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

June 18, 2009

MEMORANDUM TO: Lois M. James, Chief
Plant Licensing Branch III-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

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

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

DATES & TIMES: Tuesday, June 30, 2009
1:00 p.m. - 4:00 p.m.
and
Wednesday, July 1, 2009
8:00 a.m. - 11:00 a.m.

LOCATIONS: Tuesday - June 30, 2009
U.S. Nuclear Regulatory Commission
One White Flint North, Room 3-B4
11555 Rockville Pike
Rockville, MD 20852

Wednesday – July 1, 2009
U.S. Nuclear Regulatory Commission
One White Flint North, Room 3-B6
11555 Rockville Pike
Rockville, MD 20852

PURPOSE: The Nuclear Regulatory Commission (NRC) staff is convening this meeting with the Nuclear Energy Institute (NEI) to discuss the development of interim staff guidance on the licensing of digital I&C safety systems for operating nuclear plants. The discussion will focus on the list of draft review areas and inter channel communication. Copies of these documents are enclosed with this notice.

CATEGORY 2:* This is a Category 2 public meeting. The public is invited to participate in this meeting by providing comments and asking questions at a designated point during the meeting. There may be limited space at the meeting

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

location, and interested members of the public are encouraged to participate in this meeting via a toll-free teleconference. For details, please email the NRC meeting contact by Thursday, June 25, 2009.

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

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

NRC	Industry
W. Kemper, NRR	G. Clefton, NEI
L. James, NRR	M. Schoppman, NEI
E. Miller, NRR	

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

Project No. 689

Enclosures:
1. Agenda
2. Draft Interim Staff Guidance 6

cc w/encl: See next page

cc:

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

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

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

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

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

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

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

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

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

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

AGENDA

FORTHCOMING PUBLIC MEETING

DIGITAL INSTRUMENTATION AND CONTROL (I&C) TASK WORKING GROUP NO. 6

DEVELOPMENT OF LICENSING PROCESS GUIDANCE

June 30, 2009, 1:00 p.m. - 4:00 p.m.

July 1, 2009, 8:00 a.m. - 11:00 a.m.

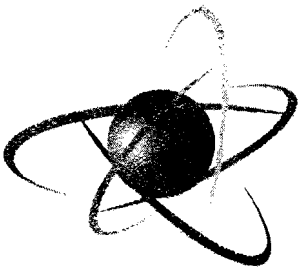
June 30, 2009 – One White Flint North, Room 3-B4

1:00 p.m. - 1:15 p.m.	Introduction of Participants and Opening Remarks
1:15 p.m. - 2:15 p.m.	Discussion of IEEE 603 Compliance Review Area
2:15 p.m. - 2:30 p.m.	Break
2:30 p.m. - 3:30 p.m.	NEI Presentation and Continuation of Discussion
3:30p.m. - 3:45 p.m.	Summary of Action Items
3:45 p.m. - 4:00 p.m.	Public Comments

July 1, 2009 – One White Flint North, Room 3-B6

8:00 a.m. - 8:15 a.m.	Introduction and Summary of Previous day
8:15 a.m. - 9:15 a.m.	Discussion of Other Review Area
9:15 a.m. - 9:30 a.m.	Break
9:30 a.m. - 10:30 a.m.	Continuation of Discussion and Discussion of Comment Matrix
10:30 a.m. - 10:45 a.m.	Summary of Action Items
10:45 a.m. - 11:00 a.m.	Public Comments

Enclosure 1



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-06

Task Working Group #6: Licensing Process

Interim Staff Guidance

(Initial Issue for Use)

Enclosure 2

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-06

Task Working Group #6: Licensing Process

Interim Staff Guidance

(Initial Issue for Use)

A. INTRODUCTION

This Interim Staff Guidance (ISG) provides the licensing process to be used in the review of digital I&C (I&C) system modifications in operating plants. This guidance is consistent with current NRC policy on digital I&C systems and is not intended to be a substitute for Nuclear Regulatory Commission (NRC) regulations, but to clarify how a licensee or applicant may efficiently request NRC approval to install a digital I&C system upgrade.

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

B. PURPOSE

The purpose of this ISG is to provide guidance for the NRC staff's review of digital I&C systems in accordance with current licensing processes. This ISG also informs licensees of the information and documentation the NRC staff will need for its review of LARs for digital I&C upgrades and when the information should be provided. Review of this document should allow licensees to prepare digital I&C upgrade applications that are complete with respect to the areas that are within the NRC staff's scope of review.

Use of this ISG is designed to be complementary to the NRC's longstanding topical report review and approval process. Where a licensee references an NRC-approved topical report, the NRC staff will be able to, where appropriate, limit its review to confirming the application of the digital I&C upgrade falls within the envelope of the topical report approval. Additionally, this ISG was developed based upon, and is designed to work in concert with, existing guidance. Where appropriate, this ISG references other guidance documents and provides their context with respect to the digital I&C licensing process for operating reactors.

The NRC staff will review proposed digital I&C upgrades against the design basis of the plant and the guidance in the Standard Review Plan (NUREG-0800), Chapter 7, and other associated guidance including ISGs. Licensees should provide a discussion of the

licensing basis for the plant, focusing these efforts on areas where the licensing basis differs from current guidance. Additionally, licensees should clearly identify those parts of the licensing basis they are updating as a result of the proposed change.

C. DIGITAL I&C REVIEW PROCESS

C.1 Process Overview

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

A flow chart of the overall process is included in Figure 1 and the various phases are further discussed in Sections C.2 through C.5.

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

The first tier is where a licensee is proposing to reference a previously approved topical report completely within the envelope of its generic approval as described in the topical report. A tier one review would be able to rely heavily upon the previous review efforts, with large parts of the review being confirmatory. The list of documents that would typically need to be submitted by the licensee in support of a tier 1 review are contained in Appendix B.1.

The second tier is where a licensee proposes to reference a previously approved topical report with deviations to suit the plant-specific situation. Deviations could include, for example, a revised software development process or new hardware. The aspects of a tier two review that are within the envelope of the generic approval would be confirmatory, while the deviations should be expected to require a more significant review effort. Typically, an application citing licensing experience from another plant's previous approval would be considered a tier two review. This, however, is dependent upon the similarities of the application. The list of documents that would typically need to be submitted by the licensee in support of a tier 2 review are contained in Appendix B.2.

The third tier is where a licensee proposes to use a completely new system with no generic approval. Licensees should expect that a tier three review will require a very significant review effort within all review areas. The list of documents that would typically need to be submitted by the licensee in support of a tier 3 review are contained in Appendix B.3. As with any of the lists provided in Appendix B, the plant specific

application may obviate the need for certain listed documents or necessitate the inclusion of other, unlisted, documents.

This guidance divides the whole of the review into a number of conceptual review areas. Doing this allows the review to be handled in a more regimented manner which fosters better tracking outstanding information needs and communication of those needs to the licensee. Additionally, this method supports knowledge transfer by allowing new reviewers to better conceptualize what needs to be reviewed versus a single large list of requirements. It should be noted that not all of the review areas directly address meeting regulatory requirements, instead, some lay the groundwork for evaluating the criteria of others. As an example, the "Hardware description" and "Hardware Design Process and Quality Control "review areas do not have criteria to be met, nor do they come directly from a regulatory requirement (other than the basic requirement to adequately describe and justify a proposed change). Instead, they discuss the level of detail to which the licensee should describe the system and supporting development, maintenance, and operation programs. This information subsequently feeds into the NRC staff's evaluation against the acceptance criteria (e.g., IEEE-603, 1991).

C.2 Pre-Application (Phase 0)

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

As a minimum, these discussions should include whether the system will have built-in diversity for all applicable events or whether the licensee will rely on diverse manual operator actions or diverse actuation systems. Further, these discussions should include whether the licensee is proposing the use of an approved topical report, any planned deviations from NRC staff positions, and specifics of the software quality assurance plan. If able, licensees should be encouraged to discuss topics from other review areas as well as how any best-estimate evaluations utilize realistic assumptions and models and address uncertainty associated with the results.

Following each meeting the NRC staff will capture the topics discussed via a meeting summary. This summary will include a preliminary NRC staff assessment of the licensee's concept (or those sub-parts of the overall concept discussed) and identify the areas that are significant to this preliminary assessment. Additionally, as appropriate, the NRC staff will include a preliminary assessment of which review tier would be applicable for the proposed upgrade. The licensee will be provided a draft copy of the meeting summary comment prior to its issuance. An example meeting summary is included in Appendix A to this document.

C.3 Initial Application (Phase 1)

Once a licensee believes it has a design that adequately addresses NRC acceptance criteria, including defense-in-depth and diversity, variances to existing guidance, and any unique or complex design features, it should prepare and submit a LAR. It is incumbent upon the licensee to identify any deviations in design and concept that may impact the NRC staff's preliminary assessment made during Phase 0. It should be noted that these changes may adversely impact the NRC staffs acceptance of the LAR for review.

To the extent possible, the LAR should include address review areas, which are discussed in further detail in the referenced sections:

- Defense-in-depth & Diversity (Section D.1)
- Hardware Architecture (Section D.2)
- Hardware Design Process and Quality Control (Section D.3)
- Communications (Section D.4)
- Software Architecture (Section D.5)
- Software Design Process (Section D.6)
- System Qualifications (Section D.7)
- System, Hardware, Software, and Methodology Modifications (Section D.8)
- IEEE 603 Compliance (Section D.9)
- IEEE 7-4.3.2 Compliance (Section D.10)
- Technical Specifications (Section D.11)
- Cyber Security (Section D.12)

Initially, the NRC staff will review the application in accordance with the NRR Office Instruction, LIC-109, "Acceptance Review Procedures," to determine if the application is sufficient for NRC staff review. It is recognized that some sets of information may not be available upon initial application and the review process may be more efficiently administered by beginning prior to their availability. Therefore, a digital I&C upgrade application may be found to be sufficient for review provided a clear schedule for submission of omitted information is included. Any proposed changes to the schedule should be agreed upon by the NRC staff prior to a given due-date. Licensees should be made aware that the NRC staff will rigorously adhere to the schedule set forth and failure to submit information in accordance with the schedule may result in denial of the application pursuant to 10 CFR 2.108.

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

As further discussed in Section C.4, the NRC staff and licensee should be aware that some information needs may be best met by the performance of an audit. Those information needs to be resolved in this manner should be documented and the Project Manager, in consultation with the licensee and technical staff, should schedule the audit. While the documentation needs discussed in Section D.1 through D.X indicate which process will likely be used (i.e., RAI or Audit), individual circumstances will dictate the appropriate vehicle for the NRC staff to obtain needed information.

C.4 Continued Review and Audit (Phase 2)

Following response to the Phase 1 RAIs but at least 12 months prior to the requested approval date, the licensee should submit a supplement containing sufficient information to address aspects of the review areas not submitted in the initial LAR or subsequent RAIs. Although 12 months is the minimum lead time the NRC staff should expect, the licensee to adhere to the submittal schedules established earlier. Further, the NRC staff should take appropriate actions in response to significant delays in receiving necessary information.

During Phase 2, the NRC staff will continue the RAI process until sufficient information has been provided for a decision to be rendered on the acceptability of the proposed digital I&C upgrade. If necessary, during the Phase 2 RAI process, the NRC staff will conduct an audit in accordance with LIC-111, "Regulatory Audits" (Note: This document is not publically available).

Any audits will likely cover information from both Phase 1 and Phase 2, and may result in further requests for information to be docketed. It is the NRC staff's intent to perform the audits as early in the process as is reasonable, but the performance of an effective and efficient audit requires that the LAR and supplements to be sufficiently detailed about the later phases of the system development lifecycle (e.g., V&V and factory acceptance testing). Although the use of an audit is discussed in Phase 2, this does not preclude the performance of an audit during Phase 1 if it is determined to be beneficial.

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

Phase 2 will conclude with the issuance of a safety evaluation (SE) documenting the approval or denial of the licensee's proposed digital I&C upgrade. The licensing process covered by this ISG ends at the issuance of the associated amendment.

C.5 Implementation and Inspection (Phase 3)

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

The startup testing is conducted in accordance with the plan submitted during Phase 2. The NRC staff review of startup testing is an inspection function that will be conducted by the appropriate regional staff in accordance with IP-52003, "Digital Instrumentation and Control Modification Inspection."

D. Review Areas

D.1 Hardware Architecture

D.1.1 Scope of Review

Reviewing the hardware architecture of the digital I&C system allows the NRC staff to understand how the high-level functional units of the system interact to accomplish the design function. Evaluation of the system at a high-level provides a solid foundation for the subsequent detailed reviews and evaluation against the acceptance criteria.

D.1.2 Information to be Provided

Consistent with the list of documents provided in Appendix B, the licensee's submittal should provide sufficient documentation and description to allow the NRC staff to identify what hardware is being used in this application, how the hardware items function, how the various hardware items are interconnected, and any software which runs on that hardware. The hardware items should be identified to the revision level. In those cases where the hardware has previously been described by the vendor and evaluated by the NRC staff, the licensee should provide reference to the description and evaluation. Any deviations or revision changes should be identified and adequately justified.

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

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

D.1.3 Regulatory Evaluation

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

D.1.4 Technical Evaluation

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

D.1.5 Conclusion

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

D.2 Hardware Design Process and Quality Control

D.2.1 Scope of Review

Supported by the review of the high-level interactions from Section D.2, the NRC staff reviews the process and quality control used during the design process for individual hardware items and the overall system under review. In particular, the NRC staff reviews the licensee and vendor quality control programs associated with the hardware development.

D.2.2 Information to be Provided

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

D.2.3 Regulatory Evaluation

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

D.2.4 Technical Evaluation

The NRC staff will provide a description of the design process and the quality control which governed that design process. This description will cover both design of the individual functional units and modules and how those units and modules were used in the application specific design.

D.2.5 Conclusion

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

D.3 Software Architecture

D.3.1 Scope of Review

D.3.2 Information to be Provided

D.3.3 Regulatory Evaluation

D.3.4 Technical Evaluation

D.3.5 Conclusion

D.4 Software Design Process

D.4.1 Scope of Review

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

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

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

D.4.2 Information to be Provided

Consistent with the list of documents provided in Appendix B, the licensee's submittal should provide sufficient documentation to support and justify the robustness of the software design plan associated with the digital I&C system. The documentation should provide sufficient justification to allow the conclusion that the plan meets the applicable

criteria, as discussed in Section D.5.4. The information provided should clearly delineate the roles and responsibilities of the various organizations contributing to the development, operation, and maintenance of the software. Additionally, the interactions and boundaries between these organizations should be clearly described.

D.4.3 Regulatory Evaluation

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

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

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

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

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

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

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

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

D.4.4 Technical Evaluation

D.4.4.1 Software management Plan

SRP BTP 7-14, in Section B.3.1.1, provides acceptance criteria for software management plans. This section states that Regulatory Guide 1.173 endorses IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" and that Clause A.1.2.7, "Plan Project Management," contains an acceptable approach to software project management. Clause A.1.2.7 states that the plan should include planning for support, problem reporting, risk management, and retirement. These requirements are applied to both licensee and vendor programs.

The purpose of the NRC staff review of the SMP is to ensure that the management aspects of the software development project are such that high quality software will

result. This necessitates a deliberate and careful development process. There are several management characteristics that are of particular interest to the staff, and the SMP should cover these aspects in detail. Since the software development will generally be done by a vendor and not by the licensee, the interface between the licensee and vendor, and the method by which the quality of the vendor effort will be judged by the licensee is critical. It is important that oversight of the vendors exists and is effective. Software or system vendors may not be familiar with nuclear requirements or with specific plant requirements, and therefore, one of the more important aspects is oversight by the licensee that is effective and meets 10 CFR Part 50, Appendix B. The SMP should describe the interaction, what checks and audits the licensee will perform, and the standard by which the success of the audit will be judged.

Another important aspect of the SMP is the relationship between the software development group and the groups which check both the quality of the software development and the software itself. Generally, these are the quality assurance organization, the software safety organization, and the software verification and validation organization. It is important that these groups maintain independence from the development organization, by both organization and function. The independence of the quality assurance organization, the software safety organization, and the software verification and validation organization should be described in terms of management, schedule, and finance. If these independence aspect are described in the planning documents of these organizations, such as the V&V Plan, Safety Plan or QA plan, the SMP should provide a pointer to the appropriate section of those plans.

When the staff reviews the duties of each member of the project's management and technical teams, the reviewer will need to ensure that the personnel responsible for various items have the experience or training to perform those duties. This information should be included in the SMP.

In addition, the SMP should include sufficient information about the security requirements for the reviewer to determine that the methods used are consistent with Regulatory Guide 1.152 and that the methods are used effectively. This needs to be an actual description of the security requirements, and not just a statement that all security requirements will be met. The review of how those requirements are being met will be in

Many of the other characteristics of the SMP are of minimal concern to the safety of the system, and therefore of minimal concern to the reviewer. These items should be included in the SMP to the degree needed by the licensee and vendors, but do not need to be enhanced for staff review, Examples of the are management indicators used and the process by which the project will be managed. This is of primarily concern to the software development organization, and will be reviewed only to the extent that safety of the final product is maintained.

The same is true of the budget and personnel from the resource characteristics. The budget and number of personnel for the project is a trade-off with the length of time required, and there is of minimal concern to the staff. The adequacy of the budget and personnel for the quality assurance organization, the software safety organization, and the software verification and validation organization is of interest, and should ensure that those groups have adequate resources to support a high quality design effort. This will require some judgment, and it may require a justification by the licensee or vendor. In addition, safety and V&V personnel should be competent in software engineering in

order to ensure that software safety and software V&V are effectively implemented. A general rule of thumb is that the V&V personnel should be at lease as qualified as the design personnel.

D.4.4.2 Software Development Plan

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

The NRC staff review of the software development is primarily intended to determine that use of the SDP results in a careful and deliberate process which will result in high quality software, suitable for use in safety-related systems in nuclear power plants. The details on how this will be done may be found in other plans, such as the SVVP, SCMP, and so forth, and if this is done, the SDP should provide pointers to the appropriate sections of those other plans. For staff review purposes, the important aspect of the software development plan is the method to be used to make sure these other plans are being applied. This would generally include a provision for effective oversight, where the strategy for managing the technical development is specified. The SDP should discuss these aspects in detail, to allow the reviewer to determine that the software development plan allows the licensee or vendor to adequately monitor the software development process, and that any deviations from the software development process will be discovered in time to take corrective action.

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

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

Under the resource characteristics, the methods and tools to be used should be evaluated. Of particular interest to the staff is the method by which the output of software tools, such as compliers or assemblers, will be verified to be correct. This aspect of tool usage should be specifically covered in the SDP. The criteria from IEEE Std 7-4.3.2-2003 is that software tools should be used in a manner such that defects not detected by the software tool will be detected by V&V activities. If this is not possible, the tool itself should be safety-related.

The SDP should list the international, national, industry, and company standards and guidelines, including regulatory guides, which will be followed, and whether or not these standards and guidelines have previously been approved by the NRC staff. If the standards have not been reviewed and approved, the staff will need to do so to ensure that adherence to the standard will result in meeting NRC requirements. Coding standards should be compared to the suggestions contained in NUREG/CR-6463, "Review Guidance for Software languages for Use in Nuclear Power Plant Safety Systems," and the any deviations should be justified.

D.4.4.3 Software Quality Assurance Plan

Quality Assurance is required by 10 CFR Part 50, Appendix B, and the Quality Assurance Plan should be implemented under an NRC approved Quality Assurance (QA) program. 10 CFR Part 50, Appendix B, allows the licensee to delegate the work of establishing and executing the quality assurance program, but the licensee shall retain responsibility. The plan should identify which QA procedures are applicable to specific programming processes, and identify particular methods chosen to implement QA procedural requirements. There are several Regulatory Guides and Standards that offer guidance.

1. Regulatory Guide 1.28, Revision 3, "Quality Assurance Program Requirements (Design and Construction)," that endorses ANSI/ASME NQA-1-1983, "Quality Assurance Program Requirements for Nuclear Facilities," and the ANSI/ASME NQA-1a-1983 Addenda, "Addenda to ANSI/ASME NQA-1-1983 "Quality Assurance Program Requirements for Nuclear Facilities."

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

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

4. NUREG/CR-6101, Section 3.1.2, "Software Quality Assurance Plan," and Section 4.1.2, "Software Quality Assurance Plan," contain guidance on these plans.

The SQAP is one of the more important plans which will be reviewed by the staff. The staff reviewer will need to determine not only that the SAQP exhibits the appropriate management, implementation and resource characteristics discussed above, but also that following the SQAP will result in high quality software that will perform the intended safety function. The NRC staff will sample the design process and products to evaluate the effectiveness of the licensee or vendor QA and V&V efforts, and to determine that the licensee or vendor QA and V&V efforts were performed correctly. If errors not already discovered and documented by either the QA organization or the V&V team are found, this indicates a potential weakness in the effectiveness of the QA organization. While 10 CFR Part 50, Appendix B, allows the licensee to delegate the work of establishing and executing the quality assurance program, and if this is done, the SQAP should show how the licensee retains the overall responsibility for the system and software, and how the licensee determines that the quality of the software is sufficient.

The organization of the software QA organization should be described in sufficient detail to show that there is sufficient authority and organizational freedom, including sufficient independence from cost and schedule to ensure that the effectiveness of the QA organization is not compromised. IEEE Std 1028-1998 can be used as guidance.

D.4.4.4 Software Integration Plan

The acceptance criteria for a software integration plan are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.4, "Software Integration Plan." This section states that Regulatory Guide 1.173, endorses IEEE Std 1074-1995, and that within that standard, Clause A.1.2.8, "Plan Integration," contains an acceptable approach relating to planning for integration. Clause A.1.2.8 states that the Software Requirements and the Software Detailed Design should be analyzed to determine the order for combining software components into an overall system, and that the integration methods should be documented. The integration plan should be coordinated with the test plan. The integration plan should also include the tools, techniques, and methodologies needed to perform the integrations. The planning shall include developing schedules, estimating resources, identifying special resources, staffing, and establishing exit or acceptance criteria.

The software integration actually consists of three major phases: integrating the various software modules together to form single programs, integrating the result of this with the hardware and instrumentation, and testing the resulting integrated product. In the first phase, the various object modules are combined to produce executable programs. The second phase is when these programs are then loaded into test systems that are constructed to be as nearly identical as possible to the ultimate target systems, including computers, communications systems, and instrumentation. The final phase consists of testing the results, and is discussed in another report.

While the Software Integration Plan is not as critical as some of the other plans, the staff will still review it to determine the adequacy of the planned software integration effort. The software integration organization is generally the same group as the software developers, but this is not always the case. If there is more than one group of software developers, or if some of the software is dedicated commercial grade or a reuse of previously developed software, the methods, procedures and controls for software integration become more critical, and should be described in sufficient detail to allow the reviewer to determine that the integration effort is sufficient.

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

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

The resource characteristics of the software integration plan should include a description of the methods, techniques, and tools that will be used to accomplish the integration

function. The plan should require that integration tools be qualified with a degree of rigor and a level of detail appropriate to the safety significance of the software being created.

D.4.4.5 Software Installation Plan

The acceptance criteria for a software installation plan are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.5, "Software Installation Plan. This section states that Regulatory Guide 1.173, endorses IEEE Std 1074-1995, and that Clause A.1.2.4 of that standard, "Plan Installation," contains an acceptable approach relating to planning for installation. This clause states that an installation plan describe the tasks to be performed during installation, and shall include the required hardware and other constraints, detailed instructions for the installer, and any additional steps that are required prior to the operation of the system . Further guidance is provided in NUREG/CR-6101, Section 3.1.8, "Software Installation Plan," and Section 4.1.8, "Software Installation Plan," that contain a sample outline of an installation plan.

Since the software is being installed in hardware, the personnel performing this installation should be a mix of the software and hardware personnel. The critical part of the software installation is the system test (Note: Per IEEE Std 1012-1998, Final System testing is considered a V&V test and is the responsibility of the V&V group).

There should be written and approved procedures for software installation, for combined hardware/software installation, and systems installation. In a sufficiently complex system, these procedures may contain some errors, thus SIP should include the mthod by which these errors are identified, corrected, and documented, and should confirm that these corrections are subject to the same quality and configuration control as the rest of the system.

D.4.4.6 Software Maintenance Plan

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

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

The Software Maintenance Plan, together with the Software Configuration Maintenance Plan, define what records are kept and who controls those records. If the software is to be modified, it is critical to ensure that the right version of the software undergoes that

modification. The procedures for testing modifications are also critical. The plan should document what controls are in place to ensure that implementing a change does not inadvertently introduce other errors. The regression testing requirements should be described in sufficient detail for the staff to be able to determine that all the acceptance tests originally performed, or a carefully selected and justified subset, will be used to ensure that no new errors have been created. The SCM should also describe the review process required to determine that the proposed software maintenance is actually maintenance, and does not introduce new functions or other design changes.

The Software Maintenance Plan should also describe how it will be determined that the personnel performing the maintenance are fully qualified. This generally means that the personnel should be equally qualified as the original design team. The SMP should also describe how the maintainer will determine that the software tools are qualified and identical to those used during the original design. The Software Maintenance Plan should have some provisions for qualifying a new revision of the tool if the original version of the tool is no longer available.

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

D.4.4.7 Software Training Plan

The acceptance criteria for a training plan are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.7, "Software Training Plan." This section states that Regulatory Guide 1.173 endorses IEEE Std 1074-1995, and that Clause A.1.2.6 of that standard, "Plan Training," contains an acceptable approach relating to planning for training. BTP 7-14, Section B.3.1.7 also states that NUREG/CR-6101, Section 3.1.10, "Software Training Plan," contains further guidance on Software Training Plans.

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

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

licensee may, however, have a qualified engineering staff to be able to do software maintenance themselves.

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

D.4.4.8 Software Operations Plan

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

The Software Operations Plan will be reviewed for completeness, and therefore the plan needs to address all operations of the system and the plant. A new criterion for operations is cyber security, and therefore the plan should discuss measures to ensure the security of the system, and in particular, the means used to ensure that there are no unauthorized changes to hardware, software, and system parameters. Additionally, the plan should show how the operators will be able to detect actual or attempted penetration of the system. There should also be provisions on how to respond to security problems. In general, the plan should show how the licensee has considered the problem and is prepared to respond.

D.4.4.9 Software Safety Plan

The acceptance criteria for a software safety plan are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.9, "Software Safety Plan" and Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities." These sections state that the Software Safety Plan should provide a general description of the software safety effort, and the intended interactions between the software safety organization and the general system safety organization. It further states that NUREG/CR-6101, Section 3.1.5 "Software Safety Plan," and Section 4.1.5 "Software Safety Plan," contain guidance on Software Safety Plans. Further guidance on safety analysis activities can be found in NUREG/CR-6101 and Regulatory Guide 1.173, Section C.3, "Software Safety Analyses," contains guidance on safety analysis activities.

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

A critical characteristic of the Software Safety Plan is its completeness. The plan needs to show how the licensee will handle the various issues. It is also possible, that the elements of software safety may be addressed in another plan such as the Software Management Plan. As long as the concepts discussed above are addresses, either

approach is acceptable, however if the elements of software safety are addressed in other plans, the software safety plan should contain pointers to the appropriate sections of those other plans.

There should be a group which specifically considers the safety issues of the digital system to determine the acceptability of the system, and the software safety plan should define that group. The safety organization should consider the security risk as well as the risk to the plant if the digital system malfunctions. Since the staff will assess whether the proper risks were considered, that the licensee addresses these risks in an appropriate manner, and stayed consistent with the software safety strategy, the software safety plan should specifically address these issues in the risk evaluations.

D.4.4.10 Software Verification and Validation Plan

The acceptance criteria for verification and validation plans are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.10, "Software Verification and Validation Plan," and Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities." These sections state that Regulatory Guide 1.168, "Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants," Revision 1, endorses IEEE Std 1012-1998, "IEEE Standard for Software Versification and Validation," as providing methods acceptable to the staff for meeting the regulatory requirements as they apply to verification and validation of safety system software. This section also states that further guidance can be found in Regulatory Guide 1.152, Revision 2, Section C.2.2.1, "System Features," and NUREG/CR-6101, Section 3.1.4 and 4.1.4.

Verification is defined as the process of determining whether the products of a given phase of the development cycle fulfill the requirements established during the previous phase. Validation is defined as the test and evaluation of the integrated computer system to ensure compliance with the functional, performance, and interface requirements. Combined, V&V is the process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill (i.e., implements) the requirements to meet the criteria imposed by the previous phase, and the final system or component complies with specified requirements. This determination may include analysis, evaluation, review, inspection, assessment, and testing of products and processes.

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

One of the most critical items in the Software Verification & Validation Plan is the independence of the V&V organization. The V&V team should be independent in management, schedule, and finance (Per IEEE Std 1012-1995). The plan should specifically show how the V&V team is independent, and why the V&V personnel are not subject to scheduling constraints or to pressure from the software designers or project

managers for reports or review effort. Since the V&V team should report to a level of management which is not exerting direct pressure for a favorable V&V report, the plan need to demonstrate this. The plan should also show how the V&V effort is sufficiently independent to adequately perform the tasks without undue influence to schedule and financial pressure.

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

The quality of the V&V personnel is also important. If a V&V engineer is to judge the output of a software design engineer, the V&V engineer should be qualified to understand the process, technology, and the software. If the V&V engineer is not qualified, the V&V effort may not be effective. The plan should address how the quality of the V&V personnel was verified. This needs to be more than a simple determination that the V&V person is an electrical engineer, and therefore acceptable. The needs to be a real evaluation of skills needed for this level of V&V, and how the proposed personnel meet those needs.

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

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

In general, the SVVP needs to document how the requirements of IEEE 1012 will be meet, and for any IEEE 1012 requirement which is not being meet, what compensatory actions are being used to demonstrate an equivalent level of verification and validation.

D.4.4.11 Software Configuration Management Plan

The acceptance criteria for configuration management plans are contained in the Standard Review Plan, BTP 7-14, Section B.3.1.11, "Software Configuration Management Plan," and Section B.3.2.3, "Acceptance Criteria for Software Configuration Management Activities." These sections states that both Regulatory Guide 1.173,

"Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" that endorses IEEE Std 1074-1995, Clause A.1.2.4, "Plan Configuration Management," and Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," that endorses IEEE Std 828-1990, "IEEE Standard for Configuration Management Plans," provide an acceptable approach for planning configuration management. BTP 7-14, Section B.3.1.11 further states that additional guidance can be found in IEEE Std 7-4.3.2-2003,"IEEE Standard Criteria for Digital Computers in Safety Systems on Nuclear Power Generating Stations," Clause 5.3.5, "Software configuration management," and in Clause 5.4.2.1.3, "Establish configuration management controls." NUREG/CR-6101, Section 3.1.3 "Software Configuration Management Plan," and Section 4.1.3, "Software Configuration Management Plan," also contain guidance.

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

The Software Configuration Management Plan is another important plan because software are made to the wrong version of the software, or the changes are not sufficiently tested to ensure that they do not introduce new errors. Configuration management starts once the initial software is initially released by the software design group.

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

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

The Software Configuration Management Plan should specify how modified software or documentation should be tested and verified, and who is to do this.

The Software Configuration Management Plan may be two different plans, one used by the software vendor during the development of the software, and one used by the licensee during the operational phase of the project. The licensee plan may be contained in an overall plant configuration management plan. If this is the case, the licensee should check that software specific issues have been addressed in the plant configuration management plan.

D.4.4.12 Software Test Plan

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

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

D.4.4.13 Software Requirements Specification

The acceptance criteria for the requirements specification is contained in the Standard Review Plan, BTP 7-14, Section B.3.3.1, "Requirements Activities - Software Requirements Specification." This sections states that Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 830-1993, "IEEE Recommended Practice for Software Requirements Specifications," and that standard describes an acceptable approach for preparing software requirements specifications for safety system software. The section also states that additional guidance can be found in NUREG/CR-6101, Section 3.2.1 "Software Requirements Specification," and Section 4.2.1, "Software Requirements Specifications."

Errors in requirements or misunderstanding of their intent are a major source of software errors. The requirements should be carefully examined by the licensee to ensure that each requirement is complete, consistent, correct, understandable, traceable,

unambiguous, and verifiable. The complexity of the SRS is, of course, dependant on the complexity of the system being proposed, and the level of detail should reflect the level of complexity.

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

D.4.4.14 Software Architecture Design

The acceptance criteria for the software architecture description is contained in the Standard Review Plan, BTP 7-14, Section B.3.3.2 "Design Activities - Software Architecture Description." This section states that the Software Architecture Description should describe all of the functional and software development process characteristics listed, and that NUREG/CR-6101, Section 3.3.1 "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance.

The SAD must show how the software works, the flow of data, and the deterministic nature of the software. The architecture should be sufficiently detailed to allow the reviewer to understand the operation of the software.

D.4.4.15 Software Design Specification

The acceptance criteria for the software design description are contained in the Standard Review Plan, BTP 7-14, Section B.3.3.3, "Design Activities - Software Design Specification." This section states that the software code accurately reflects the software requirements, and that NUREG/CR-6101, Section 3.3.2 "Software Design Specification," and Section 4.3.2, "Software Design Specifications," contain relevant guidance.

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

D.4.4.16 System Build Documents

The acceptance criteria for the system build documentation are contained in the SRP, BTP 7-14, Section B.3.3.5, "Integration Activities -System Build Documents." This section states that NUREG/CR-6101, Section 3.5.1, "System Build Documents," and Section 4.5.1, "System Build Documents," contain relevant guidance.

The build documentation is generally needed to verify that the programs actually delivered and installed on the safety system is the programming that underwent the V&V process and was tested. Any future maintenance, modifications or updates will require that the maintainers know which version of the programming to modify and, therefore, the system build documentation is closely tied to the configuration management program. The items, including programming, should check to ensure that the

programming listed in the build documentation is identified by version, revision, and date, and that this is the version and revision that was tested.

D.4.4.17 Installation Configuration Tables

The acceptance criteria for the system build documentation is contained in the SRP, BTP 7-14, Section B.3.3.6 Installation Activities -Installation Configuration Tables. This section states that in the event that the programming has options for use, variable setpoints or other data, or may operate in various methods, the programming needs to be configured for the particular plant requirements. Any item that is changeable should have the intended configuration recorded in the Installation Configuration Tables, and the reviewer should sample these configuration items to verify that they are correct. The reviewer should verify that the V&V team has already made this determination, and should then sample various items.

D.4.4.18 Requirements Traceability Matrix

The definition of a Requirements Traceability Matrix (RTM) is contained in The Standard Review Plan, BTP 7-14, Section A.3, definitions, and says: "An RTM shows every requirement, broken down in to sub-requirements as necessary, and what portion of the software requirement, software design description, actual code, and test requirement addresses that system requirement." This is further clarified in Section B.3.3, "Acceptance Criteria for Design Outputs," in the subsection on Process Characteristics. This section states that a requirements traceability matrix, that needs to show every requirement, should be broken down in to sub-requirements as necessary. The RTM should show what portion of the software requirement, software design description, actual code, and test requirement addresses each system requirement.

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

D.4.4.19 Failure Modes and Effects Analysis

There is no specific regulatory guidance on the required format, complexity or conclusions concerning the FMEA, however IEEE Std 1228-1994 and MIL-Std-882B identify techniques which can be used for identifying hazards. Each system must be independently assessed by to determine if the FMEA is sufficiently detailed to provide a useful assessment of the potential failures and the effects of those failures.

FMEA is a procedure for analysis of potential hardware or programming failure modes within a system for determination of the effect of failures on the system. This information can then be used to assess the potential for an undetectable failure or a common mode failure. The overall staff expectation is that each potential hardware and software failure will be identified, and the effect of that failure will be determined. For a complex system, this is expected to be a very complex analysis. The key attribute which the staff will be

reviewing is completeness, where all hardware and software failures are identified, and accuracy, where the analysis reaches a understandable reason for what the failure effect is for each failure mode. The FMEA is also used as in input the diversity and defense in depth analysis.

D.4.5 Conclusion

The NRC staff has reviewed the information provided describing the life-cycle development of the software to be used by and/or in support of the digital I&C system. The NRC staff finds that the information describes a well-defined, disciplined process which will produce a high quality product. The NRC staff finds that the V&V process described will provide acceptable analysis, evaluation, review, inspection, assessment, and testing or the products and processes.

D.5 System Qualifications

D.5.1 Scope of Review

D.5.2 Information to be Provided

D.5.3 Regulatory Evaluation

D.5.4 Technical Evaluation

D.5.5 Conclusion

D.6 Defense-in-Depth & Diversity

D.6.1 Scope of Review

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

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

areas: human diversity, design diversity (hardware), software diversity, functional diversity, signal diversity, and equipment diversity.

Diversity in digital I&C systems is necessitated by their vulnerability to common-cause failures (CCFs) in software even though CCFs are beyond design basis. The NRC staff review of a digital I&C system modification will ensure that sufficient diversity is provided to accomplish the required safety function subject to the potential CCF vulnerability.

D.6.2 Information to be Provided

Consistent with the list of documents provided in Appendix B, the licensee's submittal should provide sufficient documentation to support to the assertion that a proposed digital I&C system is diverse and sufficiently robust against CCF. Additional guidance is available in Interim Staff Guidance DI&C-IGS-02. As further discussed in Section D.1.3, the NRC staff will evaluate the licensee's proposed amendment using Branch Technical Position 7-19, which contains four points to be addressed. To satisfy these four points, the NRC staff would expect a submittal to include:

- An analysis of the diversity of the system with respect to the six areas discussed in Section D.1.1.
- A best-estimate evaluation of each anticipated operational occurrence (AOO) in the design basis occurring in conjunction with each single postulated common-cause failure.
- A best-estimate evaluation of each postulated accident in the design basis occurring in conjunction with each single postulated common-cause failure.
- An evaluation of all common elements or signal sources shared by two or more system echelons.
- Identification of all interconnections between the RTS and ESFAS provided for system interlocks and justification that functions required by 10 CFR 50.62 are not impaired by the interconnection.
- A list of all manual operator actions credited for diversity.
- Detailed justification for operator actions required in less than 30 minutes.

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

D.6.3 Regulatory Evaluation

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

While the NRC considers CCFs in digital systems to be beyond design basis, the digital I&C system should be protected against CCFs. The NRC staff's review of defense-in-

depth and diversity in digital I&C systems is focused on ensuring that the required safety functions can be achieved in the event of a postulated CCF in the digital system. As discussed in BTP 7-19, The NRC staff's review considered the following regulatory requirements:

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with Institute of Electrical & Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued before January 1, 1971, the applicant/licensee may elect to comply instead with their plant-specific licensing basis. For nuclear power plants with construction permits issued between January 1, 1971, and May 13, 1999, the applicant/licensee may elect to comply instead with the requirements stated in IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE Std. 603-1991, Clause 5.1, requires in part that "safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures." IEEE Std. 279-1971, Clause 4.2, requires in part that "any single failure within the protection system shall not prevent proper protective action at the system level when required."

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

Additionally, the NRC staff's review is guided by 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 21, "Protection Systems Reliability and Testability," requires in part that "no single failure results in the loss of the protection system."

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

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

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

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

D.6.4 Technical Evaluation

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

D.6.4.1 Adequate Diversity and Manual Operator Actions

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

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

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

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

D.6.5 Conclusion

The NRC staff has reviewed the licensee's submittal and finds that the proposed implementation of [SYSTEM] is sufficiently diverse and robust to protect against common-mode/common-cause failure that the [control system, RTS, ESFAS, and/or monitoring and indication] adequately address the NRC staff positions stated in BTP 7-19. Addressing the NRC staff positions in BTP 7-19 provides adequate assurance that the proposed change meet the requirements of 10 CFR 50.55a(h) and 10 CFR 50.62. Therefore, the NRC staff finds the proposed digital I&C upgrade to be acceptable with respect to defense-in-depth and diversity.

D.7 Communications

D.7.1 Scope of Review

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

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

If signal communication exists between different portions of the safety system, the evaluation will include a review to determine if a malfunction in one portion affects the safety functions of the redundant portion(s). If the safety system is connected to a digital computer system that is non-safety, the evaluation will include a review to determine if a logical or software malfunction of the non-safety system affects the functions of the safety system. These reviews will be done by examination of the communication methods used, and comparing them to each staff position within ISG #4.

D.7.2 Information to be Provided

Consistent with the list of documents provided in Appendix B, the licensee's submittal should provide sufficient documentation to support and justify the ability of the digital I&C system limit the effect of a failed channel from adversely impacting sibling channels. The documentation should provide sufficient justification to allow the conclusion that the plan meets the standards of IEEE 603-1991 Clause 5.6, IEEE 7-4.3.2 Clause 5.6, and BTP 7-11. Typically, this involves a detailed discussion of where communications are possible, the nature of those communications, the features of the system that provide the ability to preclude or account for the error.

D.7.3 Regulatory Evaluation

IEEE 603-1991 Clause 5.6, "Independence," requires independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design basis events, and (3) safety systems and other systems. SRP, Chapter 7, Appendix 7.1-C, Section 5.6 "Independence" provides acceptance criteria for this requirement, and among other guidance, provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and that if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system must not be able to affect the functions of the safety system.

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

that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

BTP 7-11 provides guidance for the application and qualification of isolation devices. BTP 7-11 applies to the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety and non-safety systems. The MSFIS does not contain connections between redundant portions of the safety systems. Therefore, this safety evaluation only considers applicability between safety and non-safety systems.

Additional Guidance on interdivisional communications is contained in ISG-4, "Highly-Integrated Control Rooms – Communication Issues," (ADAMS Accession No. ML072540138).

D.7.4 Technical Evaluation

The communication pathways of the system, including internal communications, one independent channel to another, between other safety-related systems, and between other non-safety-related systems shall be evaluated to confirm that a failure or malfunction in one does not adversely impact successful completion of the design function. Confirmation that the system is sufficiently robust against improper operation due to these communications is further discussed in ISG-4.

Section 1 of ISG # 4 provides guidance on the review of communications, includes transmission of data and information, among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related. This ISG does not apply to communications within a single division.

Section 2 of ISG #4 provides guidance applicable to a prioritization device or software function block, which receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device.

Section 3 of ISG #4 provides guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division, and applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.

D.7.5 Conclusion

The NRC staff has reviewed the design and implementation of the digital I&C system [does not employ data communication between sibling channels] or [meets the requirements of IEEE 603-1991, IEEE 7-4.3.2 by demonstrating that an error in a channel will not inappropriately impair the safety function of another. Addressing the aforementioned IEEE standards provides adequate assurance that the proposed change meet the requirements of 10 CFR 50.55a(h). Therefore, the NRC staff finds the proposed digital I&C upgrade to be acceptable with respect to data communications

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

D.8.1 Scope of Review

D.8.2 Information to be Provided

D.8.3 Regulatory Evaluation

D.8.4 Technical Evaluation

D.8.5 Conclusion

D.9 IEEE 603-1991, Compliance

D.9.1 Scope of Review

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

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

- Many of the auxiliary supporting features and other auxiliary features defined in IEEE Std. 603-1991, as typically described in Chapters 4, 5, 6, 8, 9, 10, 12, 15, 18, and 19 of the UFSAR, should be considered for the need for coordination with other technical disciplines.

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

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

- Other plant systems may necessitate additional requirements on the digital I&C systems.

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

D.9.2 Information to be Provided

D.9.3 Regulatory Evaluation

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with Institute of Electrical & Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued before January 1, 1971, the applicant/licensee may elect to comply instead with their plant-specific licensing basis. For nuclear power plants with construction permits issued between January 1, 1971, and May 13, 1999, the applicant/licensee may elect to comply instead with the requirements stated in IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE Std. 603-1991, Clause 5.1, requires in part that "safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures." IEEE Std. 279-1971, Clause 4.2, requires in part that "any single failure within the protection system shall not prevent proper protective action at the system level when required."

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

D.9.4 Technical Evaluation

D.9.4.1 IEEE 603-1991, Clause 4

Clause 4 of IEEE Std. 603-1991 requires, in part, that a specific basis be established for the design of each safety system. If this is an upgrade to a digital system from an existing system, the design basis for the new digital system may be the same as the

existing system. In this case, very little additional justification for the design basis would be needed. The new digital system may, however, have a different design basis. The design basis for the old system and a comparison to the design basis for the new system needs to be specifically addressed in the information provided.

D.9.4.1.1 IEEE 603-1991, Clause 4.1

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

D.9.4.1.2 IEEE 603-1991, Clause 4.2

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

D.9.4.1.3 IEEE 603-1991, Clause 4.3

Clause 4.3 requires documentation of the safety functions and corresponding protective actions of the execute features for each design basis event. If these have not changed, this should be clearly identified in the information provided.

D.9.4.1.4 IEEE 603-1991, Clause 4.4

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

D.9.4.1.5 IEEE 603-1991, Clause 4.5

Clause 4.5 describes the minimum criteria under which manual initiation and control of protective actions may be allowed, including the points in time and the plant conditions during which manual control is allowed, the justification for permitting initiation or control subsequent to initiation solely by manual means, the range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed, and the variables in clause 4.4 shall be displayed for the operator to use in taking manual action. If these have not changed, this should be clearly identified in the information provided. SRP BTP 7-6

provides specific guidance on determining if the timing margins for changeover from injection to recirculation mode are sufficient to allow manual initiation of the transition. Additionally, ISG-5 addresses this issue.

D.9.4.1.6 IEEE 603-1991, Clause 4.6

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

D.9.4.1.7 IEEE 603-1991, Clause 4.7

Clause 4.7 requires, in part, that the range of transient and steady-state conditions be identified for both the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform. This information will feed into additional evaluations. If these have not changed, this should be clearly identified in the information provided.

D.9.4.1.8 IEEE 603-1991, Clause 4.8

Clause 4.8 requires the identification of conditions having the potential for causing functional degradation of safety system performance, and for which provisions must be incorporated to retain necessary protective action. This information will feed into additional evaluations, including Clause 5.4.

D.9.4.1.9 IEEE 603-1991, Clause 4.9

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

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

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

D.9.4.2 IEEE 603-1991, Clause 5

Clause 5 of IEEE Std. 603-1991 requires that the safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established by design basis events. The analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met. The evaluation should confirm that the general functional requirements have been appropriately allocated to the various system components. The review in this regard should confirm that the system design fulfils the system design basis requirements established.

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

D.9.4.2.1 IEEE 603-1991, Clause 5.1

Clause 5.1 requires that any single failure within the safety system shall not prevent proper protective action at the system level when required. The analysis should confirm that the requirements of the single-failure criterion are satisfied. Guidance in the application of the single-failure criterion is provided in RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," which endorses IEEE Std. 379-1988, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

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

Components and systems not qualified for seismic events or accident environments and non-safety-grade components and systems are assumed to fail to function if failure adversely affects safety system performance. Conversely, these components and systems are assumed to inadvertently function in the worst manner if functioning adversely affects safety system performance. All failures in the safety system that can be predicted as a result of an event for which the safety system is designed to provide a protective function are assumed to occur if the failure adversely affects the safety system performance. In general, the lack of equipment qualification or a less than high quality design process may serve as a basis for the assumption of certain failures. After assuming the failures of non-safety-grade, non-qualified equipment and those failures caused by a specific event, a random single failure within the safety-related system is arbitrarily assumed. With these failures assumed, the safety system must be capable of performing the protective functions required to mitigate the consequences of the specific event.

Digital computer-based I&C systems share data, data transmission, functions, and process equipment to a greater degree than analog systems. Although this sharing forms the basis for many of the advantages of digital systems, it also raises a key concern with respect to I&C system vulnerability to a different type of failure. The concern is that a design using shared databases and process equipment has the potential to propagate a common-cause failure of redundant equipment. ISG-4, Section 1, "Interdivisional Communications," Staff Position 3, states that "A safety channel

should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system." In order to comply with this staff position, the licensee or vendor should demonstrate that any communications failure will not allow a single failure within one channel to defeat the single failure concept. This demonstration is further discussed in Section D.7, "Communications."

Another concern is that software programming errors can defeat the redundancy achieved by the hardware architectural structure. Because of these concerns, the NRC staff has placed significant emphasis on defense-in-depth against common-cause failures within and between functions. The principle of defense-in-depth is to provide several levels or echelons of defense to challenges to plant safety, such that failures in equipment and human errors will not result in an undue threat to public safety. This is addressed further in Section D.7 and ISG-4.

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

D.9.4.2.2 IEEE 603-1991, Clause 5.2

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

In addition to a description of how "seal-in" features ensure that system-level protective actions go to completion, including functional and logic diagrams sufficient to demonstrate this feature. Additionally, the information should clearly demonstrate that deliberate operator action is required to return the safety systems to normal operation.

D.9.4.2.3 IEEE 603-1991, Clause 5.3

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

The information provided should confirm that the quality assurance provisions of Appendix B to 10 CFR, Part 50, are applicable to the safety system. The adequacy of the quality assurance program is addressed further in the evaluation against Clause 5.3

of IEEE Std. 7-4.3.2-2003. It may be beneficial for a licensee to conduct a 10 CFR, Part 50, Appendix B audit of the vendor to confirm the adequacy of their quality assurance program.

D.9.4.2.4 IEEE 603-1991, Clause 5.4

Clause 5.4 states that safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting the performance requirements as specified in the design basis. Appendix 7.1-C, Section 5.4, of the SRP provides acceptance criteria for Clause 5.4. This acceptance criteria states that the licensee should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. Clause 5.4 also states that the qualification of Class 1E equipment be in accordance with the requirements of IEEE Std 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" and IEEE Std 627-1980, "IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations." Regulatory Guide 1.89 Revision 1, endorses guidance for compliance with IEEE Std 323-1974

The information provided should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal, abnormal, and accident conditions.

Mild environment qualification should conform with the guidance of IEEE Std. 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." The information provided should demonstrate how the equipment was tested, or what analysis was done. The resultant test data or analysis should also be provided to allow the NRC staff to make a determination that the testing or analysis was adequate and demonstrate that the environmental qualification envelopes the worst case accident conditions in the location where the equipment will be located for any event where the equipment is credited for mitigation. Additionally, the applicant or licensee should show why a single failure within the environmental control system, for any area in which safety system equipment is located, will not result in conditions that could result in damage to the safety system equipment, nor prevent the balance of the safety system not within the area from accomplishing its safety function. In this regard, the loss of a safety-related environmental control system is treated as a single failure that should not prevent the safety system from accomplishing its safety functions. Non safety-related environmental control systems should be assumed to fail.

Because the loss of environmental control systems does not usually result in prompt changes in environmental conditions, the design bases may rely upon monitoring environmental conditions and taking appropriate action to ensure that extremes in environmental conditions are maintained within non-damage limits until the environmental control systems are returned to normal operation. If such bases are used, the applicant/licensee should demonstrate that there is independence between environmental control systems and sensing systems that would indicate the failure or malfunctioning of environmental control systems.

Regulatory Guide 1.151 addresses review of mild environment qualifications. The reviewer should also confirm that the environmental protection of instrument sensing lines is addressed.

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

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

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

SRP Appendix 7.1-D subsection 5.4 provides additional guidance on environmental qualification of digital computers for use in safety systems.

D.9.4.2.5 IEEE 603-1991, Clause 5.5

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

The information provided should be sufficient for the NRC staff to conclude that adequate testing and analysis has been performed on the system as a whole and its components. This testing and analysis should be sufficient to demonstrate that the safety system complete its protective actions over the range of transient and steady-state conditions of both the power supply and the environment. Further, the test should demonstrate that if the system does fail, it fails in a safe state and failures detected by self-diagnostics should also place a protective function into a safe state.

D.9.4.2.6 IEEE 603-1991, Clause 5.6

Clause 5.6 requires independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design bases events, and (3) safety systems and other systems. Each case should be addressed with respect to physical, electrical, and communications independence.

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

SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence," provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety function of the redundant portions. Further, if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system must not be able to affect the functions of the safety system. Section D.7 and ISG-4 provide additional information on this topic.

D.9.4.2.6.1 IEEE 603-1991 Clause 5.6.1

Clause 5.6.1states that the safety systems shall be designed so that there is sufficient independence between redundant portions of a safety system such that the redundant portions are independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. SRP Chapter 7, Appendix 7.1-C does not provide any additional acceptance criteria beyond that in Clause 5.6.1. The information provided should demonstrate the independence between redundant portions of the safety system. Section D.7 and ISG-4 describes the requirements for demonstration of this independence.

D.9.4.2.6.2 IEEE 603-1991 Clause 5.6.2

Clause 5.6.2 states that the safety systems required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Clause 5.6.2 further states that equipment qualification in accordance with Clause 5.4 is one method that can be used to meet this requirement. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the degree of independence is sufficient.

D.9.4.2.6.3 IEEE 603-1991 Clause 5.6.3

Clause 5.6.3 states that the safety systems shall be designed such that credible failures in and consequential actions by other systems will not prevent the safety systems from meeting the requirements of this standard. This requirement is subdivided into requirements for interconnected equipment, equipment in proximity, and the effects of a

single random failure. Each of the sub-clauses will be addressed in the following paragraphs.

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

Clause 5.6.3.2 of IEEE 603, "Equipment in Proximity," states that equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, will be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment, and that physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Standard 384-1981. This clause further states that the physical barriers used to effect a safety system boundary shall meet the requirements of Clause 5.3, Clause 5.4, and Clause 5.5 for the applicable conditions specified in Clause 4.7 and Clause 4.8 of the design basis. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the degree of independence is sufficient.

Clause 5.6.3.3 of IEEE 603, "Effects of a Single Random Failure," requires that where a single random failure in a non-safety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. IEEE Std 379 provides additional guidance for the application of this requirement. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the degree of independence is sufficient.

D.9.4.2.7 IEEE 603-1991, Clause 5.7

Clause 5.7 requires the capability for testing and calibration. Guidance on periodic testing of the safety system is provided in RG 1.22, "Periodic Testing of Protection System Actuation Functions," and in RG 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems," which endorses IEEE Std. 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems." The extent of test and calibration capability provided bears heavily on whether the design meets the single-failure criterion. Any failure that is not detectable must be considered concurrently with any random postulated, detectable single failure. Periodic testing should duplicate, as closely as practical, the overall performance required of the safety system. The test should confirm operability of both the automatic and manual circuitry. The capability should be provided to permit testing during power

operation. When this capability can only be achieved by overlapping tests, the reviewer should confirm that the test scheme overlaps leave no gaps.

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

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

D.9.4.2.8 IEEE 603-1991, Clause 5.8

Clause 5.8 has four sub-clauses.

Clause 5.8.1 requires that display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions will be part of the safety systems and will meet the requirements of IEEE Std. 479-1981. The design should minimize the possibility of ambiguous indications that could confuse an operator.

Clause 5.8.2 requires that display instrumentation provide accurate, complete, and timely information pertinent to safety system status, and that this information shall include indication and identification of protective actions of the sense and command features and execute features. Further, the design should minimize the possibility of ambiguous indications that could confuse an operator.

Clause 5.8.3 requires that protective actions that have been bypassed or deliberately rendered inoperative for any other purpose be continuously indicated in the control room. Display instrumentation does not need to be considered a part of the safety system. The indication must be automatically actuated if the bypass or otherwise inoperative condition is expected to occur more frequently than once per year and is expected to occur when the affected system is required to be operable.

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

The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the four sub-clauses have been met.

D.9.4.2.9 IEEE 603-1991, Clause 5.9

Clause 5.9 requires that the safety system be designed to permit administrative control of access to the equipment. Administrative access limited to qualified plant personnel is

acceptable if done with the permission of the control room operator. The system should be designed with alarms and locks to preclude inappropriate access. Additionally, electronic access to the system (e.g., via a network connection) should be sufficiently restricted. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that Clause 5.9 has been met. The Cyber Security Review Area discusses this aspect in further detail.

D.9.4.2.10 IEEE 603-1991, Clause 5.10

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

D.9.4.2.11 IEEE 603-1991 Clause 5.11

Clause 5.11 requires that the safety system equipment be distinctly identified for each redundant portion of a safety system in accordance with IEEE Std. 384-1981 and IEEE Std. 420-1982. Further, the safety system equipment must be distinguishable from any identifying markings placed on the equipment for other purposes, that the identification methods not require the frequent use of reference materials (i.e., be "user friendly"), and that the associated documentation be distinctly identified in accordance with IEEE Std. 494-1974 (R1990). However, components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not, themselves, require identification. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the Clause 5.11 has been met.

D.9.4.2.12 IEEE 603-1991 Clause 5.12

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

The auxiliary supporting features need to be designed to the same high quality standards as the rest of the safety-related system, and the same demonstration that all requirements are being meet is required. In addition, ISG-4, Section 1, "Interdivisional Communications," Staff position 3 states that "Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system". In order to comply with this staff position, the licensee or vendor should demonstrate that any auxiliary supporting features are necessary to perform the safety function. If the licensee or vendor can not show that the supporting feature is needed, a detailed description of the feature, how it is designed and how it functions will be needed for the NRC staff to determine that having this feature will not compromise the safety or

functionality of the system. This detailed description may require the NRC staff to review actual schematics or software code to reach its conclusion.

D.8.4.2.13 IEEE 603-1991 Clause 5.13

Clause 5.13 requires that any shared structures, systems, or components between multi-unit generating stations be capable of simultaneously performing all required safety functions in any or all units. Guidance on the sharing of electrical power systems between units is contained in IEEE Std. 308-1980, and guidance on application of the single-failure criterion to shared systems is contained in IEEE Std. 379-1988. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the Clause 5.13 has been met.

D.8.4.2.14 IEEE 603-1991 Clause 5.14

Clause 5.14 requires that human factors be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operators can maintainers can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std. 1023-1988. The information provided should be sufficient to demonstrate that the guidance contained in ISG-5 has been met.

D.8.4.2.15 IEEE 603-1991 Clause 5.15

Clause 5.15 requires that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std. 352-1987 and IEEE Std. 577-1976 provide guidance for reliability analysis. To information provided should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed. For computer systems, both hardware and software should be included in this analysis. The NRC staff considers software that complies with the quality criteria of Clause 5.3, and that is used in safety systems that provide measures for defense against common-cause failures as described in Clause 5.1, to comply with the fundamental reliability requirements of GDC 21, IEEE Std. 279-1971, and IEEE Std. 603-1991.

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

The information provided should include a detailed Failure Modes and Effects Analysis and a reliability analysis in accordance with IEEE Standard 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety

Systems," and IEEE Standard 577-2004, "IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities."

D.9.4.3 IEEE 603-1991, Clause 6

Clause 6 of IEEE Std. 603-1991 provides the requirements for sensors and command features.

In addressing clauses 6.1 through 6.8, the additional considerations should be taken into account:

D.9.4.3.1 IEEE 603-1991 Clause 6.1

Clause 6.1 requires that for each design basis event, all protective actions should automatically initiate without operator action, with the exception of those justified in Clause 4.5. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the automatic initiation will be precise and reliable. The evaluation of this precision and reliability needs to address factors such as setpoints, margins, errors, and response times. Further, the evaluation should confirm that the functional requirements have been appropriately allocated into hardware and software requirements. The evaluation should confirm that the system's real-time performance is deterministic and known.

D.9.4.3.2 IEEE 603-1991 Clause 6.2

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

Clause 6.2 also requires implementation of manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4.10, with the information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators, in an environment suitable for the operator, and suitably arranged for operator surveillance and action. RG 1.62 provides further guidance on this topic.

It is important to note that this is different from a manual action which may be used as acceptable defense-in-depth required by BTP-19 as defense against common mode software failure. The manual initiation and indicators to tell the operator when to use this manual initiation required by this clause are required to be at a system level and safety-related manual controls and indications. These controls are not those used in the event of common cause software failure, and therefore these controls should be, but are not required to be independent and therefore downstream of the digital portion of the safety system. The SRM to SECY 93-087, as reflected in BTP-19, has the requirement for diverse automatic or manual controls in the event of a software CCF. These manual controls may be system level or component level, and may be non-safety, but need to be independent of any software CCF, and therefore downstream of any digital portion of the safety system. It is possible for one set of manual controls to meet both of these

requirements, by making those controls safety-related, system level, and downstream of any digital portion of the safety system.

D.9.4.3.3 IEEE 603-1991 Clause 6.3

Clause 6.3 requires that if a single credible event can both cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designed to provide principal protection against the condition, either alternate channel or alternate equipment not subject to this failure will be provided, or equipment not subject to failure caused by the same single credible event shall be provided. If the event of concern is a single failure of a sensing channel shared between control and protection functions, isolating the safety system from the sensing channel failure by providing additional redundancy or isolating the control system from the sensing channel failure by using data validation techniques to select a valid control input is acceptable. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that Clause 6.3 has been met. Additionally, the FMEA will likely contain information to address this clause.

D.9.4.3.4 IEEE 603-1991 Clause 6.4

Clause 6.4 requires that, to the extent feasible and practical, sense and command feature inputs be derived from signals that are direct measures of the desired variables as specified in the design basis. If indirect parameters are used, the indirect parameter must be shown to be a valid representation of the desired direct parameter for all events. Further, for both direct and indirect parameters, the characteristics of the instruments that product the safety system inputs, such as range, accuracy, resolution, response time, and sample rate. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the Clause 6.4 has been met.

D.9.4.3.5 IEEE 603-1991 Clause 6.5

Clause 6.5 requires that is must be possible to check, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation, including the availability of each sense and command feature required during the post-accident period. SRP Chapter 7, Appendix 7.1-C, Section 6.5, "Capability for Testing and Calibration," provides acceptance criteria for Clause 6.5. The information provided should confirm that the operational availability can be checked by varying the input to the sensor or by cross checking between redundant channels. Additionally, when only two channels of a readout are provided, the information provided must justify why is expected that an operator will not take incorrect action if the two channel readouts differ.

D.9.4.3.6 IEEE 603-1991 Clause 6.6

Clause 6.6 requires that if the applicable permissive condition are not met, a safety system must automatically prevent the activation of an operating bypass or initiate the appropriate safety function. Further, if plant conditions change such that an activated bypass is no longer permissible, the safety system must either remove the appropriate

active operating bypass, restore plant conditions to the permissive conditions, or initiate the appropriate safety functions. The requirement for automatic removal of operational bypasses means that the reactor operator may not have a role in such removal, however, the operator may take action to prevent the unnecessary initiation of a protective action. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the Clause 6.6 has been met.

D.9.4.3.7 IEEE 603-1991 Clause 6.7

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

D.9.4.3.8 IEEE 603-1991 Clause 6.8

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

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

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

D.9.4.4 IEEE 603-1991, Clause 7

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

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

D.9.4.4.1 IEEE 603-1991 Clause 7.1

Clause 7.1 requires that the safety system have the capability incorporated into the execute features to receive and act upon automatic control signals from the sense and command features consistent with Clause 4.4. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the Clause 7.1 been met.

D.9.4.4.2 IEEE 603-1991 Clause 7.2

Clause 7.2 requires that if manual control of any actuated component in the execute features is provided, the additional features needed to accomplish such manual control shall not defeat the requirements of Clauses 5.1 and 6.2, and that any capability to receive and act upon manual control signals from the sense and command features is consistent with the design basis. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the Clause 7.2 has been met.

D.9.4.4.3 IEEE 603-1991 Clause 7.3

Clause 7.3 requires that the design of the execute features be such that once initiated, the protective actions of the execute features shall go to completion. However, this requirement does not preclude the use of equipment protective devices identified in Clause 4.11 of the design basis or the provision for deliberate operator interventions. Additionally, when the sense and command features reset, the execute features shall not automatically return to normal, but shall require separate, deliberate operator action to be returned to normal. The information provided should include functional and logic diagrams. The NRC staff notes that the seal-in feature may incorporate a time delay as appropriate for the safety function. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the Clause 7.3 has been met.

D.9.4.4.4 IEEE 603-1991 Clause 7.4

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

D.9.4.4.5 IEEE 603-1991 Clause 7.5

Clause 7.5 contains similar requirements as Clause 6.7, but also requires that portions of the execute features with a degree of redundancy of one must be designed such that when a portion is placed in maintenance bypass, the remaining portions provide acceptable reliability. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to determine that the Clause 7.5 has been met.

D.9.4.5 IEEE 603-1991, Clause 8

Clause 8 of IEEE Std. 603-1991 provides the requirements for the power sources supporting the digital I&C system. Clause 8 requires that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of IEEE 603-1991 and are considered a portion of

the safety systems. Clauses 8.1 and 8.2 apply the requirements of IEEE 603-1991 to electrical and non-electrical power sources, respectively.

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

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

D.9.5 Conclusion

The NRC staff has reviewed the licensee's submittal against the requirements of IEEE 603-1991 and finds that the proposed implementation of meets the standard. Therefore, the NRC staff finds the proposed digital I&C upgrade to be acceptable with respect to IEEE 603-1991 and 10 CFR 50.55a(h)(2).

D.10 IEEE 7-4.3.2 Compliance

D.10.1Scope of Review

D.10.2Information to be Provided

D.10.3Regulatory Evaluation

While compliance with IEEE Std. 7-4.3.2 is not required by regulation, it is a de-facto standard used by the NRC staff in evaluating digital I&C upgrades. Where a licensee wishes to demonstrate compliance with another standard in lieu of IEEE Std. 7-4.3.2, the licensee must include an evaluation that allows the NRC staff to conclude that adherence provides reasonable assurance of a *high quality system.* This activity should be expected to require a significant amount of additional review time and effort.

D.10.4Technical Evaluation

D.10.5Conclusion

D.11 Technical Specifications

D.11.1Scope of Review

The scope of review includes the information necessary to ensure compliance with 10 CFR 50.36.

As discussed previously, the complex nature of digital I&C systems allows for individual channels to be aware of other channels and system functions. This abillty has the potential to obviate the need for some of the Surveillance Requirements (SRs) classically associated with I&C. Specifically, the need for channel checks, channel calibrations, etc, may no longer be necessary if these functions can be performed internally by the digital I&C system. While utilization of digital I&C systems may allow

the deletion of some existing SRs, those that are necessary to assure that the quality of the system and its components is maintained need to be maintained or proposed for addition to the TSs.

Additionally, if a licensee anticipates a later need to make changes to the digital I&C programming or system settings without prior NRC approval, it may be necessary for the appropriate developmental methodologies to be references in the administrative section of the TSs.

D.11.2Information to be Provided

In addition to a marked up copy of the TSs, the licensee should provide a justification for each change. This includes a detailed basis for how the digital I&C system internally accomplishes each SR proposed for deletion and what verification is accomplished for each SR proposed for addition. These justifications, taken together, should demonstrate that the proposed TSs provide sufficient limits such that the digital I&C system will be able to maintain safe operation of the facility with respect to its associated functions.

D.11.3Regulatory Evaluation

10 CFR 50.36(c)(2)(i) states that limiting conditions for operation (LCO) are the lowest functional capability or performance levels of equipment required for safe operation of the facility. When a LCO of a nuclear reactor is not met, the licensee shall shut down the reactor of follow any remedial action permitted by the technical specifications until the condition can be met. A limiting condition for operation needs to be established for anything that meets one or more of the four criterion given in 10 CFR 50.36(c)(2)(ii).

10 CFR 50.36(c)(3) states that the TSs must contain SRs relating to test, calibration, or inspection to assure the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met.

10 CFR 50.36(c)(5) states that administrative controls are the provisions relating to organization and management, procedures, recordkeeping, review and audit, and reporting necessary to assure operation of the facility in a safe manner.

D.11.4Technical Evaluation

The Technical Specification LCOs being proposed for deletion are evaluated against the four criterion of 10 CFR 50.36(d)(2)(ii). If none of the criterion are met, the LCO may be deleted. Additionally, the LCOs being proposed for addition should be to ensure that they adequately define the lowest functional capability or performance levels of the system required for safe operation of the facility. This review includes the adequacy of the proposed LCOs and the potential need for additional ones not proposed for addition to the TSs.

The SRs associated with the LCOs that will govern system operation should be sufficient to test, calibrate, and inspect the system and its functions such that the necessary quality of the system is assured. As with the review of the LCOs, this should evaluate those SRs proposed and the need for additional ones.

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

D.11.5Conclusion

The NRC staff has reviewed the proposed TS changes associated with the implementation of the digital I&C system and finds that the LCOs and SRs that will govern the operations, test, and maintenance of the digital I&C system are adequate to reasonably assure that the system will perform its design function. Additionally, the NRC staff finds that the appropriate methodologies have been proposed for incorporation into the administrative section of the TSs. Therefore, the NRC staff finds the proposed digital I&C upgrade to be acceptable with respect to technical specifications.

D.12 Cyber Security

D.12.1Scope of Review

Cyber Security will be addressed following the issuance of separate NRC guidance on this issue.

D.12.2Information to be Provided

D.12.3Regulatory Evaluation

D.12.4Technical Evaluation

D.12.5Conclusion

MEMORANDUM TO: [NAME], Director
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

[NAME], Director
Division of Engineering
Office of Nuclear Reactor Regulation

FROM: [NAME], Project Manager
Plant Licensing Branch [X-X]
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

SUBJECT: SUMMARY OF [MONTH DAY, YEAR], CATEGORY 1 PUBLIC MEETING TO DISCUSS [LICENSEE] PLANS TO REQUEST NRC APPROVAL OF A DIGITAL I&C UPGRADE OF [SYSTEM] USING [PLATFORM]

On [DATE], the Nuclear Regulatory Commission (NRC) staff conducted a Category 1 public meeting to discuss [LICENSEE]'s plans for upgrading the [PLANT] [SYSTEM] to the [PLATFORM] digital instrumentation and control (I&C) system.

The purpose of this meeting was to discuss the initial design concepts and any site specific issues identified by [LICENSEE]. These discussions focused on the how [LICENSEE] will address the review area of defense-in-depth and diversity.

In these discussions, the licensee identified the following characteristics and design specifications that contribute to the [PLATFORM]s diversity and robustness against common cause failure (CCF).

- Item 1
- Item 2...

The NRC staff provided feedback to [LICENSEE] that the following aspects of the design seemed conducive to finding the proposed upgrade consistent with the NRC staff's position on defense-in-depth and diversity:

- Item 1
- Item 2...

Additionally, the NRC staff identified that the following aspects of the design would require additional review before finding the proposed upgrade fully consistent with the NRC staff's position on defense-in-depth and diversity:

- Item 1
- Item 2...

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

Appendix B

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

Tier			Document to be submitted with LAR
1	2	3	
	X	X	Commercial Grade Dedication Plan
X	X	X	D3 analysis
X	X	X	System description (Sufficient to determine ISG-4 compliance)
X	X	X	Design Analysis Report
	X	X	Design Report on Computer Integrity, Test and Calibration, and Fault Detection
	X	X	Theory of Operation Description
	X	X	Equipment Qualification Testing Plans (Including EMI, Temperature, Humidity, and Seismic to the degree to which these are affected by the plant specific application)
	X	X	Software QA Plan and Procedures
X	X	X	System Description (To block diagram level)
X	X	X	Hardware and Software Architecture Descriptions
	X	X	Preliminary FMEA
		X	Quality Assurance Plan for digital hardware and software
X	X	X	Preliminary reliability analysis
X	X	X	Safety analysis
X	X	X	System requirements specification
X	X	X	System test plan
		X	Vendor software plan
X	X	X	Software design specification
	X	X	Software development plan
X		X	Software installation plan
		X	Software integration plan
X	X		Software maintenance plan
		X	Software management plan
X	X		Software operation plan
X		X	Software project risk management program
		X	Platform software requirements specification (Platform specific)
X	X	X	Application software requirements specification (Plant Specific)
X	X	X	Software safety plan
X	X	X	Software test plan
	X	X	Software tool verification program
X	X		Software training plan
	X	X	Software V&V plan and procedures
X	X	X	Requirement traceability matrix

Tier			Document to be submitted 12 months prior to requested approval date
1	2	3	
	X	X	Commercial Grade Dedication Report
	X	X	Commercial grade dedication procedures
		X	Final configuration lists
		X	Final configuration tables
X	X	X	Final design description
	X	X	Final FMEA
X	X	X	Final logic diagrams
X	X	X	Final reliability analysis
	X	X	Final report on acceptance of commercial grade dedication
X	X	X	Final system configuration documentation
X	X	X	Final factory acceptance test reports
X	X	X	Installation test plans and procedures
X			Operation manuals
	X	X	Qualification test procedures
		X	Quality assurance procedures for digital hardware and software
	X	X	Summary of final EMI, temperature, humidity, and seismic testing results
X	X	X	Summary of test results (Including FAT)
X	X	X	System test procedures
	X	X	Software management implementing procedures
X	X	X	Software project risk management report
X	X	X	Software test procedures
	X	X	Software tool analysis report
X	X	X	V&V reports

Tier			Document to available for audit
1	2	3	
X	X	X	Completed factory acceptance test procedure and results
X	X	X	Configuration management reports
X	X	X	Detailed system and hardware drawings
X	X	X	Final circuit schematics
X	X	X	Final software integration report
X	X	X	Individual completed test procedures and reports
X	X	X	Individual V&V problem reports up to FAT
X			Maintenance manuals
X			Operations procedures
X	X	X	Software code listings
			Training manuals & course material
X	X	X	Vendor build documentation

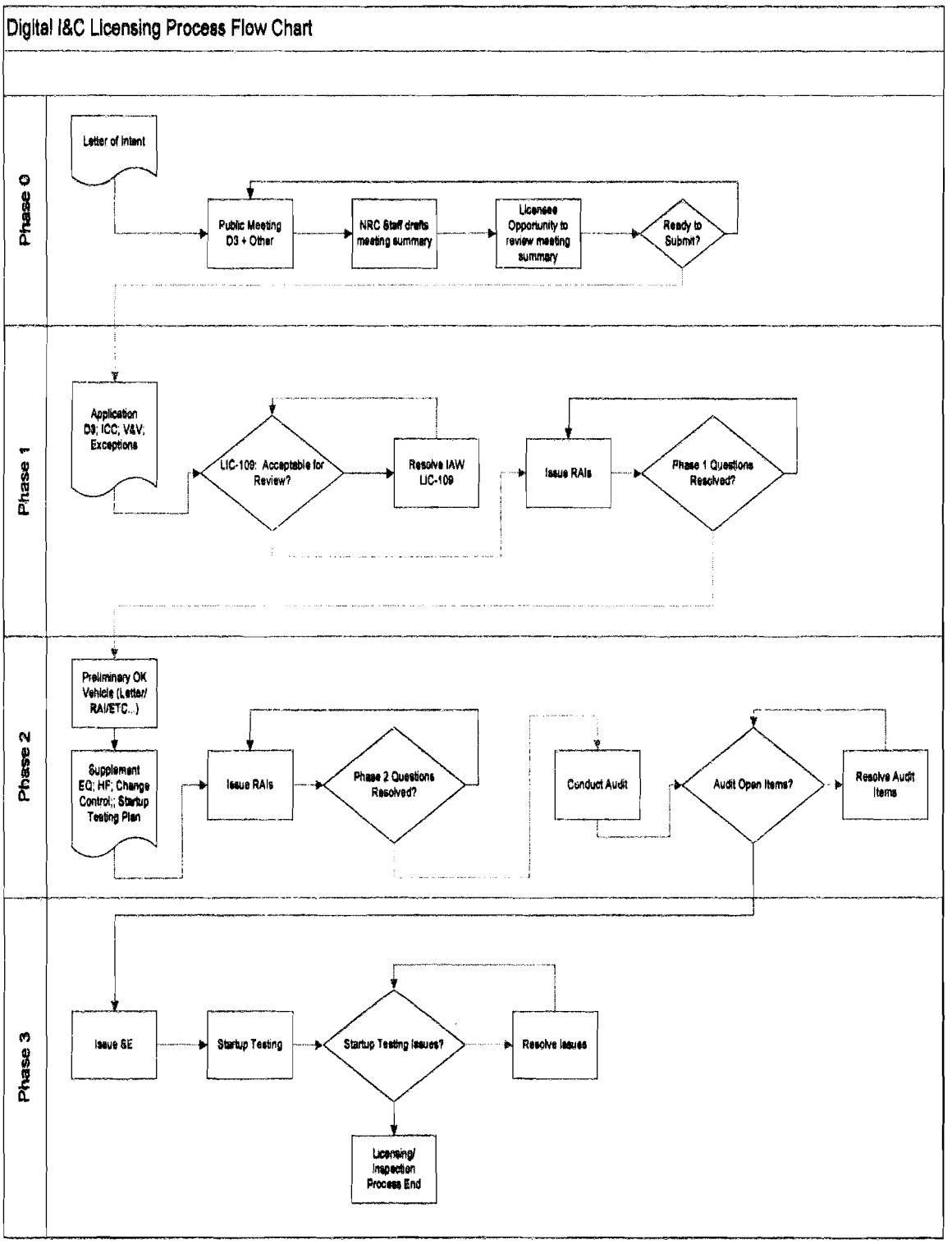


FIGURE 1, "Process Flow Chart"

location, and interested members of the public are encouraged to participate in this meeting via a toll-free teleconference. For details, please email the NRC meeting contact by Thursday, June 25, 2009.

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

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

NRC	Industry
W. Kemper, NRR	G. Clefton, NEI
L. James, NRR	M. Schoppman, NEI
E. Miller, NRR	

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

Project No. 689

Enclosures:
1. Agenda
2. Draft Interim Staff Guidance 6

cc w/encl: See next page
DISTRIBUTION:
PUBLIC
RidsAcrsAcnw_MailCTR Resource
RidsNrrDorl Resource
RidsNrrDorlLpl1-2 Resource
RidsNrrDorlLpl2-2 Resource
RidsNrrDorlLpl3-2 Resource
RidsNrrPMEMiller
RidsOgcMailCenter Resource
RidsRgn1MailCenter Resource
RidsRgn3MailCenter Resource
L. Trocine, EDO R-I & R III
S. Williams, EDO R-IV
R. Hannah, OPA R-II
V. Dricks OPA RIV
L. James, NRR
PMNS Resource
TWFN Receptionist
am@nei.org
jhr@nei.org
mas@nei.org
LPL1-2 R/F
RidsNrrAdro Resource
RidsNrrDorlLpl1-1 Resource
RidsNrrDorlLpl2-1 Resource
RidsNrrDorlLpl3-1 Resource
RidsNrrDorlLpl4 Resource
RidsNrrLAABaxter Resource
RidsOpaMail Resource
RidsRgn2MailCenter Resource
RidsRgn4MailCenter Resource
J. Adams EDO R-II
D. Screnci, OPA R-I
V. Mitlyng, OPA R-III
S. Bailey, NRR
J. Wermiel, NRR
OWFN Receptionist
C. Tucci, NRR
gac@nei.org
W. Kemper, NRR
S. Burnell, OPA

ADAMS Accession Number: ML091540780

OFFICE	LPLI-2/PM	LPLI-2/LA	LPLIII-1/BC
NAME	GEMiller	ABaxter	LJames
DATE	6/18/09	6/10/09	6/18/09

OFFICIAL RECORD COPY