b. evidence that the plans were followed in an acceptable software life cycle

c. evidence that the process produced acceptable design outputs

In Enclosure B of this ISG, Columns 1, 2, and 3 (for the Tier 1, 2, and 3 processes, respectively) provide a template that may be used when a license amendment is to be completed in the late stages of design and development after completion of FAT. This method involves a two-phase submittal to allow licensing review activities to be performed in parallel with the design implementation and test activities of the software development process.

For the Alternate Review Process, acceptability of the platform is based on the tiered review process (see Section C.1) as documented in the applicable topical report. Acceptability of the system application is based on the following:

a. the I&C system development processes, as summarized in accordance with Section D.4

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

c. the regulatory commitments the licensee makes to ensure that the vendor produces lifecycle outputs that meet the associated lifecycle requirements

In Enclosure B, Column AR (for Alternate Review Process) may be used if a license amendment is to be completed earlier (i.e., during functional design but before completion of detailed design, implementation, or testing). The information docketed can be derived from a variety of documents including conceptual design, system requirements, hardware requirements, software requirements, and human-system interface requirements. The Section D review guidance can be used as a basis for developing inspection plans.

See Section D.4 (for the Alternate Review Process) and Section D.9 (for Tiers 1, 2, and 3) for the review guidance for system development process. The NRC staff audits the documentation and development products that are referenced in the LAR. Enclosure B provides guidance on the content of the licensing application.

[1] "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. (From IEEE Std 7-4.3.2-2016)

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

Recognizing that DI&C plant modifications represent a significant licensee resource commitment, a phased approach is appropriate. In this approach, the NRC staff initially vets critical, fundamental system information before taking subsequent steps in the DI&C system development and licensing process. Therefore, the NRC staff encourages the use of public meetings before the submittal of the LAR to discuss issues regarding the system development. The intent 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 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. The licensee and the NRC discuss the timing of specific information availability in the Phase 0 meetings and establish the timing during the acceptance review period.

Figure C.1 below is a flowchart of the overall review process. This figure illustrates the various review phases, discussed in Sections C.1.1 through C.1.4.

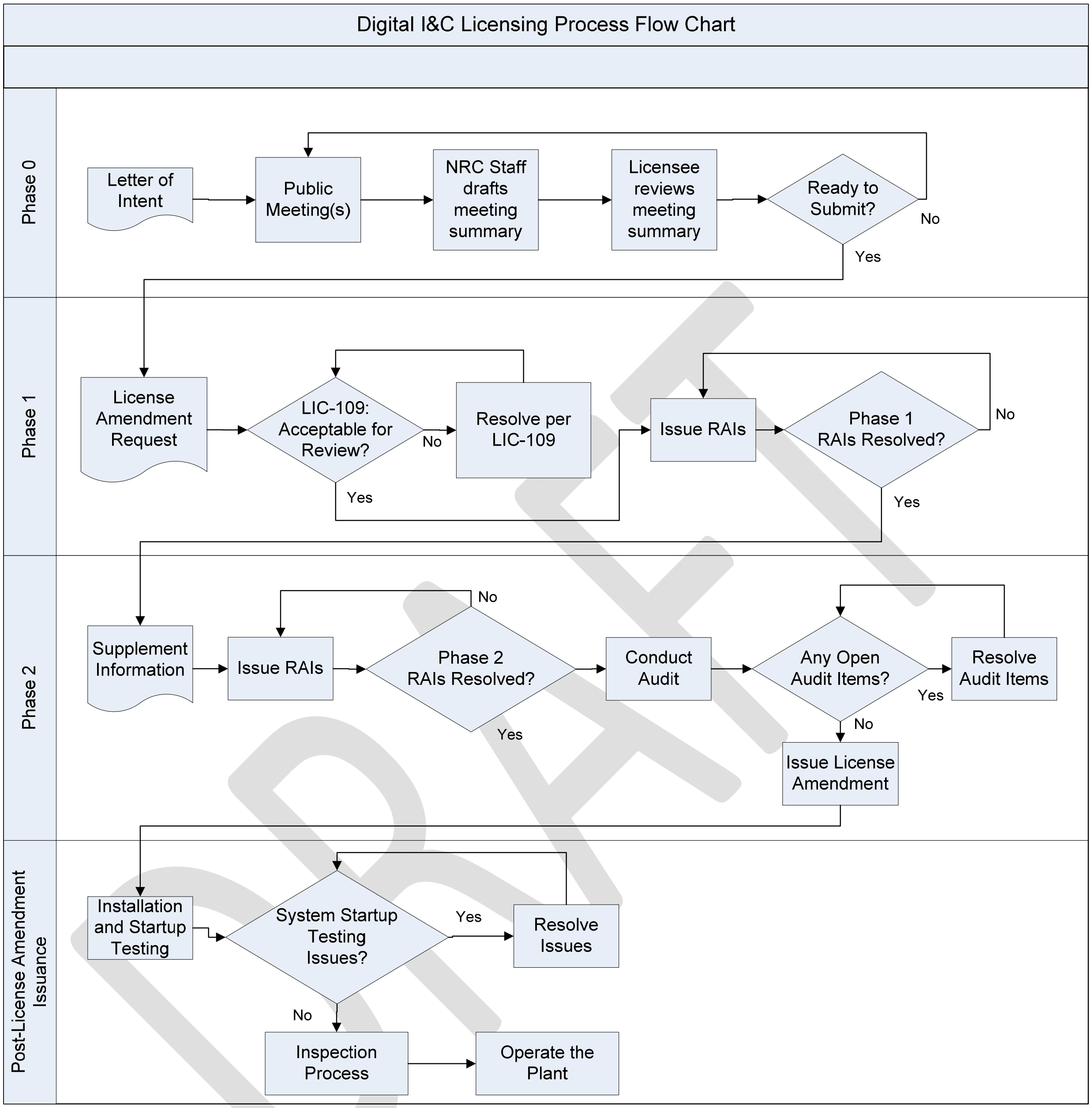

Figure C.1 DI&C Licensing Process and Post-License Amendment Issuance Flowchart for Tiers 1, 2, and 3

The NRC staff recognizes that licensees can use and apply an NRC-approved topical report for an I&C platform in different ways. Therefore, the NRC staff should consider applications to be within one of the following 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)

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

within the envelope of its generic approval as described in the topical report. A Tier 1 review would rely on previous review efforts. In Enclosure B, the Tier 1 column (1) shows the information that a licensee would typically submit in support of a Tier 1 review. This list would not include those documents already reviewed and approved by the NRC staff. See Section D.5 for applying an NRC-approved topical report safety evaluation.

Tier 2

Tier 2 applies to license amendments proposing to reference an NRC-approved topical report with deviations to suit the specific application. Deviations could include, for example, a revised software development process or new hardware. An evaluation 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 the information that a licensee would typically submit 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 evaluations generally include Tier 1 review scope and 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. Licensees should expect that 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 the information that a licensee would typically submit in support of a Tier 3 review. Tier 3 evaluations generally include Tier 1 review scope and topical report review scope. The typical topical review scope includes hardware, software, developmental tools, and associated developmental methods (e.g., application restrictions and integration methods).

These tier labels are 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 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 review of certain listed documents and necessitate the inclusion of other unlisted documents.

C.1.1 Pre-Application (Phase 0)

Before submitting an LAR, the licensee should have an overall design concept that adequately addresses NRC regulatory requirements and policy on key issues. To this end, the NRC staff intends to use the public meeting process to discuss with licensees how their proposed DI&C modification LAR will address the following:

a. key design concepts, including the four fundamental design principles

b. significant variances from current guidance

c. the NRC's determination of the appropriate "tier" of review

d. any tools proposed for reading files

e. defining the portion of the plant system to be replaced and its impact on the plant, calibration, surveillance testing (and associated impacts on plant staff), and FSAR impacts

f. the protocol for providing and submitting on the docket specific versions of living documents or the information they contain (see Section B.1.2)

g. establishment of an appropriate licensee living document schedule

h. other unique or complex topics associated with the proposed design

i. other changes to the plant system not included in the LAR being discussed

These meetings are intended to be two-way discussions in which the licensee presents the concept and the NRC staff provides feedback on the critical aspects of the proposed design that are likely to affect the NRC staff's evaluation.

Further, these discussions should include whether the licensee is proposing the use of an NRC-approved topical report, any planned deviations from staff positions, and specifics of the platform or application software processes. Licensees are encouraged to discuss topics from other review areas, as well as the potential use of any best-estimate evaluations to generate realistic assumptions (or models) and address uncertainty associated with the results.

These meetings will also address the schedule and scope of audits.

All proposed deviations from the submittal information guidance in Enclosure B should be discussed in the Phase 0 meeting or meetings. The Phase 0 meeting summary should document any associated agreements.

Following each meeting, the NRC staff should capture the topics discussed in a meeting summary. This summary should include a preliminary NRC staff assessment of the licensee's concept (or those subparts of the overall concept discussed) and identify the areas significant to this preliminary assessment. Additionally, as appropriate, the NRC staff should include a preliminary assessment of which review tier would be applicable for the proposed modification. Enclosure A to this document presents an example of a meeting summary.

C.1.2 Initial Application (Phase 1)

Once a licensee believes it has a design that adequately addresses NRC criteria, the licensee should prepare and submit an LAR (see Enclosure B for information to be provided with the LAR). The licensee should identify any design features and concepts that may affect the staff's preliminary assessment made during Phase 0.

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

Initially, the NRC staff should review the application in accordance with the NRR Office Instruction LIC-109, "Acceptance Review Procedures," to determine whether the application contains sufficient information for NRC staff review. The NRC should document the acceptability of an application in a letter to the licensee.

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

Some information may not be available upon initial application, and the review process may be more efficiently administered by beginning before that information is available. Therefore, a DI&C modification application may be found to be sufficient for review provided that a clear schedule for submission of omitted information is included. The NRC staff should agree to any proposed changes to the schedule in advance of any document due date.

During Phase 1, the NRC staff should draft the safety evaluation and issue RAIs 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 licensee should respond to the RAIs before submitting the Phase 2 information. Although the NRC staff may have additional questions based on the responses to the Phase 1 RAIs, the licensee should not delay submission of the Phase 2 information.

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 and licensee should consider having publicly-noticed, periodic conference calls to discuss staff questions. Following each call, the NRC staff should capture 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.

If necessary, the NRC staff should conduct one or more audits in accordance with NRR Office Instruction LIC-111, "Regulatory Audits." As discussed further in Section C.1.3, the NRC staff and the licensee 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, and the NRC project manager, in consultation with the licensee and NRC technical staff, should schedule the audit. The staff may request that some portion of the audited materials be docketed.

C.1.3 Continued Review (Phase 2)

After responding to the Phase 1 RAIs and with sufficient lead time to support the requested approval date, the licensee should submit a supplement containing sufficient information to address aspects of the review areas not submitted in the initial LAR or subsequent responses to RAIs (see Enclosure B for information to be submitted before the requested approval date). The NRC staff should expect the licensee to adhere to previously established submittal schedules.

During Phase 2, the NRC staff should continue the RAI process until the licensee has provided sufficient information for a decision to be made 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, but the performance of an effective and efficient audit necessitates that the LAR and supplements be sufficiently detailed regarding the later phases of the system development life cycle.

Although the plans and other available information should be submitted as early as possible, it is acceptable to submit certain documentation as mutually agreed in the Phase 0 meetings, but before the planned completion date of 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. While Figure C.1 contains post-license amendment issuance activities, the licensing process covered by this ISG ends at the issuance of the license amendment.

As determined during both the Phase 0 meetings and the review, the licensee should make additional documents available electronically for NRC evaluation as requested by the NRC. Electronic documents can be established on a vendor’s shared site, to allow the NRC to audit the documents and to determine if docketing is necessary to support the licensing review. The licensee should protect the documents made available electronically. The licensee should ensure that staff members cannot download or print whole documents or portions of documents made available electronically to their NRC computers.

Consisent with licensing review guidance, the staff should develop a safety evaluation report that documents the basis for approval. The safety evaluation should document applicable regulatory requirements, the information provided by the applicant including regulatory commitments, and the summary of the staff evaluation, and the basis for the determination that the application meets applicable requlatory requirements. Since commitments made by a licensee in support of a license amendment request are not legally binding, the staff’s safety evaluation should not rely on commitments as a basis for any part of the staff’s approval of a proposed amendment**.** The NRC staff may escalate some proposed licensing commitments into license conditions based on their safety or regulatory significance.

In addition, the staff should separately in the safety evaluation identify “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 be used as safety basis for the LAR approval.

C.1.4 Post-License Amendment Issuance

The licensing process covered by this ISG ends at the issuance of the license amendment. Following regulatory approval of the DI&C system, licensees may implement the modification by installing the system, implementing associated procedural and technical specifications (TS) changes, and completing startup testing. SRP Chapter 7.0, Section V, contains guidance for establishing inspections.

The startup testing is conducted in accordance with the plan submitted during Phase 2. NRC regional staff may review the startup testing as an inspection function conducted by the appropriate regional staff in accordance with Inspection Procedure 52003, “Digital Instrumentation and Control Modification Inspection.” Licensing staff may need to advise and assist inspection staff as appropriate to verify the development, implementatation, and/or installation phases of the approved digital modification.

After approval of the LAR, changes are controlled and implemented by licensee programs which, in turn, are governed by 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities,” Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” and other regulatory requirements. The regulation in 10 CFR 50.59, “Changes, Tests and Experiments,” governs the need for prior NRC review and approval.

C.2 Alternate Review Process Overview

The NRC staff recognizes that there are different approaches available to licensees regarding use and application of NRC-approved topical reports. Recognizing that DI&C modifications represent a significant licensee resource commitment, an alternate approach is provided for 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 of a proposed plant modification. The Tier 1, 2, and 3 review process includes NRC evaluation of software design, implementation, and testing. The Alternate Review Process is based on detailed system design information (see Section C.2.1), additional design information as described in Section D.2, and application planning and processes as described in Section D.4. For the NRC staff to reach a safety determination using the Alternate Review Process, the licensee is expected to provide the required information at the time of LAR submission.

For this alternate approach, the licensee provides critical, fundamental system information to the NRC staff for review and approval, before taking subsequent steps in the DI&C hardware and software development process. As in the process described in Section C.1 above, the NRC staff encourages the use of public meetings before submittal of the LAR to discuss issues regarding the system development. The licensee recognizes that there is a licensee risk that the system design submitted and approved by NRC may have implementation challenges that necessitate a modification. The modification could require NRC review and approval of a subsequent LAR, or some changes may be completed without NRC approval through the 10 CFR 50.59 process, which are 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) lists the information that the licensee typically should submit in support of an Alternate Review Process review. See Section D.5 for applying a topical report safety evaluation previously approved by the NRC.

The NRC staff encourages the use of Pre-Application Coordination meetings before submittal of the LAR to discuss issues regarding the system development. The early meetings help ensure that the licensee will meet regulatory requirements early in the process. During Pre-Application Coordination meetings, licensee and NRC staff discuss any design features that may challenge the NRC staff’s ability to assess the system’s compliance with NRC regulations.

Unlike the Tier 1, 2, and 3 Process, the Alternate Review Process does not include provisions for Phase 2 document submittals. Instead, the licensee should provide all information identified in Enclosure B to the NRC at the time of application submittal. A safety evaluation conducted

This draft is for presentation of the NRC staff’s current thinking. It has not been through the NRC’s review processes and remains subject to change.

for an Alternate Review Process submittal will base its safety conclusions on information provided in accordance with Enclosure B and any supplemental information.

The staff should evaluate key licensee regulatory commitments related to the software design, implementation, and testing activities as potential license conditions. Such conditions should (1) address issues of high safety or regulatory significance; (2) be worded such that the meaning is clear and not open to different interpretations; and (3) explicitly define the conditions for satisfaction of the condition. The license conditions should not be open ended or require NRC action to complete.

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 application, the NRC staff will credit the results of these previous evaluations to the extent practicable. Therefore, the NRC staff may accept licensee regulatory commitments to perform some detailed design, implementation, and integration activities to address topical report application specific action items. The NRC staff may convert these regulatory commitments into license conditions based on their safety or regulatory significance.

The staff will review design information related to the site-specific configuration at a level that is sufficient to demonstrate compliance with the applicable regulations and associated guidance as described in the SRP. The docketed LAR should contain necessary and sufficient information to demonstrate regulatory compliance. The Alternate Review Process provides guidance for information to be included in an LAR. This information can be derived from a variety of concept, system requirement, hardware or software requirement, or design documents, each of which may be considered as providing 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.

Licensees should determine whether the development life-cycle outputs meet the specified design requirements. The LAR describes the licensee’s vendor oversight plan, which ensures that the vendor executes the project consistent with the LAR and the 2015 version of the American Society of Mechanical Engineers standard 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.” 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.

Sections D.2, D.3, and D.4 identify the review areas applicable to the Alternate Review Process. 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 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 the 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." Thus, the reviewer should consider the relevant guidance in the SRP to supplement the guidance provided in this ISG.

For the Alternate Review Process, the Enclosure B tables provide 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. It is possible that the plant-specific application of a digital system may depend on the use of other unlisted documents. The licensee and staff should identify and discuss these differences during the Pre-Application Coordination meeting or meetings.

Figure C.2 below is a flowchart of the overall Alternate Review Process. This figure illustrates the various stages of the review, discussed further in Sections C.2.2 through C.2.4.

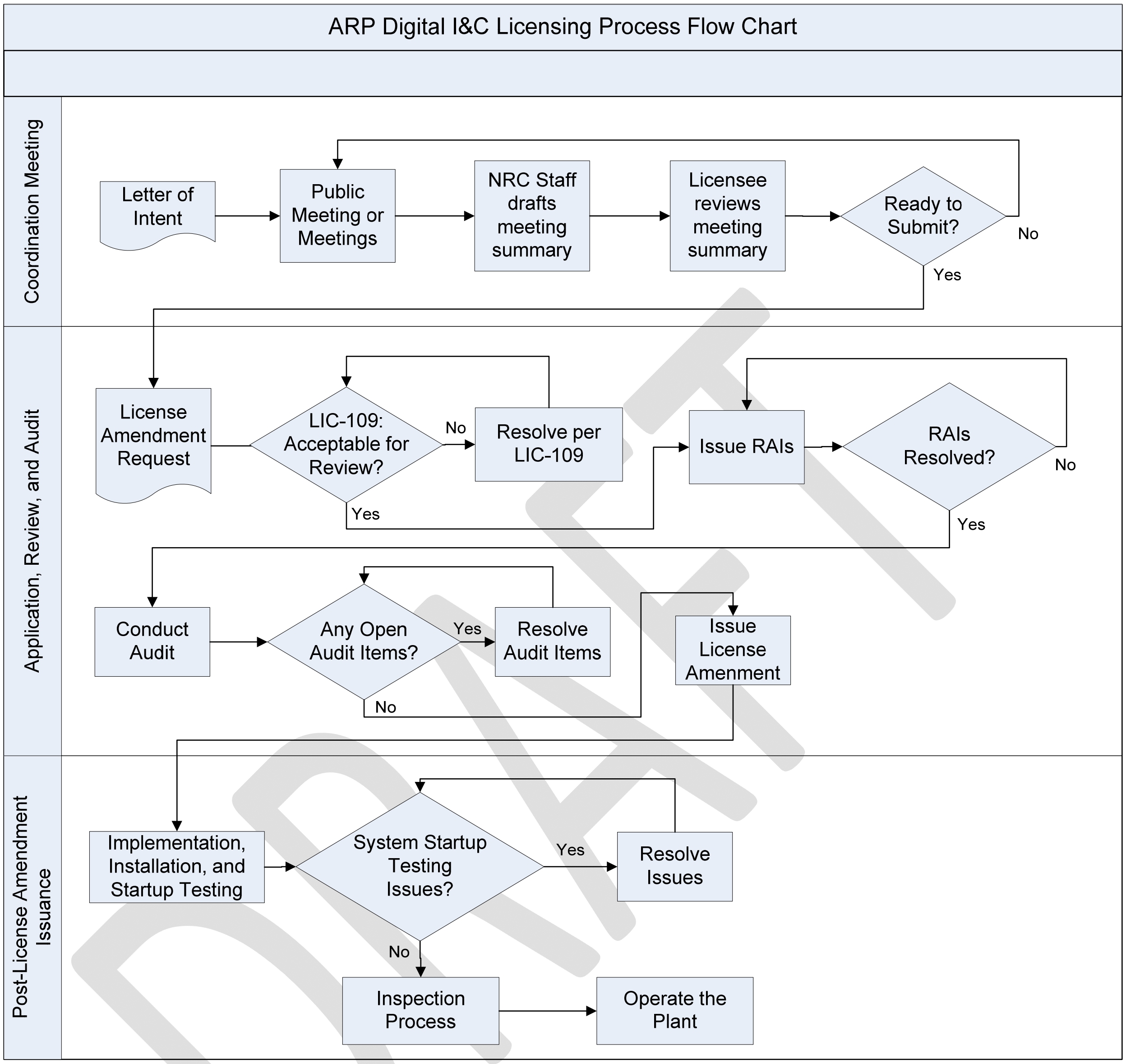
ARP Digital I&C Licensing Process Flow Chart
Coordination Meeting
Letter of Intent
Public Meeting or Meetings
NRC Staff drafts meeting summary
Licensee reviews meeting summary
Ready to Submit?
No
Yes
Application, Review, and Audit
License Amendment Request
LIC-109: Acceptable for Review?
No
Yes
Resolve per LIC-109
Issue RAIs
RAIs Resolved?
No
Yes
Conduct Audit
Any Open Audit Items?
Yes
No
Resolve Audit Items
Issue License Amenment
Post-License Amendment Issuance
Implementation, Installation, and Startup Testing
System Startup Testing Issues?
Yes
No
Resolve Issues
Inspection Process
Operate the Plant

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

C.2.2 Licensee Prerequisites for the Alternate Review Process

To use the Alternate Review Process, the licensee should address the following items:

1. Describe the licensee’s Vendor Oversight Plan in the LAR. The plan ensures that the vendor executes the project consistently with (1) the LAR and (2) the 2015 version of NQA-1, Part II, Subpart 2.7. The Vendor Oversight Plan helps ensure that the vendor will meet both the process and technical regulatory requirements. Vendor oversight is a series of interactions with the vendor and progresses throughout the entire system

This draft is for presentation of the NRC staff’s current thinking. It has not been through the NRC’s review processes and remains subject to change.

development life cycle. The plan should address the intended interactions between design, test, V&V, and quality assurance (QA) within the vendor's organization.

2. DI&C Approved Topical Report
    a. The proposed DI&C modification references an NRC-approved DI&C topical report (also referred to as the "-A version").
    b. The proposed DI&C modification is within the scope of the referenced topical report's applicability.
    c. The vendor of the NRC-approved topical report will perform detailed software design, implementation, and testing.

3. Appropriate Licensee Commitments in Consideration of Early License Amendment Issuance
    a. The LAR includes appropriate commitments to complete plant-specific actions that are included in the referenced topical report.
    b. The LAR includes appropriate commitments to complete life-cycle activities under the licensee's QA program, which would be included in a Tier 1 licensing review but cannot be performed because of an early license amendment issuance.

C.2.3 Pre-Application Coordination Meetings

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. To this end, the staff intends to use the Pre-Application Coordination meeting process to engage licensees in a discussion of how their proposed DI&C modification LAR will address the following:

a. use of the Alternate Review Process

b. key design concepts, including the four fundamental design principles

c. significant variances from current guidance

d. significant variances from the NRC-approved topical report

e. application of the selected system (platform) to the plant system

f. defining the portion of the plant system to be replaced and its impact on the plant, calibration, surveillance testing (and associated impacts on plant staff), and FSAR impacts

g. any tools proposed for sharing files (e.g., SharePoint site)

h. establishment of an appropriate licensee living document schedule

i. other unique or complex topics associated with the proposed design

j. other changes to the plant system not included in the LAR but with the potential to change safety conclusions (e.g., elimination of single points of vulnerability within channels, redundant field power supplies)

These meetings are intended to be two-way discussions in which the licensee presents the concept and the staff provides feedback on the critical aspects of the proposed design that are likely to affect the staff's evaluation.

Further, 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 and issued a safety evaluation on the NRC-approved topical report, any planned deviations from staff positions, and specifics of the application software processes to be used. Licensees are encouraged to discuss topics from other review areas (e.g., how to use best-estimate evaluations with realistic assumptions or models and the impact on uncertainty associated with the results).

All proposed deviations from the submittal information guidance described in Enclosure B should be discussed in the Pre-Application Coordination meetings. The Pre-Application Coordination meeting summary should document any associated agreements.

The meetings will also address the schedule and scope of audits and potential inspections, which may be updated as the NRC staff's review progresses.

Following each meeting, the staff should capture the topics discussed in a meeting summary. This summary should include a preliminary staff assessment of the licensee's concept (or those subparts of the overall concept discussed) and identify the areas that are significant to this preliminary assessment. Additionally, the staff should include a preliminary assessment that the Alternate Review Process is applicable for the proposed modification. Enclosure A to this document presents an example of a meeting summary.

C.2.4 Application, Review, and Audit

Once a licensee concludes that a sufficient design has been documented that adequately addresses NRC criteria, as discussed in the Pre-Application Coordination meeting, the licensee should prepare and submit an LAR, based on the information suggested in Enclosure B (Column AR). The licensee should identify any design features and concepts that may affect the staff's preliminary assessment made during Pre-Application Coordination meetings.

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 NRC review and be submitted on the docket under oath and affirmation. The documents will contain materials necessary to reference in the safety evaluation.

The staff should review the application in accordance with NRR Office Instruction LIC-109 to determine whether the application is sufficient for staff review.

As determined during both the Pre-Application Coordination meetings and the review, the licensee should make additional documents available electronically for NRC evaluation as requested by the NRC. Electronic documents can be established on a vendor's shared site to allow the NRC to audit the documents and to determine if docketing is necessary to support the licensing review. The licensee should protect the documents made available electronically. The licensee should ensure that members of the NRC staff cannot download or print whole documents or portions of documents made available electronically to their NRC computers to prevent the proprietary information in the documents from becoming discoverable and thus potentially released to the public under the Freedom of Information Act.

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

During the review, the staff and licensee should consider having periodic conference calls to discuss staff questions. The questions raised by the staff should be kept in an “open items” list, along with the responses from the licensee. The open items list should contain information to track issues to closure. The staff may determine that some items and responses should be formalized into RAIs.

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

If necessary, the NRC staff can conduct one or more audits in accordance with NRR Office Instruction LIC-111. The staff and the licensee 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 and the NRC project manager, in consultation with the licensee and technical staff, should schedule the audit. Individual circumstances will dictate the appropriate vehicle for the staff to obtain the necessary information. To support the LAR review, the staff may request that some of the materials provided electronically be docketed.

During the review of an LAR, certain items may be identified that apply to the system configuration, testing, or operation that will be completed after the safety evaluation is issued. The NRC staff should separately in the safety evaluation identify such items as “potential items for inspection” as recommendations to help inform the focus of post-license amendment vendor and site inspections. However, the “potential items for inspection” cannot be relied upon or be used as safety basis for the LAR approval.

While Figure C.2 contains post-license amendment issuance activities, the Alternate Review Process licensing process covered by this ISG ends at the issuance of the license amendment.

C.2.5 Post-License Amendment Issuance

Although the Alternate Review Process discussed in this ISG ends at the issuance of the license amendment, following regulatory approval of the DI&C system, licensees complete the design and install the system, implementing associated procedural and TS changes and completing startup testing. SRP Chapter 7.0, Section V, contains guidance for establishing inspections.

NRC quality assurance and vendor inspection staff may review the software design and implementation activities prior to transfer 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 as an inspection function conducted by the appropriate NRC staff in accordance with applicable inspection guidance (e.g., Inspection Procedure 52003). Licensing staff may need to advise and assist inspector staff as appropriate to verify the development, implementatation, and/or installation phases of the approved digital modification.

Changes after approval of the LAR are controlled and implemented by licensee programs which, in turn, are governed by Appendix B to 10 CFR Part 50 and other regulatory requirements. The regulation in 10 CFR 50.59 governs the need for prior NRC review and approval.

D Review Areas for the License Amendment Process

As noted in Enclosure B, Sections D.2, D.3, and D.4 apply only 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. Depending on the plant modification, the plant system description could consist of one or more systems; one or more subsystems, and/or; one or more components. This description should be 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). In cases where the NRC has evaluated the digital equipment proposed, the licensee should refer to the description and evaluation, including any available ADAMS accession numbers. 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 individual channels or divisions should be described, including the signal flows between the various digital equipment items. Second, the overall system should be described, with particular emphasis on additional hardware items not included in the description of the channels or divisions, such as voters, communications with workstations or nonsafety-related systems, bypass functions/switches, and diverse actuation systems (DASs).

D.1.2 Evaluation

The reviewer should determine if the LAR information presents a comprehensive explanation of the system. From this, the reviewer should determine the scope of review and identify any constraints on the approval of the system.

The NRC's understanding of the plant system and digital equipment should be documented in the safety evaluation to explain system operation and to support the technical evaluations of other sections.

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. separation and independence requirements within the system (e.g., channels, trains, isolation)
d. connections and internal interfaces within the safety 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 nonsafety-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 existing system equipment in the plant

This description should also identify which portion(s) of the system are being replaced. (While system design functions are listed here, Section D.2.3.1 describes their design basis.)

D.2.1.2 Evaluation

The reviewer should understand the changes the replacement system will require to existing input and output interfaces with the plant and 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 NRC's understanding of the existing system architecture should be documented in the reviewer's safety evaluation to support the technical evaluations of other sections.

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. Changes to the existing architecture should be clearly designated and described, including the reason for the changes. This description provides a basis for discussion of the fundamental design principles in Section D.2.6.

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). Sufficient information should be provided to enable understanding of the changes required by 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, reflecting the final plant system, installed in the plant and should clearly describe any changes made to items (a) to (j) 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 will document any restrictions on the new system architecture based on physical plant location, such as size, cooling, or power supply.

The LAR should identify the digital equipment vendor and the NRC-approved topical report and revision based on the approving safety evaluation.

The LAR should describe all design functions and service/test functions. Sections D.2.3.1 and D.2.3.2 describe and evaluate these functions. The licensee's submittal should describe each design function that is performed by the portion(s) of the system being replaced. All new design functions proposed in the LAR should also be described. 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 with the design functions. Service/test functions are digital equipment features to support the design functions. The service/test functions, unlike the design 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 maintaining a secure operational environment (SOE). The topical report may have described the service/test functions. These functions may also be implemented in application software, which the topical report may not have described. Although any portions of the service/test functions that remain unchanged from the topical report should not require repeating a prior evaluation, they should be identified in the LAR.

The LAR should demonstrate how any self-test portions of the service/test functions provide fault detection capabilities and thus conform with IEEE Standard (Std) 7-4.3.2, “IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations,” Clauses 5.5.2 and 5.5.3, consistent with IEEE Std 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Clause 5.7. The discussion of self-tests and self-diagnostics should demonstrate conformance to existing applicable TS and any proposed change to TS.

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

a. How the application interfaces with and uses the self-test and self-diagnostic features defined in the NRC-approved topical report and evaluated in the safety evaluation. This should include a discussion of the malfunction detection coverage considering the combination of TS surveillances and the automated features.

b. For communications messages, describe 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, along with the use of each message (e.g., voting, bypass). Error detection means provided in communications messaging and processing (see DI&C-ISG-04, Revision 1, “Highly Integrated Control Rooms—Communications Issues,” Section 1, Item 12, dated March 6, 2009 (ADAMS Accession No. ML083310185)) apply to communications messages used by safety functions. This section of the LAR could reference the DI&C-ISG-04 compliance assessment containing this data.

c. How the design prevents software failures from affecting the 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.

d. Treatment and detection of malfunctions in the system inputs, including sensors and transmitters, in the system logic including internal voters within the safety system or voters external to the safety system, and malfunctions 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.

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 an information-only markup of the plant’s FSAR, showing how the new design will be incorporated. 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 content in Section D.7.

This draft is for presentation of the NRC staff’s current thinking. It has not been through the NRC’s review processes and remains subject to change.

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

a. the primary protection system
b. any portions of the existing system that remain
c. the priority logic (if applicable)
d. credited manual operator actions
e. maintenance, test, surveillance, and other similar actions
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, 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, 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, the status indications, or the bypassed indications, the LAR should describe how the modifications support the ability of the operator to use the indications, in accordance with IEEE Std 603, Clause 5.8.4.

D.2.2.2 Evaluation

The safety evaluation should include the reviewer's understanding of 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, 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).

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:

a. between safety-related systems
b. between safety-related and nonsafety-related systems

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

a. plant system design functions
b. connections within the safety system, including cross-divisional interfaces and connections to human-system interfaces
c. connections between safety-related systems
d. connections between safety-related and nonsafety-related systems and identification of signal and data isolation devices
e. indications used for manual control
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 evaluate whether the LAR documents the service/test functions and design functions as they are implemented in the architecture. 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, Clauses 5.5.2 and 5.5.3 (thereby meeting the requirements of IEEE Std 603, 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.

Section D.7.2.1 addresses the evaluation for consistency between TS and the self-tests and self-diagnostics implemented in the architecture.

If the design includes a DAS, then the reviewer should evaluate whether the LAR describes how the integration of the system and 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 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, the status indications, or the bypassed indications, the reviewer should evaluate those changes in accordance with IEEE Std 603, 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 use in a safety function as well as in a display in the control room).

Each design function’s description should include the following:

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

b. all monitored variables used to control each protective action

c. minimum number and location of sensors and equipment required for protective purposes

d. functionality, including input/output ranges and setpoints (for trip functions, the documentation defines the margins between setpoints and allowable values (e.g., those including all applicable uncertainties))

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

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

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

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

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

The LAR should address each of the listed IEEE Std 603 requirements for each service/test function. As with design functions, some service/test functions may be addressed for the system. The service/test functions should demonstrate compliance with the following:

a. Clauses 5.2 and 7.3, “Completion of Protective Action”
b. Clause 5.5, “System Integrity”
c. Clauses 5.7, 6.5, 6.5.1, and 6.5.2, “Capability for Testing and Calibration”
d. additional specifications for digital equipment, extending the Clause 5.5 guidance in IEEE Std 7-4.3.2, Clause 5.5.2, Test and Calibration, as reflected in IEEE Std 603, Clause 5.7
e. additional specifications for digital equipment, extending the Clause 5.5 guidance in IEEE Std 7-4.3.2, Clause 5.5.3, “Fault Detection and Self-Diagnostics”, as reflected in IEEE Std 603, Clause 5.7
f. Clause 5.8, “Information Displays”
g. Clause 5.9, “Control of Access”
h. Clause 5.10, “Repair”
i. Clauses 6.6 and 7.4, “Operating Bypasses”
j. Clauses 6.7 and 7.5, “Maintenance Bypass”
k. 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 conformance to any proposed TS for new system functions.

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

D.2.3.2 Evaluation

Through review of system design information, the reviewer should evaluate whether the licensee’s submittal contains information sufficient to demonstrate that the design-basis information satisfies Clause 4 of IEEE Std 603. 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 clauses listed in Section D.2.3.1. The service/test functions (e.g., internal diagnostics, calibration, and surveillance test support) may have been previously reviewed as part of the digital equipment’s topical report safety evaluation. 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.

This draft is for presentation of the NRC staff’s current thinking. It has not been through the NRC’s review processes and remains subject to change.

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

D.2.3.3 System Requirements Documentation

D.2.3.3.1 Information To Be Provided

The licensee should submit a System Requirements Specification (SyRS) or other document with equivalent content. While the document may have a different title, the content should be consistent with the descriptions below. The SyRS is used to confirm that what is being designed is consistent with what is being reviewed in the LAR. The SyRS is a modification artifact and bounds the design.

For the Alternate Review Process, this section uses the definitions from the International Electrotechnical Commission (IEC) 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, to include (but not be limited by) the following:

a. defining 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
b. defining the plant layout for the modification scope
c. defining the operational context for the modification scope and changes required in the modification
d. structuring the overall I&C architecture and assigning I&C functions to the modification scope
e. identifying the required design criteria for the modification scope, including ensuring that features providing defense in depth in the existing system are not compromised and to minimize the potential for common-cause failure (CCF)
f. describing how the modification fits within the overall architecture of the plant’s I&C systems and any required changes to the architecture
g. defining system interfaces and the reasons for the interfaces (see Section D.2.5.1)

The SyRS should address the requirements that are specific to digital implementations. The licensee will ensure 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 requirements for digital equipment quality to comply with IEEE Std 603, Clause 5.3.

The SyRS should contain the 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:

a. Functionality, including input/output ranges and setpoints. For trip functions, the specification defines the margins between setpoints and allowable values (e.g., those including all applicable uncertainties)
b. Performance, including accuracy and response times. Where appropriate, performance requirements are defined for different initial plant conditions and design basis events
c. Appropriate signal filtering, signal validation, and interlocks should be specified to minimize the potential of spurious actions

The SyRS should specify boundaries and interfaces with other systems, including isolation requirements. Other boundary and interface information to be specified should include the following:

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

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

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

d. interfaces with the operator or maintenance technician

The SyRS should specify environmental conditions applicable to the system (see Section D.3). 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 to be specified should include the following:

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

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

c. power supply and heating and ventilation conditions

d. specify environmental qualification of hardware required based on design bases functions (For computer-based systems, this qualification addresses the hardware (including compliance with 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, Clause 5.4, and IEEE Std 603, 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 determine whether the SyRS is consistent with the material presented in the LAR. The intent of the review is 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 demonstrate the allocation of design and service/test functions (see Section D.2.2.1 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 describe, using text and drawings, 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 meets the assumptions of the accident analysis for the applicable modes of replacement system operation.

The LAR should describe the mapping of logic drawings (i.e., functions) to logic elements in the system. The LAR should demonstrate 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 meets the assumptions of the accident analysis for the applicable modes of replacement system operation.

Regulatory guidance for reviewing digital system real-time system architectures in I&C systems is contained in SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance."

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 the new licensing basis.

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

During this evaluation, the reviewer should consider IEEE Std 603, Clauses 5.1 and 5.6.

SRP Appendix 7.1-C provides acceptance criteria for IEEE Std 603 for those clauses applicable to this section. SRP Appendix 7.1-D provides acceptance criteria for IEEE Std 7-4.3.2 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, hardwired or data communication, whether 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:

a. input and output interfaces with the plant and plant sensor or actuators, whether hardwired or using some form of data communication, including requirements for any required isolation

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 requirements for any required isolation (including credited manual operator actions)

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 requirements for any required isolation

The LAR should identify and describe each of the following:

a. Support and auxiliary systems, normal power sources, emergency power sources, and heating, ventilation, and air conditioning (HVAC). The LAR should address 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.

b. Communication features from the NRC-approved topical report that are proposed for the replacement system.

c. How identified hazards are controlled in communication features.

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.

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

f. Features that affect the SOE (see Section D.8.1).

g. If multidivisional controls and displays are applied, the LAR should demonstrate that 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 to ensure that malfunctions in the interfaces minimize the potential for spurious actuation.

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 the required safety functions while power sources are bypassed for maintenance for compliance with IEEE Std 603, Clauses 8.1, 8.2, and 8.3.

The LAR should demonstrate how the communication features meet the criteria of IEEE Std 603, 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, 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 compliance with 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, Clause 5.13.

The LAR should describe the human-system interfaces to be provided, addressing 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, 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:

a. whether they are permanently installed or portable

b. whether they provide direct or indirect control of safety equipment (e.g., nonsafety-related workstations that interface with other safety-related workstations to control safety equipment)

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

Regarding the guidance in DI&C-ISG-04 that addresses communications features in safety 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:

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

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

The NRC reviewer should evaluate the following:

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

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

c. whether the LAR defines the connections between this system and any nonsafety systems with a rationale and set of requirements for each connection

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

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

f. whether the safety function and the SOE required for the safety system are compromised by any connection

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

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

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

i. whether the defined use of the hardwired interfaces is consistent with the previous system and with any changes documented and the rationale for the change discussed

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 features that affect the SOE are mentioned here, Section D.8 presents guidance for their review.

The reviewer should evaluate how the communication features meet the criteria of IEEE Std 603, 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, Clause 5.6, and how they 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 function of each hardwired connection is described, 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 function of each data communication connection is described, 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 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 provides appropriate isolation by describing the electrical connections in sufficient detail to define the electrical division assigned to the connection, where cross-divisional signals change electrical divisions through isolation, 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 nonsafety systems provide anticipatory trip signals to safety systems.

The reviewer should evaluate whether those portions of the design associated with multi-unit stations comply with IEEE Std 603, 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, Clause 5.14.

The reviewer should evaluate whether each applicable clause in DI&C-ISG-04 has been addressed in sufficient detail, or whether the proposed alternatives address the underlying hazard. The LAR should provide an explanation, but not a detailed evaluation, for why criteria do not apply, to enable the reviewer to forego the associated reviews. The proposed alternative is assessed against the following regulatory requirements and guidance:

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

b. IEEE Std 7-4.3.2, as endorsed by RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” provides guidance on how digital systems can meet the independence requirement in IEEE Std 603, Clause 5.6.

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 systems or between safety and nonsafety systems.

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

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

The reviewer should evaluate whether the LAR addresses compliance with the guidance in IEEE Std 603, Clause 5.12, "Auxiliary Features," and in IEEE Std 7-4.3.2 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 guidance in IEEE Std 603, Clauses 8.1, 8.2, and 8.3.

If separate priority logic modules are provided, the reviewer should evaluate whether the LAR describes the compliance with the guidance in Section 2 of DI&C-ISG-04 and in Sections 1 and 3 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 conformance with the guidance in DI&C-ISG-04, Section 2.

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

D.2.6 Fundamental Design Principles in the New Architecture

This section addresses how the new architecture reflects the fundamental design principles.

D.2.6.1 Information To Be Provided

In accordance with Section D.2.2.1, the LAR should include a description of 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 subsections below (i.e., redundancy, independence, deterministic behavior, defense in depth and diversity (D3), and simplicity). Additional information needed to support a particular subsection is described in that subsection.

D.2.6.2 Evaluation

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

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

D.2.6.2.1 Redundancy

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

D.2.6.2.1.1 Information To Be Provided

The licensee should demonstrate the use and application of redundancy in the new architecture.

The licensee should demonstrate, by implementing an FMEA, that the use and application of redundancy in the new architecture ensure 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 licensee should demonstrate that the use and application of redundancy in the new architecture supports the associated TS (e.g., limiting conditions for operation (LCOs), action statements, and surveillance requirements). 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 when applying the associated guidance of IEEE Std 7-4.3.2:

a. Clause 5.1, "Single-Failure Criterion"
b. Clause 5.15, "Reliability"
c. Clause 6.7, "Maintenance Bypass"
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 Nuclear Power Plant Protection 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:

a. GDC 21, "Protection System Reliability and Testability"
b. GDC 24, "Separation of Protection and Control Systems"

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

D.2.6.2.2 Independence

Independence ensures that hazards are not propagated across independent domains.

D.2.6.2.2.1 Information To Be Provided

The licensee should demonstrate the use and application of physical, electrical, and functional independence in the new architecture. Section D.2.5 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 when applying the associated guidance of IEEE Std 7-4.3.2:

a. Clause 5.6, Independence
b. Clause 5.11, Identification
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 systems do not depend on information from other independent portions of the safety system. (Coincidence voting is permitted to depend on information from other independent portions of the safety system.) The reviewer should evaluate whether the use and application of independence in the new architecture meet the following GDC:

a. GDC 13, “Instrumentation and Control”
b. GDC 21, “Protection System Reliability and Testability”
c. GDC 22, “Protection System Independence”
d. GDC 23, “Protection System Failure Modes”
e. GDC 24, “Separation of Protection and Control Systems”

D.2.6.2.3 Deterministic Behavior

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

D.2.6.2.3.1 Information To Be Provided

The licensee should demonstrate the use and application of deterministic behavior in the new architecture.

This draft is for presentation of the NRC staff’s current thinking. It has not been through the NRC’s review processes and remains subject to change.

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 when applying the associated guidance of IEEE Std 7-4.3.2 (as applicable):

a. Clause 5.2, Completion of Protective Action
b. Clause 5.5, System Integrity
c. Clause 6.1, Automatic Control
d. Clause 6.2, Manual Control
e. Clause 7.1, Automatic Control
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:

a. GDC 13, "Instrumentation and Control"
b. GDC 21, "Protection System Reliability and Testability"
c. GDC 23, "Protection System Failure Modes"
d. GDC 29, "Protection Against Anticipated Operational Occurrences"

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

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

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 timely completion of credited actions.

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

a. System timing requirements derived from the analyses of design-basis events are satisfied by the replacement system architecture.

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.

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

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

a. The system design and architecture information specify the use of the platform's standard data communications.

b. The deterministic behavior of these communications has already been reviewed and approved by the NRC as part of the topical report.

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

Compliance with any restrictions on the platform communications should be reviewed to confirm compliance with the NRC-approved topical report safety evaluation. The review should evaluate whether the response time requirements can be met using the standard platform communications.

D.2.6.2.4 Defense in Depth and Diversity

Defense in depth and diversity are methods that can be used to protect against CCFs.

D.2.6.2.4.1 Information To Be Provided

The licensee should demonstrate, via a D3 evaluation, that the use and application of D3 in the new architecture ensure that the safety functions can be achieved 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 D3 evaluation 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 meet 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

This principle is more subjective than the others; therefore, rather than attempting to evaluate the adequacy of the modified system design’s simplicity on some absolute basis, 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 licensee should demonstrate the use and application of simplicity in the new architecture, focusing on the resultant simplicity (or lack thereof) of design decisions that affect redundancy, independence, deterministic behavior, and D3.

The licensee should demonstrate, for design decisions resulting in more complex approaches than might otherwise have been chosen, that the benefit(s) obtained, particularly with respect to the fundamental design principles, justify the reduction in simplicity. Design decisions involving

This draft is for presentation of the NRC staff’s current thinking. It has not been through the NRC’s review processes and remains subject to change.

such tradeoffs may be driven by the need to satisfy a regulatory requirement (e.g., surveillance testing, improved maintainability and/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 fundamental design principles, justifies the reduction in simplicity.

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

D.3 Hardware Equipment Qualification

D.3.1 Information To Be Provided

The licensee should demonstrate that the system meets or exceeds the design-basis requirements for the site location in which the equipment will be installed. The licensee should include 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 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 test requirements. The LAR should describe and justify any discrepancies between equipment qualification test limits and plant requirements.

In those cases where the hardware qualification has previously been demonstrated by the vendor and evaluated by the NRC staff, the licensee should reference 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 within the specified environment. This includes both the normal operating conditions and the worst conditions expected during abnormal and accident conditions in which the equipment is expected to perform its safety function.

The following provide regulatory criteria for environmental qualifications of safety-related equipment:

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, Clause 5.4

c. RG 1.152, which endorses IEEE Std 7-4.3.2, Clause 5.4

d. 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

e. RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems”

If any portions of this equipment will be subject to harsh environment, then additional disciplines should be involved 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 Power Plants,” to ensure that the requirements for equipment qualification to harsh environments are met.

D.4 I&C System Development Processes

D.4.1 Information To Be Provided

The licensee should describe the proposed framework being used to design and develop I&C safety 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 I&C safety systems. Development documents expected to be available during the LAR review should be identified in the pre-application meetings.

The framework should describe the following system development process activities:

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

b. Translate these concepts into system requirements.

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

d. Implement the design into hardware and software functions.

e. Integrate system elements such as software and hardware.

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

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

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

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

The licensee should demonstrate that the software life-cycle process follows guidance in RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” or, alternately, describe how the regulatory requirements referenced in RG 1.173 are satisfied. Demonstration that the software life-cycle process follows the guidance consists of the following:

a. description of the software life-cycle processes to be used
b. identification of any planned exceptions and clarifications
c. description of how these planned exceptions and clarifications meet the underlying regulations

For any RGs referenced, the licensee should demonstrate how the RG-specific activity follows the guidance of the RG or, alternately, describe how the underlying regulatory requirements referenced in the RG are satisfied. Demonstration for RG-specific activity consists of the following:

a. description of the RG-specific activity
b. identification of any planned exceptions and clarifications
c. description of how these planned exceptions and clarifications meet the underlying regulations

The licensee should identify which of the development activities are 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 have not been previously reviewed and approved by the NRC). The licensee should also address the applicable plant-specific action items (PSAIs) defined in the referenced topical reports (see Section D.5).

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 I&C safety system.

The activities, including relevant PSAIs, that are part of the development process defined for NRC-approved DI&C platform activities should be credited to the degree allowed by the platform safety evaluation. The LAR review should focus on the application-specific software development activities not previously reviewed and approved by the NRC. 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.4.2.1.1 through D.4.2.1.9 describe the criteria against which the NRC reviewer should evaluate the I&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 during the LAR review for the Alternate Review Process. Sections D.4.2.1.5 through D.4.2.1.9 are process evaluations that are part of the NRC review scope during the LAR review for the Alternate

Review Process. The licensee is responsible for ensuring vendor use of procedures and 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 if the LAR describes input information, life-cycle activities, and output information necessary to develop I&C safety 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 I&C safety 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 contains a description of life-cycle activities and tasks, including inputs and outputs that will be implemented in the development of the proposed I&C safety 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 below.

Based on the agreement reached during the pre-application (Phase 0) meeting, 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 review procedure in SRP BTP 7-14, Section B.4, should be applied to the extent the design documents are available during the LAR review.

D.4.2.1.1 Plant and I&C System Safety Analysis

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

a. To meet Clause 4 of IEEE Std 603, 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 I&C system modification and justify the acceptability of the changes to the plant design basis (see Section D.2).

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 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 I&C System Requirements

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

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

b. All identified system requirements 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 I&C system requirements).

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

D.4.2.1.3 I&C System Architecture

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

a. An I&C system architecture should be developed on the basis of a defined methodology that provides all necessary I&C functions needed to ensure safe plant operation. It should include the technical elements described in Section D.2.

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

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

D.4.2.1.4 I&C System Design

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

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

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

c. I&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 I&C system safety analyses. I&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 I&C system design should be analyzed, reviewed, approved, baselined, updated as necessary, and placed under CM.

e. The I&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 I&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 system requirements allocated to software should be identified. 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.

   Demonstration for the software requirement specification development will 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 others.
   - Design constraints imposed on an implementation—Describe any required standards in effect, implementation language, policies for database integrity, resource limits, operating environment(s), etc.

   Ranking requirements for importance or stability for safety systems is not mandatory. The reviews of the software requirements development process should focus on activities not previously reviewed and approved by the NRC unless there are safety-significant changes in the NRC acceptance criteria.

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, I&C system architecture, and system requirements.

- The 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 I&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 I&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 regulatory guides for the technical review of software designs. The reviewer should use the review guidance in items (b) through (j) below for evaluating 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 be developed and define 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 components, modules, and units will be refined into lower levels, including software modules to allow coding, compiling, and testing; and the division of the software into a set of interacting components, modules, and units, including the description of those components, modules, and units, defining their interfaces and dependencies in a structured fashion.

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

e. The relationship between component(s), and software module(s), and software unit(s) should be established.

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 I&C system. In those instances, unless otherwise demonstrated as part of the platform qualification, the licensee should identify those unused capabilities, evaluate whether those functions may affect 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, 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.

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

i. The 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 for testing software components, modules, and units and the 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 maintained. The applicable review principles for software unit testing activities can be found in SRP BTP 7-14, Section B.3.2.4, and should be applied to the description of the test process and controls for the Alternate Review Process LAR review. Demonstration for the software implementation process consists of the following:

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

   The software unit testing process reviews should focus on activities not previously reviewed and approved by the NRC unless there are safety-significant changes in the NRC acceptance criteria.

   The reviewer should evaluate whether the software implementation process description demonstrates that the software life-cycle process meets the guidance of 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.

This draft is for presentation of the NRC staff’s current thinking. It has not been through the NRC’s review processes and remains subject to change.

g. Demonstration for the development of software test documentation consists 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 not previously reviewed and approved by the NRC unless there are safety-significant changes in the NRC acceptance criteria.

   The reviewer should evaluate whether the software implementation process description demonstrates that the 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, I&C system architecture, and system requirements.

j. The 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 fulfill the design documentation. Applicable review guidance for code listings can be found in SRP BTP 7-14, Section B.3.3.4.3, and 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. The review principles for the software integration process can be found in SRP BTP 7-14, Section B.3.1.4.4, which may need to be adapted to 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. Applicable review guidance for documenting these activities can be found in SRP BTP 7-14, Section B.3.3.5.3, 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. The applicable review guidance for this activity is contained in SRP BTP 7-14, Section B.3.2.4, 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, I&C system architecture, and I&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 I&C System Testing

The reviewer should evaluate whether the I&C system testing process description 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 I&C system, consistent with the architectural design. The independent V&V team should develop the V&V test plans. The applicable review guidance for the system V&V test plans is found in SRP BTP 7-14, Section B.3.1.12.4.

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 I&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 I&C system requirements have been satisfied. Applicable review guidance for documenting test results is found in SRP BTP 7-14, Section B.3.2.4, 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 I&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 I&C safety 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 be used to inform the review of the software management process description.

Use of NUREG/CR-6463, "Review Guidelines for 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 using tool-based methods of modern DI&C platforms and will apply only to the software coding languages used in the system development.

When the reviewer evaluates the LAR description of the organizational and project management processes, the reviewer 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, with additional guidance on software-related project risk activities of IEEE Std 7-4.3.2, Clause 5.3.6

e. establishment of quality metrics throughout the life cycle to assess whether the quality requirements of IEEE Std 603, Clause 5.3, are being met, with additional guidance from IEEE Std 7-4.3.2, Clause 5.3

f. adequate control of software tools to support system development and software V&V processes, with additional guidance in IEEE Std 7-4.3.2, 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 there are safety-significant changes in the NRC acceptance criteria.

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 quality assurance processes. SRP BTP 7-14, Section B.3.1.3.4, can inform the review of the software quality assurance process description to the extent practicable for an Alternate Review Process LAR review. The process used to develop the DI&C safety 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 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 requirements for systematic software reviews, it does not establish the need to conduct specific reviews. Demonstration for the 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 there are safety-significant changes in the NRC acceptance criteria.

D.4.2.4 Software Verification and Validation Processes

The reviewer should evaluate the LAR description of the software V&V processes. The applicable review guidance for software V&V processes is found in IEEE Std 1012, as endorsed by RG 1.168. The IEEE standard and RG 1.168 are referenced in SRP BTP 7-14, Sections B.3.1.10 and B.3.2.2. To the extent practicable, the IEEE standard and regulatory guide 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, alternately, describe how the regulatory requirements referenced in RG 1.168 are satisfied. Demonstration for the software V&V processes will address the following:

a. V&V organization responsibilities

b. V&V processes, activities, and tasks

c. V&V reporting requirements

d. V&V administrative controls for anomaly resolution and reporting, task iteration policy, and deviation policy

e. V&V test documentation requirements

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 for 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 there are safety-significant changes in the NRC acceptance criteria.

D.4.2.5 Software Configuration Management Processes

The reviewer should evaluate the LAR description of the software CM processes. The applicable review guidance for software CM processes can be found in IEEE Std 828, as endorsed by RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” SRP BTP 7-14, Sections B.3.1.11.4 and B.3.2.3, reference the IEEE standard and RG 1.169. To the extent practicable, reviewers should use the IEEE standard and the RG to inform their review of the software CM process description for the Alternate Review Process LAR review. RG 1.152 endorses IEEE Std 7-4.3.2, subject to the positions and modifications identified in the regulatory guide. IEEE Std 7-4.3.2, Clause 5.3.5, provides guidance on software CM.

The reviewer should evaluate whether the software CM processes follow the guidance in RG 1.169 or, alternately, describe how the regulatory requirements referenced in RG 1.169 are satisfied. Demonstration for the software CM processes will address the following:

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

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

The NRC review of software CM process controls should focus on the application-specific software development activities rather than the platform development process defined in an NRC-approved DI&C platform unless there are safety-significant changes in the NRC acceptance criteria.

This draft is for presentation of the NRC staff’s current thinking. It has not been through the NRC’s review processes and remains subject to change.

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

This section describes how the NRC staff should assess a referenced NRC-approved I&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. Section D.5 is not applicable if there is no 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 intent 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 original NRC-approved topical report safety evaluation, the LAR should provide information that supports review of these changes during the safety evaluation. Where appropriate, the LAR should cross-reference any NRC-approved documents to the items listed in Enclosure B. The LAR should state whether the cited document has changed since the last NRC review. For documents, including system, hardware, and software descriptions that have changes affecting the conclusions of the safety evaluation, the licensee should submit, on the docket, a report describing the changes. If the changes are minor, the licensee can choose to include a description of the change in the LAR. 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 titled "Plant-Specific Action Items" or "Application-Specific Action Items" or a similar title. These are open items that the licensee is expected to 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 licensee should describe 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 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, this is to be interpreted as the role of the licensee in accordance with the licensee's QA program and vendor oversight plan.

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

For PSAIs that are addressed in the LAR and implemented by the licensee subsequent to issuance of the license amendment, a license condition should be established to resolve these PSAIs before system operation or as established in the license condition.

The LAR should evaluate PSAIs involving planning documents against the regulatory guidance in Section D.4 or include a description of 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 intended use 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 a previous 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. Any PSAI that involves planning documents should be reviewed against the regulatory guidance in Section D.4 or covered by licensee processes or programs.

D.6 Compliance Matrix for IEEE Standards 603 and 7-4.3.2

This section contains an example of the compliance matrix the licensee should provide. This example matrix provides a row for each clause in IEEE Std 603 and in IEEE Std 7-4.3.2. Extended clauses are provided if needed to point to different LAR sections. The table also provides titles from the standards, defining the clause.

In the appropriate "Compliance" column cell, each row should state 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 is achieved
b. why partial compliance is acceptable and why full compliance is not required
c. why the alternative exception proposed is acceptable
d. why the clause does not apply

For the example provided in Table D.1, IEEE Std 7-4.3.2 does not provide any additional guidance for Clause 4 requirements in IEEE Std 603. However, IEEE Std 7-4.3.2 defines several extended clauses under Clause 5.3. For both examples, each cell in "Compliance" and

"LAR Section" would be completed, and the LAR should discuss the methods to be used to meet IEEE Std 603 when applying the associated guidance of IEEE Std 7-4.3.2.

The "DI&C-ISG-06 Section" column refers to the potential topic where the subject clause is discussed. The section or sections depend on the review process (i.e., Alternate Review Process or Tiers 1, 2, or 3).

Clauses under IEEE Std 7-4.3.2 that are marked with an asterisk (*) indicate that the standard does not add anything beyond IEEE Std 603.

Table D.1 IEEE Standards 603 and 7-4.3.2 Compliance Table

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance	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.9.9
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.9.9
4.6					D.2.3.1
4.7					D.2.3.1, D.9.9
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.4, D.9.9
	5.3.1	Software Development			D.4
	5.3.1.1	Software Quality Metrics			D.4

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance	LAR Section	DI&C-ISG-06 Section
	5.3.2	Software Tools			D.4
	5.3.3	Verification and Validation			D.4, D.9.6
	5.3.4	Independent V&V (IV&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, D.9.9
	5.4.1	Computer System Testing			D.3.1, D.9.9
	5.4.2	Qualification of Existing Commercial Computers			D.9.9, D.9.10
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.8, D.9.1, D.9.2,

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance	LAR Section	DI&C-ISG-06 Section
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
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.2.5.2
5.13	5.13*	Multi-Unit Stations			D.2.5.1
5.14	5.14*	Human Factors Considerations			D.2.5.1
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.2.6.5
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

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance	LAR Section	DI&C-ISG-06 Section
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.

D.7 Technical Specifications

D.7.1 Information To Be Provided

The LAR should provide proposed TS changes that demonstrate compliance with 10 CFR 50.36, "Technical Specifications." This includes proposed changes to instrument setpoints included in the TS.

Self-diagnostics in digital equipment can be used in some cases as an alternate means of accomplishing some surveillance requirements (SRs), or justifying less frequent manual surveillance and calibration. Performance of channel checks, channel calibrations, etc., may no longer be necessary if the digital equipment's internal self-test and self-diagnostic functions can be credited. The SRs necessary to ensure the operability of the system and its components should be reflected in the proposed TSs. Any extension, modification, or deletion of TS should be documented and justified by the licensee.

In addition to a markup copy of the TS, the licensee should justify 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 provide for maintaining safe operation of the facility with respect to its associated functions.

D.7.2 Evaluation

D.7.2.1 Technical Specifications

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

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

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, in combination with manual testing and external cross-checks, are sufficient to support existing TS and any proposed TS changes. This evaluation should include consistency between the TS and the self-tests and self-diagnostics implemented in the architecture (see Section D.2.2.1) for new system functions (see Section D.2.3.1) and to address system interfaces (Section D.2.5.1). This evaluation should also include consistency between the TS and the TS assumptions regarding redundancy (Section D.2.6.2.1.1).

Reviewers evaluate TS LCOs being proposed for deletion against the four 10 CFR 50.36(c)(2)(ii) criteria 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 being proposed for addition should adequately define the lowest functional capability or performance levels of the system required for safe operation of the facility. This review includes the adequacy of the proposed LCOs and the potential need for additional LCOs that have not been proposed for addition to the 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, Clause 6.8, in consideration of the uncertainties between the process analytical limit documented in Clause 4.4. The setpoint should be determined using a documented methodology.

Additional guidance on the establishment of instrument setpoints can be found in RG 1.105, “Setpoints for Safety-Related Instrumentation,” and Regulatory Issue Summary (RIS) 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. SRP BTP 7-3, “Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service,” provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

The information provided should sufficiently describe the hardware and software so that the NRC staff is able to conclude that IEEE Std 603, Clause 6.8, has been met.

D.8 Secure Development and Operational Environment

D.8.1 Information To Be Provided

The LAR should demonstrate the proposed DI&C system is adequately robust to perform its safety function within its design-basis, normal, and adverse environments.

For Tiers 1, 2, and 3, 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) for the SOE controls

The following information should be provided in support of the secure environment. The staff recognizes that different organizations may have a different name for the same document. In addition, some licensees may address certain documentation needs in another software-related document. While including the secure environment criteria in another document is acceptable, licensees are urged to devote a separate section of the LAR to issues concerning a secure environment and to include a roadmap to these issues in the application.

The licensee should perform a vulnerability assessment identifying the vulnerabilities that could affect the secure development and reliable and secure operation of the digital safety system. RG 1.152, Section B, page 5, presents a discussion of 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 vulnerability assessment should be available for review by the NRC staff.

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 review by the NRC staff. 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 review by the NRC staff.

D.8.2 Evaluation

The reviewer should determine whether the LAR demonstrates compliance with RG 1.152, Regulatory Position 2, for the SDOE of the system under review. For Tier 1 and the Alternate Review Process, the review is limited to the application software and hardware.

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

a. was (or will be, in the case of the Alternate Review Process) designed, 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 LAR review does not need to evaluate the adequacy of cyber security features for compliance with 10 CFR 73.54.

D.9 Sections Applicable to 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. This guidance is intended to be applied to Tier 1, 2, and 3 reviews as needed. Because Alternate Review Process evaluations are to be completed before completion of late-stage product development activities, the documentation necessary to perform the evaluations covered in this section are not expected to be available to the NRC reviewer before issuance of a 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). This section contains SRP references to applicable guidance:

a. Regulatory Guide 1.172
b. IEEE Std 830, "IEEE Recommended Practice for Software Requirements Specifications," which describes an acceptable approach for preparing an SRSs for safety system software
c. NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," issued June 11, 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 system to be addressed in the software design.

D.9.1.2 Evaluation

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

Two SRSs may require review, one for the platform software and another for the applications software. Each of these may be reviewed separately.

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

The NRC staff should review the SRS using 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. The

NRC staff should expect to find sufficient V&V documentation to show that there was a 100-percent V&V of the software criteria by the V&V organization.

D.9.2 Software Design Specification

D.9.2.1 Information To Be Provided

Review (Phase 1): Software Design Specification

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

The engineer 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 software specifications are to be implemented. The SDS should also be traceable to software implementation code or function block diagrams.

D.9.2.2 Evaluation

The NRC staff should review 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 there was a 100-percent V&V of the software design specifications by the V&V organization.

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 if the safety conclusions reached by a previous review remain valid. Completion of this review could result in an update to the platform safety evaluation if the changes affect the platform’s safety evaluation conclusions.

If the platform vendor has a platform change review process, the NRC staff should review the results of that process and determine if the staff concurs with the conclusions relative to the NRC-approved topical report impact.

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

RG 1.168 endorses IEEE Std 1012 as providing methods acceptable to the staff for meeting the regulatory requirements as they apply to an SSA, subject to the exceptions listed in the regulatory positions.

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, contains this SRP reference to applicable guidance: RG 1.169 endorses IEEE Std 828, subject to specific provisions identified in the RG, as providing guidance that is acceptable for carrying out software CM.

D.9.5.2 Evaluation

The LAR should present 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, contains SRP references to applicable guidance:

a. In RG 1.168, Sections 7.2, “Regression Analysis and Testing,” and 7.4, “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 Verification and Validation 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 requires that the safety systems be designed such that the system can accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," provides review criteria for system integrity.

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

D.9.7.2 Evaluation

Evaluation of computer system hardware integrity should be included in the evaluation against IEEE Std 603. 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 system equipment components and the system racks and panels as a whole to demonstrate that the safety system performance is adequate to ensure completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment. The 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 if adequate testing and analysis have been performed on the system as a whole and its components.

The review of system integrity should determine if the design provides for safety systems to fail in a safe state, or into a state that has been demonstrated to be acceptable on some other defined basis, if conditions such as disconnection of the system, loss of energy, or adverse environments are experienced. This aspect is typically evaluated through evaluation of the licensee's failure modes and effects analysis.

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 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 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 system signals) should be in accordance with appropriate plant procedures.

D.9.9 Equipment Environmental Qualifications

D.9.9.1 Information To Be Provided

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

Review (Phase 2): (1) Qualification Test Methodologies

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

The licensee's submittal should provide sufficient documentation to support the assertion that a proposed DI&C system is adequately robust to perform its safety function within its design basis for normal and adverse environments. This information should be found in the equipment qualifications test plans, methodologies, and test reports. The summary should document the results of the qualification testing. Section D.9.10 elaborates on the information necessary to address the various aspects of environmental qualification.

RG 1.152, which endorses IEEE Std 7-4.3.2, with a few noted exceptions, identifies an acceptable method for addressing computer system qualification testing (see IEEE Std 7-4.3.2 Clause 5.4.1, “Computer System Testing,” and Section D.10.4.2.4.1).

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

D.9.9.2 Evaluation

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 expected extremes of temperature, humidity, radiation, electromagnetic and radio interference, and seismic input. While testing against all of these stressors, the system should be functioning with 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. However, if significant aging mechanisms are identified, the qualification program should address them. An aging mechanism is significant if, in the normal or abnormal service environments, it causes degradation during the installed life of the system that progressively and appreciably renders the equipment vulnerable to failure. Such mechanisms may be addressed by testing (e.g., preconditioning before testing), operating experience, or surveillance and maintenance. Where feasible, the preconditioning and surveillance and maintenance assessments should be based on quantifiable acceptance criteria. If the system has one or more significant aging mechanisms, preconditioning is necessary before testing to the degree that the mechanism is not accounted for by surveillances and maintenance. For example, if an aging mechanism exists and there is a surveillance performed to quantify the progress of the aging mechanism, the system should be preconditioned to account for the acceptance criteria of the surveillance plus the expected aging until the next performance of the surveillance.

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

D.9.10 Qualification of Commercial Computers

D.9.10.1 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 presents the fundamental criteria for demonstrating that a commercial computer will perform its intended safety functions. Additional guidance is provided in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," issued October 1996, as accepted 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 for Safety-Related Applications in Nuclear Power Plants," issued December 1996, as accepted 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 licensee should show 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 comply with the criteria of Clause 5.4.2 of IEEE Std 7-4.3.2. The guidance of SRP BTP 7-14 may be applied 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 (PLCs).

D.9.10.2 Evaluation

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

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 item being dedicated is equivalent to equipment developed under a 10 CFR Part 50, Appendix B, program.

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

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

D.9.11 Hardware Development Process

D.9.11.1 Information To Be Provided

Review (Phase 1): Hardware Development Process

The licensee should demonstrate 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 used 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 with the criteria of IEEE Std 603, Clause 5.3 “Quality.”

Where the hardware development process and quality control methods used have previously been described by the vendor and evaluated by the NRC staff, the licensee should refer to that description and evaluation. The licensee should identify and justify deviations from previously reviewed and approved processes or methods and revision changes since NRC approval.

D.9.11.2 Evaluation

The reviewer should evaluate the licensee information on the hardware development process to determine whether the licensee satisfies the following criteria:

a. 10 CFR 50.54(jj) and 10 CFR 50.55(i) require that structures, systems, and components 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) incorporates, based on the date the construction permit was issued, either IEEE Std 279, Clause 4.3, or IEEE Std 603, Clause 5.3.

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

d. RG 1.164, “Dedication of Commercial-Grade Items for Use in Nuclear Power Plants.”

Enclosure A—Sample Summary of Initial Public Meeting To Discuss Plans To Request NRC Approval in Support of a Digital I&C 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 I&C 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 upgrading the [PLANT] [SYSTEM] to the [PLATFORM] digital instrumentation and control (I&C) system.

The purpose of this meeting was to discuss the initial design concepts and any site-specific issues identified by [LICENSEE]. These discussions focused on how the [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 criteria in [REVIEW AREA].

– Item 1
– Item 2…

The NRC staff provided feedback to [LICENSEE] noting that the following aspects of the design seemed conducive to finding the proposed plant modification consistent with the NRC staff's position on [REVIEW AREA]:

– Item 1
– Item 2…

Review areas to be discussed may include the following:

- relevant precedents for similar systems in other plants
- communications interfaces
- secure development and operating environment

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

- 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 determination of the 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, 3 or Alternate Review Process] guidance. Based on this determination, the licensee is expected to prepare its license amendment request (LAR) in accordance with [TIER LEVEL] guidance provided in this interim staff guidance.

[For Tier 1, 2, or 3 submittals for Phase 1, 2, and 3 only] 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 Tier 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.] [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 concerning the documentation submittal schedule.]

The NRC staff identified the following aspects of the design as needing additional review before finding the proposed modification fully consistent with the NRC staff's position on defense in depth and diversity:

– Item 1
– Item 2…

Concurrence for this memorandum shall include the Chief, Instrumentation & Controls Branch, the Chief, Plant Licensing Branch X-X, and any other Branch Chiefs whose review authorities may have been discussed.

Enclosure B—Information Provided in Support of a License Amendment Request for a Digital I&C Modification

The list of information to be submitted represents a typical system modification. Specific system modifications may require different information to support the U.S. Nuclear Regulatory Commission's (NRC's) evaluation against the applicable acceptance criteria, depending on the scope and complexity of the 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.

		Tier			**Plant-Specific Information Submitted with License Amendment Request (Phase 1 for Tier 1, Tier 2, Tier 3)**
	A R	1	2	3	
1.1	X				**System Architecture** (see D.2)
1.2	X				**(Summary of) Application Software Planning and Processes** (see D.4)
1.3	X				**(Summary of) Hardware Equipment Qualification** (see D.3)
1.4	X	X	X		**Approved Topical Report Safety Evaluation** (see D.5)
1.5	X	X	X	X	**System Description** (see D.1)
1.6	X	X	X	X	**(Unified Compliance Matrix for) IEEE Stds 603 and 7-4.3.2** (see D.6)
1.7	X	X	X	X	**(Changes to) Technical Specifications** (see D.7)
1.8	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
1.9	X	X	X	X	**Secure Development and Operational Environment** (see D.8)
1.10		X	X	X	**Software Requirements Specification** (see D.9.1)
1.11		X	X	X	**Software Design Specification** (see D.9.2)
1.12		X	X	X	**Design Analysis Reports for Platform Changes** (see D.9.3)
1.13		X	X	X	**System Response Time Analysis Report** (see D.9.7)
1.14			X	X	**Design Report on Computer integrity, Test and Calibration, and Fault Detection** (see D.9.7)
1.15				X	**Commercial-Grade Dedication Plan** (see D.9.10)

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.

		Tier			**Plant-Specific Information Submitted with License Amendment Request**
	A R	1	2	3	**(Phase 1 for Tier 1, Tier 2, Tier 3)**
1.16				X	**Quality Assurance Plan for Hardware** (see D.9.11)
1.17				X	**Equipment Qualification Testing Plans (Including Electromagnetic Interference, Temperature, Humidity, and Seismic)** (see D.9.9)
1.18				X	**(Summary of) Hardware Development Process** (see D.9.11)

	Tier			**Phase 2 – Submitted before Requested Approval (Tier 1, Tier 2, Tier 3 only)**
	1	2	3	Note: This table does not apply to Alternate Review Process applications.
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 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.9.9)
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.9.9)
2.10			X	**Commercial-Grade Dedication Report(s)** (see D.9.10)

Enclosure C—Sample Safety Evaluation Contents for a Digital I&C License Amendment

This draft is for presentation of the NRC staff's current thinking. It has not been through the NRC's review processes and remains subject to change.