



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

NEW

Section 7.0. Instrumentation and Controls — Overview of Review Process

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Introduction

Chapter 7 of the SRP provides guidance for review of the instrumentation and control (I&C) portions of (1) applications for nuclear reactor licenses or permits and (2) amendments to existing licenses. The SRP guidance may also be applied in the review of topical reports submitted to NRC for safety evaluation, especially reports requesting generic acceptance of systems or components that may be used in nuclear power plant I&C systems. For an overview of the purpose, content, and use of the SRP in general refer to the introductory section of the SRP.

Section 7.0 provides an overview of the process used by HICB staff to review both the I&C portion of license applications and the I&C portions of generic safety evaluations of specific topics. Guidance is provided to the reviewer in applying Chapter 7 of the SRP to these reviews.

Figure 7.0-1 provides an overview of the HICB review process. Each of the reviewer activities shown in this figure is discussed below. Ideally, applicants will request that the Staff's review begin during the early stages

Rev. 4 —June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

of the development life cycle. Early interaction with the applicant is important so that differences between the Staff and the applicant may be identified as early as possible. The Staff should work with the applicant to expeditiously resolve these issues in order to minimize the impact upon design and implementation activities. Early resolution of fundamental issues minimizes the rework necessary in areas where changes to the design bases are needed to resolve Staff concerns. This helps to assure that the changes are correctly propagated through the design effort, thus improving the Staff's confidence in design quality.

II. Application Types

The type of application under review largely determines the review activities to be conducted and impacts the complexity and scope of the review. NRC regulations provide for the following types of license applications relevant to nuclear power reactors.

1. *Construction permits (CPs)* as discussed in 10 CFR 50.10(b) and 10 CFR 50.23. An application for a construction permit must be accompanied by a preliminary safety analysis report (PSAR). Construction permit applications may be submitted for construction of a new facility or alteration of an existing facility.
2. *Operating license (OL) applications* as discussed in 10 CFR 50.21 and 50.22. Operating license applications must be accompanied by a final safety analysis report (FSAR) and proposed technical specifications.
3. *Early site permits*, or early site permit renewal as discussed in 10 CFR 52, Subpart A. HICB will not normally be involved in the review of early site permit applications.
4. *Standard design certifications (DCs)* as discussed in 10 CFR 52, Subpart B. Applications for standard design certification are accompanied by a safety analysis report (SAR) and certified design material.
5. *Renewal of standard design certification* as discussed in 10 CFR 52.57. Applications for renewal of standard design certifications will not be submitted before the year 2007; therefore, Section 7.0 does not address these reviews.
6. *Combined licenses (CLs)* as discussed in 10 CFR 52, Subpart C. Combined license applications will be accompanied by an FSAR, plant-specific technical specifications, and plant-specific inspections, tests, analyses and acceptance criteria (ITAAC).
7. *Amendments to existing operating licenses, construction permits, or combined licenses* as discussed in 10 CFR 50.90 and 10 CFR 50.59(c). (Note that these sections apply to changes to combined licenses by the provisions of 10 CFR 52.83.) Amendments to existing licenses or permits must be accompanied by supporting information and proposed technical specification changes.
8. *Manufacturing licenses* as discussed in 10 CFR 52, Appendix M. Section 7.0 does not address review of manufacturing license applications.
9. *Review of standard designs, or major portions thereof* as discussed in 10 CFR 52 Appendix O. Applications for review of standard designs are typically accompanied by one or more topical reports describing the design.

10. *License renewal* as discussed in 10 CFR 54. HICB will not normally be involved in the review of license renewal applications.

11. *Topical reports* may be submitted to obtain NRC review of specific proposals independent of an application for a license or license amendment. For example, systems, components, or operational practices that are being considered for use in multiple plants may be submitted for generic review.

III. Review Scope and Contents

The reviewer should determine the scope of the review needed to support evaluation of the application. The scope of the review will impact the information needed by the reviewer and the extent of review planning.

Regardless of the type of application under consideration, the fundamental purpose of the NRC review is to determine whether the facility and equipment, the proposed use of the equipment, the operating procedures, the processes to be performed, and other technical requirements provide reasonable assurance that the applicant/licensee will comply with the regulations of 10 CFR Chapter I, and that public health and safety will be protected.

It is not intended that the review, audit, or inspection activities by the reviewer completely evaluate all aspects of the design and implementation of the I&C system. The review scope needs only to be sufficient to allow the reviewer to reach the conclusion of reasonable assurance described above.

Subject to compliance with existing license commitments, compliance with current applicable regulations, and protection of the public health and safety, the HICB review may consider and use previous interpretations of the regulations as they apply to the application being reviewed. The scope of review includes those I&C systems that are identified as substantially identical to systems that have been previously reviewed and approved by the staff. The evaluation of these systems in subsequent sections of Chapter 7 may be based upon prior Staff approval. If any aspect of a design is not identical to that which is referenced, an evaluation must be made to address the adequacy of the different design. Conclusions drawn from this review must be included in the safety evaluation report.

Figure 7.0-2 illustrates the life cycle for any I&C system, and relates the application types described below to the life-cycle activities that should be addressed by the application. The review of any application should involve all the applicable life-cycle activities. Reviews should confirm the acceptability of system requirements and the adequacy with which the final system meets these requirements. Review of non-digital computer-based system implementation may focus on component and system requirements, design outputs, and validation (e.g., type testing). Review of computer-based systems should focus on confirming the acceptability and correct implementation of the life-cycle activities.

Section 7.1 discusses the review of the overall I&C system concept and generic system requirements. Appendices 7.1-A, 7.1-B, and 7.1-C discuss the review procedures for each acceptance criterion relevant to I&C systems. Sections 7.2 through 7.9 describe the review of system-specific requirements, system design, and implementation. For computer-based systems or components with embedded computers, Appendix 7.0-A describes a generic process for reviewing the unique aspects of computer-based systems, including hardware/software integration. The appendices to Sections 7.0 and 7.1 are to be used in conjunction with Sections 7.1 through 7.9.

The HICB review of each life-cycle activity should address the review points covered in Sections III.A and III.B. The Staff's review emphasis should be commensurate with the safety significance of the given system

or aspect of a system's design under review. Probabilistic risk assessments (PRAs), such as those conducted under the Individual Plant Evaluation program or required as part of applications under 10 CFR 52, provide information that may prove helpful in determining the appropriate level of review. Review scope should be coordinated with secondary review branches as discussed in Section V below.

The review considers material that is formally submitted for the docket, provided informally for Staff consideration, and material that is available for audit at the applicant's site.

HICB reviewers should be familiar with all sections of the SAR that have a bearing on the I&C systems under review. The following SAR sections are typically relevant to the review of I&C systems.

Chapter 1	For familiarization with the general operation of the plant, both safety and non-safety aspects.
Chapter 2	For familiarization with environmental conditions and natural phenomena hazards that could affect I&C systems.
Chapter 3	For a general understanding of the principal architectural and engineering designs of those structures, components, equipment, and systems important to safety.
Section 3.1	For exceptions to criteria applicable to the I&C control systems, and for structures suitable for housing this equipment.
Section 3.10 and 3.11	For an understanding of the seismic and environmental qualification program for I&C sections control system components.
Chap. 4 & 5	For an understanding of the reactor and the reactor coolant system and its interconnections with the ESF systems.
Chapter 6	For the design bases, design features, and functional performance requirements of the ESF systems.
Chapter 8	For an understanding of the electrical power systems.
Chapter 9	For the design bases, design features, and functional performance requirements of essential auxiliary support (EAS) systems.
Chapter 10	For an understanding of the steam and power conversion systems and their interconnections with the I&C systems.
Chapter 12	For an understanding of radiation monitoring systems and their interaction with the I&C systems addressed in Chapter 7.
Chapter 14	For an understanding of the initial test program and its role in verification and validation of I&C systems. For applications made under 10 CFR 52, HICB will also participate in the review of ITAAC as described in Chapter 14.
Chapter 15	For a description of accidents for which the I&C system actuates or controls protective functions, the effects of failures of the protective functions, and the assumptions and initial conditions that form the bases of the accident analyses.

- Chapter 16 For the proposed limiting conditions for operation and surveillance requirements for the I&C systems.
- Chapter 17 For an understanding of Quality Assurance activities during design and construction and the role QA plays in the engineering life cycle for I&C systems.
- Chapter 18 For the human factors considerations in the design of I&C control system user interfaces.
- Chapter 19 For a discussion of the contribution to risk of the I&C control systems in the probabilistic risk assessment and the insights into I&C control system design features derived from that assessment.

III.A Design Certification or Construction Permit Applications

The review scope for design certification or construction permit applications should include evaluation of the system concept, system requirements, system design, and plans for implementing the system design.

System Concept Evaluation

The system concept evaluation should be based on the following review points:

1. The overall I&C system design's relationship to both the functions required by 10 CFR 50 and the functions required to support the assumptions of the plant accident analysis. (See Section 7.1.)
2. The adequacy of any research and development plan necessary to resolve any outstanding questions concerning the design of systems or components.
3. Compliance with the technically relevant portions of 10 CFR 50. (See Section 7.1.)
4. Proposed resolution of technically relevant unresolved safety issues and medium- and high-priority generic safety issues identified more than six months prior to the application. (See SRP Chapter 20.)

System Requirements Evaluation

The system requirements evaluation should be based on the following review points:

1. Principal design criteria with respect to the guidance of 10 CFR 50.55a(h) (ANSI/IEEE Std 279¹) and 10 CFR 50, Appendix A. (See Section 7.1.)
2. The design bases, including functional design requirements, and the relationship of the design bases to the principle design criteria. (See Sections 7.2 through 7.9.)

¹IEEE Std 603 is an alternative to ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," which is no longer an active standard. The current version of this standard is IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations."

The following additional review points apply to applications under 10 CFR 52 only:

3. Inspections, tests, analyses and acceptance criteria (ITAAC) proposed to provide reasonable assurance that, if the inspections, tests, and analyses are performed, the acceptance criteria are met, and a plant is built according to the design, then the plant will operate in accordance with the design certification. SRP Section 14.3 describes the general acceptance criteria and review procedures for ITAAC. Section 14.3.5 describes the specific acceptance criteria and review procedures for I&C system ITAAC.
4. The interface requirements and a representative conceptual design for those portions of the plant not included in the design certification application. (See Sections 7.2 through 7.9.)

System Design Evaluation

The system design evaluation should be based on the following review points:

1. The key characteristics, performance requirements, general arrangements, and materials of construction of the systems to confirm that there is reasonable assurance the final design will conform to the design bases with adequate margin for safety. (See Sections 7.2 through 7.9.)
2. The identification of I&C functions and variables to be probable subjects of technical specifications for the facility. (See Sections 7.2 through 7.9.)
3. Proposed technical specifications (Technical Specifications Branch (TSB) has lead responsibility. See SRP Chapter 16.)
4. The applicant/licensee's analysis and technical justification to show that the I&C system design, including the underlying design bases and performance requirements, can perform appropriate safety functions.

Hardware and Software Planning Evaluation

The evaluation should include reviewing plans for the implementation and overall management of system development, quality assurance, integration, installation, maintenance, training, operations, safety analysis, verification and validation, and configuration management. (See Appendix 7.0-A.)

Note: Review of design certification applications should extend to cover detailed design. However, for digital computer-based I&C systems, it may be premature to complete final design details at the design certification (DC) stage. Waiting until the combined license (CL) stage to complete the final design of such systems will allow the CL applicant/licensee to use the most recent technology for each plant. Therefore, the review of DC applications for digital computer-based I&C may be limited to (1) a detailed review at the functional block diagram level, (2) a review of the applicant/licensee's commitment to prescribed limits, parameters, procedures, and attributes for the detailed design process, and (3) ITAAC adequate to demonstrate that the as-built facility conforms to these commitments. Branch technical position (BTP) HICB-16 provides guidance for use in judging the completeness of a DC application where the applicant/licensee proposes to wait until the CL stage to complete the final design of digital computer-based I&C systems.

III.B Operating License and Combined License Applications

For operating license and CL applications, normally the NRC will have reviewed the items discussed in Section III.A above and issued a safety evaluation report (SER) based upon that review. Therefore, NRC review at the OL and CL stage is confined to the following items and changes to commitments made at the construction-permit or design-certification stage.

Hardware and Software Requirements, Detailed Design, Fabrication, Test, and Integration Evaluation

The hardware and software requirements, detailed design, fabrication, test, and integration evaluation should be based on the following review points:

1. Implementation of development plans. (See Appendix 7.0-A.)
2. Conformance of design outputs with system requirements. (See Sections 7.2-7.9 and Appendix 7.0-A.)
3. Evidence of design process characteristics in design outputs. (See Appendix 7.0-A.)
4. The description and evaluation of the results of the applicant/licensee's research and development to demonstrate that any safety questions identified at the CP stage have been resolved. (See Section 7.2 through 7.9 and Appendix 7.0-A.)

System Validation Evaluation

The system validation evaluation should be based on the following review points:

1. The applicant/licensee's testing, analysis, and technical justification to show that I&C system design, including the underlying design bases and performance requirements, can perform appropriate safety functions. (See Section 7.2 through 7.9 and Appendix 7.0-A.)

The following additional review points apply only to CL applications:

2. The applicant/licensee's demonstration of compliance with interface requirements, for applications referencing a certified standard design.
3. ITAAC proposed to provide reasonable assurance that, if the inspections, tests, and analyses are performed, the acceptance criteria met, and a plant is built according to the design, then the plant will operate in accordance with the design certification. (Applications that reference a certified standard design must apply the certified design ITAAC to those portions of the facility covered under the DC.) (See SRP Chapter 14.)

Installation, Operations, and Maintenance Evaluation

The installation, operations, and maintenance evaluation should be based on the following review points:

1. Site visit. (See Appendix 7-B.)

The following additional review point applies only to CL applications:

2. Implementation of ITAAC. (See SRP Chapter 14.)

III.C License Amendments and Topical Reports

The scope of license amendment applications and topical reports is highly variable. The reviewer should develop an application-specific review scope for the item under consideration. All of the points discussed above that are relevant to the application under consideration should be considered.

Regardless of the review scope, the reviewer should examine Section 7.1 and Table 7.1-1 to identify the SRP sections, BTPs, and acceptance criteria applicable to the application. If the application involves the use of digital computer-based I&C systems or computers embedded in systems or components, the review process of Appendix 7.0-A also applies.

IV. Acceptability of Applications

Before substantial review effort is expended, the reviewer should confirm that the application contains enough information to allow the review to begin and to substantially progress. Table 7.0-1 below identifies the acceptance criteria for the various types of applications and the guidance that may be used in assessing acceptability. Detailed guidance on the specific I&C system information that an application should contain may be found in Reg. Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants," each applicable SRP section, the "Information to be Reviewed" sections of each applicable BTP, and SRP Appendix 7.0-A. BTP HICB-16 and SRP Chapter 14 contain additional information on the material that should be contained in an application for standard design certification under the provisions of 10 CFR 52.

Table 7.0-1. Acceptance Criteria for Applications

Type of Application	Acceptance Criteria
Construction Permit	10 CFR 50.34(a)
Operating License	10 CFR 50.34(b) and (f)
Standard Design Certification	10 CFR 52.47
Combined License	10 CFR 52.79
Manufacturing License	10 CFR 50.34(a)
Topical Report	Depends upon scope
License Amendment	10 CFR 50.90
Design Certification Renewal	10 CFR 52.57(a)

V. Application-Specific Review Plan

The reviewer should develop a review plan specific to the application under consideration. The purpose of the plan is to (1) communicate planned activities and schedules to management, (2) identify, early in the review, resources that the reviewer needs to support the review, and (3) ensure that review participants have a common understanding of review criteria and the roles of the individual reviewers.

Scope

The plan should briefly describe what is to be reviewed as determined in Section III above.

Review Criteria

The plan should identify the criteria against which the application will be evaluated. For new applications, the applicable criteria will normally be the applicable CFR sections and the detailed acceptance criteria contained in the SRP, supporting BTPs, and regulatory guides. Safety evaluation reports for previous applications, topical reports, and unreviewed or generic safety issue closeouts are also useful sources of information about Staff positions and interpretations that can be used to develop specific review criteria.

For license amendment applications, the review criteria will consist of original license commitments. Where the original license commitments do not completely cover all aspects of the proposed modification, the Staff may supplement the original commitments with additional criteria from the SRP.

Review Activities

The plan should describe the review activities planned to accomplish the review, and the approximate order in which these activities will be performed. Activities that have a broad impact on the review, such as the review of commitments to codes and standards or the defense-in-depth and diversity review, should occur early in the review process.

Review activities should give particular emphasis to the review of functional design requirements, as errors at this level impact all successive aspects of the system design.

For each activity, the plan should identify the approximate resources required (e.g., number of staff-weeks, access to detailed design documents, access to completed hardware), the approximate start and finish dates, and the external meetings or audits anticipated as part of the activity. The goals of the external meetings and audits that will be part of the review activities should be defined.

Review Assignments

NRC staff and contractors who will participate in the review should be named, and their roles defined with respect to the review activities.

Interfaces

The plan should identify interfaces with other NRC organizations such as the project manager, regional offices, other technical branches, and applicant/licensee personnel. The plan should describe the actions and information that the HICB needs from each organization and include a schedule showing when each item is to be delivered. Likewise, the plan should also identify the information and actions the interfacing organizations

need from HICB and include a schedule showing when these items will be needed. The plan should identify meetings and site trips as necessary. Schedule information may be absolute (a specific date) or relative (time before or after some milestone). The plan should address time required for requests for additional information (RAIs) and iterations of reviews.

HICB will coordinate with other NRC technical branches in the review of the following I&C system design features:

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

The coordinated reviews include the following:

- The Reactor Systems Branch (SRXB) evaluates the adequacy of protective, control, display, and interlock functions and confirms that they are consistent with the accident analysis, the operating requirements of the I&C systems, and the requirements of GDC 10, 15, 28, 33, 34, and 35.
- The Plant Systems Branch (SPLB) evaluates the adequacy of the requirements for the EAS systems to ensure the EAS systems satisfy the applicable acceptance criteria. These systems include compressed (instrument) air, cooling water, boration, lighting, heating, and air conditioning. This review confirms that (1) the design of the EAS systems is compatible with the single-failure requirements of the I&C systems and (2) the EAS systems will maintain the required environmental conditions in the areas containing I&C equipment. This review includes the design criteria and testing methods employed in the seismic design and installation of EAS equipment. SPLB also evaluates the adequacy of protective, control, display, and interlock functions, and confirms that they are consistent with the operating requirements of the supported system and the requirements of GDC 41 and 44.
- The Containment Systems and Severe Accident Branch (SCSB) reviews the containment ventilation and atmospheric control systems provided to maintain required environmental conditions for electrical and instrumentation equipment located inside containment. SCSB also evaluates the adequacy of protective, control, display, and interlock functions associated with containment systems and severe accidents, and confirms they are consistent with the accident analysis, operating requirements, and GDC 16 and 38.
- The Electrical Engineering Branch (EELB) (1) evaluates the adequacy of physical separation criteria for cabling and electrical power equipment, (2) determines that power supplied to redundant systems is supplied by appropriate redundant sources, and (3) confirms the adequacy of the instrumentation and controls associated with the proper functioning of the onsite and offsite power systems. EELB also reviews the environmental qualification of I&C equipment. The scope of this review includes the design criteria and qualification testing methods and procedures for I&C equipment.
- The Mechanical Engineering Branch (EMEB) reviews the seismic qualification demonstration for I&C equipment including the design criteria and qualification testing methods and procedures.

- The Human Factors Assessment Branch (HHFB) evaluates the adequacy of the arrangement and location of instrumentation and controls, and confirms that the capabilities of the instrumentation and controls are consistent with the operating procedures and emergency response guides.
- The Quality Assurance and Maintenance Branch (HQMB) reviews the adequacy of administrative, maintenance, testing, and operating procedure programs as part of its primary review responsibility for SRP Sections 13.5.1.2 and 13.5.2.2. The reviews of design, construction, and operations phase quality assurance programs, including the general methods for addressing periodic testing, maintenance, and reliability assurance, are also coordinated and performed by the HQMB as part of its primary review responsibility for SRP Chapter 17. HQMB also reviews the proposed preoperational and startup test programs to confirm that they are in conformance with the intent of Regulatory Guide 1.68 as part of its primary review responsibility for SRP Section 14.2.

For design certification or combined license applications made under 10 CFR 52, proposed or completed inspections, tests, analyses, and acceptance criteria (ITAAC) are reviewed by HICB as part of its review responsibility for SRP Section 14.3.5.

VI. Review

The review is to be accomplished in accordance with the application-specific review plan using the acceptance criteria and review processes of the SRP. The review will be documented by the preparation of an SER.

VII. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

IEEE Std 603-1991. "Criteria for Safety Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.70. "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants."
Office of Standards Development, U.S. Nuclear Regulatory Commission, November 1978.

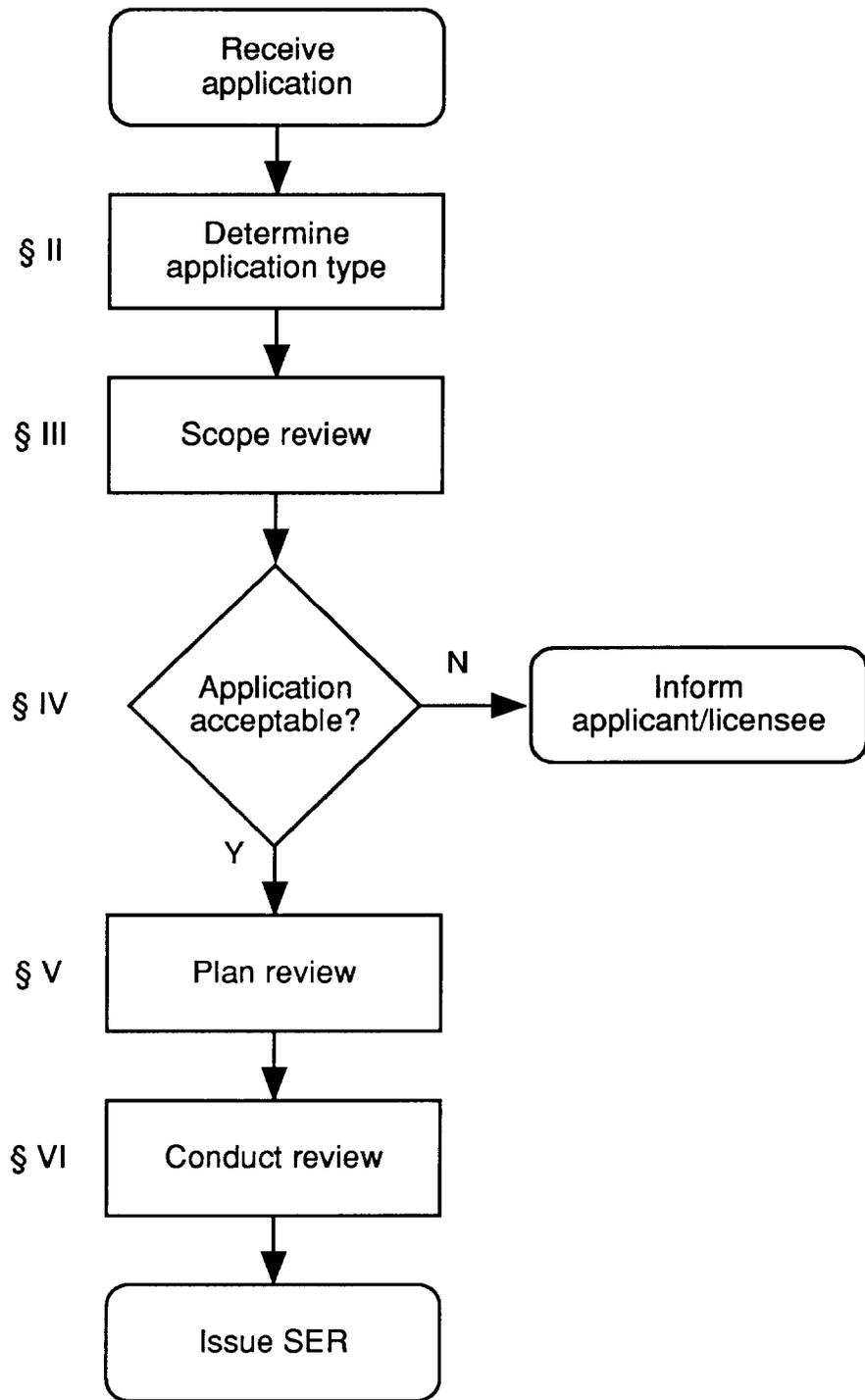


Figure 7.0-1 Overview of Review Process

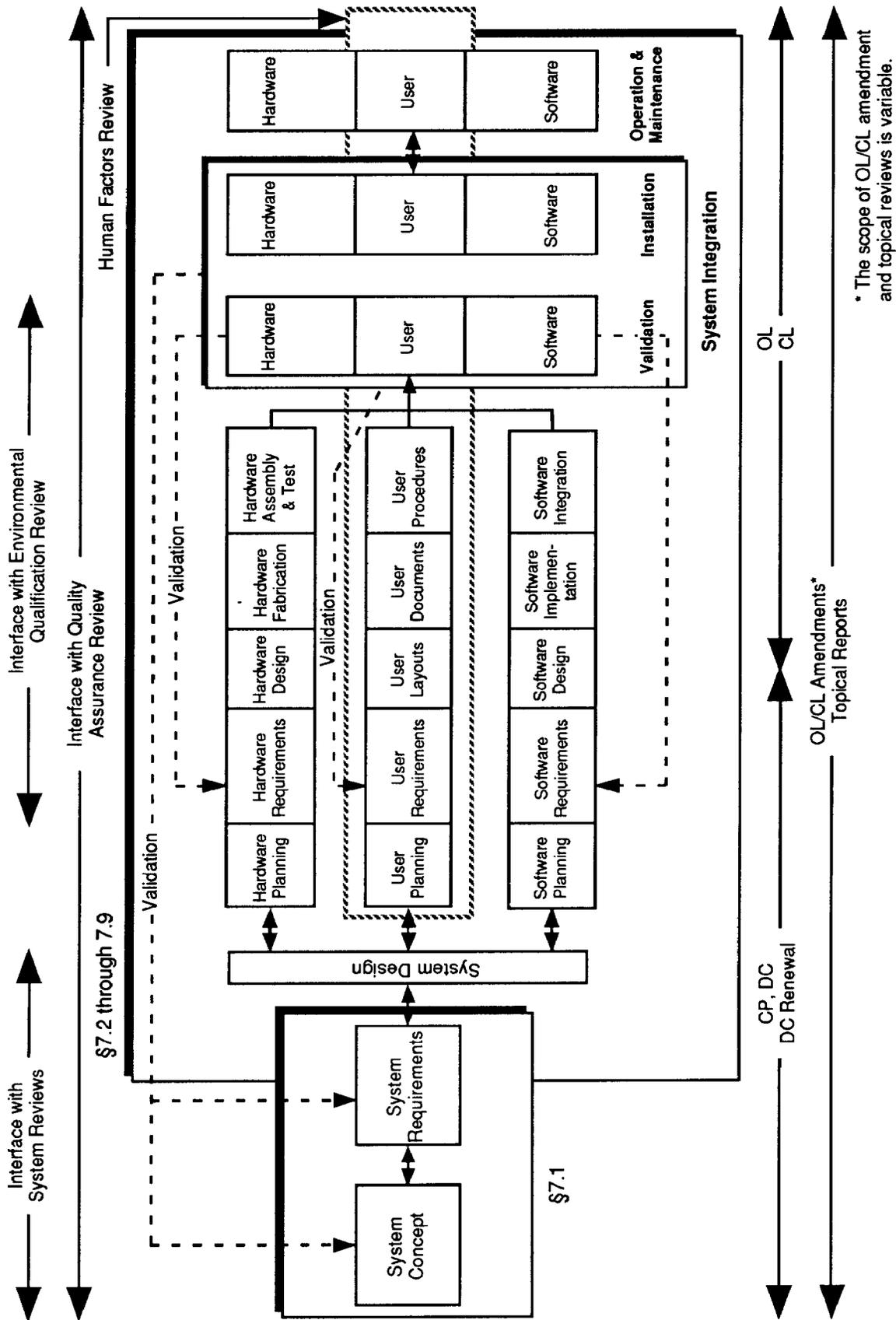


Figure 7.0-2. Relationship Between Development Life Cycle Stages, Review Types, and SRP Sections



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

NEW

Appendix 7.0-A
Review Process for Digital Instrumentation and Control Systems

Version 11.0, June 24, 1997

A. Introduction

This appendix provides an overview of the process for reviewing the unique aspects of digital instrumentation and control (I&C) systems. It supplements the description of the process for review of (1) the overall I&C system design described in Section 7.0, (2) the design criteria and commitments described in Section 7.1, and (3) the individual digital I&C systems described in Sections 7.2 through 7.9. This appendix illustrates how the review activities interact with each other and with the overall I&C review process described in Sections 7.1 through 7.9. Additional information relevant to the review process can be found in the references in Section D of this appendix.

More detailed information on the regulatory bases, acceptance criteria, and review processes for specific issues are described in Section 7.1, related branch technical positions (BTPs), and regulatory guides.

Definitions

An *activity group* is a collection of software life cycle activities, all of which are related to a specific life-cycle topic. Eight activity groups are recognized in this appendix: planning, requirements, design, implementation, integration, validation, installation, and operations and maintenance.

Critical characteristics are those properties or attributes that are essential for performance of an equipment's safety function (IEEE Std 934, "Requirements for Replacement Parts for Class 1E Equipment in Nuclear Power Generating Stations"). A similar definition is provided in EPRI NP-5652, "Guideline for the

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

Utilization of Commercial Grade Items in Nuclear Safety Related Applications," in relation to commercial dedication.

Design output includes documents, such as drawings and specifications, that define technical requirements of structures, systems, and components (ASME Std NQA-1, "Quality Assurance Requirements for Nuclear Facility Applications"). For software, design outputs are the products of the development process that describe the end product that will be installed in the plant. The design outputs of a software development process include software requirements specifications, software design specifications, hardware and software architecture, code listings, system build documents, installation configuration tables, operations manuals, maintenance manuals, and training manuals.

The *design process* comprises technical and management processes that commence with identification of design input and lead to and include the issuance of design output documents (ASME Std NQA-1).

A *design requirement* is a requirement that specifies or constrains the design of a system or system component (IEEE Std 610.12, "IEEE Standard Glossary of Software Engineering Terminology").

Deterministic refers to a property of a computer or communication system such that the time delay between stimulus and response has a guaranteed maximum and minimum.

Embedded software or *firmware* is software that is built into (stored in read-only memory) a computer dedicated to a pre-defined task. Normally, embedded software cannot be modified by the computer that contains it, nor will power failure erase it; some computers may contain embedded software stored in electrically erasable programmable read-only memory (EEPROM), but changing this memory typically requires a special sequence of actions by maintenance personnel.

A *function* is a specific purpose of an entity or its characteristic action (IEEE Std 610.12, "IEEE Standard Glossary of Software Engineering Terminology").

A *functional characteristic* is a trait or property of a design output that implements a functional requirement, a portion of a functional requirement, or a combination of functional requirements. BTP HICB-14 identifies specific functional requirements considered in software reviews.

A *functional requirement* is a requirement that specifies a function that a system or system component must be capable of performing (IEEE Std 610.12). In this appendix, the term functional requirement includes design requirements, interface requirements, performance requirements, and physical requirements, as described in IEEE Std 610.12.

Hardware critical characteristics are those properties or attributes of computer, peripheral, or communication hardware that are essential for performance of the connected equipment's safety function. This includes meeting specifications that are required to execute the software intended to run on the hardware, as well as attributes of reliability, testability, or predictability upon which the Staff's safety findings are based.

Predeveloped software (PDS) is software that already exists, is available as a commercial or proprietary product, and is being considered for use in a computer-based function (IEC Std 880, "Software for Computers in the Safety Systems of Nuclear Power Stations," Supplement 1 draft). Commercial off-the-shelf (COTS) software is a subset of PDS.

Software critical characteristics are those properties or attributes of a software or firmware product that are essential for performance of the related equipment's safety function. This includes functional requirements that are allocated to the software product, as well as attributes of robustness, testability, or dependability upon which the Staff's safety findings are based.

A *software development process characteristic* is a trait or property of a software development process design output that results from the implementation of a design process. BTP HICB-14 identifies specific software development process characteristics considered in software reviews.

A *software development process requirement* describes an activity, or activities, that a software development process must include.

A *software life cycle* is a project-specific, sequenced mapping of activities (Reg. Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorsing IEEE Std 1074, "IEEE Standard for Developing Software Life Cycle Processes"). The software life cycle typically includes a planning phase, requirements phase, design phase, implementation phase, integration phase, validation phase, installation phase, and operation and maintenance phase. The purpose of such a mapping is to permit concurrent execution of related activities, and to provide staged checkpoints at which product and process characteristics are verified during the development process.

B. Background

The fundamental acceptance criteria for I&C systems are described in 10 CFR 50.55a; ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations;" Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations;" and Appendix A of 10 CFR 50 (General Design Criteria). Appendix B of 10 CFR 50 (Quality Assurance Criteria) provides criteria for quality assurance programs to be applied to the design, fabrication, construction, and testing of I&C safety systems. The criteria of 10 CFR 50 apply to digital I&C systems and are sufficient to support licensing of such systems. For applications under 10 CFR 52, the technical acceptance criteria of 10 CFR 50 apply.

Certain characteristics of digital I&C systems necessitate that augmented review approaches and different review perspectives be used in assessing compliance with the fundamental acceptance criteria of 10 CFR 50. These characteristics are important to the evaluation of (1) design qualification of digital systems, (2) protection against common-mode failure, and (3) selected functional requirements of IEEE Std 603 and the General Design Criteria that pose new assurance challenges when implemented using computers. These topics are discussed in more detail below.

B.1. Qualification of Digital Instrumentation and Control Systems and Components

Digital I&C systems require additional design and qualification approaches than are typically employed for analog systems. The performance of analog systems can typically be predicted by the use of engineering models. These models can also be used to predict the regions over which an analog system exhibits continuous performance. The ability to analyze design using models based upon physics principles, and the ability to use these models to establish a reasonable expectation of continuous performance over substantial ranges of input conditions are important factors used in the qualification of analog systems design. These factors enable extensive use of type testing, acceptance testing, and inspection of design outputs in qualifying the design of analog systems and components. If the design process ensures continuous behavior over a fixed

range of inputs, and testing at a finite sample of input conditions in each of the continuous ranges demonstrates acceptable performance, then performance at intermediate input values between the sampled test points can be inferred to be acceptable with a high degree of confidence.

Digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and implementation can cause them to exhibit unexpected behavior. Consequently, the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing at a sample of input conditions. The use of inspections, type testing, and acceptance testing of digital systems and components does not alone accomplish design qualification at high confidence levels. To address this issue, the Staff's approach to the review of design qualification for digital systems focuses, to a large extent, upon confirming that the applicant/licensee employed a high-quality development process that incorporated disciplined specification and implementation of design requirements. Inspection and testing is used to verify correct implementation and to validate desired functionality of the final product, but confidence that isolated, discontinuous point failures will not occur derives from the discipline of the development process.

B.2. Defense Against Common-Mode Failure

In digital I&C systems, code, data transmission, data, and hardware may be common to several functions to a greater degree than is typical in analog systems. Although this commonality is the basis for many of the advantages of digital systems, it also raises a key concern: a design using shared data or code has the potential to propagate a common-cause or common-mode failure via software errors, thus defeating the redundancy achieved by the hardware architectural structure. Greater commonality or sharing of hardware among functions within a channel increases the consequences of the failure of a single hardware module and reduces the amount of diversity available within a single safety channel.

Because of this concern, the staff review of digital I&C systems emphasizes quality and defense-in-depth and diversity (D-in-D&D) as protection against propagation of common-mode failures within and between functions.

B.3. System Aspects of Digital Instrumentation and Control

Certain functional requirements that apply to I&C safety systems involve system aspects that pose new assurance challenges when applied to digital systems. These aspects include real-time performance, independence, and on-line testing. The review process for these topics must recognize the special characteristics of digital systems.

C. Review Process

C.1. Summary

The overall process for reviewing the unique aspects of digital I&C systems is outlined in Figure 7.0-A-1. Figure 7.0-A-2 shows the issue-resolution process applicable to each item in 7.0-A-1. The process shown in Figure 7.0-A-1 applies to any digital I&C system or function proposed in a license application or a license amendment application.

The scope of the review process is the same for any I&C safety function; however, the effort required to implement the review will be considerably less for a system that implements only a few safety requirements than it will be for a complex system such as a complete, integrated, digital safety system design. While

acceptance criteria remain the same,¹ the Staff's review emphasis should be commensurate with the safety significance of the given system or aspect of a system's design under review. Probabilistic risk assessments (PRAs), such as those conducted under the Individual Plant Evaluation program (see Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities") or required as part of applications under 10 CFR 52, provide information that may prove helpful in determining the appropriate level of review.

The following seven topics should be addressed in any digital I&C system review:

1. The adequacy of design criteria and guidance to be applied to the proposed system.
2. Identification of review topics — The subsequent review process depends upon the I&C systems addressed in the application.
3. Defense-in-depth and diversity — For applications that involve a reactor trip system (RTS) or an engineered safety features actuation system (ESFAS), the ability of the combination of I&C systems to cope with common-mode failure should be reviewed. This review should confirm that D-in-D&D design conforms to the guidance of Section 7.1 and BTP HICB-19.
4. The adequacy of system functions and commitments for the individual I&C systems — The requirements for each system are outlined in Sections 7.1 through 7.9. For digital systems, this review should address the functional requirements of IEEE 603 and the General Design Criteria that pose new assurance challenges when implemented using computers. The supplemental guidance for digital computer-based safety systems in Section 7.1 describes the system aspects that need careful consideration in digital systems.
5. Life cycle process planning — The adequacy of the computer system development process, particularly the software life cycle activities for digital systems, should be reviewed. This is addressed by confirming that software life cycle plans have commitments to coordinated execution of activity groups, and to staged checkpoints at which product and process characteristics are verified during the development process, as described in Section 7.1 and BTP HICB-14, Section B.3.1.
6. The adequacy of the software life cycle process implementation — A sample of verification and validation, safety analysis, and configuration management documentation for various life-cycle phases should be audited to confirm that the applicant/licensee's life-cycle activities have been implemented as planned. BTP HICB-14, Section B.3.2, describes acceptance criteria and review procedures that provide guidance for the conduct of these audits.
7. Software life cycle process design outputs — The conformance of the hardware and software to the functional and process requirements derived from the design bases should be audited. A sample of software design outputs should be reviewed to confirm that they address the functional requirements allocated to the software, and that the expected software development process characteristics are evident in the design outputs. The review of validation and installation activities should include confirmation of

¹The Staff discussed the issues of classification and requirements grading in SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," and noted that, "A graded set of requirements based on the importance to safety of the functions being performed with respect to reduction in the potential for radiation exposure could be adopted." IEEE Std 603 and IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," endorsed by Reg. Guide 1.153 and Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," do not provide for classification, although the foreword to IEEE Std 7-4.3.2 recommends the addition of grading to future versions of IEEE Std 603.

the adequacy of the system test procedures and test results (validation tests, site acceptance tests, pre-operational and start-up tests) that provide assurance that the system functions as intended. BTP HICB-14, Section B.3.3, describes functional characteristics and software development process characteristics that are verified by these audits.

Review of D-in-D&D (topic 3 above) will involve the review of several I&C systems to determine how the overall I&C design functions interact to protect against common-mode failure. This review may involve both non-computer systems and computer-based systems. The review of topics 4, 5, and 6 may be conducted once to evaluate a design process that is common to multiple systems. The review of topic 7 should involve a sample of the products from each digital I&C system described in Chapter 7 of the applicant/licensee's safety analysis report.

For a system incorporating commercial-grade digital equipment, the seven topics still apply, but the review of the commercial-grade elements will be performed differently. For a commercial-grade element of the system, there should be evidence of the application of an acceptance process that has determined that there is reasonable assurance that the equipment will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program. The acceptance process itself is subject to the applicable provisions of 10 CFR Part 50, Appendix B. This process might vary depending on the specifics of the particular commercial-grade equipment and its intended application; however, it must establish the required assurance. The subject of qualification of existing commercial computers is addressed in Reg. Guide 1.152 Rev. 1, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." An acceptable process is described in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications."

C.2. Review Process for Software in Digital Instrumentation and Control Systems

For software, the interaction between review topics 4, 5, 6, and 7 is illustrated in Figure 7.0-A-3. In this figure, software requirements are depicted as two subsets of requirements: I&C system-level functional requirements, and software development process requirements. I&C system-level functional requirements describe what function the system is to perform, while software development process requirements describe how the process of building the system is to be performed.

The functional and process requirements come together in the development process. As a result, the design outputs exhibit both functional and process characteristics.

Functional characteristics are described in the design outputs so the resulting system will perform the required functions.

Process characteristics end up in the design outputs as an artifact of the development process. Their presence is evidence that a disciplined development process was employed, and the goal of high-quality software has been achieved. For example, internal consistency of the software requirements specification is a characteristic of a design output. Confirmation that the design output possesses this attribute increases confidence that the development process was disciplined and controlled.

The Staff's review process for software in digital I&C systems, shown in Figure 7.0-A-3, includes each of the following items.

- Review of I&C system-level functional requirements confirms compliance with fundamental requirements embodied in the CFR and guidance in the regulatory guides, standards, and SRP. This review should confirm that the special design considerations of digital systems are appropriately considered and that critical digital hardware and software characteristics are identified.
- Review of software life cycle process plans confirms that the specified software development process requirements documented in the plans establish a commitment to an effective and disciplined software development process and implementation.
- Inspection of the development process confirms that the process life cycle implementation conforms with the software development process requirements described in the plans, and that appropriate safety analysis, verification and validation, and configuration control activities are conducted.
- Audits of design outputs confirm that functional requirements are traceable through all intermediate design products to the final product. Audits of design outputs also confirm that the software development process characteristics and the required software functional characteristics are present.
- Reviews of the acceptance process for PDS, and of the results, confirm that system elements incorporating PDS demonstrate reasonable assurance that they will perform their intended safety function. The reviews should confirm that the critical characteristics of each PDS have been adequately identified and verified.

The review of software in digital I&C systems should be performed within the context of the overall system life cycle stages, shown in Figure 7.0-2. Through the system design activities, system requirements are allocated to components and give rise to hardware and software requirements. Software development activities proceed in parallel with hardware development and become integrated with hardware activities during the system validation stage. Software is validated against software requirements, integrated with hardware, and the complete system is validated against system requirements.

Requirements specification and allocation activities, particularly for software, have proven to be an important source of errors in system development. Much of the software life cycle is devoted to ensuring faithful implementation of the specified software requirements. Therefore, appropriate attention should be given to requirements when addressing topics 4 through 7. The adequacy of system functional requirements is the subject of topic 4. In reviewing these requirements for conformance to ANSI/IEEE Standard 279 (Appendix 7.1-B) or to IEEE Standard 603 (Appendix 7.1-C), achievement of the design basis characteristics discussed in the appendices (7.1-B, Section 3 and 7.1-C, Section 4) is an important element in preventing errors in requirements specification. With respect to topics 5, 6, and 7, the planning and implementation activities should exhibit appropriate emphasis on the allocation of system functional requirements to components, the capture of functional and related software requirements, and the verification and control of those system and software requirements. The software requirements specification should exhibit the functional and process characteristics described in Section 3.3.a of BTP HICB-14.

Formal or semi-formal methods are available for use in preparing some design outputs. Formal specification languages and high-level design languages (e.g., function block diagrams, logic diagrams, and ladder logic diagrams) are examples of such methods which can be useful for specifying certain aspects of software requirements. For example, function block diagrams are usually sufficient to specify the logical functions to be performed by a protection system.

The use of such languages reduces ambiguity and can make incomplete and inconsistent requirements easier to recognize. Furthermore, analytical tools are often available to support evaluation of ambiguity, completeness, consistency, and correctness. While the use of such languages may help to accurately specify certain aspects of requirements or design, existing languages do not support complete specification of requirements or design. For example, many formal design methods do not address timing or robustness requirements. Therefore where such formal or high-level languages are used, care must be taken to ensure that requirements are not overlooked simply because they cannot be described by the specification or design language selected. All requirements must be identified and addressed. Requirements or designs may be described by any combination of languages, including any effective combination of formal languages, high-level languages, and natural languages, provided the interfaces between requirements expressed in different forms are appropriately addressed.

Many formal methods deal only with a single life cycle activity. Often the outputs of one activity must be manually transformed to provide inputs for methods or tools used in subsequent activities. Where such combinations of formal methods are used, the review should confirm that the transformations are appropriately verified.

Note that in some methods a single high-level description may be part of more than one design output. For example, in some programmable logic controller (PLC) implementations a single ladder logic description may describe logic requirements in the SRS, describe logic design in the SDD, and serve the function of source code. Such uses are acceptable provided that the BTP HICB-14 criteria for each design output are met.

The review process described above is applicable to any digital I&C system. However, the complexity and depth of the review can vary substantially depending upon the extent, complexity, and safety significance of the systems involved. Each of these review topics is described in more detail below.

C.3. Discussion of Digital System Review Topics

This section provides detailed information on each of the digital system review topics identified above; information on the review of the acceptance of commercial-grade digital equipment is also provided. Where an applicant/licensee proposes a digital system that the NRC staff has previously approved, the staff review scope would be significantly reduced and would focus only on plant-specific issues associated with the modification (e.g., environmental qualification and configuration management). The staff would not review again generic aspects of the proposed design, such as the software development process, products, and documents, unless these aspects have changed or been affected by plant-specific differences. Where differences exist between prior approvals, they should be identified and the review should confirm that an adequate basis has been provided to accommodate the differences. The review should include an evaluation of differences to confirm that they are acceptable.

C.3.1. Adequacy of Design Criteria and Guidance

Section 7.1 discusses the general review of design criteria and guidance. For new digital systems, the applicant/licensee should have committed to the guidance in Reg. Guide 1.152, which endorses IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and a set of software engineering standards sufficient to describe the software development process. This should include, as a minimum, a commitment to the software engineering regulatory guides (Reg. Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.170, "Software Test

Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," and Reg. Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants") or an acceptable alternative approach.

C.3.2. Identification of Review Topics

The digital I&C review topics to be addressed depend upon the system under review, as outlined in Table 7.0-A-1.

Table 7.0-A-1. Review Topics Depend on the System Under Review

Topic	Protection System (7.2–7.3)	Other Safety Systems (7.4–7.6)	Control System (7.7)	Diverse I&C System (7.8)	Data Communication System (7.9)
D-in-D&D	Review	*	*	*	Same review as supported system(s)
Functional Requirements	Review	Review	Limited review	Review	Same review as supported system(s)
Development Process	Review	Review	Limited review	Review	Same review as supported system(s)
Process Implementation	Review	Review	Limited review	Review	Same review as supported system(s)
Design Outputs	Review	Review	Limited review	Review	Same review as supported system(s)

* While D-in-D&D analysis is not required for systems other than RTS and ESFAS, changes to other I&C systems in plants that have existing digital RTS and ESFAS should be reviewed to confirm that the proposed changes do not affect assumptions and commitments made in the existing D-in-D&D analysis. This includes ensuring compliance with the diversity requirements of 10 CFR 50.62, as discussed in Section 7.8.

The level of review depends upon the importance to safety of the system under review. Control systems receive a limited review as necessary to confirm that control system failures cannot have an adverse effect on safety system functions and will not pose frequent challenges to the safety systems. An area of special emphasis for control systems will be to ensure that the control system design is consistent with the commitments for control system/safety system independence. Isolation of safety systems from control system failures should be addressed.

Data communication systems are treated as support systems (see Section 7.9), although they are often composed of specialized hardware, embedded software, and communication protocol software that runs on the computers linked together by the data communication system. They may support protection systems, other safety systems, diverse I&C systems, control systems, or any combination thereof. A design may provide separate safety and non-safety data communication systems. The review topics applicable to any data communication system are the combination of topics applicable to the I&C systems supported by that data communication system.

Computer internal data communication is at present accomplished by high-speed databuses that are usually designed by the makers of the computer system package itself. There are a number of standardized computer internal buses, and, unlike data communication systems, no software is involved (other than operating system software). Operation of computer internal buses is usually under the control of hardware. Unless this situation changes, computer internal data communication should be reviewed by confirming critical hardware characteristics. If software is involved in computer internal data communication, the review should proceed as described above under data communication systems.

C.3.3. Review of Defense-in-Depth and Diversity

I&C safety systems incorporating digital computer technology in the reactor protection system or ESFAS must comply with the NRC position on D-in-D&D described in the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." Figure 7.0-A-4 illustrates the process for review of the system-level D-in-D&D features to determine compliance with the position. BTP HICB-19 describes in detail the regulatory bases, material to be reviewed, acceptance criteria, and review process. For simple modifications, such as incorporating a single digital function into an otherwise analog I&C system, the D-in-D&D analysis may be very simple. Extensive and detailed analyses may be required for completely integrated computer-based reactor protection and control systems.

C.3.4. Review of Software Life Cycle Process Planning

The Staff's conclusion regarding the quality and reliability of digital computer systems will be based upon confirmation of the following points:

1. Plant and overall I&C system requirements are correctly decomposed into the digital I&C system requirements for each digital I&C system under review. Critical hardware and software characteristics are identified.
2. A development process is specified and documented such that implementation of the process gives a high degree of confidence that the functional requirements will be or are implemented in the computer system. The life cycle process plan describes a coordinated engineering process in which design outputs at each planned stage of the design process are verified to implement the input requirements of the stage.
3. The specified process and products, including design outputs, are designed to be inspected at staged checkpoints.
4. The installed system functions as designed. Validation and integration tests, acceptance tests, and on-site pre-operational and start-up functional tests demonstrate that the identified critical hardware and software characteristics are verified.

As discussed above, the Staff's determination of the qualification of digital I&C systems and components is based in part on confirmation that the software for the systems is developed using a disciplined engineering process. Typically, this process is described in a set of software life cycle process development planning documents, which define the process requirements and the commitments the applicant/licensee makes regarding software life cycle activities. Figure 7.0-A-5 identifies the software life cycle planning topics that should be considered for review. These commitments must be consistent with the commitments made for the design criteria and guidance discussed in Section C.3.1 above. Figure 7.0-A-6 outlines the procedures for reviewing software life cycle process planning. BTP HICB-14 describes the detailed regulatory bases and

material to be reviewed for evaluating software development life cycle process planning. Section B.3.1 of that BTP describes the acceptance criteria for this review. In addition to confirming the acceptability of the applicant/licensee's plans, this review activity should also identify the higher-risk activities of the software life cycle process for subsequent audit by the NRC staff.

Almost every computer system will involve some use of PDS. PDS may be used directly in plant computers or in processes used to develop in-plant software. The applicant/licensee's process for qualification of PDS should be reviewed as part of the evaluation of the development process.

For new applications and license amendment applications, review of software life cycle process plans is confined to any changes in the plans if all of the following conditions hold: (1) the applicant/licensee has previously developed a digital I&C safety system under a process acceptable to the Staff, (2) the applicant/licensee has made commitments to software development plans similar to those identified in BTP HICB-14, and (3) these plans have been accepted by the NRC staff.

C.3.5. Review of Functional Requirements for Individual Systems

The functional requirements and commitments for each I&C system must be reviewed against the requirements of 10 CFR 50, as described in Section 7.1 and the individual SRP sections applicable to the system under review. Certain review topics need to be considered differently for digital systems. These topics are:

- Equipment qualification, including electromagnetic compatibility.
- Real-time, deterministic performance.
- On-line and periodic test provisions.
- Communications independence.
- Control of access.

Figure 7.0-A-7 outlines the review of these topics. Detailed regulatory bases, material to be reviewed, acceptance criteria, and review processes for each of these topics are contained in Sections 7.1 and 7.9, Appendix 7.1-C, and BTPs HICB-17 and HICB-21.

C.3.6. Audit of Software Life Cycle Process Implementation

The applicant/licensee's implementation of life cycle activities should be audited to confirm that the planned process is being implemented. Figure 7.0-A-8 provides an overview of the process for auditing the implementation process. Figure 7.0-A-5 identifies the software life cycle process implementation topics that should be considered as candidates for audit. BTP HICB-14, Section B.3.2, describes the acceptance criteria for software life cycle process implementation. The scope and depth of the inspection should be consistent with the extent and complexity of the proposed digital system and the potential safety impact of system failure. For simple, limited, low-impact retrofits to existing systems, the process audit may be a very limited-scope "desk audit" of selected examples of process documentation. Review of extensive digital I&C systems, such as an integrated digital control and protection system, should involve detailed reviews of a wide range of software process documentation. Ideally, these reviews would occur in process audits of several of the life cycle phases, as indicated in Figure 7.0-A-5. The audit of a given set of life cycle activities and the

inspection of products generated by those activities, as discussed in Section C.3.7 below, may be combined into a single audit.

One effective audit technique is the string audit, in which the reviewer selects a sample of specific software development process requirements and specific functional requirements and confirms that they are implemented throughout the life cycle.

C.3.7. Audit of Software Life Cycle Process Design Outputs

The products of a design process include both the design outputs that describe the technical requirements of systems and components, and the systems and components themselves. The review of digital systems should include inspection of these products on an audit basis to confirm that the systems and components meet the functional requirements. Figure 7.0-A-9 provides an overview of the process for inspection of design outputs. Candidate items for inspection include the items described in Appendix 7-B, BTP HICB-17, HICB-21, and HICB-14, Section B.3.3.

Software product inspection is performed by inspecting a representative sample of the design outputs, i.e., software requirements specifications, software design specifications, hardware and software architecture, code listings, build documents, configuration tables, operations manuals, maintenance manuals, and training manuals.

The inspections should examine functional characteristics to confirm that system functional requirements have been properly implemented at each phase of the software development process. Verification and validation analyses and test reports should also be examined to extract information about the design output's conformance with system functional requirements and to verify critical hardware and software characteristics.

The inspections should also examine software development process characteristics to confirm that the products embody characteristics that are evidence of an effective and visible software development process. This step provides confidence that positive findings for the sample functional requirements to be inspected are representative of the software product as a whole. The combination of positive findings in the review of development plans, process implementation, and design outputs provides a high degree of confidence that all of the software conforms with the fundamental system requirements.

This approach requires that the integrity of design outputs be maintained in the translation of code to machine language. Consequently, the Staff's review should include confirmation of the integrity of this conversion. This will normally be accomplished by confirming the qualification of the mechanism and tools for performing this translation (e.g., a COTS compiler and linker) and reviewing integrated system testing, installation, and pre-operational test reports.

One approach to conducting product inspections that has proved successful is the use of string audits that follow selected functional requirements through the design outputs previously described. The scope and depth of the product inspections should be tailored to the extent, complexity, and safety significance of the digital system under review. BTP-14, Section B.3.3, presents specific criteria from which the inspection activities for a specific product may be derived.

For operating license, operating license amendment, or combined license applications, the product inspections should also confirm that the systems reviewed are installed, operated, and maintained appropriately. NRC Inspection Manual, Part 2500, "Digital Retrofits Receiving Prior Approval," provides guidance for inspecting these activities.

C.3.8. Review of the Acceptance of Commercial-Grade Digital Equipment

All software, including operating systems, resident on safety system computers at run time must be qualified for their intended applications. Qualification may be established either by producing the PDS items under a 10 CFR Appendix B quality assurance program or by dedicating the item for use in the safety system as defined in 10 CFR Part 21. Review topics for the former case are described above. Review in the latter case requires a determination that a suitable acceptance process has demonstrated reasonable assurance that the equipment will perform its intended safety function. 10 CFR Part 21 states that “this assurance is achieved by identifying the critical characteristics of the item and verifying their acceptability by inspections, tests, or analyses performed by the purchaser or third-party dedicating entity after delivery, supplemented as necessary by one or more of the following: commercial grade surveys; product inspections or witness at holdpoints at the manufacturer’s facility, and analysis of historical records for acceptable performance.”

An acceptable set of fundamental requirements for this process is described in IEEE 7-4.3.2, Section 5.3.2, and guidance given in Annex D (Informative) of the standard. This standard is endorsed in Reg. Guide 1.152, Rev. 1. In this guidance, the qualification process is accomplished by comparing the commercial-grade item to the design criteria of the standard. This standard allows the use of engineering judgment for the acceptance of existing software, and the use of compensating factors to substitute for missing elements of the software development process. These provisions should not be interpreted to permit unsupported subjectivity in the acceptance of existing software. The guidance provided herein for the review of newly developed software provides technical background pertinent to evaluating the use of the engineering judgment and compensating factors provisions. The standard requires the acceptance, and its basis, to be documented and maintained with the qualification documentation.

In order to demonstrate reasonable assurance, the acceptance process for most PDS can be expected to comprise a variety of technical activities conducted in significant detail. Guidance on these activities has been provided in EPRI TR-106439. The NRC has issued a safety evaluation report (SER) on the EPRI guideline in which it determined that “TR-106439 contains an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications.”

If the guidance in EPRI TR-106439 is applied in the dedication of a component, the following items should be noted by the reviewer:

- TR-106439 is not intended to be used as a detailed “how-to” manual. There may be significant variation in specific steps taken depending on vendors, components, and applications. Detailed specific information, in addition to that provided in the report examples, will be needed to perform an actual commercial dedication. Use of TR-106439 in connection with a license amendment or 10 CFR 50.59 evaluation should include descriptions of alternatives selected and deviations from the guidance in the documentation of the acceptance process.
- The dedication effort can be “graded” based on safety significance and relative complexity.
- TR-106439 references EPRI NP-5652, which discusses four methods for use in commercial dedication:(1) special tests and inspections, (2) commercial-grade survey of supplier, (3) source verification, and (4) acceptable supplier/item performance record. As noted in TR-106439, supported by Generic Letters 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products," and 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs," for typical applications no one method will suffice by itself, and it is likely that methods 1, 2, and 4 will all be needed.

- The examples listed in TR-106439 are not all-inclusive. Depending on application and product specifics, some of the evaluations may not be needed or additional verification activities, beyond those listed in the example, might be necessary.
- Engineering judgement applied in the acceptance process must be documented sufficiently to allow a comparably qualified individual to reach the same conclusion.
- The validity of the commercial-grade item dedication must be maintained as long as the item remains in service. Dedicated software items should not be updated to new revision levels without prior evaluation to determine if a design change is required. Commercially dedicated items should not be operated in a configuration outside the bounds of the original dedication.
- The utility should arrange to be notified by the vendor when defects are discovered. This requires confirmation that the vendor's processes will support this need.
- TR-106439 notes that not all commercial items can be successfully dedicated.

D. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ASME Std NQA-1-1994. "Quality Assurance Requirements for Nuclear Facility Applications."

EPRI NP-5652. "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications." Final Report, Electric Power Research Institute, June 1988.

EPRI Topical Report TR-106439. "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." Electric Power Research Institute, October 1996.

Generic Letter 88-20. "Individual Plant Examination for Severe Accident Vulnerabilities." November 23, 1988.

Generic Letter 89-02. "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products." 1989.

Generic Letter 91-05. "Licensee Commercial-Grade Procurement and Dedication Programs." 1991.

IEC Std 880. "Software for Computers in the Safety Systems of Nuclear Power Stations." IEC Publication, 1986.

IEC Std 880, Supplement 1 Draft. "Software for Computers in the Safety Systems of Nuclear Power Stations." IEC Publication, October 1996.

IEEE Std 1074-1995. "IEEE Standard for Developing Software Life Cycle Processes."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

IEEE Std 610.12-1990. "IEEE Standard Glossary of Software Engineering Terminology."

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

IEEE Std 934-1987. "Requirements for Replacement Parts for Class 1E Equipment in Nuclear Power Generating Stations."

NRC Inspection Manual, Chapter 52001. "Digital Retrofits Receiving Prior Approval."

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Rev. 1. Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Rev. 1. Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.168. "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.169. "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.170. "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.171. "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.172. "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.173. "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission.

SECY-91-292. "Digital Computer Systems for Advanced Light-Water Reactors." September 1991.

Safety Evaluation by the Office of Nuclear Reactor Regulation. "EPRI Topical Report TR-106439." May 1997.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.

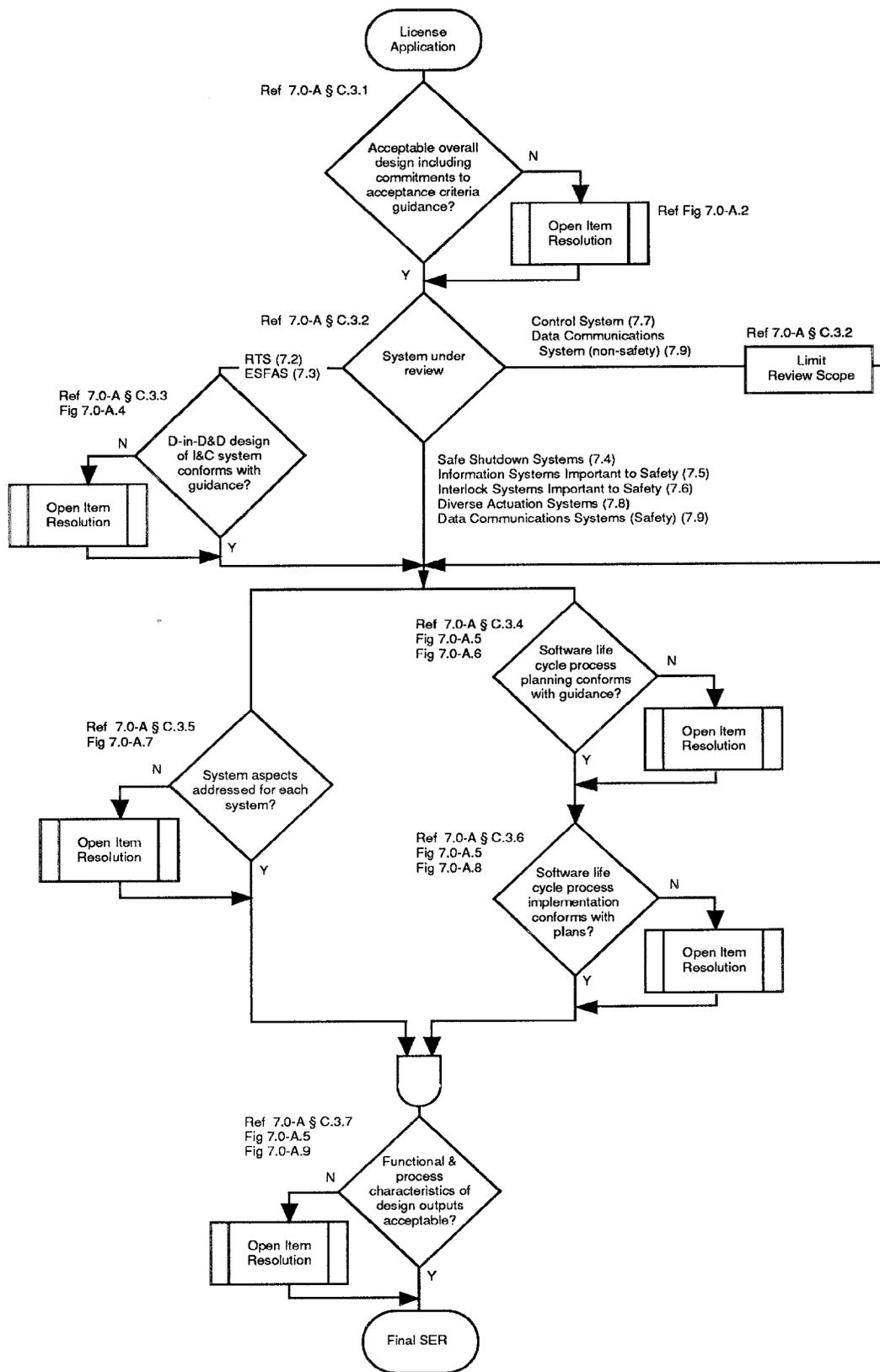


Figure 7.0-A-1. Overview of the Process for Reviewing the Unique Aspects of Digital Instrumentation and Control Systems

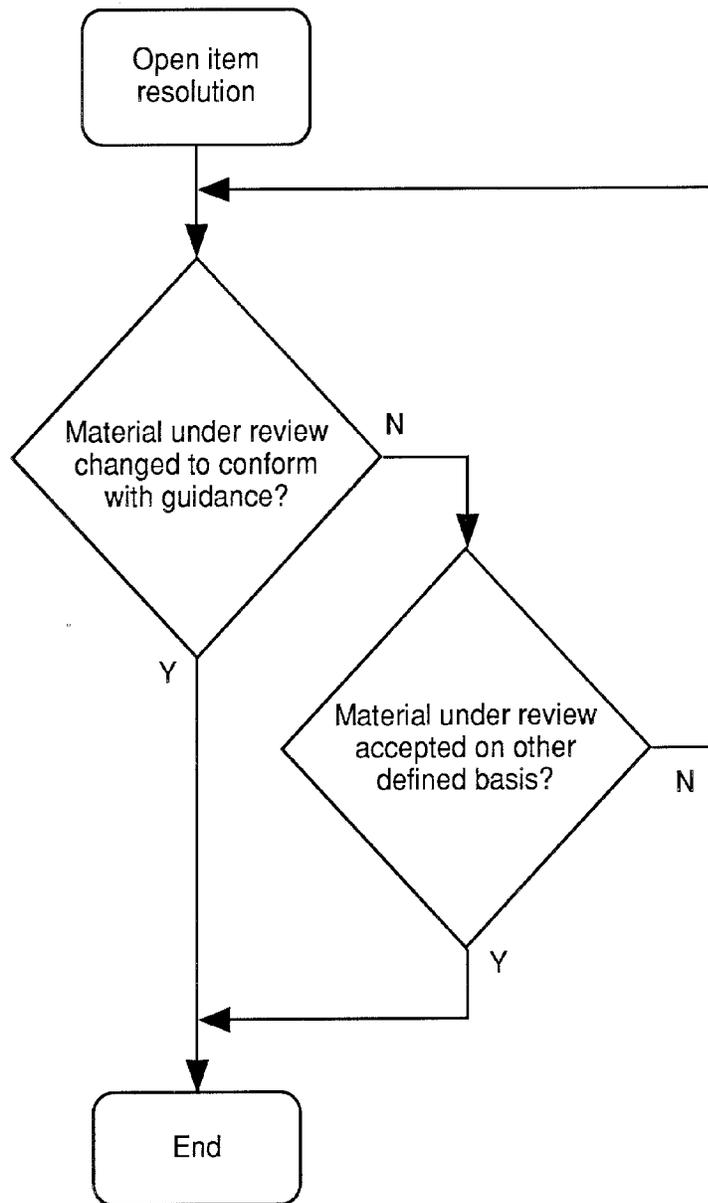


Figure 7.0-A-2. Open Item Resolution Process

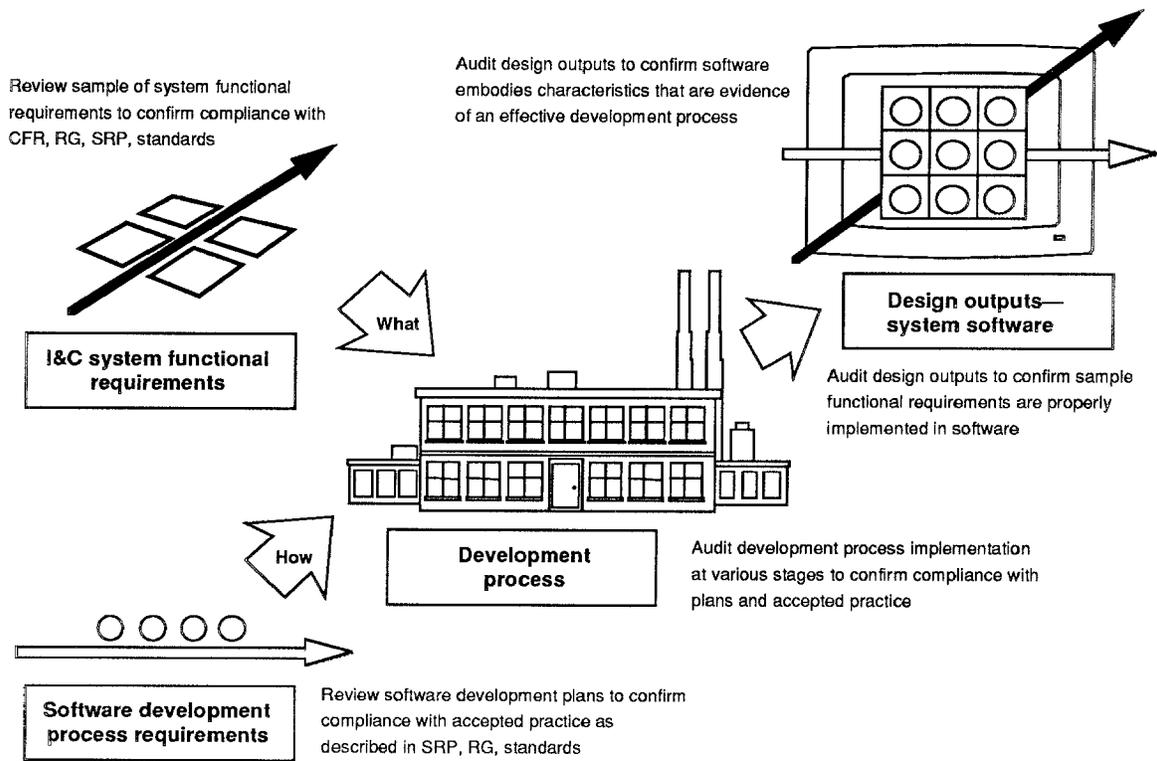


Figure 7.0-A-3. Software Review Process

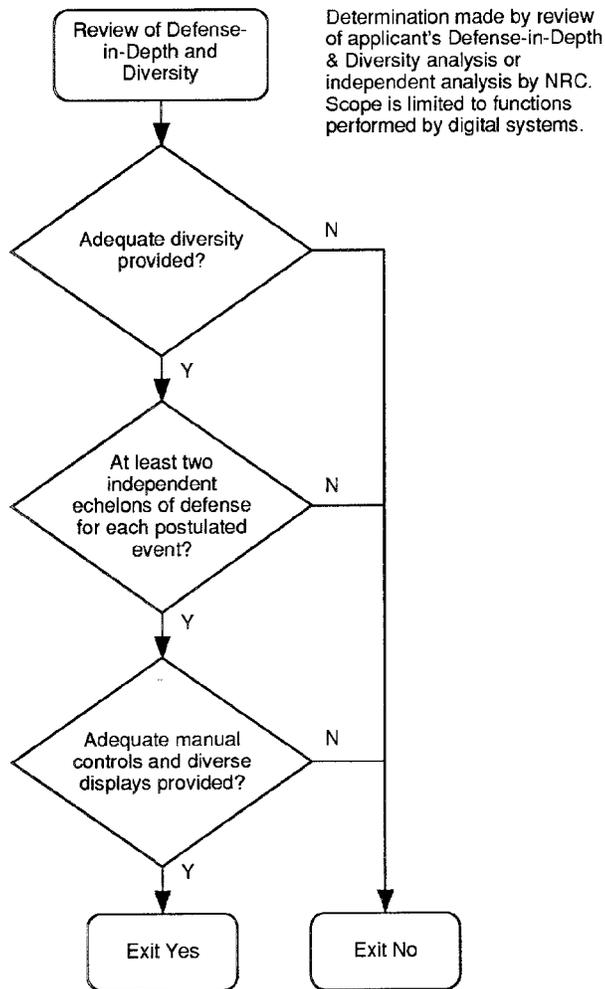
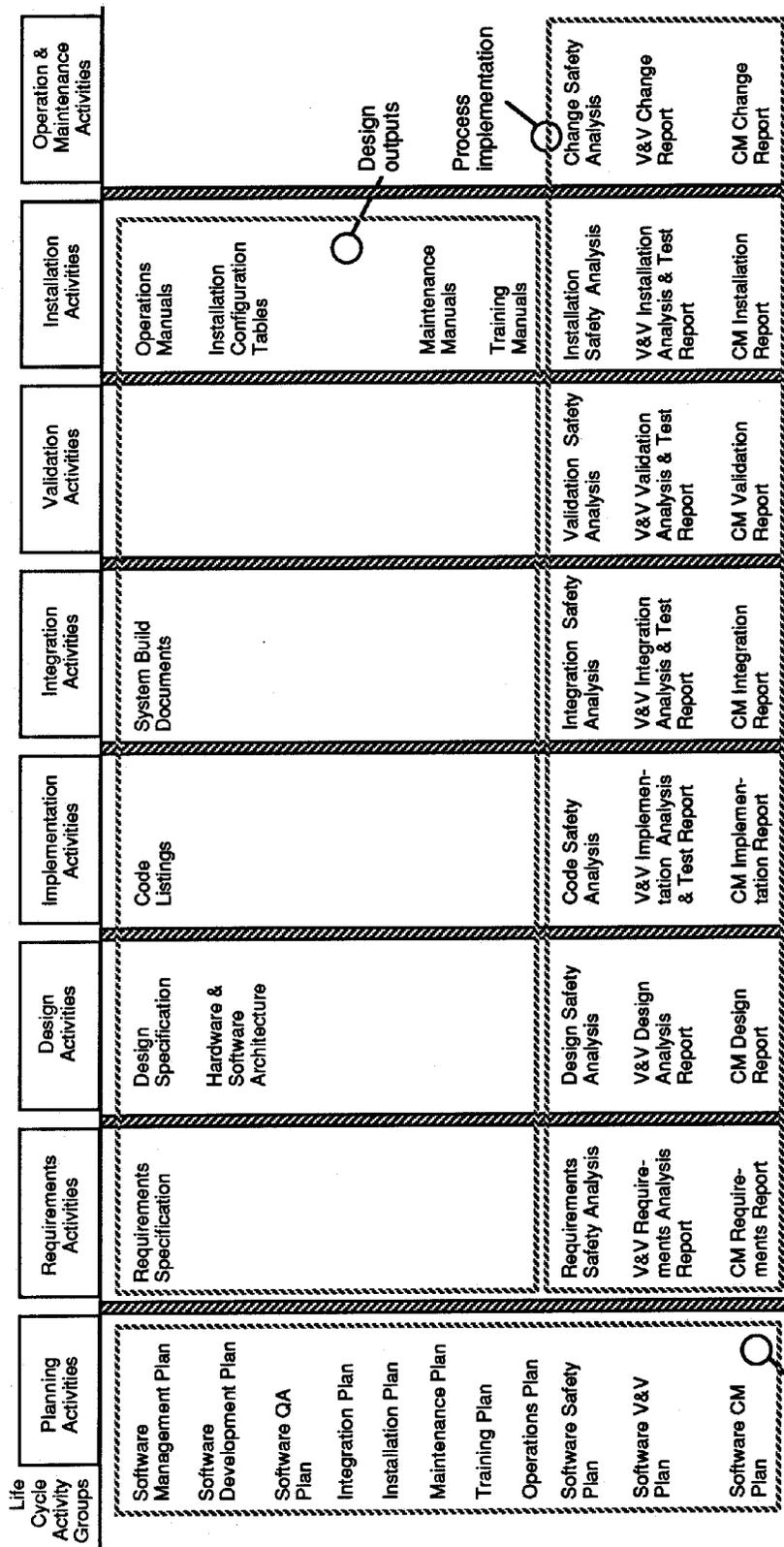


Figure 7.0-A-4. Defense-in-Depth and Diversity Review



Note: A separate document is not required for each topic identified; however, project documentation should encompass all of the topics.

Figure 7.0-A-5. Software Life Cycle Activities

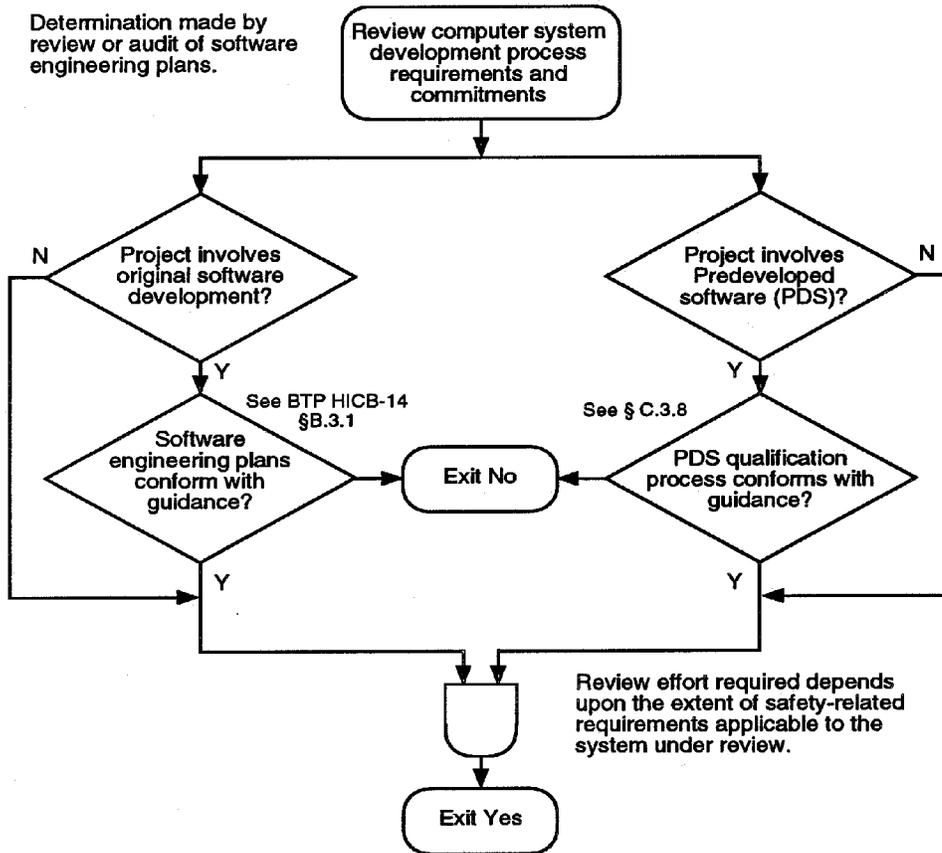


Figure 7.0-A-6. Review of Software Life Cycle Process Planning

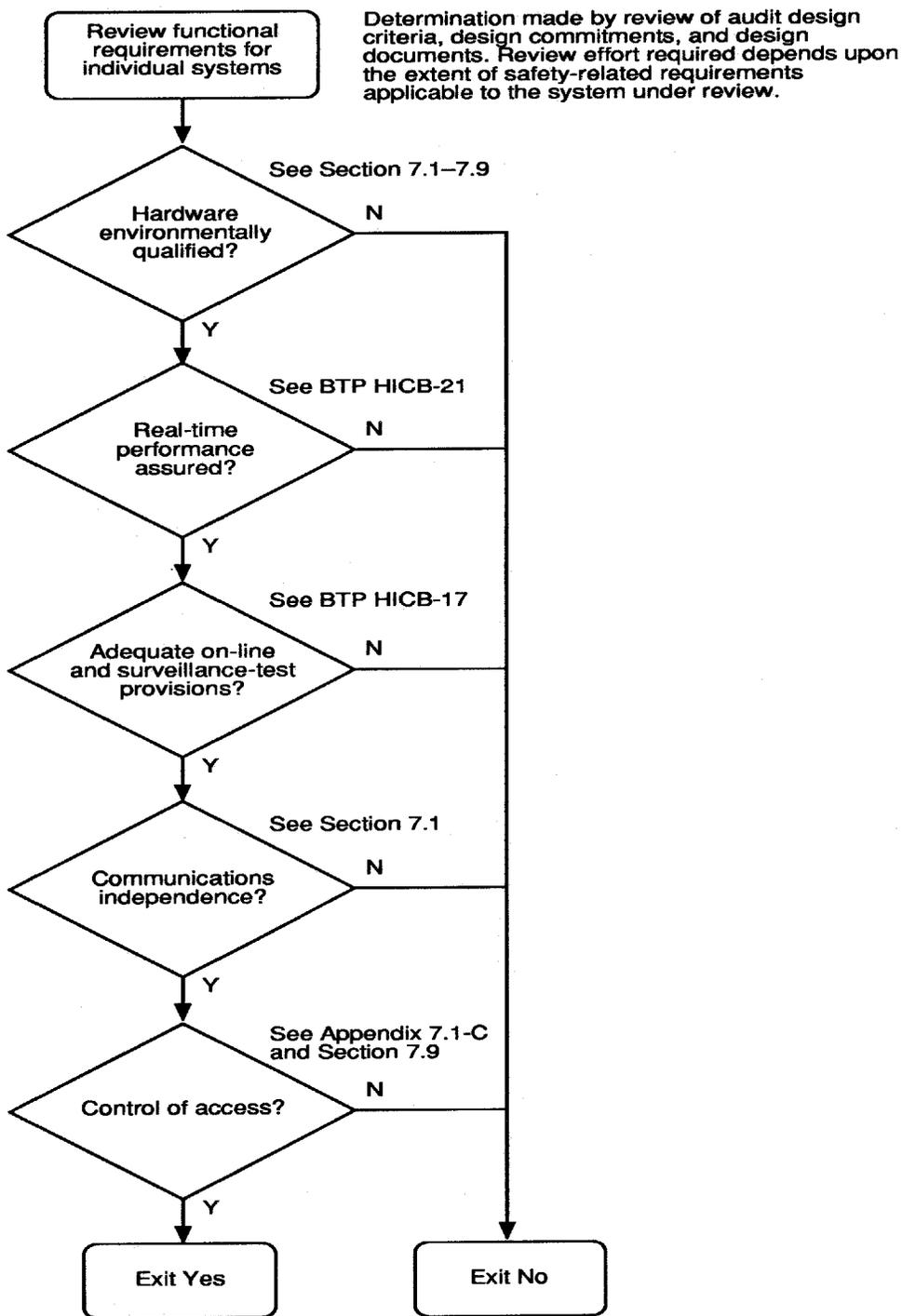


Figure 7.0-A-7. Special Considerations in the Review of Functional Requirements for Digital Instrumentation and Control Systems

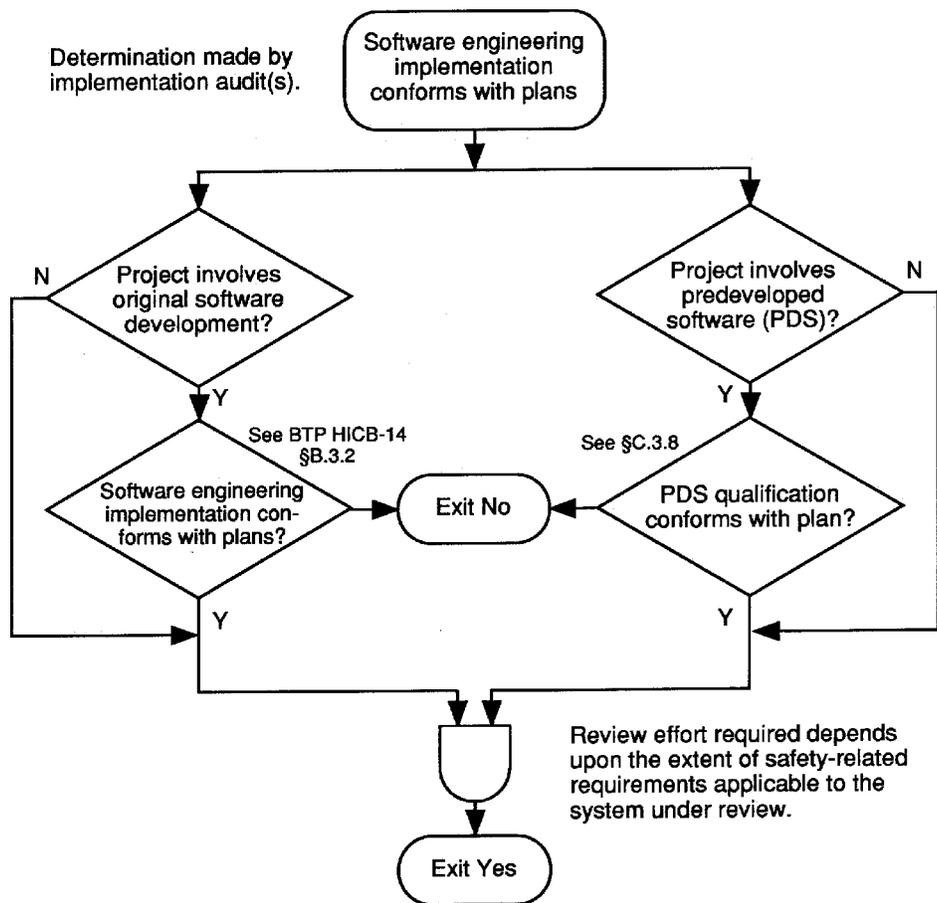


Figure 7.0-A-8. Review of Software Development Process Implementation

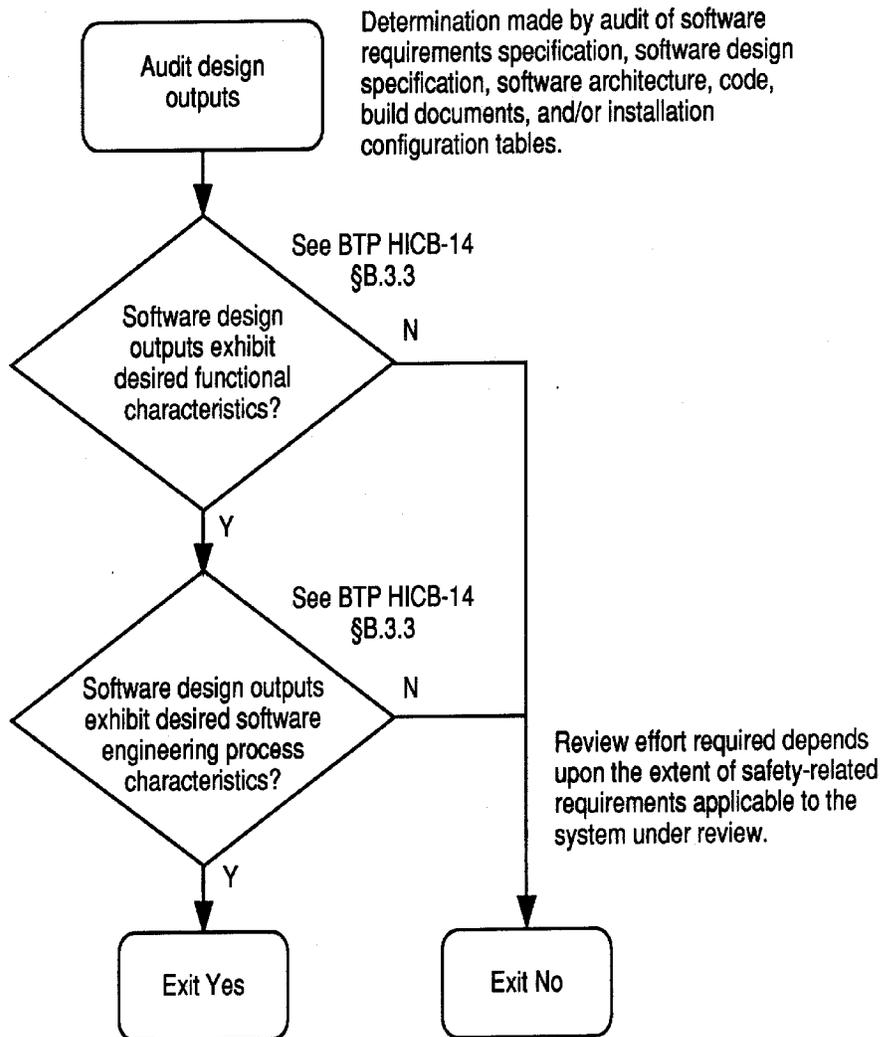


Figure 7.0-A-9. Review of Design Outputs



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Section 7.1. Instrumentation and Controls — Introduction

Version 11.0, June 24, 1997

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

The instrumentation and control (I&C) systems within the scope of Chapter 7 fall into the following nine categories and are addressed in detail in subsequent sections of the Safety Analysis Report (SAR) Chapter 7 or other sections of the SAR: reactor trip systems (RTS), engineered safety features actuation systems (ESFAS), safe shutdown systems, information systems important to safety, interlock systems important to safety, control systems, diverse I&C systems, data communication systems, and essential auxiliary supporting systems. Protection systems are those I&C systems which initiate safety actions to mitigate the consequences of design basis events. The protection systems include the RTS and the ESFAS.

1. *Reactor trip systems (RTS)* are those systems that initiate rapid control rod insertion to mitigate the consequences of design basis events. The RTS is discussed in Section 7.2 of the SAR.
2. *Engineered safety features actuation systems (ESFAS)* are those I&C systems that initiate and control safety equipment that remove heat or otherwise assist in maintaining the integrity of the three physical barriers to radioactive release (cladding, reactor coolant pressure boundary, and containment). The ESFAS is discussed in Section 7.3 of the SAR.

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

3. *Safe shutdown systems* are those systems which function to achieve and maintain a safe shutdown condition of the plant. The safe shutdown systems include those I&C systems used to maintain the reactor core in a subcritical condition and provide adequate core cooling to achieve and maintain both hot and cold shutdown conditions. Safe shutdown systems are discussed in Section 7.4 of the SAR.
4. *Information systems important to safety* are those systems which provide information for the safe operation of the plant during normal operation, anticipated operational occurrences, and accidents. The information systems important to safety include those systems which provide information for manual initiation and control of safety systems. They indicate that plant safety functions are being accomplished and provide information from which appropriate actions can be taken to mitigate the consequences of anticipated operational occurrences and accidents. During normal plant operation, the information systems important to safety provide information on the normal status and the bypassed and inoperable status of safety systems. Information systems important to safety are discussed in Section 7.5 of the SAR.
5. *Interlock systems important to safety* are those systems which operate to reduce the probability of occurrence of specific events or to maintain safety systems in a state to assure their availability in an accident. These systems differ from protection systems in that interlock system safety action is taken prior to or to prevent accidents. Interlock systems important to safety are discussed in Section 7.6 of the SAR.
6. *Control systems* are those systems used for normal operation that are not relied upon to perform safety functions following anticipated operational occurrences or accidents, but which control plant processes having a significant impact on plant safety. Control systems are discussed in Section 7.7 of the SAR.
7. *Diverse instrumentation and control systems* are those systems provided expressly for diverse backup of the reactor protection system and engineered safety features actuation systems. Diverse I&C systems account for the possibility of common-mode failures in the protection systems. The diverse I&C systems category includes the anticipated transient without scram (ATWS) mitigation system as required by 10 CFR 50.62. For plants with digital computer-based instrumentation and controls, diverse I&C systems may also include hardwired manual controls, diverse displays, and any diverse actuation systems specifically installed to meet the guidance of the Staff Requirements Memorandum (SRM) on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." This SRM describes the NRC position on defense-in-depth and diversity. Diverse I&C systems are discussed in Section 7.8 of the SAR.
8. *Data communication systems* transmit signals between systems and between components of systems. Data communications systems may include analog and digital multiplexers as well as non-multiplexed transmission. Where such systems are included in a design, they support one or more of the systems described above. They may also support I&C functions addressed in other sections of the SAR. Data Communications Systems are discussed in Section 7.9 of the SAR.
9. *Essential auxiliary supporting systems* are those systems that function before the I&C systems important to safety can perform their functions. Heating, ventilation and air conditioning systems, electrical power systems, and cooling water systems are typical examples of essential auxiliary supporting systems. Essential auxiliary supporting systems are discussed primarily in Chapters 8 and 9 of the SAR. The I&C aspects of essential auxiliary supporting systems are addressed in the review of those SAR sections which discuss those systems. To the extent that the operation of essential auxiliary

supporting systems are initiated by the protection system, this aspect is included in the review of Sections 7.2 or 7.3 of the SAR.

All other I&C for systems important to safety, such as fire protection, fuel handling control, security systems, radiation monitoring, and control of essential auxiliary supporting systems are addressed in the review of other Standard Review Plan (SRP) sections which discuss these systems. HICB supports the review of these systems as a secondary reviewer. The acceptance criteria and review procedures of Chapter 7, Section 7.7 in particular, are also applicable to these other I&C systems.

HICB is a primary reviewer for one of these other SRP sections, Section 9.5.2, "Voice Communications." HICB is a secondary reviewer for the I&C functions discussed in the other SRP sections. For applications made under 10 CFR 52, HICB also has lead review responsibility for inspections, tests, analyses and acceptance criteria (ITAAC) that demonstrate the adequacy of I&C systems. ITAAC are intended to provide reasonable assurance that, if the inspections, tests, and analyses are performed, the acceptance criteria are met, and a plant is built according to the design, then the plant will operate in accordance with the design certification. SRP Section 14.3 describes the general acceptance criteria and review procedures for ITAAC. Section 14.3.5 describes the specific acceptance criteria and review procedures for I&C system ITAAC.

The review of Section 7.1 of the SAR includes the tabulation of I&C systems important to safety and the acceptance criteria and guidelines applicable to each of these systems. The review also identifies those I&C systems important to safety that are identical to those previously reviewed by the Staff, and those where the adequacy of the system is based upon prior NRC approval. The bases for prior approval includes the Staff's evaluation of applications for construction permits and operating licenses, preliminary and final design approvals for standardized plants, and topical reports.

Additional background or detailed information relevant to the acceptance criteria and the review process of this section can be found in the references to this section.

II. Acceptance Criteria

The General Design Criteria (GDC) provided in the NRC regulations establish minimum requirements for the design of nuclear power plants. ANSI/IEEE Std 279 is also incorporated in 10 CFR Part 50, 50.55a(h) of the NRC's regulations. These criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety. The structures, systems, and components important to safety are those that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public. Although ANSI/IEEE Std 279 contains acceptance criteria only for protection systems, the concepts of ANSI/IEEE Std 279 are applicable as guidance to other I&C safety systems and to non-safety I&C system for which high functional reliability is a goal.

Regulatory guides amplify specific regulations, describe acceptable methods for meeting their requirements, and provide guidance to applicant/licensees. Industry codes and standards set forth requirements and recommended practices applicable to I&C systems for nuclear power plants. These standards are endorsed by regulatory guides, with or without modification, and provide acceptable methods for meeting the requirements of the regulations.

The acceptance criteria consist of the technical requirements of 10 CFR 50 including ANSI/IEEE Std 279 and the GDC, which establish the NRC requirements for I&C systems important to safety. The regulatory guides

and the endorsed industry codes and standards are the guidelines used as a basis for the evaluation of conformance to the requirements of the NRC's regulations. Table 7-1, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety," lists the acceptance criteria and guidelines applicable to I&C systems important to safety which are included in the evaluation of these systems as addressed in Chapter 7 of the SAR. Three Mile Island (TMI) Action Plan requirements for I&C systems important to safety are also identified in Table 7-1. Appendix 7.1-A describes the general process for reviewing any I&C system against the acceptance criteria and guidance identified in Table 7-1.

The IEEE superseded ANSI/IEEE Std 279 with IEEE Std 603 "Criteria for Safety Systems for Nuclear Power Generating Stations." The requirements and recommendations of IEEE Std 603, as endorsed by Reg. Guide 1.153 "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," incorporate the requirements and recommendations of ANSI/IEEE Std 279. The guidance described in IEEE Std 603 will be used by the NRC staff in its evaluation of the design, reliability, qualification, and testability of the power, I&C, and control portions of safety systems.

The scope of IEEE Std 603 includes all I&C safety systems, which are the systems covered in Sections 7.2 through 7.6 of the safety analysis report (SAR). Therefore, while the guidance of IEEE Std 603 and the requirements of ANSI/IEEE Std 279 are equally applicable to protection systems, IEEE Std 603 is more directly applicable to I&C safety systems other than the protection systems (i.e., information systems, safe shutdown systems, and interlock systems). The guidance of IEEE Std 603 is also more readily adaptable for use in the review of non-safety I&C systems.

Non-safety I&C systems are reviewed to ensure that they conform to the acceptance criteria and guidelines, that the controlled variables can be maintained within prescribed operating ranges, and that effects of operation or failure of these systems are bounded by the accident analyses in Chapter 15 of the SAR. This includes verification that non-safety systems are appropriately isolated from safety systems and that the quality and reliability of these systems is sufficient to minimize challenges to safety systems.

Supplemental Guidance for Digital Computer-Based Safety Systems

For designs that include digital computer-based I&C systems (including hardware, software and firmware), additional issues should be considered when evaluating compliance with 10 CFR 50. Appropriate references to review criteria and review procedures are also included in Appendices A, B, and C to this section.

Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors," and SECY-93-087 describe the additional issues involved. These issues and review criteria are summarized below. It is important to note that all criteria of 10 CFR 50 apply to safety-related digital I&C systems. The information here is intended only to clarify the application of certain of these requirements to digital systems, not to replace existing requirements or guidance.

Reg. Guide 1.28, "Quality Assurance Program Requirements (Design and Construction)," endorses the 1983 edition of ASME Std NQA-1, "Quality Assurance Requirements for Nuclear Facility Applications." The 1994 edition of NQA-1 also includes the former ASME Std NQA-2a, Part 2.7 of which addresses computer software. ASME Std NQA-2a, Part 2.7 is referenced by IEEE Std 7-4.3.2, Section 5.3.1, but has not been endorsed by the NRC.

1. Electromagnetic compatibility — Section 3(7) of ANSI/IEEE Std 279 requires that the design basis for protection systems document the range of transient and steady-state conditions throughout which the system must perform. IEEE Std 603 contains similar requirements. For digital computer-based systems, the range of conditions considered should include the electromagnetic environment, including electrostatic discharge. Electrical Power Research Institute (EPRI) topical report TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," and the associated Staff safety evaluation report describe an adequate guideline for qualifying digital I&C equipment for a plant environment. Lightning protection should be addressed as part of the review of electromagnetic compatibility. Lightning protection features should conform to the guidance of NFPA Std 78, "Lightning Protection Code," and ANSI/IEEE Std 665, "Guide for Generation Station Grounding."
2. Computer system quality — In order for safety-related, digital computer-based I&C systems to comply with the quality and reliability requirements of ANSI/IEEE Std 279, GDC 1, GDC 21, GDC 29, and 10 CFR 50 Appendix B, the computers (including embedded software) must be of high quality. The quality requirements applicable to hardware are well documented in ANSI/IEEE Std 279, IEEE Std 603, and ASME Std NQA-1. IEEE Std 7-4.3.2 identifies five areas where additional guidance is needed to support evaluation of digital systems with respect to these requirements.
 - a. Software development and hardware/software integration — An acceptable means of ensuring the quality of computer systems and their embedded software includes developing the software and then performing system integration using a well-structured and well-executed software engineering process. This process should (1) be in accordance with the requirements of 10 CFR 50 Appendix B, (2) be consistent with the guidance of ASME Std NQA-2a Part 2.7, and (3) implement a software engineering life cycle in accordance with the guidance of Reg. Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." BTP HICB-14 describes the characteristics of an acceptable software engineering process in more detail. The inspections and tests conducted as part of this process should demonstrate that the final product exhibits the qualities that characterize high quality software and the computer system, with its embedded software, performs as designed. BTP HICB-14 describes the characteristics the Staff expects I&C system software and software life cycle processes to exhibit.
 - b. Qualification of existing commercial computers, including predeveloped software (PDS) — To meet the fundamental quality requirements, the following should be qualified for use in the plant instrumentation systems: existing computers and predeveloped software (commercial off-the-shelf software, or PDS produced for another purpose). All software, including operating systems, resident on safety system computers at run time must be qualified for their intended applications. IEEE Std 7-4.3.2, Section 5.3.2 describes an acceptable set of fundamental requirements for this qualification process. This standard allows the use of engineering judgment for the acceptance of existing software, and the use of compensating factors to substitute for missing elements of the software development process. These provisions should not be interpreted to permit unsupported subjectivity in the acceptance of existing software. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," provides more detail on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors.

Programmable logic controllers (PLCs) are a possible means of implementing safety-related I&C using existing commercial computers. BTP HICB-18 describes an acceptable process for applying the recommendations of this section to PLC implementations.

- c. Software tools — Compliance with the fundamental quality requirements necessitates that computer-based tools used in the design of digital I&C not introduce faults into the software which is resident on the computer at run time. IEEE Std 7-4.3.2, Section 5.3.3 describes an acceptable means of preventing such faults. The qualification process described in EPRI TR-106439 and the development process described in BTP HICB-14 are acceptable alternative processes for ensuring the quality of software tools is adequate to minimize the introduction of faults into plant software.
 - d. Verification and validation — As described in Section 5.3.4 of IEEE Std 7-4.3.2, an acceptable software development process and hardware/software integration process will include verification and validation that provides adequate confidence that both the safety system requirements and those requirements defined at each stage of development, including handling of credible abnormal conditions, have been implemented. Implementation of a software engineering process as described by BTP HICB-14 will ensure adequate verification and validation. Reg. Guides 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," and 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describe acceptable approaches to planning and conducting certain verification and validation activities of a software engineering process.
 - e. Software configuration management — As described in Section 5.3.5 of IEEE Std 7-4.3.2, an acceptable software development process will include software configuration management in accordance with ASME NQA-2a Part 2.7. BTP HICB-14 describes the characteristics that the Staff expects software configuration management processes will exhibit. Reg. Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describes an acceptable method for implementing software configuration management.
3. Equipment qualification — To comply with the requirements of GDC 4, 10 CFR 50.49, and ANSI/IEEE Std 279 Sections 3.7, 4.4, & 4.5, environmental qualification must demonstrate that the design basis and performance requirements of the I&C system are met when the equipment is exposed to normal and adverse environments. SRP Appendices 7.1-B and 7.1-C describe the review of qualification for all environments.
 4. System integrity — ANSI/IEEE Std 279, Section 4.5 and GDC 21 require that all protection system channels maintain necessary functional capability under extremes of conditions relating to environment, energy supply, malfunctions, and accidents. Section 5.5 of IEEE Std 603 includes similar requirements for safety systems. Evaluation of digital systems with respect to these requirements includes assuring design for computer integrity and design for test and calibration.
 - a. Design for computer integrity — As discussed in Section 5.5.1 of IEEE Std 7-4.3.2, digital systems must be designed to perform their safety function when subjected to all conditions that have significant potential for defeating their safety function. Evaluation with respect to the other topics discussed for computer-based systems addresses many aspects of design for integrity. In addition, design for computer integrity involves selecting system architectures and design standards to ensure that system real-time performance is predictable and within design requirements. BTP HICB-21 describes the review of digital computer real-time performance.

- b. Design for test and calibration — Digital computer-based systems generally cannot be designed such that all failure modes are either "fail-safe" or revealed by indication of the failure. Therefore, automated self-test features may be necessary for failure detectability. Special features may also be needed to provide the capability to support surveillance testing. IEEE Std 603, Section 5.7 describes the fundamental guidance applicable to test and calibration features. BTP HICB-17 describes the automatic self-testing and surveillance testing features characteristic of an acceptable digital system.
5. Communications independence — Sections 4.6 and 4.7 of ANSI/IEEE Std 279 require independence between redundant channels of the protection system and between safety systems and non-safety systems. IEEE Std 603, Section 5.6 contains similar requirements as do GDC 21, 22, and 24. Evaluation of digital systems with respect to these requirements should consider the effect of data communications on independence and the isolation of safety and non-safety portions of computer software. This is in addition to the need to consider electrical and physical independence within any I&C system as discussed elsewhere in this chapter. Annex G of IEEE Std 7-4.3.2 describes acceptable approaches to computer communication independence. The preferred approach to communication independence ensures that (1) redundant safety-grade equipment communicate via one-way communications paths, (2) safety-grade systems do not receive information from non-safety-grade systems except when under test, (3) if two-way communications are used, failure of coordination or handshaking between sending and receiving systems does not prevent either system from functioning correctly, and (4) the control of communications links resides in the sending system. SRP Appendix 7.1-C provides guidance for the review of communications independence.
6. Reliability — GDC 21 and ANSI/IEEE Std 279 require that protection systems be designed with high functional reliability. IEEE Std 603 requires the analysis of system design to confirm that safety systems achieve the reliability goals established by the design basis. As discussed in Section 5.15 of IEEE Std 7-4.3.2, when reliability goals are established at the system level, the proof of meeting the goals must address software reliability.

The Staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the NRC's regulations for the reliability of digital computers used in safety systems. The NRC staff's acceptance of the reliability of the computer system is based on deterministic criteria for both the hardware and software rather than on quantitative reliability goals. This topic is discussed further in Reg. Guide 1.152 and SRP Appendix 7.1-C.

Nevertheless, qualitative reliability estimation using a combination of analysis, testing, and operating experience can provide an added level of confidence in a system's reliable performance. Qualitative estimation of software reliability should address the fact that 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.

Software that complies with the quality criteria of item 2 above and that is used in safety systems that provide measures for defense against common mode failures as described below are considered by the Staff to comply with the fundamental reliability requirements of GDC 21, ANSI/IEEE Std 279, and IEEE Std 603.

7. Defense against common-mode failures — Experience shows that flaws in requirements and design can be expected to exist in even the highest quality software despite good engineering processes and testing. These residual flaws pose the concern that the use of common software has the potential to propagate

common-cause or common-mode failures that can defeat the redundancy provided by hardware architectural structure. To address this issue, designs that incorporate digital computer-based protection systems must comply with the NRC position on defense-in-depth and diversity as described in the Staff Requirements Memorandum on SECY-93-087. BTP HICB-19 describes acceptable means for complying with this position.

8. Use of emerging software methods — Software engineering is a maturing field. Certain techniques that are still under development may be proposed by applicant/licensees. Two general areas of emerging methods are formal methods and the use of non-procedural languages. There may be other methods that should be considered. Proposal of such techniques for development of systems or components important to safety, or the use of commercial items using such techniques in systems important to safety, will require careful consideration by the reviewer.
 - a. Formal methods — Formal methods are approaches based on the use of mathematical techniques and notations for describing and analyzing properties of software systems. Descriptions of the system are written using notations based on mathematical expressions rather than a natural language such as English. This allows formal proof that the specification has certain properties such as completeness and internal consistency. Formal methods, knowledgeably applied, can improve the software development process. Therefore, the Staff encourages the informed use of formal methods as part of a applicant/licensee's software engineering process. The Staff, however, neither requires the use of formal methods nor will allow the use of formal methods to replace compliance with the fundamental acceptance criteria described in items 1 through 7 above. Section C.3.7 of Appendix 7.0-A discusses in more detail the use of formal and semiformal languages for describing software requirements and design.
 - b. Non-procedural languages — Non-procedural software techniques include expert systems, neural networks, fuzzy systems, and genetic algorithms. These methods are not sufficiently mature at this time to support the definition of processes for evaluating conformance with the acceptance criteria of 10 CFR 50 and ANSI/IEEE Std 279.

Application of the Supplemental Guidance to Computer-Based Systems Important to Safety

Digital computers may be used in non-safety systems that are important to safety and are provided to comply with:

- GDC 13 (Instrumentation & Control)
- GDC 19 (Remote Shutdown)
- 10 CFR 50 Appendix R, Section III.G.1.b (Remote Cold Shutdown)
- 10 CFR 50 Appendix R, Section III.L.1 (Alternate or Dedicated Shutdown)
- 10 CFR 50.62 (ATWS)
- 10 CFR 50.63 (Station Blackout)

- 10 CFR 50.47 (Emergency Response)

GDC 1 and 10 CFR 50.55a(a)(1) require that these systems be designed to quality standards commensurate with the importance of the safety function to be performed. Items 1, 2, 4, 6, and 8 above should be considered when evaluating such systems with respect to these criteria. Item 3 above should also be considered for systems whose failure under postulated environmental conditions could prevent satisfactory accomplishment of safety functions. Item 5 above should also be considered for reactivity control systems required for remote, alternate, or dedicated shutdown systems required by GDC 19 or 10 CFR 50 Appendix R.

Other acceptance criteria which are applicable to I&C systems important to safety are not included when the evaluation of conformance to such criteria is addressed in the review of other SAR sections. For example, GDC 3, "Fire Protection," is not included in Table 7-1 since conformance to the requirements of GDC 3 is addressed in the review of Section 9.5.1 of the SAR.

Appendix A to this SRP section provides guidance on the applicability and review methods to be used in evaluating conformance to the acceptance criteria and guidelines for I&C systems important to safety. Appendix B to this SRP section provides guidance to be used in the evaluation of conformance to the requirements of ANSI/IEEE Std 279. Appendix C to this SRP section provides guidance for evaluation of conformance to IEEE Std 603.

III. Review Procedures

Section 7.0 provides an overview of the review process for I&C systems. Within this process, the objectives of the review of Section 7.1 of the SAR are to confirm that the I&C systems important to safety are addressed in Chapter 7 of the SAR and that the applicant/licensee commits to appropriate acceptance criteria and guidelines applicable to each of these systems. This identification meets the applicable requirements of General Design Criterion 1, "Quality Standards and Records," of 10 CFR Part 50 Appendix A. General Design Criterion 1 requires that, "Structures, systems and components important to safety shall be designed, fabricated, erected and tested to quality standards commensurate with the importance of the safety function to be performed." Therefore, the review of Section 7.1 should confirm that the SAR includes (1) a discussion regarding the applicability of each criterion and guideline for each system important to safety, and (2) a statement that the criteria and guidelines are implemented or will be implemented in the design of I&C systems important to safety. If exceptions to the guidelines are taken, the review confirms that an acceptable basis has been provided for those exceptions.

The review of Section 7.1 of the SAR is performed as follows:

1. Section 7.1 is reviewed to confirm that all I&C systems important to safety are included in Chapter 7. Normally, Chapter 7 of the SAR should address each of the I&C systems included in the areas of review for Section 7.1 of the SRP. This review should confirm that all I&C systems, including embedded computers and software necessary to support the operation of safety systems, are identified in Section 7.1 and discussed in subsequent sections of Chapter 7. The safety systems supported by the I&C system are described in other sections of the SAR (particularly in Chapters 5, 6, 8, 9, 10, 15, and 18). The review of the systems identified is coordinated with the branches which have primary review responsibility for the supported systems.
2. The acceptance criteria applicable to each of the I&C systems important to safety are reviewed to confirm that the appropriate criteria have been identified for each system. Appendix 7.1-A identifies the

acceptance criteria applicable to the I&C systems important to safety, and describes the method and scope of the review to verify conformance.

3. The guidelines applicable to each of the I&C systems important to safety are reviewed to confirm that the appropriate guidelines have been identified for each system. Appendix 7.1-A identifies the guidelines applicable to the I&C systems important to safety, and describes the method and scope of the review to verify conformance.
4. When the applicant/licensee takes exceptions to the guidelines applicable to I&C systems important to safety, the bases for such exception are reviewed to confirm that they are acceptable. The bases for the exceptions to the guidelines should demonstrate that a significant reduction in the margin of safety does not result, and that the exceptions do not result in nonconformance to the requirements of the acceptance criteria.
5. When the applicant/licensee proposes I&C systems that incorporate digital computers, the review includes the supplemental guidance for digital computer based systems described in part II above. Appendix 7.0-A describes the review process.
6. The review includes those I&C systems important to safety that are identified as identical to systems that have been reviewed and approved by the Staff. The evaluation of these systems in subsequent sections of Chapter 7 is based upon prior Staff approval. Where differences exist between prior approvals, they should be identified, and the review should confirm that an adequate basis has been provided. The review should include an evaluation of differences to confirm that they are acceptable.
7. If the proposed systems employ technologies that have not previously been accepted by the Staff, the reviewer should identify these technologies and establish a basis for acceptance prior to proceeding with the review.
8. The proposed resolution of unresolved safety issues (USIs) and medium- and high-priority generic safety issues (GSIs) are reviewed. Appendix 7.1-A identifies the guidance for review of the resolution of USIs and GSIs.

Additional Review Steps for Design Certification or Combined License Applications

Under 10 CFR Part 52:

9. The certified design material (CDM) is reviewed to confirm that it describes the key characteristics, performance requirements and proposed inspections, tests, analyses and acceptance criteria (ITAAC) for each instrumentation system important to safety. SRP Chapter 14 contains guidance for the review of CDM. Additionally, the ITAAC implementation is reviewed to confirm that the as-built systems conform to the certified design.

IV. Evaluation Findings

The review confirms that sufficient information has been provided and that the review supports conclusions of the following type to be included in the Staff's safety evaluation report (SER).

The applicant/licensee has identified the I&C systems which are important to safety in accordance with Reg. Guide 1.70, Revision 3, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants," November 1978.

The applicant/licensee has identified the acceptance criteria consisting of the General Design Criteria and ANSI/IEEE Std. 279, included in the NRC's regulations, which are applicable to those systems as identified in the SRP. The applicant/licensee has also identified the guidelines consisting of the regulatory guides and the industry codes and standards which are applicable to the systems as identified in the SRP. [If exception to the guidelines has been taken by the applicant/licensee, an evaluation of the exception or a reference to the section of the SER which addresses those exceptions should be provided.] The Staff concludes that the implementation of the identified acceptance criteria and guidelines satisfies the requirements of GDC 1 with respect to the design, fabrication, erection, and testing to quality standards commensurate with the importance of the safety functions to be performed.

Note: the following finding applies only to applications under 10 CFR 52.

The review confirms that each of the safety systems identified in the SAR also has an associated design description and ITAAC.

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the Staff in its evaluation of conformance with NRC regulations.

Implementation schedules for conformance to parts of the method discussed herein are contained in the referenced regulatory guides.

VI. References

ANS Std 4.5. "Criteria for Accident Monitoring Functions in Light Water Cooled Reactors."

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std 323-1974. "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

ANSI/IEEE Std 665-1987. "Guide for Generation Station Grounding."

ANSI/IEEE Std 829-1983. "IEEE Standard for Software Test Documentation."

ANSI/IEEE Std 1008-1987. "IEEE Standard for Software Unit Testing."

ANSI/IEEE Std 1012-1986. "IEEE Standard for Software Verification and Validation Plans."

ASME Std NQA-1-1994. "Quality Assurance Requirements for Nuclear Facility Applications."

ASME Std NQA-2a-1990 Part 2.7. "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications."

EPRI Topical Report TR-102323. "Guidelines for Electromagnetic Interference Testing in Power Plants." Electric Power Research Institute, September 1994.

EPRI Topical Report TR-106439. "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." Electric Power Research Institute, October 1996.

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

IEEE Std 338-1987. "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."

IEEE Std 384-1992. "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

IEEE Std 828-1990. "IEEE Standard for Software Configuration Management Plans."

IEEE Std 830-1993. "IEEE Recommended Practice for Software Requirements Specifications."

IEEE Std 1028-1988. "IEEE Standard for Software Reviews and Audits."

IEEE Std 1042-1987. "IEEE Guide to Software Configuration Management."

IEEE Std 1074-1991. "IEEE Standard for Developing Software Life Cycle Processes."

ISA-S67.02-1980. "Nuclear-Safety-Related Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants."

ISA-S67.04-1994. "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants."

NFPA Std 78. "Lightning Protection Code." National Fire Protection Association, 1992.

NUREG/CR-6421. "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications." March 1996.

NUREG-0694. "TMI-Related Requirements for New Operating Reactor Licenses." 1980.

NUREG-0718 R01. "Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License." 1981.

NUREG-0737. "Clarification of TMI Action Plan Requirements." 1980.

NUREG-0933. "A Prioritization of Generic Safety Issues." Updated periodically.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.168. "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.169. "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.170. "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.171. "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.173. "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.28. "Quality Assurance Program Requirements (Design and Construction)." 1985.

Regulatory Guide 1.70. "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants." Office of Standards Development, U.S. Nuclear Regulatory Commission, November 1978.

Regulatory Guide 1.89. "Environmental Qualification of Certain Electric Equipment Important to Safety in Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1984.

Safety Evaluation by the Office of Nuclear Reactor Regulation. "EPRI Topical Report TR-102323." April 17, 1996.

Safety Evaluation by the Office of Nuclear Reactor Regulation. "EPRI Topical Report TR-106439." March 1997.

SECY-91-292. "Digital Computer Systems for Advanced Light Water Reactors." September 16, 1991.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.

Table 7-1. Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety

Version 12.0, May 2, 1997

The matrix of Table 7-1 identifies the acceptance criteria (denoted by "A") and the guidelines (denoted by "G") and their applicability to the various sections of Chapter 7 of the SAR. These acceptance criteria include the applicable General Design Criteria and ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," which establish the NRC requirements for the instrumentation and control systems important to safety. The guidelines for implementation of these requirements are provided in the current versions of regulatory guides, the endorsed industry standards, and the branch technical positions (BTPs) of the Instrumentation and Control Systems Branch (HICB). The BTPs listed in this table are contained in Appendix 7-A. The guidelines are not mandatory and only set forth acceptable methods of implementing the acceptance criteria. The BTPs are used when a particular design problem has an identified and acceptable solution; they also are not mandatory. In all cases, the primary basis for acceptance of the design is conformance to the acceptance criteria.

Industry standards that are not endorsed by regulatory guides or incorporated in regulations or BTPs, or that have not been previously used and accepted in the licensing process, must be reviewed before they can be accepted as a sole basis for approval of a design. They are useful as guidance for identifying the subjects of importance to be considered in the review of the systems important to safety.

TMI action plan requirements for instrumentation and control systems important to safety are imposed by 10 CFR 50.34(f) for applications approved after February 16, 1982. For operating reactors that had approved construction permits prior to February 16, 1982, the TMI action plan requirements were imposed by Generic Letters that required conformance with NUREG-0718, "Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License," NUREG-0737, "Clarification of TMI Action Plan Requirements," NUREG-0737, Supplement 1, "Clarification of TMI Action Plan Requirements — Requirements for Emergency Response Capability," and NUREG-0694, "TMI-Related Requirements for New Operating Reactor Licenses." Table 7.1 identifies both the CFR and TMI action plan reference numbers for the TMI action plan requirements relevant to Chapter 7 of the safety analysis report. The Action Plan references are given in brackets under the reference to the equivalent requirement of 10 CFR 50.34(f). Appendix 7.1-A presents specific acceptance criteria for TMI Action Plan items. However, important context information is found in the concepts contained in the referenced reports.

Table 7-1. Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety

Criteria	Title	Applicability									Remarks
		7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9		
1. 10 CFR Parts 50 and 52											
a.	50.55a(a)(1)	Quality Standards for Systems Important to Safety	A	A	A	A	A	A	A	A	
b.	50.55a(h)	Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Std 279)	A	A	*	*	*	*	*	**	
c.	50.34(f)(2)(v) [I.D.3]	Bypass and Inoperable Status Indication	A	A		A	A			**	See NUREG-0718, -0737, -0737 Supplement 1, and -0694
d.	50.34(f)(2)(xii) [II.E.1.2]	Auxiliary Feedwater System Automatic Initiation and Flow Indication		A		A					Applies only to PWRs. See NUREG-0718, -0737, and -0694
e.	50.34(f)(2)(xvii) [II.F.1]	Accident Monitoring Instrumentation				A					See NUREG-0718, -0737 Supplement 1, and -0694
f.	50.34(f)(2)(xviii) [II.F.2]	Inadequate Core Cooling Instrumentation				A					See NUREG-0694
g.	50.34(f)(2)(xiv) [II.E.4.2]	Containment Isolation Systems		A							See NUREG-0737
h.	50.34(f)(2)(xix) [II.F.3]	Instruments for Monitoring Plant Conditions Following Core Damage				A					See NUREG-0718
i.	50.34(f)(2)(xx) [II.G.1]	Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves			A	A					Applies only to PWRs. See NUREG-0737
j.	50.34(f)(2)(xxii) [II.K.2.g]	Failure Mode and Effect Analysis of Integrated Control System						A			Applies only to B&W plants. See NUREG-0718, -0737, and -0694
k.	50.34(f)(2)(xxiii)(II.K.2.10)	Anticipatory Trip on Loss of Main Feedwater or Turbine Trip	A								Applies only to B&W plants. See NUREG-0737, and -0694

* The ANSI/IEEE Std 279 requirement to provide adequate separation between protection and control function (item 4.7.2) applies to all instrumentation and control systems. The requirements for display of bypass and inoperable status indication (item 4.13) also apply to information systems important to safety (Section 7.5). Although not required by NRC regulations, the other criteria of ANSI/IEEE Std 279 and Reg. Guide 1.153 address considerations such as design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing that are used as guidance, where appropriate, for systems addressed in these sections of the SRP.

** The data communication systems (DCS) addressed by Section 7.9 are support systems for one or more of the systems addressed by Section 7.2 through 7.8. Acceptance criteria for a specific DCS derive from the acceptance criteria for the systems supported by that DCS. The criteria marked as ** are likely to apply to the DCS in one or more possible DCS applications. Section 7.9 gives more detailed guidance on the applicability of these criteria to specific DCS applications.

Criteria		Title	Applicability								Remarks
			7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9	
l.	50.34(f)(2)(xxiv) [II.K.3.23]	Central Reactor Vessel Water Level Recording				A					Applies only to BWRs. See NUREG-0718
m.	50.62	Requirements for Reduction of Risk from Anticipated Transients without Scram							A	**	
n.	52.47(a)(1)(iv)	Resolution of Unresolved and Generic Safety Issues	A	A	A	A	A	A	A	A	Applies only to applications for design certification or licensing of certified designs under Part 52
o.	52.47(a)(1)(vi)	ITAAC in Design Certification Applications	A	A	A	A	A	A	A	A	Applies only to applications for design certification or licensing of certified designs under Part 52
p.	52.47(a)(1)(vii)	Interface Requirements	A	A	A	A	A	A	A	A	Applies only to applications for design certification or licensing of certified designs under Part 52
q.	52.47(a)(2)	Level of Detail	A	A	A	A	A	A	A	A	Applies only to applications for design certification or licensing of certified designs under Part 52
r.	52.47(b)(2)(i)	Innovative Means of Accomplishing Safety Functions	A	A	A	A	A			A	Applies only to applications for design certification or licensing of certified designs under Part 52
s.	52.79(c)	ITAAC in Combined Operating License Applications	A	A	A	A	A	A	A	A	Applies only to applications for combined licenses under Part 52.
2. General Design Criteria (GDC) 10 CFR Part 50 Appendix A											
a.	GDC 1	Quality Standards and Records	A	A	A	A	A	A	A	A	
b.	GDC 2	Design Bases for Protection Against Natural Phenomena	A	A	A	A	A			**	
c.	GDC 4	Environmental and Missile Design Bases	A	A	A	A	A			**	
d.	GDC 13	Instrumentation and Control	A	A	A	A	A	A	A	**	
e.	GDC 19	Control Room	A	A	A	A	A	A	A	**	
f.	GDC 20	Protection System Functions	A	A							
g.	GDC 21	Protection Systems Reliability and Testability	A	A						**	

Criteria		Title	Applicability							Remarks	
			7.2	7.3	7.4	7.5	7.6	7.7	7.8		7.9
h.	GDC 22	Protection System Independence	A	A						**	
i.	GDC 23	Protection System Failure Modes	A	A						**	
j.	GDC 24	Separation of Protection and Control Systems	A	A	A	A	A	A	A	A	
k.	GDC 25	Protection System Requirements for Reactivity Control Malfunctions	A				A				
l.	GDC 29	Protection Against Anticipated Operational Occurrences	A					A		**	
3. Staff Requirements Memoranda											
a.	SRM to SECY 93-087 II.Q	Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems	A	A				A	A	**	See BTP HICB-19
b.	SRM to SECY 93-087 II.T	Control Room Annunciator (Alarm) Reliability				A				**	Applies only to advanced light water reactors
4. Regulatory Guides											
a.	Reg. Guide 1.22	Periodic Testing of Protection System Actuation Functions	G	G					G	**	See BTP HICB-8
b.	Reg. Guide 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System	G	G		G	G			**	
c.	Reg. Guide 1.53	Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems	G	G	G	G	G			**	See ANSI/IEEE Std 379 (ANSI N41.2)
d.	Reg. Guide 1.62	Manual Initiation of Protection Actions	G	G					G		
e.	Reg. Guide 1.75	Physical Independence of Electric Systems	G	G	G	G	G	G	G	G	See ANSI/IEEE Std 384 (ANSI/N41.14)
f.	Reg. Guide 1.97	Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident				G					See ANSI/ANS 4.5
g.	Draft Reg. Guide DG-1045	Proposed Revision 3 to Reg. Guide 1.105, "Instrument Spans and Setpoints"	G	G	G	G	G	G	G	G	See ISA Std S67.04 and BTP HICB-12
h.	Reg. Guide 1.118	Periodic Testing of Electric Power and Protection Systems	G	G	G	G	G		G	**	See IEEE Std 338
i.	Reg. Guide 1.151	Instrument Sensing Lines	G	G	G	G	G	G	G		See ANSI/ISA-S67.02
j.	Reg. Guide 1.152	Digital Computers in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See IEEE Std 7-4.3.2
k.	Reg. Guide 1.153	Power Instrumentation and Control Portions of Safety Systems	G	G	G	G	G	*	*	**	See IEEE Std 603

Criteria		Title	Applicability									Remarks
			7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9		
l.	Reg. Guide 1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See IEEE Std 828 and IEEE Std 1042	
m.	Reg. Guide 1.168	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See ANSI/IEEE Std 1012 and IEEE Std 1028	
n.	Reg. Guide 1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See IEEE Std 830	
o.	Reg. Guide 1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See ANSI/IEEE Std 829	
p.	Reg. Guide 1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See ANSI/IEEE Std 1008	
q.	Reg. Guide 1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See IEEE Std 1074	
5. Branch Technical Positions (BTP) HICB												
a.	BTP HICB-1	Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System					G					
b.	BTP HICB-2	Guidance on Requirements on Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines					G					
c.	BTP HICB-3	Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service	G	G								
d.	BTP HICB-4	Guidance on Design Criteria for Auxiliary Feedwater Systems		G								
e.	BTP HICB-5	Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors	G				G	G				
f.	BTP HICB-6	Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode		G								
g.	BTP HICB-7	Not used										

Criteria		Title	Applicability							Remarks	
			7.2	7.3	7.4	7.5	7.6	7.7	7.8		7.9
h.	BTP HICB-8	Guidance on Application of Regulatory Guide 1.22	G	G						**	
i.	BTP HICB-9	Guidance on Requirements for Reactor Protection System Anticipatory Trips	G								
j.	BTP HICB-10	Guidance on Application of Regulatory Guide 1.97				G					
k.	BTP HICB-11	Guidance on Application and Qualification of Isolation Devices	G	G	G	G	G	G	G	**	
l.	BTP HICB-12	Guidance on Establishing and Maintaining Instrument Setpoints	G	G	G	G	G		G	G	
m.	BTP HICB-13	Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors	G	G	G	G					
n.	BTP HICB-14	Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems	G	G	G	G	G	G	G	G	
o.	BTP HICB-15	Not used									
p.	BTP HICB-16	Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52.	G	G	G	G	G	G	G	G	
q.	BTP HICB-17	Guidance on Self-Test and Surveillance Test Provisions	G	G	G	G	G	G	G	G	
r.	BTP HICB-18	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems	G	G	G	G	G	G	G	G	
s.	BTP HICB-19	Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems	G	G				G	G	G	
t.	BTP HICB-20	Not used									
u.	BTP HICB-21	Guidance on Digital Computer Real-Time Performance	G	G	G	G	G	G	G	G	



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Appendix 7.1-A

Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety

The acceptance criteria and guidelines for instrumentation and control (I&C) systems important to safety are divided into four categories: (1) regulations including ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," (paragraph 50.55a(h) of 10 CFR 50), (2) the General Design Criteria (GDC) of 10 CFR 50 Appendix A, (3) regulatory guides (including endorsed industry codes and standards), and (4) branch technical positions (BTPs). An "applicability" statement describes how each criterion and guideline applies to the review of I&C systems. Conformance to the requirements of GDC 1 is evaluated in the review of Section 7.1 of the safety analysis report (SAR). Conformance to the remaining requirements of the GDC applicable to I&C systems is evaluated on a system basis in the review of Sections 7.2 through 7.9 of the SAR. Likewise, the degree of conformance to the guidelines provided in the SRP, regulatory guides, and industry codes and standards is evaluated on a system basis in the review of Sections 7.2 through 7.9 of the SAR. Where exceptions are taken to the guidance provided by regulatory guides, and endorsed industry codes and standards, they should be evaluated as a part of the review of the applicability of these criteria. The evaluation findings should be provided as a part of the review of Section 7.1 of the SAR, or the exception should be noted and a reference provided to the section where it is addressed.

Three Mile Island (TMI) action plan requirements for I&C system systems important to safety are imposed by 10 CFR 50.34(f) for applications approved after February 16, 1982. For operating reactors that had approved construction permits prior to February 16, 1982, the TMI action plan requirements were imposed by Generic Letters that required conformance with NUREG-0718, "Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License," NUREG-0737, "Clarification of TMI

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

Action Plan Requirements," NUREG-0737 Supplement 1, "Clarification of TMI Action Plan Requirements — Requirements for Emergency Response Capability," and NUREG-0694, "TMI-Related Requirements for New Operating Reactor Licenses." This appendix identifies both the CFR and TMI action plan reference numbers for the TMI action plan requirements relevant to Chapter 7 of the SAR. The action plan references are given in brackets following the reference to the equivalent requirement of 10 CFR 50.34(f). This appendix presents specific acceptance criteria for Three Mile Island (TMI) action plan items; however, important context information is found in the concepts contained in the referenced reports.

Acceptance criteria and guidelines are not included herein when the primary review responsibility for these aspects of I&C systems are reviewed in accordance with sections other than SRP Chapter 7.

1. Regulations — 10 CFR 50 and 10 CFR 52

a. 50.55a(a)(1) Quality Standards for Systems Important to Safety

"Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed."

Applicability — All I&C systems

Review Methods — The licensee should commit to conformance with the regulatory guides and standards referenced in Sections 7.1 through 7.9 and Chapter 7 Appendix A. The design should conform with all regulatory guides and standards committed to by the applicant/licensee.

b. 50.55a(h) (ANSI/IEEE Std 279)

Applicability — The protection systems: reactor trip system (RTS), engineered safety features actuation system (ESFAS), and supporting data communication systems. One part of ANSI/IEEE Std 279, section 4.7.2, "Isolation Devices," applies to all I&C systems. Section 4.13, "Indication of Bypasses," also applies to information systems important to safety.

Review Methods — Appendix 7.1-B provides guidance for evaluating conformance to the requirements of ANSI/IEEE Std 279, including the applicable regulatory guides. NRC staff will use the criteria of Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," in the evaluation of the design, reliability, qualification and testability of the power instrumentation control portions of safety related systems. Appendix 7.1-C provides guidance for evaluating conformance to the guidance of Reg. Guide 1.153.

c. 50.34(f)(2)(v) [TMI Action Plan Item I.D.3] Bypass and Inoperable Status Indication

"Provide for automatic indication of the bypassed and operable status of safety systems."

Applicability — The protection systems, RTS, ESFAS, information systems important to safety, interlock systems, and supporting data communication systems.

Review Methods — Review of compliance with 10 CFR 50.34(f)(2)(v) should address the following characteristics described in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics.

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Auxiliary features	6	17
Indication of bypasses	14	13
Control and protection system interaction	8	24

The evaluation of conformance with this requirement should be addressed in the review of Sections 7.2, 7.3, and 7.6 of the SAR. Bypass and inoperable status indication is required only for selected information system and interlock functions, as discussed in SRP Sections 7.5 and 7.6.

d. 50.34(f)(2)(xii) [TMI Action Plan Item II.E.1.2] Auxiliary Feedwater System Automatic Initiation and Flow Indication

"Provide automatic and manual auxiliary feedwater (AFW) system initiation, and provide auxiliary feedwater system flow indication in the control room. (Applicable to PWRs only)."

Applicability — ESFAS and information systems important to safety in pressurized water reactors (PWRs).

Review Methods — AFW initiation and flow indication should conform with the requirements applicable to the ESFAS and instrumentation systems. NUREG-0737 provides additional guidance on conformance with this requirement. The evaluation of conformance with this requirements should be addressed in the review of Section 7.3 and 7.5 of the SAR.

e. 50.34(f)(2)(xvii) [TMI Action Plan Item II.F.1] Accident Monitoring Instrumentation

"Provide instrumentation to measure, record and readout in the control room: (A) containment pressure, (B) containment water level, (C) containment hydrogen concentration, (D) containment radiation intensity (high level), and (E) noble gas effluents at all potential, accident release points. Provide for continuous sampling of radioactive iodines and particulates in gaseous effluents from all potential accident release points, and for onsite capability to analyze and measure these samples."

Applicability — Information systems important to safety.

Review Methods — The accident monitoring instrumentation functions required by 10 CFR 50.34(f)(2)(xvii) should be included in the information systems important to safety and reviewed in accordance with the review guidance provided in SAR Section 7.5. The evaluation of conformance with this requirement should be addressed in the review of Section 7.5 of the SAR.

f. 50.34(f)(2)(xviii) [TMI Action Plan Item II.F.2] Instrumentation for the Detection of Inadequate Core Cooling

"Provide instruments that provide in the control room an unambiguous indication of inadequate core cooling, such as primary coolant saturation meters in PWRs, and a suitable combination of signals from indicators of coolant level in the reactor vessel and in-core thermocouples in PWRs and BWRs."

Applicability — Information systems important to safety

Review Methods — Inadequate core cooling instrumentation functions should be included in the information systems important to safety and reviewed in accordance with the review guidance provided in SRP Section 7.5. Inadequate core cooling instrumentation should provide unambiguous indication of these conditions. It should provide the operator with sufficient information during accident situations to take planned manual actions, and to determine whether safety systems are operating properly. In addition, the instrumentation should also provide sufficient data for the operator to be able to evaluate the potential for core uncover and gross breach of protective barriers, including the resultant release of radioactivity to the environment. NUREG-0737 provides additional guidance on conformance with this requirement. The evaluation of conformance with this requirement should be addressed in the review of Section 7.5 of the SAR.

g. 50.34(f)(2)(xiv) [TMI Action Plan Item II.E.4.2] Containment Isolation Systems

"Provide containment isolation systems that (A) ensure all non-essential systems are isolated automatically by the containment isolation system; (B) for each non-essential penetration (except instrument lines) have two isolation barriers in series; (C) do not result in reopening of the containment isolation valves on resetting of the isolation signal; (D) utilize a containment set point pressure for initiating containment isolation as low as is compatible with normal operation; and (E) include automatic closing on a high radiation signal for all systems that provide a path to the environs."

Applicability — ESFAS — note that item (B) is not included in the scope of HICB review.

Review Methods — The containment isolation functions of the ESFAS should be reviewed to confirm that the ESFAS automatically closes each isolation device on each nonessential penetration. Signal diversity should be provided for the containment isolation function. For plants with digital-computer based ESFAS, signal diversity can be confirmed by review of the licensee/applicant's defense-in-depth and diversity analysis.

Reopening of isolation valves should be performed on a valve-by-valve basis, or on a line-by-line basis, provided that electrical independence and the single-failure criterion for the ESFAS functions continue to be satisfied. Ganged reopening of containment isolation valves is not acceptable.

Draft Reg. Guide DG-1045 (the proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems"), and BTP HICB-12 provide guidance on establishing and maintaining instrument setpoints. For isolation of nonessential containment penetrations, however, the trip setpoint should be established by adding measurement error terms to the highest pressure value expected during normal plant operations, rather than subtracting error terms from an accident analysis analytical limit. The setpoint should also be shown to be low enough to ensure protection system functions are actuated before analytical limits are reached. The pressure setpoint selected should be far enough above the maximum observed, or expected, pressure inside

containment during normal operation so that inadvertent containment isolation does not occur during normal operation from instrument drift or fluctuations due to the accuracy of the pressure sensor. The containment pressure history during normal operation should be used as a basis for arriving at an appropriate minimum pressure setpoint for initiating containment isolation. Applicants for new licenses should use pressure history data from similar plants that have operated for more than one year, if possible, to arrive at a minimum containment setpoint pressure.

Containment purge lines and other penetrations that provide a path to the environment should be isolated on a high radiation signal as one of the diverse isolation functions.

The review of these design provisions to address 10 CFR 50.34(f)(2)(xiv) should be addressed in the review of Section 7.3 of the SAR and should be coordinated with the Containment Systems and Severe Accident Branch (SCSB). NUREG-0737 provides additional guidance on conformance with these requirements.

h. 50.34(f)(2)(xix) [TMI Action Plan Item II.F.3] Instrument for Monitoring Plant Conditions Following Core Damage

"Provide instrumentation adequate for monitoring plant conditions following an accident that includes core damage."

Applicability — Information systems important to safety.

Review Methods — Instrumentation for monitoring plant conditions following core damage should be included in the information systems important to safety. There should be instrumentation of sufficient quantity, range, availability, and reliability to permit adequate monitoring of plant variables and systems during and after an accident. Sufficient information should be provided to the operator for (1) taking planned manual actions to shut the plant down safely; (2) determining whether the reactor trip, engineered safety feature systems, and manually initiated safety-related systems are performing their intended safety functions (i.e., reactivity control, core cooling, and maintaining reactor containment system (RCS) and containment integrity); and (3) determining the potential for causing a gross breach of the barriers to radioactivity release (i.e., fuel cladding). The evaluation of conformance with this requirement should be addressed in the review of Section 7.5 of the SAR.

i. 50.34(f)(2)(xx) [TMI Action Plan Item II.G.1] Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves

"Provide power supplies for pressurizer relief valves, block valves, and level indicators such that: (A) Level indicators are powered from vital buses, (B) motive and control power connections to the emergency power sources are through devices qualified in accordance with requirements applicable to systems important to safety, and (C) electric power is provided from emergency power sources. (Applicable to PWRs only)."

Applicability — Information systems important to safety in PWRs, and safe shutdown systems.

Review Methods — Pressurizer level indication, block valve position indication, and relief valve position indication should be supplied from a source of emergency power in the event of a loss of offsite power. The power supplies should conform with the guidance of NUREG-0737. The evaluation of conformance with this

requirement should be addressed in the review of Sections 7.4 and 7.5 of the SAR. The review of this requirement should be coordinated with the Electrical Engineering Branch (EELB).

j. 50.34(f)(2)(xxii) [TMI Action Plan Item II.K.2.9] Failure Mode and Effect Analysis of Integrated Control System

"Perform a failure modes and effects analysis of the integrated control system (ICS) to include consideration of failures and effects of input and output signals to the ICS. (Applicable to B&W-designed plants only)."

Applicability — Control systems in Babcock and Wilcox (B&W)-designed plants.

Review Methods — The recommendations of the generic failure modes and effects analysis described in BAW-1564, "Integrated Control System Reliability Analysis," should be incorporated into the design if this analysis applies to the plant. Otherwise a plant-specific failure mode and effect analysis should be conducted in accordance with NRC orders on B&W plants, and NUREG-0694. The evaluation of conformance with this requirement should be addressed in the review of Section 7.7 of the SAR.

k. 50.34(f)(2)(xxiii) [TMI Action Plan Item II.K.2.10] Anticipatory Trip on Loss of Main Feedwater or Turbine Trip

"Provide, as part of the reactor protection system, an anticipatory reactor trip that would be actuated on loss of main feedwater and on turbine trip. (Applicable to B&W-designed plants only)."

Applicability — RTS in B&W-designed plants.

Review Methods — The design should comply with the guidance of NUREG-0694 item II.K.1 and IEEE Std 279. Appendix 7.1-B item 6 and Appendix 7.1-C item 17 provide guidance on the review of auxiliary features such as anticipatory trips. The evaluation of conformance with this requirement should be addressed in the review of Section 7.2 of the SAR.

l. 50.34(f)(2)(xxiv) [TMI Action Plan Item II.K.3.23] Central Reactor Vessel Water Level Recording

"Provide the capability to record reactor vessel water level in one location on recorders that meet normal post-accident recording requirements. (Applicable to BWRs only)."

Applicability — Information systems important to safety in BWRs.

Review Methods — The capability should be provided to record water level over the range from the top of the vessel dome to the lowest pressure tap. This range of water level indication should be available in one location on recorders that meet normal post-accident recording requirements. The evaluation of conformance with this requirement should be addressed in the review of Section 7.5 of the SAR.

m. 50.62 Requirements for Reduction of Risk from Anticipated Transients without Scram

"(1) Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to

perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system. (2) Each pressurized water reactor manufactured by Combustion Engineering or by Babcock and Wilcox must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from sensor output to interruption of power to the control rods). (3) Each boiling water reactor must have an alternate rod injection (ARI) system that is diverse (from the reactor trip system) from sensor output to the final actuation device. The ARI system must have redundant scram air header exhaust valves. The ARI must be designed to perform its function in a reliable manner and be independent (from the existing reactor trip system) from sensor output to the final actuation device. (4) Each boiling water reactor must have a standby liquid control system (SLCS). The SLCS and its injection location must be designed to perform its function in a reliable manner. The SLCS initiation must be automatic and must be designed to perform its function in a reliable manner for plants granted a construction permit after July 26, 1984, and for plants granted a construction permit prior to July 26, 1984, that have already been designed and built to include this feature. (5) Each boiling water reactor must have equipment to trip the reactor coolant recirculating pumps automatically under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner."

Applicability — Systems and equipment used for mitigating ATWS events pursuant to the requirements of 10 CFR 50.62 and supporting data communication systems.

Review Methods — Section 7.8 provides guidance for the evaluation of conformance to the requirements of 10 CFR 50.62.

n. 52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

"An application for design certification must contain proposed technical resolutions of those unresolved safety issues and medium- and high-priority generic safety issues that are identified in the version of NUREG-0933 current on the date six months prior to application and that are technically relevant to the design."

Applicability — All I&C systems that are part of applications for design certification under 10 CFR 52, Subpart B, or combined licenses under 10 CFR 52, Subpart C.

Review Methods — The design must address the unresolved and generic safety issues applicable to I&C systems as discussed above. As of April 1, 1997, these items are the following:

1. Task Action Plan Items

- A-9 ATWS. Refer to Section 7.8.
- A-24 Qualification of Class 1E safety equipment. Refer to SRP Chapter 3, Appendix 7.1-B item 5, and Appendix 7.1-C item 9.
- A-47 Safety implications of control systems. Refer to resolution of Generic Letter 89-19.

2. Generic Issues

- 3 Setpoint drift in instrumentation. Refer to Draft Reg. Guide DG-1045 and BTP HICB-12.
- 45 Inoperability of instrumentation due to extreme cold weather. Refer to Reg. Guide 1.151, "Instrument Sensing Lines."
- 48 Limiting conditions for operation for Class 1E vital instrument buses in operating reactors. Refer to plant technical specification review in Chapter 16.
- 64 Identification of protection system instrument sensing lines. Refer to Appendix 7.1-B item 22, Appendix 7.1-C item 16, and Reg. Guide 1.151.
- 67.3.3 Improved accident monitoring. Refer to Reg. Guide 1.97 review in Section 7.5, BTP HICB-10 and 10 CFR 50.34 (f)(2)(xvii) and (xix) review.
- 75 Generic implications of ATWS events at Salem Nuclear Plant. Generic Letter 83-28. Refer to Appendix 7.1-B items 10 and 11 or Appendix 7.1-C items 12 and 27. Refer to Section 7.8 for review of ATWS mitigation systems.
- 120 On-line testability of protection systems. Refer to Appendix 7.1-B items 10 and 11 or Appendix 7.1-C items 12 and 27.
- 142 Leakage through electrical isolators in instrumentation circuits. Refer to Appendix 7.1-B items 3, 6, 7, and 8, or Appendix 7.1-C items 6, 10, 11, and 24.

3. Incorporation of Operating Experience

- Bulletin 80-06 "ESF Reset Controls."
- Bulletin 80-19 "Failures of Mercury-Wetted Matrix Relays in the RPS."
- Bulletin 80-20 "Failures of Westinghouse Type W-2 Spring Return to Neutral Control Switches."
- Bulletin 90-01 and Supplement 1 to Bulletin 90-01 "Loss of Fill-Oil in Transmitters Manufactured by Rosemount."
- Generic Letter 83-28 "Required Actions Based on Generic Implications of Salem ATWS Events."
- Generic Letter 85-06 "Quality Assurance Guidance for ATWS Equipment That is not Safety-Related."
- Generic Letter 89-19 "Request for Action Related to Resolution of USI A-47."
- Generic Letter 93-08 "Relocation of Technical Specification Tables of Instrument Response Time Limits."
- Generic Letter 95-02 "Use of NUMARC/EPRI Report TR-102348, 'Guideline on Licensing Digital Upgrades,' in Determining Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59."

The evaluation of conformance with this requirement for I&C systems should be addressed in the review of Section 7.1 through 7.9 of the SAR and the review of design certification documentation. The reviewer may document compliance with these requirements in Section 7 of the SER or may provide input to a separate SER section regarding resolution of generic issues.

o. 52.47(a)(1)(vi) ITAAC in Design Certification Applications

"An application for design certification must contain proposed tests, inspections, analyses, and acceptance criteria which are necessary and sufficient to provide reasonable assurance that, if the tests, inspections and analyses are performed and the acceptance criteria met, a plant which references the design is built and will operate in accordance with the design certification."

Applicability — All I&C systems that are part of applications for design certification under 10 CFR 52, Subpart B, or combined licenses under 10 CFR 52, Subpart C.

Review Methods — The ITAAC for I&C systems important to safety should be provided for each system in subsequent sections of Chapter 7 of the SAR. SECY-91-178, "Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) for Design Certifications and Combined Licenses," and Section 14.3 provide guidance on conformance to 10 CFR 52.47(a)(1)(vi). The evaluation of conformance with this requirement for I&C systems should be addressed by review of Section 7.1 through 7.9 of the SAR and the review of design certification documentation in conjunction with review of Section 14.3.5 of the SAR. Section 14.3 of the SRP describes the general acceptance criteria and review procedures for ITAAC. Section 14.3.5 describes the specific acceptance criteria and review procedures for I&C system ITAAC. The Staff review with respect to these requirements is documented in Section 14.3 of the SER.

p. 52.47(a)(1)(vii) Interface Requirements

"An application for design certification must contain the interface requirements to be met by those portions of the plant for which the application does not seek certification. These requirements must be sufficiently detailed to allow completion of the final safety analysis and design-specific probabilistic risk assessment required by paragraph (a)(1)(v) of this section."

Applicability — All I&C systems that are part of applications for design certification under 10 CFR 52, Subpart B, or combined licenses under 10 CFR 52, Subpart C.

Review Methods — The evaluation of conformance with this requirement for I&C systems should be addressed by review of Section 7.1 through 7.9 of the SAR and the review of design certification documentation in conjunction with review of Section 14.3.5 of the SAR. SRP Section 1.8 describes the review methods for interface requirements.

q. 52.47(a)(2) Level of Detail

"The application must contain a level of design information sufficient to enable the Commission to judge the applicant/licensee's proposed means of assuring that construction conforms to the design and to reach a final

conclusion on all safety questions associated with the design before the certification is granted. The information submitted for a design certification must include performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant/licensee. The Commission will require, prior to design certification, that information normally contained in certain procurement specifications and construction and installation specifications be completed and available for audit if such information is necessary for the Commission to make its safety determination."

Applicability — All I&C safety systems that are part of applications for design certification under 10 CFR 52, Subpart B, or combined licenses under 10 CFR 52, Subpart C.

Review Methods — Sufficient information for an NRC safety determination should be provided for each I&C system. BTP HICB-16 provides additional guidance for evaluating the sufficiency of the information about I&C system in design certification applications made under 10 CFR 52, Subpart B.

r. 52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

"Certification of a standard design which differs significantly from the light water reactor designs described in paragraph (b)(1) of this section or utilizes simplified, inherent, passive, or other innovative means to accomplish its safety functions will be granted only if (A) (1) The performance of each safety feature of the design has been demonstrated through either analysis, appropriate test programs, experience, or a combination thereof; (2) Interdependent effects among the safety features of the design have been found acceptable by analysis, appropriate test programs, experience, or a combination thereof; (3) Sufficient data exist on the safety features of the design to assess the analytical tools used for safety analyses over a sufficient range of normal operating conditions, transient conditions, and specified accident sequences, including equilibrium core conditions; and (4) The scope of the design is complete except for site-specific elements such as the service water intake structure and the ultimate heat sink; or (B) There has been acceptable testing of an appropriately sited, full-size, prototype of the design over a sufficient range of normal operating conditions, transient conditions, and specified accident sequences, including equilibrium core conditions. If the criterion in paragraph (b)(2)(i)(A)(4) of this section is not met, the testing of the prototype must demonstrate that the non-certified portion of the plant cannot significantly affect the safe operation of the plant."

Applicability — The protection systems, RTS and ESFAS in applications for design certification under 10 CFR 52, Subpart B, or combined licenses under 10 CFR 52, Subpart C.

Review Methods — The reviewer should identify technologies that have not previously been accepted by the Staff and establish a basis for acceptance prior to proceeding with the review.

s. 52.79(c) ITAAC in Combined License Applications

"The application for a combined license must include the proposed inspections, tests and analyses, including those applicable to emergency planning, which the licensee shall perform and the acceptance criteria therefore which are necessary and sufficient to provide reasonable assurance that, if the inspections, tests and analyses are performed and the acceptance criteria met, the facility has been constructed and will operate in conformity with the combined license, the provisions of the Atomic Energy Act, and the NRC's

regulations. Where the application references a certified standard design, the inspections, tests, analyses and acceptance criteria contained in the certified design must apply to those portions of the facility design which are covered by the design certification."

Applicability — All I&C systems that are part of applications for combined licenses under 10 CFR 52, Subpart C.

Review Methods — The ITAAC for I&C systems important to safety should be provided for each system in subsequent sections of Chapter 7 of the SAR. SECY-91-178 and SRP Section 14.3 provide guidance on conformance to 10 CFR 52.47(c). The evaluation of conformance with this requirement for I&C systems should be addressed by review of Section 7.1 through 7.9 of the SAR and the review of combined license documentation in conjunction with review of Section 14.3.5 of the SAR. Section 14.3 of the SRP describes the general acceptance criteria and review procedures for ITAAC. Section 14.3.5 describes the specific acceptance criteria and review procedures for I&C system ITAAC. The Staff review with respect to these requirements is documented in Section 14.3 of the SER.

2. 10 CFR 50 Appendix A, General Design Criteria

a. Criterion 1 — Quality Standards and Records

"Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit."

Applicability — All I&C systems and components important to safety.

Review Methods — Regulatory guides and endorsed codes and standards applicable to I&C systems important to safety are identified in Section 4 of this appendix. These guidelines provide the information needed to determine their applicability. The review of Section 7.1 of the SAR should confirm that the appropriate regulatory guides and endorsed standards are identified as applicable for each instrument and control system important to safety.

The evaluation of the quality assurance program and appropriate records are addressed in the review of Section 17 of the SAR.

b. Criterion 2 — Design Bases for Protection Against Natural Phenomena

"Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunamis, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy,

quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena, and (3) the importance of the safety functions to be performed."

Applicability — All instrumentation and control safety systems and supporting data communication systems.

Review Methods — The design bases for protection against natural phenomena for I&C systems important to safety should be provided for the I&C system. The design bases should identify those systems and components which should be qualified to survive the effects of earthquakes and other natural phenomena. The review should confirm that the I&C systems important to safety are qualified for protection against natural phenomena consistent with the analysis of these events as provided in Chapter 3 of the SAR, and that they are located and housed in structures consistent with these requirements.

The evaluation of the adequacy of qualification programs to demonstrate the capability of I&C systems to withstand the effects of natural phenomena is addressed in the review of Section 3.10 of the SAR.

The instrumentation systems needed for severe accidents must be designed so there is reasonable assurance that they will operate in the severe-accident environment for which they are intended, and over the time span for which they are needed. They need not be subject to additional environmental or seismic qualification testing or analysis.

The review of conformance with GDC 2 should be coordinated with the Plant Systems Branch (SPLB) and the Mechanical Engineering Branch (EMEB).

c. Criterion 4 — Environmental and Missile Design Bases

"Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids that may result from equipment failures and from events and conditions outside the nuclear power unit."

Applicability — All I&C safety systems and supporting data communication systems.

Review Methods — The environmental and missile design bases for I&C systems important to safety should be provided for each system in subsequent sections of Chapter 7 of the SAR. The design bases should identify those systems and components that are qualified to accommodate the effects of environmental conditions and protected from dynamic effects of missiles, pipe whipping, and discharging fluids. If systems or components are qualified to survive the environmental effects of postulated accidents for limited periods of time, the bases for limited operability should be provided. Review of equipment qualification for environmental conditions should be conducted in accordance with the guidance provided in Appendix 7.1-B item 5 and Appendix 7.1-C item 9.

The instrumentation systems needed for severe accidents must be designed so there is reasonable assurance that they will operate in the severe-accident environment for which they are intended and over the time span for which they are needed. They need not be subject to additional environmental qualification requirements.

The review of this requirement should be coordinated with EELB.

d. Criterion 13 — Instrumentation and Control

"Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges."

Applicability — All I&C systems and supporting data communication systems.

Review Methods — Review of compliance with GDC 13 should include consideration of the following topics.

- Instrumentation to monitor plant variables and systems — See SRP Sections 7.5 and 7.7.
- Instrumentation to monitor the status of protection systems — See Appendix 7.1-B items 10, 13, 18, and 20, or Appendix 7.1-C items 13 and 27.
- Instrumentation and controls for manual initiation of safety functions — See Appendix 7.1-B items 18 and 20 or Appendix 7.1-C items 13, 18, and 23.
- Instrumentation and controls to support diverse actuation of safety functions — See Section 7.8.
- Instrumentation and controls to regulate ESF systems — See Section 7.3.
- Interlocks to maintain variables and systems within safe states — See Section 7.6.
- Instrumentation and controls to maintain variables and systems within normal operational limits — See Section 7.7.
- Protection of instrument sensing lines from environmental extremes — See Reg. Guide 1.151.
- Setpoints for instrumentation system alarms and control system actions — See BTP HICB-12.
- Data communication systems that support plant instrumentation and controls — See Section 7.9.

Instrumentation and control systems should support conformance to the regulatory requirements applicable to the process systems which they control. Requirements to be noted in this regard include the following General Design Criteria.

General Design Criterion	Lead Reviewer	Location of Review Guidance
GDC 10 Reactor Design	Reactor Systems Branch (SRXB)	SRP Chapter 4
GDC 12 Suppression of Reactor Power Oscillations	SRXB	SRP Section 4.3
GDC 15 Reactor Coolant System Design	SRXB	SRP Section 5.4
GDC 16 Containment Design	Containment and Severe Accident Branch (SCSB)	SRP Section 6.2
GDC 28 Reactivity Limits	SRXB	SRP Section 4.3
GDC 33 Reactor Coolant Makeup	SRXB	SRP Chapter 9
GDC 34 Residual Heat Removal	SRXB	SRP Sections 5.4.6 and 5.4.7
GDC 35 Emergency Core Cooling	SRXB	SRP Section 6.3
GDC 38 Containment Heat Removal	SCSB	SRP Section 6.2.2
GDC 41 Containment Atmosphere Cleanup	Plant Systems Branch (SPLB)	SRP Section 6.5
GDC 44 Cooling Water	SPLB	SRP Chapter 9

Depending upon the applicant/licensee instrumentation and control system architecture, review of instrumentation and controls for these functions may be an HICB primary review responsibility as part of the review of SAR Chapter 7, or a secondary responsibility supporting other branches' review of other SAR sections. The review methods described in this Appendix should be used as appropriate. The review guidance of Appendix 7.1-B or Appendix 7.1-C should also be applied to I&C systems required for operation of engineered safety feature systems or their essential auxiliary systems.

e. Criterion 19 — Control Room

"A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident.

"Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures."

Applicability — All I&C systems and supporting data communication systems.

Review Methods — The evaluation of the instrumentation and controls available to operate the nuclear power unit under normal and accident conditions is addressed in the review of Sections 7.3, 7.5, and Section 7.7 of the SAR. The evaluation of reactor trip functions, interlock functions, and diverse I&C functions that support safe operation are addressed in the review of Sections 7.2, 7.6, and 7.8 of the SAR. The evaluation of safe shutdown and remote shutdown capabilities are addressed in the review of Section 7.4 of the SAR.

The adequacy of the human factor aspects of the control room design is addressed in the review of Chapter 18 of the SAR. The evaluation of the habitability aspects of GDC 19 with respect to radiation protection is addressed in the review of Section 6.4 of the SAR.

Guidelines for the review of safe shutdown capabilities, including remote shutdown capabilities, are provided in SRP Section 7.4.

f. Criterion 20 — Protection System Functions

"The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences, and (2) to sense accident conditions and to initiate the operation of systems and components important to safety."

Applicability — The protection systems, RTS and ESFAS.

Review Methods — Review of compliance with GDC 20 should address the following characteristics described in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics.

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Design basis requirements	1	4
General function requirements	2	5 and 22
System integrity	6	10
Setpoints	1	30

The evaluation of conformance with this requirement should be addressed in the review of Sections 7.2 and 7.3 of the SAR.

g. Criterion 21 — Protection System Reliability and Testability

"The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function, and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred."

Applicability — The protection systems, RTS, ESFAS, and supporting data communication systems.

Review Methods — Review of compliance with GDC 21 should address the following characteristics described in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics.

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Design basis reliability requirements and reliability determination methods	1	4
Single-failure criterion	3	6
Completion of protective action once initiated	17	7 and 25
Quality	4	8
System integrity	6	10
Physical, electrical, and communications independence	7 and 8	11 and 24
Capability for test and calibration	10 and 11	12 and 27
Indication of bypass	14	13
Control of access to safety system equipment	15 and 19	14
Repair and troubleshooting provisions	21	15
Identification of protection system equipment	22	16
Auxiliary features	6	17
Multi-unit stations	6	18
Human factors considerations	20	19
Reliability	2	20

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Manual controls	18	23
Derivation of system inputs	9	26
Operating bypasses	13	28
Maintenance bypasses	12	29
Multiple setpoints	16	30
Power sources	6	31

The evaluation of conformance with this requirement should be addressed in the review of Sections 7.2 and 7.3 of the SAR.

h. Criterion 22 — Protection System Independence

"The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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."

Applicability — The protection systems — RTS, ESFAS, and supporting data communication systems.

Review Methods — Review of compliance with GDC 22 should address the following characteristics described in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics.

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Design basis reliability requirements	1	4
Single-failure criterion	3	6
Quality	4	8
Equipment qualification	5	9
System integrity	6	10
Physical, electrical, and communications independence	7 and 8	11 and 24
Manual controls	18	23

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Setpoints	1	30
Power sources	6	31

i. Criterion 23 — Protection System Failure Modes

"The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire pressure, steam, water, and radiation) are experienced."

Applicability — The protection systems, RTS, ESFAS, and supporting data communication systems.

Review Methods — Review of compliance with GDC 23 is accomplished as part of the review of system integrity requirements discussed in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics. Appendix 7.1-B item 7 and Appendix 7.1-C item 10 provide review guidance that encompass the review with respect to compliance with GDC 23. The evaluation of conformance with this requirement should be addressed in the review of Sections 7.2 and 7.3 of the SAR.

j. Criterion 24 — Separation of Protection and Control Systems

"The protection system shall 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 which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

Applicability — All I&C systems.

Review Methods — Review of compliance with GDC 24 should address the following characteristics described in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics.

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Single-failure criterion	3	6
Independence	7	11

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Control–protection interaction	8	24
Auxiliary features	6	17
Power sources	6	31

Separation of protection and control systems should be considered in the review of all sections of Chapter 7 of the SAR to confirm that all interfaces between control systems and protection systems have been properly identified and addressed.

k. Criterion 25 — Protection System Requirements for Reactivity Control Malfunctions

"The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods."

Applicability — The reactor trip system. Also reactivity control system interlocks identified in Chapter 15 as required to ensure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems.

Review Methods — Confirmation that the protection system is designed for an appropriate spectrum of reactivity control system malfunctions is addressed in the review of protection system design basis requirements as discussed in ANSI/IEEE Std 279 and IEEE Std 603. Appendix 7.1-B item 1 and Appendix 7.1-C item 4 provide review guidance for this topic. The evaluation of conformance with this requirement should be addressed in the review of Section 7.2 of the SAR.

l. Criterion 29 — Protection Against Anticipated Operational Occurrences

"The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences."

Applicability — The protection systems, reactivity control functions of control systems, and supporting data communication systems.

Review Methods — Evaluation with respect to the requirements of GDC 29 is based upon conformance of the protection system and reactivity control systems to the applicable GDCs discussed in Sections a through k above. Probabilistic reliability assessments may be performed by the NRC staff to provide a basis for development of deterministic criteria for specific systems. The review of these systems will address conformance to the deterministic criteria so established. Conformance of the reactivity control systems to GDC 29 is addressed in the review of Section 7.2 of the SAR.

3. Staff Requirements Memoranda

Note: This section quotes positions that are extracted from Staff Requirements Memoranda (SRM) and the associated SECY memoranda. Specific positions are not necessarily separated from explanatory material in these documents. The quotes given here do not include the explanatory material provided in the SECY or SRM. The quotes may also combine material from the SRM and SECY to fully represent the NRC position.

a. Item II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control systems" of Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.
2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the SAR using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.
3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

Applicability — RTS, ESFAS, diverse instrumentation and control systems, control systems, and supporting data communication systems in plants utilizing digital computer-based RTS or ESFAS.

Review Methods — BTP HICB-19 provides guidance for the evaluation of compliance with this requirement. SRP Sections 7.7 and 7.8 provide guidance for the review of control system and diverse instrumentation and control system features that are credited as non-safety diverse means of protecting against common-mode failure within the safety systems.

b. Item II.T, "Control Room Annunciator (Alarm) Reliability," of Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"

The annunciator system is considered to consist of sets of alarms (which may be displayed on tiles, video display units (VDUs), or other devices) and sound equipment; logic and processing support; and functions to enable operators to silence, acknowledge, reset, and test alarms.

The main control room (MCR) shall contain compact, redundant operator workstations with multiple display and control devices that provide organized, hierarchical access to alarms, displays, and controls. Each workstation shall have the full capability to perform MCR functions as well as support division of tasks between two operators.

The display and control features shall be designed to satisfy existing regulations, for example: separation and independence requirements for Class 1E circuits (IEEE Std 384, "Criteria for Separation of Class 1E Equipment and Circuits"); criteria for protection systems (ANSI/IEEE Std 279); and requirements for manual initiation of protective actions at the systems level (Reg. Guide 1.62, "Manual Initiation of Protection Action"). The designer shall use existing defensive measures (e.g., segmentation, fault tolerance, signal validation, self-testing, error checking, and supervisory watchdog programs), as appropriate, to ensure that alarm, display, and control functions provided by the redundant workstations meet these standards.

Alarms that are 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, shall meet the applicable requirements for Class 1E equipment and circuits.

Applicability — Information systems important to safety and supporting data communication systems in advanced light water reactors.

Review Methods — Section 7.5 describes methods for review of annunciator systems in ALWRs.

4. Regulatory Guides (including endorsed industry codes and standards) and Branch Technical Positions

a. Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions"

Applicability — RTS, ESFAS, diverse instrumentation and control systems, and supporting data communication systems.

Review Methods — Reg. Guide 1.22 provides bases for evaluating conformance to GDC 21 and ANSI/IEEE Std 279, Sections 4.10 through 4.13. BTP HICB-8 describes the Staff position on the scope of periodic testing in protection systems. BTP HICB-17 provides additional guidance on acceptable periodic testing provisions for digital computer-based systems.

b. Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"

Applicability — RTS, ESFAS, information systems important to safety, safety interlock systems, and supporting data communication systems.

Review Methods — Reg. Guide 1.47 provides bases for evaluating conformance to GDC 21 and ANSI/IEEE Std 279, Sections 4.13 and 4.20 for protection systems. The regulatory guide also provides bases for evaluating the adequacy of bypass and inoperable status indication for I&C systems important to safety as addressed in the review of Section 7.5 of the SAR.

- c. *Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems,"* (Endorses ANSI/IEEE Std 379, Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems")

Applicability — All I&C safety systems and supporting data communication systems.

Review Methods — Reg. Guide 1.53 provides a basis for evaluating conformance to GDC 21 and ANSI/IEEE Std 279, Section 4.2.

- d. *Regulatory Guide 1.62, "Manual Initiation of Protection Action"*

Applicability — RTS, ESFAS, and diverse instrumentation and control systems.

Review Methods — Reg. Guide 1.62 provides a basis for evaluating conformance to ANSI/IEEE Std 279, Section 4.17. Reg. Guide 1.62 also provides guidance that should be considered in the review of manual initiation of ATWS mitigation and diverse actuation system functions.

- e. *Regulatory Guide 1.75, "Physical Independence of Electrical Systems,"* (Endorses IEEE Std 384, "Criteria for Separation of Class 1E Equipment and Circuits")

Applicability — All I&C systems.

Review Methods — Reg. Guide 1.75 provides a basis for evaluating conformance to GDC 21 and ANSI/IEEE Std 279, Sections 4.6 and 4.22 for protection systems and for evaluating the adequacy of I&C systems important to safety that incorporate redundant or diverse features to satisfy the single-failure criterion. The HICB evaluation is limited to the review of components and electrical wiring inside racks, panels, and control boards for systems important to safety. The evaluation of the physical separation of electrical cables is addressed in the review of Chapter 8 of the SAR.

- f. *Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident"*

Applicability — Information systems important to safety.

Review Methods — Reg. Guide 1.97 provides a basis for evaluating conformance to GDC 13. The HICB evaluation is limited to the review of instrumentation for monitoring plant conditions. The evaluation of instrumentation for monitoring environs conditions and radiation monitoring systems are addressed in the review of other sections of the SAR. Section 7.5 and BTP HICB-10 describe the review of post-accident monitoring systems.

- g. *Draft Regulatory Guide DG-1045, proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems,"* (Endorses ISA-S67.04, "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants")

Applicability — All I&C systems.

Review Methods — Draft Reg. Guide DG-1045 provides a basis for evaluating conformance to GDC 13 and ANSI/IEEE Std 279, Section 3. BTP HICB-12 provides guidance for establishing and maintaining instrument set points.

Draft Reg. Guide DG-1045 and ISA-S67.04 are specifically directed at establishing setpoints for trip functions. Nevertheless, their guidance is equally relevant to accounting for measurement uncertainties when determining the indicated plant conditions at which emergency procedures will require operator action, determining the setpoint for interlock functions, and determining setpoints for control functions provided to maintain plant variables and systems within prescribed operating ranges. Therefore, the guidance of Draft Reg. Guide DG-1045 is useful in reviewing all I&C systems important to safety even if no automatic trip functions are involved.

h. Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," (Endorses IEEE Std 338, Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems")

Applicability — All I&C safety systems, diverse instrumentation and control systems, and supporting data communication systems.

Review Methods — Reg. Guide 1.118 provides a basis for evaluating conformance to GDC 21 and ANSI/IEEE Std 279, Section 4.10. The HICB evaluation is limited to the review of testing of protection systems. The evaluation of testing of electric power systems is addressed by others in the review of Chapter 8 of the SAR. BTP HICB-17 discusses periodic test provisions in digital computer-based systems.

i. Regulatory Guide 1.151, "Instrument Sensing Lines," (Endorses ANSI/ISA-S67.02, "Nuclear Safety-Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants")

Applicability — I&C sensing lines and sensing line environmental control systems.

Review Methods — Reg. Guide 1.151 provides a basis for evaluating conformance to GDC 13. Environmental control systems for all I&C systems are addressed in the review of Section 7.7 of the SAR.

j. Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," (Endorses IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations")

Applicability — All instrumentation and control safety systems and supporting data communication systems.

Review Methods — Reg. Guide 1.152 provides a basis for evaluating conformance of computers with GDC 21. Appendix 7.1-C provides review guidance for the evaluation of conformance to the guidance of Reg. Guide 1.152 in conjunction with Reg. Guide 1.153.

k. Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," (Endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations")

Applicability — All instrumentation and control safety systems and supporting data communication systems.

Review Methods — Reg. Guide 1.153 provides an acceptable method of addressing the requirements of ANSI/IEEE Std 279. Appendix C to Section 7.1 provides guidance for the evaluation of conformance to the guidance of Reg. Guide 1.153 as supplemented by Reg. Guide 1.152.

- l. Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,"* (Endorses ANSI/IEEE Std 1012, "IEEE Standard for Software Verification and Validation Plans," and IEEE Std 1028, "IEEE Standard for Software Reviews and Audits")

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.168 provides a basis for evaluating conformance with 10 CFR 50.55a(a)(1), 50.55a(h), GDC 1 and Criteria I, II, III, XI, and XVIII of 10 CFR 50 Appendix B for computer-based systems. It endorses, with comments, ANSI/IEEE Std 1012 for planning the verification and validation of safety system software. It also endorses, with comments, IEEE Std 1028 as providing acceptable approaches for carrying out software reviews, inspections, walkthroughs, and audits.

BTP HICB-14 describes the review of planning, and implementation of verification, validation, and audits of digital computer software.

- m. Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,"* (Endorses IEEE Std 828, "IEEE Standard for Software Configuration Management Plans," and ANSI/IEEE Std 1042, "IEEE Guide to Software Configuration Management")

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.169 provides a basis for evaluating conformance with 10 CFR 50.55a(a)(1), 50.55a(h), GDC 1 and Criterion III of 10 CFR 50 Appendix B for computer-based systems. It endorses, with comments, IEEE Std 828 for planning the configuration management of safety system software. It also endorses, with comments, ANSI/IEEE Std 1042 as acceptable guidance for carrying out configuration management plans produced under the auspices of IEEE Std 828.

BTP HICB-14 describes the review of configuration management for digital computer software.

- n. Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,"* (Endorses IEEE Std 829, "IEEE Standard for Software Test Documentation")

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.170 provides a basis for evaluating conformance with 10 CFR 50.55a(h), GDC 1, GDC 21, and Criteria I, III, IV, VI, XI, and XVII of 10 CFR 50 Appendix B for computer-based

systems. It endorses, with comments, IEEE Std 829 as providing acceptable approaches for documenting software testing.

BTP HICB-14 describes the review of testing of digital computer software.

- o. Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," (Endorses ANSI/IEEE Std 1008, "IEEE Standard for Software Unit Testing")*

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.171 provides a basis for evaluating conformance with 10 CFR 50.55a(h), GDC 1, GDC 21 and Criteria I, II, III, V, VI, XI, and XVII of 10 CFR 50 Appendix B for computer-based systems. It endorses, with comments, ANSI/IEEE Std 1008 as providing acceptable approaches to unit testing of software.

BTP HICB-14 describes the review of testing of digital computer software.

- p. Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," (Endorses IEEE Std 830, "IEEE Recommended Practice for Software Requirements Specifications")*

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.172 provides a basis for evaluating conformance with 10 CFR 50.55a(h), GDC 1 and Criterion III of 10 CFR 50 Appendix B for computer-based systems. It endorses, with comments, IEEE Std 830 as describing an acceptable approach to the development of software requirements specifications.

BTP HICB-14 describes the review of software requirements specifications.

- q. 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, "IEEE Standard for Developing Software Life Cycle Processes")*

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.173 provides a basis for evaluating conformance with 10 CFR 50.55a(h), GDC 1 and Criteria I, II, III, VI, XV, and XVII of 10 CFR 50 Appendix B for computer-based systems. It endorses, with comments, IEEE Std 1074 as providing acceptable approaches to defining software development processes.

BTP HICB-14 describes the review of software development plans and software project management plans which should outline the licensee/applicant's software life cycle. BTP HICB-14 also describes the review of each activity group described in IEEE Std 1074.

5. Branch Technical Positions

Applicability — As noted in Table 7-1.

Review Methods — The BTPs provide bases for evaluating specific review areas.

References

ANS Std 4.5. "Criteria for Accident Monitoring Functions in Light Water Cooled Reactors."

ANSI/IEEE Std 1008-1987. "IEEE Standard for Software Unit Testing."

ANSI/IEEE Std 1012-1986. "IEEE Standard for Software Verification and Validation Plans."

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

ANSI/IEEE Std 829-1983. "IEEE Standard for Software Test Documentation."

BAW-1564. "Integrated Control System Reliability Analysis." Babcock and Wilcox, August 17, 1979.

Bulletin 80-06. "ESF Reset Controls." March 13, 1980.

Bulletin 80-19. Rev. 1 " Failures of Mercury-Wetted Matrix Relays in the RPS," August 15, 1980.

Bulletin 80-20. " Failures of Westinghouse Type W-2 Spring Return to Neutral Control Switches." July, 1980.

Bulletin 90-01. "Loss of Fill-Oil in Transmitters Manufactured by Rosemount." March 9, 1990.

Bulletin 90-01 Supplement. "Loss of Fill-Oil in Transmitters Manufactured by Rosemount." December 22, 1992.

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

EPRI Topical Report TR-102348. "Guideline on Licensing Digital Upgrades." Electric Power Research Institute.

Generic Letter 83-28. " Required Actions Based on Generic Implications of Salem ATWS Events." July 8, 1993.

Generic Letter 85-06. "Quality Assurance Guidance For ATWS Equipment That Is Not Safety-Related." April 16, 1985.

Generic Letter 89-19. "Request for Action Related to Resolution of USI A-47." September 20, 1989.

Generic Letter 93-08. "Relocation of Technical Specification Tables of Instrument Response Time Limits." December 29, 1993.

Generic Letter 95-02. "Use of NUMARC/EPRI Report TR-102348 in Determining Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59." April 26, 1995.

Generic Letter 96-01. "Testing of Safety-Related Logic Circuits." January 10, 1996.

IEEE Std 1028-1988. "IEEE Standard for Software Reviews and Audits."

IEEE Std 1042-1987. "IEEE Guide to Software Configuration Management."

IEEE Std 1074-1995. "IEEE Standard for Developing Software Life Cycle Processes."

IEEE Std 338-1987. "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."

IEEE Std 384-1992. "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

IEEE Std 828-1990. "IEEE Standard for Software Configuration Management Plans."

IEEE Std 830-1993. "IEEE Recommended Practice for Software Requirements Specifications."

ISA-S67.04-1994. "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants."

NUREG-0694. "TMI-Related Requirements for New Operating Reactor Licenses." 1980.

NUREG-0718. "Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License." 1981.

NUREG-0737. "Clarification of TMI Action Plan Requirements." 1982.

NUREG-0737 Supplement 1. "Clarification of TMI Action Plan Requirements — Requirements for Emergency Response Capability." January 1983.

Regulatory Guide 1.118. "Periodic Testing of Electric Power and Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1995.

Regulatory Guide 1.151. "Instrument Sensing Lines." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1983.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.168. "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.169. "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.170. "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.171. "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.172. "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.173. "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.22. "Periodic Testing of Protection System Actuation Functions." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.53. "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.62. "Manual Initiation of Protection Action." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.70. "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants." Office of Standards Development, U.S. Nuclear Regulatory Commission, November 1978.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

Regulatory Guide 1.97. "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident." Revision 3, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, May 1983.

SECY 91-178. "Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) for Design Certifications and Combined Licenses." June 12, 1991.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Appendix 7.1-B

Guidance for Evaluation of Conformance to ANSI/IEEE Std 279

10 CFR Part 50, 50.55a(h) requires that protection systems meet the requirements of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." The scope of ANSI/IEEE Std 279 includes those systems that actuate a reactor trip, and that in the event of a serious reactor accident, actuate engineered safety features. This appendix discusses the requirements of ANSI/IEEE Std 279, Sections 3 and 4, as they are used in the review of the reactor trip systems (RTS) and engineered safety features actuation systems (ESFAS) to determine that these systems meet the NRC regulations. Although required by NRC regulations only for protection systems, the criteria of ANSI/IEEE Std 279 address considerations such as design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing that may be used as review guidance, where appropriate, for any instrumentation and control (I&C) system, as elaborated in Sections 7.2 through 7.9. Therefore, for I&C systems not a part of the protection system, but having a high degree of importance to safety, the reviewer may use the concepts of ANSI/IEEE Std 279 as a starting point for the review of these systems.

Applications involving digital computer-based safety systems should conform with the guidance of Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," and be reviewed using Appendix 7.1-C.

This appendix discusses the requirements of ANSI/IEEE Std 279 as they are used in the review of safety systems; however, it is not intended to be a stand-alone document. Each section of this appendix relates directly to one or more sections of the standard. Additional background or detailed information relevant to this review can be found in the references to this section.

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

An HICB review of safety systems that follows the guidance of ANSI/IEEE Std 279 should be coordinated with other branches as appropriate to address the following considerations:

- Many of the auxiliary supporting features and other auxiliary features are described in Chapters 4, 5, 6, 8, 9, 10, and 12 of the safety analysis report (SAR). HICB reviewers must coordinate with the reviewers of these sections to ensure that auxiliary features are appropriately addressed by the review.
- The site characteristics, systems (both physical and administrative), and analyses described in the other sections of the SAR may impose requirements on the I&C systems. HICB reviewers should coordinate with the reviewers of these sections to ensure the I&C systems appropriately address these requirements.
- I&C systems may impose requirements upon other plant systems and analyses. HICB reviewers should coordinate with the reviewers of the affected systems to ensure that the reviewers are aware of these requirements.
- Other plant systems will impose requirements on the I&C systems. HICB reviewers should coordinate with the reviewers of the interfacing systems to ensure that these requirements are considered in the review.

The coordination review needed for each I&C system is discussed in SRP Section 7.0.

1. Section 3 — Design Basis

Section 3 of ANSI/IEEE Std 279 requires in part that a specific protection system design basis be provided. The design basis should be reviewed to confirm that it has the following characteristics:

- **Completeness** — The design basis should address all system functions necessary to fulfill the system's safety intent. The design basis for protection systems should be shown to address the requirements of 10 CFR 50 Appendix A, General Design Criterion (GDC) 20. Information provided for each design basis item should be sufficient to enable the detailed design of the I&C system to be carried out. All functional requirements for the I&C system and the operational environment for the I&C system should be described. As a minimum, each of the design basis aspects identified in ANSI/IEEE Std 279 Sections 3(1) through (9) should be addressed.
- **Consistency** — The information provided in the design basis should be analyzed to confirm its consistency with the plant safety analysis, including the design basis event analysis of Chapter 15 of the SAR; the mechanical and electrical system designs; and other plant system designs.

The design bases should not contain contradictory requirements.

- **Correctness** — The information provided for the design basis items should be technically accurate.
- **Traceability** — It should be possible to trace the information in each design basis item back to the safety analyses, plant system design documents, regulatory requirements, applicant/licensee commitments, or other plant documents.

- Unambiguity — The information provided for the design basis items, taken alone and in combination, should have one and only one interpretation.
- Verifiability — The information provided for the design basis items should be stated or provided in such a way as to facilitate the establishment of verification criteria, and the performance of analyses and reviews of the various safety systems.

In addition to these characteristics, the following should be noted about the parts of ANSI/IEEE Std 279 Section 3.

Section 3(1) requires in part the identification of conditions that require protective action. This information should be consistent with the analysis provided in Chapter 15 of the SAR. BTP HICB-4 provides specific guidance on the failures and malfunctions that should be considered in identification of design basis events for systems that initiate and control auxiliary feedwater systems. BTP HICB-5 provides specific guidance on the reactivity control malfunctions that should be considered in the identification of conditions requiring protective action. The malfunctions assumed should be consistent with the control system failure modes described in Section 7.7 of the SAR and the reactivity control interlock functions described in Section 7.6 of the SAR.

Section 3(2) requires in part the identification of variables that are monitored in order to provide protective action. The tables in Sections 7.2 and 7.3 of the SAR should provide this information.

Section 3(3) requires in part the identification of the minimum number and location of sensors for those variables in 3(2) that have a spatial dependence. The applicant/licensee's analysis should demonstrate that the number and location of sensors are adequate. Item 3 below discusses the consideration of the single failure criterion in the evaluation of this analysis.

Sections 3(4), 3(5), and 3(6) require in part the identification of operational limits, the margin between operational limits, and the level for the onset of unsafe conditions (setpoint), and limits that require protective action (safety limit — i.e., value assumed in the safety analysis) for each variable. The applicant/licensee's analysis should confirm that an adequate margin exists between operating limits and setpoints, such that a low probability exists for inadvertent actuation of the system. The applicant/licensee's analysis should confirm that an adequate margin exists between setpoints and safety limits, such that the system initiates protective actions before safety limits are exceeded. Draft Reg. Guide DG-1045 (the proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems") and BTP HICB-12 provide guidance on the establishment of safety system setpoints. The instrument performance data used in setpoint analyses should be consistent with the performance requirements established in the design basis as discussed in section 3(9). BTP HICB-6 provide specific guidance for determining if the timing margins for changeover from injection to recirculation mode are sufficient to allow manual initiation of the transition.

Section 3(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 is used in subsequent evaluations.

Section 3(8) requires in part the identification of malfunctions, accidents, or other unusual events that could physically damage protective system components or could cause environmental changes leading to functional degradation of system performance, and for which provisions must be incorporated to retain necessary

protective action. This information is used in subsequent evaluations, with special attention given to Section 4.4 of the standard, "Equipment Qualification."

Section 3(9) requires in part the identification of the performance requirements — including system response times, system accuracies, ranges, and rates of change of sensed variables — to be accommodated until conclusion of the protective action. The applicant/licensee's analysis, including the applicable portion provided in Chapter 15, should confirm that the system performance requirements are adequate to ensure completion of protective actions.

2. Section 4.1 — General Functional Requirements

This section requires in part that the protection system shall, with precision and reliability, automatically initiate protective action for the range of conditions and performance enumerated in Sections 3(7) through 3(9). The applicant/licensee's analysis should confirm that the protection 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. Automatic initiation is required for all protective functions; a manual initiation capability is also a requirement (see Section 4.17 and Reg. Guide 1.62, "Manual Initiation of Protection Action"). The evaluation of the precision of the protection system is addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. The topic of reliability is addressed in the following paragraphs.

Staff acceptance of system reliability is based on the deterministic criteria described in ANSI/IEEE Std 279 rather than on quantitative reliability goals. The NRC staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the requirements for reliability of safety systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience can provide an added level of confidence in the reliable performance of the I&C system.

The applicant/licensee 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.

3. Section 4.2 — Single-Failure Criterion

This section requires in part that any single failure within the protection system shall not prevent proper protective action at the system level when required. The applicant/licensee's 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 Reg. Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," which endorses ANSI/IEEE Std 379, "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 Reactor Systems Branch (SRXB) 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 protection system

performance. Conversely, these components and systems are assumed to function if functioning adversely affects protection system performance. All failures in the protection system that can be predicted as a result of an event for which the protection system is designed to provide a protective function are assumed to occur if the failure adversely affects the protection system performance. In general, the lack of equipment qualification 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 is arbitrarily assumed. With these failures assumed, the protection system must be capable of performing the protective functions required to mitigate the consequences of the specific event.

4. Section 4.3 — Quality of Components and Modules

The applicant/licensee should confirm that quality assurance provisions of Appendix B to 10 CFR 50 are applicable to the protection system. The evaluation of the adequacy of the quality assurance program is addressed in the review of Chapter 17 of the SAR.

5. Section 4.4 — Equipment Qualification

The applicant/licensee should confirm that the protection system equipment is designed to meet the functional performance requirements over the range of environmental conditions for the area in which it is located, as identified by 3(7) and 3(8), discussed above.

HICB reviews mild environment qualification and electromagnetic interference (EMI) qualification of protection system I&C equipment, and consults with other branches to confirm qualification for harsh environments and seismic loads. The review of harsh environment qualification is coordinated with the Electrical Engineering Branch (EELB). The review of seismic qualification is coordinated with the Mechanical Engineering Branch (EMEB).

Mild environment qualification should conform with the applicable guidance of ANSI/IEEE Std 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." Additionally, the applicant/licensee should confirm that a single failure within the environmental control system, for any area in which protection system equipment is located, will not result in conditions that could result in damage to the protection system equipment, nor prevent the balance of the protection system not within the area from accomplishing its safety function. In this regard, the loss of an environmental control system is treated as a single failure that should not prevent the protection system from accomplishing its safety functions.

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 confirm that there is independence between environmental control systems and sensing systems that would indicate the failure or malfunctioning of environmental control systems.

Review of mild environment qualification should also include confirmation that the environmental protection of instrument sensing lines conforms with the guidance of Reg. Guide 1.151.

EMI qualification in accordance with the guidance of EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," 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. Lightning protection features should conform to the guidance of NFPA Std 78, "Lightning Protection Code," and ANSI/IEEE Std 665, "Guide for Generation Station Grounding."

The EELB and EMEB evaluation of conformance to the requirements of GDC 2 and 4 and 10 CFR 50.49 satisfies the requirements for equipment qualification to harsh environments and seismic events. Guidance for the review of this equipment qualification is given in SRP Sections 3.10 and 3.11.

6. Section 4.5 — Channel Integrity

Information provided in Sections 3(7) and 3(8) is reviewed to confirm that the design includes the qualification of equipment for the conditions identified in the design bases. Failures may not be credited to protect the integrity of other equipment. The review should confirm that tests have been conducted on protection system equipment components and the system racks and panels as a whole to demonstrate the functional performance requirements of the protection system over the range of transient and steady-state conditions of both the energy supply and the environment. Where tests have not been conducted, the applicant should confirm that the protection system components are conservatively designed to operate over the range of service conditions.

Auxiliary features necessary to support safety system performance should meet all of the requirements of IEEE Std 279. Other auxiliary features that are part of the safety system, but not isolated from the safety system, should be designed to meet the criteria of IEEE Std 279 as necessary to assure that these components and systems do not degrade the safety systems below an acceptable level. BTP HICB-9 provides specific guidance for the review of anticipatory trips that are auxiliary features of a reactor protection system.

The sharing of structures, systems, and components between units in multi-unit stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. The review of shared displays and controls should be coordinated with the Human Factors Assessment Branch (HHFB) to confirm that shared user interfaces are sufficient to support the operator needs for each of the shared units.

The EELB and Plant Systems Branch (SPLB) review power source requirements. HICB reviewers should coordinate with these branches to confirm that I&C safety system power sources are adequate.

The review of channel integrity should confirm that the design provides for protection systems to fail in a safe state, or into a state that has been demonstrated to be acceptable on some other defined basis, if conditions such as disconnection of the system, loss of energy, or adverse environments are experienced. This aspect is typically evaluated through evaluation of the applicant/licensee's failure modes and effects analysis. The analysis should justify the acceptability of each failure effect. RTS functions should typically fail in the tripped state. ESFAS functions should fail to a predefined safe state. For many ESFAS functions this predefined safe state will be that the actuated component remains as-is.

7. Section 4.6 — Channel Independence

Two aspects of independence should be addressed:

- Physical independence.

- Electrical independence.

Guidance for evaluation of physical and electrical channel independence is provided in Reg. Guide 1.75, "Physical Independence of Electrical Systems," which endorses IEEE Std 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." The applicant/licensee should confirm that the protection system design precludes the use of components that are common to redundant channels, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features that could compromise the independence of redundant channels. Physical independence is attained by physical separation and physical barriers. Electrical independence shall include the utilization of separate power sources. (EELB and SPLB review power source requirements. HICB reviewers should coordinate with these branch requirements to confirm that I&C safety system power sources are adequate.) Transmission of signals between independent channels should be through isolation devices.

BTP HICB-11 provides guidance for the application and qualification of isolation devices.

8. Section 4.7 — Control and Protection System Interaction

Control and protection system interaction involves more than examining the electrical isolation and interconnection. The functional performance of control systems must be such that a control system cannot prevent proper action of a protection system. This section of ANSI/IEEE Std 279, with regard to isolation devices and multiple failures resulting from a credible single event, is explained by example in the document (See Section 4.2 of ANSI/IEEE Std 279). The applicant/licensee's analysis should confirm that the requirements for control and protection system interaction are satisfied.

9. Section 4.8 — Derivation of System Inputs

A protection system that requires loss of flow protection would, for example, normally derive its signal from flow sensors. A design might use an indirect parameter such as a pressure signal or pump speed. However, the applicant/licensee should verify that any indirect parameter is a valid representation of the desired direct parameter for all events.

Even a directly measured variable should be reviewed and its response to postulated events compared with the credit taken for the parameter in the events for which it provides protection.

For both direct and indirect parameters, the applicant/licensee should verify that the characteristics (e.g., range, accuracy, resolution, response time) of the instruments that produce the protection system inputs are consistent with the analysis provided in Chapter 15 of the SAR.

10. Section 4.9 — Capability for Sensor Checks

The most common method used to verify the availability of the input sensors is by cross checking between redundant channels that have available readout. When only two channels of readout are provided, the applicant/licensee should state the basis used to ensure that an operator will not take incorrect action when the two channel readouts differ. The applicant/licensee should state the method to be used for checking the operational availability of non-indicating sensors.

11. Section 4.10 — Capability for Test and Calibration

Guidance on periodic testing of the protection system is provided in Reg. Guide 1.22, "Periodic Testing of Protection System Actuation Functions," and in Reg. Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," which endorses IEEE Std 338, "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 protection 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 test scheme must be such that the tests do, in fact, overlap from one test segment to another. Test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation.

The review of test and calibration provisions should be coordinated with the Technical Specifications Branch (TSB) to confirm that the system design supports the types of testing required by the technical specifications. The system design should also support the compensatory actions required by technical specifications when limiting conditions for operation are not met. Typically, the design should allow for tripping or bypass of individual functions in each protection system channel.

12. Section 4.11 — Channel Bypass and Removal from Operations

The review of bypass and removal from operations should be coordinated with TSB to confirm that the provisions for this bypass are consistent with the required actions of the proposed plant technical specifications.

13. Section 4.12 — Operating Bypass

The requirement for automatic removal of operational bypasses means that the reactor operator shall have no role in such removal. The operator may take action to prevent the unnecessary initiation of a protective action.

14. Section 4.13 — Indication of Bypass

Guidance on bypasses and inoperable status indication is provided in Reg. Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System."

15. Section 4.14 — Access to Means for Bypassing

Administrative control is acceptable to ensure that access to the means for bypassing is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access.

16. Section 4.15 — Multiple Setpoints

The Staff interpretation of "positive means" is that automatic action is provided to ensure that the more restrictive setpoint is used when required.

BTP HICB-3 provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

17. Section 4.16 — Completion of a Protective Action Once it is Initiated

The Staff review of this item should include review of functional and logic diagrams to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion. The seal-in feature may incorporate a time delay as appropriate for the safety function. Additionally, the seal-in feature need not function until it is confirmed that a valid protective command has been received, provided the system meets response time requirements.

18. Section 4.17 — Manual Initiation

Features for manual initiation of protective action should conform with Reg. Guide 1.62, "Manual Initiation of Protection Action."

The review of manual controls should be coordinated with the Human Factors Assessment Branch (HHFB) to confirm that the functions controlled and the characteristics of the controls (e.g., location, range, type, and resolution) allow plant operators to take appropriate manual actions.

The review of manual controls should include confirmation that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified) during plant conditions under which manual actions may be necessary.

19. Section 4.18 — Access to Setpoint Adjustments, Calibrations, and Test Points

The review of access control should confirm that design features provide the means to control physical access to protection system equipment, including access to test points and means for changing setpoints. Typically such access control includes provisions such as alarms and locks on safety system panel doors, or control of access to rooms in which safety system equipment is located.

20. Section 4.19 — Identification of Protective Actions

Section 4.20 — Information Read-Out

The review of information displays should be coordinated with the SRXB to confirm that the information displayed and characteristics of the displays (e.g., location, range, type, and resolution) support operator awareness of system and plant status and will allow plant operators to make appropriate decisions.

The review of information displays for manually controlled actions should include confirmation that displays will be functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary.

Safety system bypass and inoperable status indication should conform with the guidance of Reg. Guide 1.47.

21. Section 4.21 — System Repair

Safety systems may include self-diagnostic capabilities to aid in troubleshooting.

22. Section 4.22 — Identification

Guidance on identification is provided in Regulatory Guide 1.75, which endorses IEEE Std 384. The preferred identification method is color coding of components, cables, and cabinets.

References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std 323-1974. "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

ANSI/IEEE Std 665-1987. "Guide for Generation Station Grounding."

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

EPRI Topical Report TR-102323. "Guidelines for Electromagnetic Interference Testing in Power Plants." Electric Power Research Institute, September 1994.

IEEE Std 338-1987. "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."

IEEE Std 384-1992. "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."

NFPA Std 78. "Lightning Protection Code." National Fire Protection Association, 1992.

Regulatory Guide 1.118. "Periodic Testing of Electric Power and Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1995.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.22. "Periodic Testing of Protection System Actuation Functions." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.53. "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.62. "Manual Initiation of Protection Action." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

NEW

Appendix 7.1-C

Guidance for Evaluation of Conformance to IEEE Std 603

10 CFR 50.55a(h) requires protection systems to meet the requirements of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." Although required by NRC regulations only for protection systems, the criteria of ANSI/IEEE Std 279 address considerations such as design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and test may be used as review guidance, where appropriate, for any instrumentation and control (I&C) system, as elaborated in Sections 7.2 through 7.9. IEEE Std 603, "Criteria for Safety Systems for Nuclear Power Generating Stations," has since superseded ANSI/IEEE Std 279. The guidance in IEEE Std 603, as endorsed by Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," incorporates the guidance of ANSI/IEEE Std 279, and includes all I&C safety systems within its scope. The guidance described in IEEE Std 603 may be used by the NRC staff in its evaluation of I&C safety systems. The reviewer may also use the concepts of IEEE Std 603 as a starting point for the review of other I&C systems.

IEEE Std 603 does not directly discuss digital systems. It is supplemented by IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," which provides criteria for applying IEEE Std 603 to computer systems. IEEE Std 7-4.3.2 is endorsed by Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." References to IEEE Std 603 in the remainder of this appendix should be read as including IEEE Std 7-4.3.2, Reg. Guide 1.152, and Reg. Guide 1.153.

This appendix discusses the guidance of IEEE Std 603 as it is used in the review of safety systems to determine that these systems meet NRC regulations. The appendix is not a stand-alone discussion of IEEE

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

Std 603 and IEEE Std 7-4.3.2. Each section of this appendix relates directly to one or more sections of the standards. Additional background or detailed information relevant to this review can be found in the references to this section.

1. Section 1 — Scope

The scope of IEEE Std 603 includes all I&C safety systems, which are the systems covered in Sections 7.2 through 7.6 of the safety analysis report (SAR). Except for the requirements for independence between control systems and protection systems, IEEE Std 603 does not directly apply to the non-safety systems such as the control systems and diverse I&C systems described in SAR Sections 7.7 and 7.8, respectively. Although intended only for safety systems, the criteria for IEEE Std 603 are applicable to any I&C system. Therefore, for non-safety I&C systems that have a high degree of importance to safety, the reviewer may use the concepts of IEEE Std 603 as a starting point for the review of these systems. Applicable considerations include design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing. Digital data communication systems as described in 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 is directly applicable to those parts of data communication systems that support safety system functions.

An HICB review of safety systems that follows the guidance of IEEE Std 603 should be coordinated with other branches as appropriate to address the following considerations:

- Many of the auxiliary supporting features and other auxiliary features defined in IEEE Std 603 are described in Chapters 4, 5, 6, 8, 9, 10, and 12 of the SAR. HICB reviewers should coordinate with the reviewers of these sections to ensure auxiliary features are appropriately addressed by the review.
- The site characteristics, systems (both physical and administrative), and analyses described in the other sections of the SAR may impose requirements on the I&C systems. HICB reviewers should coordinate with the reviewers of these sections to ensure that the I&C systems appropriately address these requirements.
- I&C systems may impose requirements upon other plant systems and analyses. HICB reviewers should coordinate with the reviewers of the affected systems to ensure that the reviewers are aware of these requirements.
- Other plant systems will impose requirements on the I&C systems. HICB reviewers should coordinate with the reviewers of the interfacing systems to ensure that these requirements are considered in the review.

The coordination review needed for each I&C system is discussed in SRP Section 7.0.

2. Section 2 — Definitions

No review guidance needed.

3. Section 3 — References

In addition to the references listed in IEEE Std 603, HICB reviewers should be familiar with the standards, regulatory guides, branch technical positions (BTPs), and other guidance relevant to the topics under review.

The applicable documents are identified in the discussion of each review topic below. Additional background or detailed information relevant to this review can be found in the references to this section.

4. Section 4 — Safety System Designation

Section 4 of IEEE Std 603 requires in part that a specific basis be established for the design of each safety system. The design basis should be reviewed to confirm that it has the following characteristics:

- **Completeness** — The design basis should address all system functions necessary to fulfill the system's safety intent. For protection systems, the design basis should be shown to address the requirements of 10 CFR 50 Appendix A, General Design Criterion (GDC) 20. Information provided for each design basis item should be sufficient to enable the detailed design of the I&C system to be carried out. All functional requirements for the I&C system and the operational environment for the I&C system should be described. As a minimum, each of the design basis aspects identified in IEEE Std 603 Sections 4.1 through 4.12 should be addressed.
- **Consistency** — The information provided in the design basis should be analyzed to demonstrate its consistency with the plant safety analysis, including the design basis event analysis of Chapter 15 of the SAR; the mechanical and electrical system designs; and other plant system designs.

The design bases should not contain contradictory requirements.

- **Correctness** — The information provided for the design basis items should be technically accurate.
- **Traceability** — It should be possible to trace the information in each design basis item to the safety analyses, plant system design documents, regulatory requirements, applicant/licensee commitments, or other plant documents.
- **Unambiguity** — The information provided for the design basis items, taken alone and in combination, should have one and only one interpretation.
- **Verifiability** — The information provided for the design basis items should be stated or provided in such a way as to facilitate the establishment of verification criteria and the performance of analyses and reviews of the various safety systems.

In addition to these characteristics, the following should be noted about the parts of ANSI/IEEE Std 603 Section 4.

Section 4.1 requires in part the identification of the design basis events applicable to each mode of operation. This information should be consistent with the analysis provided in Chapter 15 of the SAR. BTP HICB-4 provides specific guidance on the failures and malfunctions that should be considered in identification of design basis events for systems that initiate and control auxiliary feedwater systems. BTP HICB-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 Section 7.7 of the SAR and the reactivity control interlock functions described in Section 7.6 of the SAR.

Section 4.4 requires in part the identification of variables that are monitored in order to provide protective action. The tables in Sections 7.2 and 7.3 of the SAR should provide this information. Performance requirements — including system response times, system accuracies, ranges, and rates of change of sensed

variables to be accommodated until conclusion of the protective action — should also be identified in the system designation. The applicant/licensee's analysis, including the applicable portion provided in Chapter 15, should confirm that the system performance requirements are adequate to ensure completion of protective actions.

Section 4.5 describes the minimum criteria under which manual initiation and control of protective actions may be allowed. BTP HICB-6 provide specific guidance on determination if the timing margins for changeover from injection to recirculation mode are sufficient to allow manual initiation of the transition.

Section 4.6 requires in part the identification of the minimum number and location of sensors for those variables in 4.4 that have a spatial dependence. The applicant/licensee's analysis should demonstrate that the number and location of sensors are adequate. Item 6 below discusses the consideration of the single failure criterion in the evaluation of this analysis.

Section 4.4 requires in part the identification of the analytical limit associated with each variable. Review considerations in confirming that an adequate margin exists between analytical limits and setpoints are discussed in item 30 below.

Section 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 is used in subsequent evaluations.

Section 4.8 requires in part 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 is used in subsequent evaluations, with special attention given to Section 5.4 of the standard, "Equipment Qualification."

Section 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 or quantitative reliability goals imposed on the system design have been met. Staff acceptance of system reliability is based on deterministic criteria described in IEEE Std 603 and IEEE Std 7-4.3.2, rather than on quantitative reliability goals. Therefore, the system design basis should discuss the methods to be used to confirm that these deterministic criteria have been met.

The NRC staff does not endorse the concept of quantitative 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 in the reliable performance of the I&C system.

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 by software. For example, reliability of hardware components might be demonstrated by an evaluation of system redundancy and quantitative reliability modeling. Reliability of software might be demonstrated by evaluation of the development process combined with testing under a wide range of input conditions.

5. Section 5 — Safety System Criteria

This section requires that the safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established by design basis events. The applicant/licensee's analysis should confirm that the protection 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 HICB review in this regard should confirm that the system design fulfills the system design basis requirements established. Confirming the adequacy of system design basis requirements and verifying that the system meets these requirements will normally be a substantial portion of the HICB review.

The subsections of Section 5, and Sections 6, 7, and 8 (discussed below) deal with specific guidance that safety systems should meet as part of fulfilling the design basis requirements. Most of these items identify deterministic criteria that, if met, will normally provide the level of reliability needed for safety systems. These criteria may be relevant for both individual system elements, as well as the system as a whole.

6. Section 5.1 — Single-Failure Criterion

This section requires that any single failure within the safety system shall not prevent proper protective action at the system level when required. The applicant/licensee's 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 Reg. Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," which endorses ANSI/IEEE Std 379, "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 Reactor Systems Branch (SRXB) 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. These components and systems are assumed to function 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 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 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-mode failure of redundant equipment. 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-mode 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.

A detailed defense-in-depth and diversity study should be made to address common-mode failures in digital computer-based systems. The NRC's position for providing defense against common-mode 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). BTP HICB-19 provides guidance for addressing the potential of common-mode failures.

7. Section 5.2 — Completion of Protective Action

The Staff review of this item should include review of functional and logic diagrams to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion.

8. Section 5.3 — Quality

The applicant/licensee should confirm that quality assurance provisions of Appendix B to 10 CFR 50 are applicable to the safety protection system. The evaluation of the adequacy of the quality assurance program is addressed in the review of Chapter 17 of the SAR.

For digital computer-based systems, the applicant/licensee should address the quality requirements described in Section 5.3 of IEEE Std 7-4.3.2. BTP HICB-14 describes the characteristics of a software development process that the Staff may evaluate when assessing compliance with Sections 5.3.1, 5.3.4, and 5.3.5 of IEEE Std 7-4.3.2. The quality exhibited by the software engineering process and the products of that process should be appropriate to the safety significance of the safety system.

EPRI TR-106439 "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," provides guidance for the evaluation of existing commercial computers and software to comply with the requirements of Section 5.3.2 of IEEE Std 7-4.3.2. The guidance of BTP HICB-14 may be applied to the evaluation of vendor processes described in EPRI TR-106439.

The guidance of BTP HICB-14 or the guidance of EPRI TR-106439 may be applied to the qualification of software tools, as discussed in Section 5.3.3 of IEEE Std 7-4.3.2. As discussed in the standard, the activities involved in tool qualification may be tailored based upon the potential safety impact the tool may have. Section 5.3.3 discusses a case in which the tool safety impact may be limited by verification and validation of tool outputs. NUREG/CR-6421, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications," describes criteria that may be used in tailoring the qualification process for software tools.

9. Section 5.4 — Equipment Qualification

The applicant/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, as identified by Sections 4.7 and 4.8.

HICB reviews mild environment qualification and electromagnetic interference (EMI) qualification of safety system I&C equipment, and consults with other branches to confirm qualification for harsh environments and seismic loads. The review of harsh environment qualification is coordinated with the Electrical Engineering Branch (EELB). The review of seismic qualification is coordinated with the Mechanical Engineering Branch (EMEB).

Mild environment qualification should conform with the guidance of ANSI/IEEE Std 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." Additionally, the applicant/licensee should confirm that a single failure within the environmental control system, for any area in which safety system equipment is located, will not result in conditions which 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 an environmental control system is treated as a single failure that should not prevent the safety system from accomplishing its safety functions.

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 confirm that there is independence between environmental control systems and sensing systems which would indicate the failure or malfunctioning of environmental control systems.

Review of mild environment qualification should also include confirmation that the environmental protection of instrument sensing lines conform with the guidance of Reg. Guide 1.151.

EMI qualification in accordance with the guidance of EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," 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. Lightning protection features should conform to the guidance of NFPA Std 78, "Lightning Protection Code," and ANSI/IEEE Std 665, "Guide for Generation Station Grounding."

The EELB and EMEB evaluation of conformance to the requirements of GDC 2 and 4 and 10 CFR 50.49 satisfy the requirements for equipment qualification to harsh environments and seismic events. Guidance for the review of this equipment qualification is given in SRP Sections 3.10 and 3.11.

10. Section 5.5 — System Integrity

Information provided in Sections 4.7 and 4.8 is reviewed to confirm that the design includes the qualification of equipment for the conditions identified in the design bases. Failures may not be credited to protect the integrity of other equipment. The review 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. Where tests have not been conducted, the applicant/licensee should confirm that the safety system components are conservatively designed to operate over the range of service conditions.

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

Section 4.10. BTP HICB-21 provides supplemental guidance on evaluating response time for digital computer-based systems, and discusses design constraints that allow greater confidence in the results analyses or prototype testing to determine real-time performance.

IEEE Std 7-4.3.2 indicates that design for computer system integrity and design for test and calibration should be addressed as part of safety system integrity. Evaluation of computer system hardware integrity should be included in the evaluation against the requirements of IEEE Std 603. Computer system software integrity (including the effects of hardware-software interaction) should be demonstrated by the applicant/licensee's software safety analysis activities. Section 3.1.i of BTP HICB-14 describes the acceptable characteristics of software safety plans. Section 3.2.a of BTP HICB-14 describes the characteristics of acceptable software safety analyses.

Evaluation of computer system design for test and calibration is covered in item 12 below.

The review of system integrity should confirm that the design provides for safety systems to fail in a safe state, or into a state that has been demonstrated to be acceptable on some other defined basis, if conditions such as disconnection of the system, loss of energy, or adverse environments are experienced. This aspect is typically evaluated through evaluation of the applicant/licensee's failure modes and effects analysis. The analysis should justify the acceptability of each failure effect. Reactor trip system (RTS) functions should typically fail in the tripped state. Engineered safety feature actuation system (ESFAS) functions should fail to a predefined safe state. For many ESFAS functions this predefined safe state will be that the actuated component remains as-is.

Computer-based protection systems should, upon detection of inoperable input instruments, automatically actuate the protective functions associated with the failed instrument(s) (e.g., automatically place the affected channel(s) in trip. Hardware or software failures detected by self-diagnostics should also cause protective function actuation. Failure of computer system hardware or software should not inhibit manual initiation of protective functions or the operator performance of preplanned emergency or recovery actions. During either partial or full system initialization or shutdown after a loss of power, control output to the protection system actuators should fail to a predefined, preferred failure state. System restart upon restoration of power should not automatically transfer the actuators out of the predefined failure state. Changes to the state of plant equipment from the predefined state following restart and reinitialization (other than changes in response to valid protection system signals) should be under the control of the operator in accordance with appropriate plant procedures.

11. Section 5.6 — Independence

This section requires in part 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. Three aspects of independence should be addressed in each case:

- Physical independence.
- Electrical independence.
- Communications independence.

Guidance for evaluation of physical and electrical independence is provided in Reg. Guide 1.75, "Physical Independence of Electrical Systems," which endorses IEEE Std 384, "IEEE Standard Criteria for

Independence of Class 1E Equipment and Circuits." The applicant/licensee should confirm that the safety system design precludes the use of 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 which could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence should include the utilization of separate power sources. (The EELB and Plant Systems Branch (SPLB) review power source requirements. HICB reviewers should coordinate with these branch requirements to confirm that I&C safety system power sources are adequate.) Transmission of signals between independent channels should be through isolation devices.

BTP HICB-11 provides guidance for the application and qualification of isolation devices.

Annex G of IEEE Std 7-4.3.2, as discussed in SRP Section 7.1.II, describes an acceptable means for providing communications independence. The review of communications independence should include confirmation that the routing of signals related to safety maintains (1) proper channeling through the communication systems, and (2) proper data isolation between redundant channels.

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 portion(s). If a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, the review should confirm that a logical or software malfunction of the non-safety system cannot affect the functions of the safety system.

12. Section 5.7 — Capability for Test and Calibration

Guidance on periodic testing of the protection system is provided in Reg. Guide 1.22, "Periodic Testing of Protection System Actuation Functions," and in Reg. Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," which endorses IEEE Std 338, "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 protection 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 test scheme must be such that the tests do, in fact, overlap from one test segment to another. Test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation.

For digital computer-based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer deadlock. BTP HICB-17 describes additional considerations in the evaluation of test provisions in digital computer-based systems.

The review of test and calibration provisions should be coordinated with the Technical Specifications Branch (TSB) to confirm that the system design supports the types of testing required by the technical specifications. The system design should also support the compensatory actions required by technical specifications when limiting conditions for operation are not met. Typically, the design should allow for tripping or bypass of individual functions in each safety system channel. BTP HICB-17 discusses considerations in performing this evaluation for digital computer-based systems.

13. Section 5.8 — Information Displays

The review of information displays should be coordinated with the SRXB to confirm that the information displayed and the characteristics of the displays (e.g., location, range, type, and resolution) support operator awareness of system and plant status and will allow plant operators to make appropriate decisions.

The review of information displays for manually controlled actions should include confirmation that displays will be functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary.

Safety system bypass and inoperable status indication should conform with the guidance of Reg. Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

14. Section 5.9 — Control of Access

Administrative control is acceptable to assure that the access to the means for bypassing safety system functions is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access.

The review of access control should confirm that design features provide the means to control physical access to protection system equipment, including access to test points and means for changing setpoints. Typically such access control includes provisions such as alarms and locks on safety system panel doors, or control of access to rooms in which safety system equipment is located.

Review of digital computer-based systems should consider controls over electronic access to safety system software and data. Controls should address access via network connections, and via maintenance equipment.

15. Section 5.10 — Repair

Digital safety systems may include self-diagnostic capabilities to aid in troubleshooting. BTP HICB-17 describes characteristics that digital computer-based diagnostic systems should exhibit.

16. Section 5.11 — Identification

Guidance on identification is provided in Reg. Guide 1.75, which endorses IEEE Std 384. The preferred identification method is color coding of components, cables, and cabinets.

Configuration management is generally sufficient for maintaining the identification of computer software. BTP HICB-14 discusses the review of software configuration management.

17. Section 5.12 — Auxiliary Features

BTP HICB-9 provides specific guidance for the review of anticipatory trips that are auxiliary features of a reactor protection system.

18. Section 5.13 — Multi-Unit Stations

The review of shared displays and controls should be coordinated with the Human Factors Assessment Branch (HHFB) to confirm that shared user interfaces are sufficient to support the operator needs for each of the shared units.

19. Section 5.14 — Human Factors Considerations

Safety system human factors design should be consistent with the applicant/licensee's commitments documented in Chapter 18 of the SAR. The review of human-factors considerations should be coordinated with HHFB.

20. Section 5.15 — Reliability

The applicant/licensee 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 reliability should be analyzed. Reg. Guide 1.152 describes the Staff position on software reliability determination. BTP HICB-14 provides guidance for software development processes that are expected to produce reliable software. Software that complies with the quality criteria of item 8 above and that is used in safety systems that provide measures for defense against common mode failures as described in item 6 above are considered by the staff to comply with the fundamental reliability requirements of GDC 21, IEEE Std 279, and IEEE Std 603.

The assessment of reliability should consider the effect of possible hardware and software failures and the design features provided to prevent or limit the effects of these failures. Hardware failure conditions considered should include failures of portions of the computer itself and failures of portions of communication systems. Both hard failures and transient failures should be considered. Both sustained and partial failures should be considered. Software failure conditions considered should include, as appropriate, software common-mode failure, cascading failures, and undetected failures.

Reg. Guide 1.152 indicates that the concept of quantitative reliability goals is not sufficient as a sole means of meeting the NRC's regulations for the reliability of digital computers used in safety systems. This is discussed in more detail as part of item 4 above.

21. Section 6 — Sense and Command Features — Functional and Design Requirements

This section provides requirements for sensors and command features. Section 7, Executive Features — Functional and Design Requirements, provides requirements for actuators and other executive features. The review guidance for items in these sections are discussed together.

22. Sections 6.1 and 7.1 — Automatic Control

The safety system should, with precision and reliability, automatically initiate and execute protective action for the range of conditions and performance except as justified in Section 4.5. The applicant/licensee's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met. The evaluation of the precision of the protection system should be addressed to the

extent that setpoints, margins, errors, and response times are factored into the analysis. BTP HICB-12 discusses considerations for the review of the process for establishing safety system setpoints.

For digital computer-based systems, the evaluation should confirm that the general functional requirements have been appropriately allocated into hardware and software requirements. The evaluation should also confirm that the system's real-time performance is deterministic and known. BTP HICB-21 provides guidance for this evaluation.

23. Sections 6.2 and 7.2 — Manual Control

Features for manual initiation of protective action should conform with Reg. Guide 1.62, "Manual Initiation of Protection Action."

The review of manual controls should be coordinated with the HHFB to confirm that the functions controlled and the characteristics of the controls (e.g., location, range, type, and resolution) allow plant operators to take appropriate manual actions.

The review of manual controls should include confirmation that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified) during plant conditions under which manual actions may be necessary.

24. Section 6.3 — Interaction Between the Sense and Command Features and Other Systems

The reviewer should confirm that non-safety system interactions with protection systems are limited such that the requirements of 10 CFR 50 Appendix A, GDC 24 are met.

Where the event of concern is simple failure of a sensing channel shared between control and protection functions, previously accepted approaches have included:

- Isolating the protection system from channel failure by providing additional redundancy.
- Isolating the control system from channel failure by using data validation techniques to select a valid control input.

25. Section 7.3 — Completion of Protective Action

The Staff review of this item should include review of functional and logic diagrams to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion. The seal-in feature may incorporate a time delay as appropriate for the safety function. Additionally, the seal-in feature need not function until it is confirmed that a valid protective command has been received, provided the system meets response time requirements.

26. Section 6.4 — Derivation of System Inputs

A safety system that requires loss of flow protection would, for example, normally derive its signal from flow sensors. A design might use an indirect parameter such as a pressure signal or pump speed. However, the applicant/licensee should verify that any indirect parameter is a valid representation of the desired direct parameter for all events.

Even a directly measured variable should be reviewed and its response to postulated events compared with the credit taken for the parameter in the events for which it provides protection.

For both direct and indirect parameters, the applicant/licensee should verify that the characteristics (e.g., range, accuracy, resolution, response time, sample rate) of the instruments that produce the protection system inputs are consistent with the analysis provided in Chapter 15 of the SAR.

27. Section 6.5 — Capability for Testing and Calibration

The most common method used to verify the availability of the input sensors is by cross checking between redundant channels that have available readout. When only two channels of readout are provided, the applicant/licensee should state the basis used to ensure that an operator will not take incorrect action when the two channel readouts differ. The applicant/licensee should state the method to be used for checking the operational availability of non-indicating sensors. BTP HICB-17 discusses issues that should be considered in sensor check and surveillance test provisions for digital computer I&C systems.

28. Sections 6.6 and 7.4 — Operating Bypasses

The requirement for automatic removal of operational bypasses means that the reactor operator shall have no role in such removal. The operator may take action to prevent the unnecessary initiation of a protective action.

29. Sections 6.7 and 7.5 — Maintenance Bypass

The review of bypass and removal from operations should be coordinated with TSB to confirm that the provisions for this bypass are consistent with the required actions of the proposed plant technical specifications.

30. Section 6.8 — Setpoints

The applicant/licensee's 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. The applicant/licensee's analysis should confirm that an adequate margin exists between setpoints and safety limits, such that the system initiates protective actions before safety limits are exceeded. Draft Reg. Guide DG-1045 (proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems") and BTP HICB-12 provide guidance on the establishment of safety system setpoints.

Where it is necessary to provide multiple setpoints as discussed in Section 6.8.2, the Staff interpretation of "positive means" is that automatic action is provided to ensure that the more restrictive setpoint is used when required. BTP HICB-3 provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

31. Section 8 — Power Source Requirements

The EELB and Plant Systems Branch (SPLB) review power source requirements. HICB reviewers should coordinate with these branches to confirm that I&C safety system power sources are adequate.

References

- ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."
- ANSI/IEEE Std 323-1974. "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
- ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."
- ANSI/IEEE Std 665-1987. "Guide for Generation Station Grounding."
- Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.
- EPRI Topical Report TR-102323. "Guidelines for Electromagnetic Interference Testing in Power Plants." Electric Power Research Institute, September 1994.
- EPRI Topical Report TR-106439. "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." Electric Power Research Institute, October 1996.
- IEEE Std 338-1987. "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."
- IEEE Std 384-1992. "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."
- IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
- IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
- IEEE Std 828-1990. "IEEE Standard for Software Configuration Management Plans."
- NFPA Std 78. "Lightning Protection Code." National Fire Protection Association, 1992.
- NUREG/CR-6421. "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications." March 1996.
- Regulatory Guide 1.118. "Periodic Testing of Electric Power and Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1995.
- Regulatory Guide 1.151. "Instrument Sensing Lines." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1983.
- Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.22. "Periodic Testing of Protection System Actuation Functions." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.53. "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.62. "Manual Initiation of Protection Action." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

Safety Evaluation by the Office of Nuclear Reactor Regulation. "EPRI Topical Report TR-106439." May 1997.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Section 7.2. Reactor Trip System

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — none

I. Areas of Review

This SRP section describes the review process and acceptance criteria for the reactor trip system (RTS), which is part of the reactor protection system, and includes all equipment (including hardware, software, and firmware) from sensors to actuation devices (power sources, sensors, signal conditioners, initiation circuits, logic, bypasses, interlocks, racks, panels, control boards, interconnections, and actuation devices) that are required to initiate reactor shutdown. The RTS is designed to automatically initiate the reactivity control system (control rods) to ensure that specified acceptable fuel design limits are not exceeded. The controls, inhibits, and interlocks for the withdrawal, insertion, and sequence of control rods are described in Sections 7.6 and 7.7 of the safety analysis report (SAR).

The objectives of the review are to confirm that the RTS (1) satisfies the requirements of the acceptance criteria and guidelines applicable to the protection system and (2) performs its safety functions for all plant conditions under which they are required.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

type of application under consideration and for a description of coordination between HICB and other branches.

II. Acceptance Criteria

The acceptance criteria and guidelines applicable to the RTS are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified as applicable for this system. The review of the RTS confirms that this system conforms to the requirements of the acceptance criteria and guidelines.

Acceptance criteria for the review of the RTS are based on meeting the relevant requirements of the following regulations:

1. Acceptance criteria applicable to any RTS

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations."

10 CFR 50.34(f), "Additional TMI-Related Requirements," or equivalent TMI action requirements imposed by Generic Letters.

(2)(v), "Bypass and Inoperable Status Indication."

(2)(xxiii), "Anticipatory Trip on Loss of Main Feedwater or Turbine Trip."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 2, "Design Basis for Protection Against Natural Phenomena."

General Design Criterion 4, "Environmental and Missile Design Basis."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 20, "Protection Systems Functions."

General Design Criterion 21, "Protection System Reliability and Testability."

General Design Criterion 22, "Protective System Independence."

General Design Criterion 23, "Protection System Failure Modes."

General Design Criterion 24, "Separation of Protection and Control Systems."

General Design Criterion 25, "Protection System Requirements for Reactivity Control Malfunctions."

General Design Criterion 29, "Protection Against Anticipated Operational Occurrences."

Item II.Q., Defense Against Common-Mode Failures in Digital Instrument and Control Systems, of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs."

2. Additional acceptance criteria applicable to RTS proposed for design certification under 10 CFR 52

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

10 CFR 52.47(b)(2)(i), "Innovative Means of Accomplishing Safety Functions."

3. Additional acceptance criteria applicable to RTS proposed as part of combined license applications under 10 CFR 52

10 CFR 52.79(c), "ITAAC in combined Operating License Applications."

As described in Reg. Guide 1.153, "Criteria for Power, Instrumentation and Control Portions of Safety Systems," compliance with IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as modified and supplemented by the regulatory guide, is considered by the NRC staff to satisfy the provisions of ANSI/IEEE Std 279.

Section 7.1, Table 7-1, and Appendix 7.1-A list standards, regulatory guides, and branch technical positions that provide information, recommendations, and guidance that describe a basis acceptable to the NRC staff. This basis may be used to implement the relevant requirements of the NRC regulations identified above.

III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any instrumentation and control system. This part of Section 7.2 highlights specific topics that should be emphasized in the RTS review.

The review should include an evaluation of the protection system design against the requirements of ANSI/IEEE Std 279, or Reg. Guide 1.153, which endorses IEEE Std 603, depending upon the applicant/licensee's commitment regarding design criteria. This procedure is detailed in Appendix 7.1-B for ANSI/IEEE Std 279 and in Appendix 7.1-C for IEEE Std 603. The procedures in Appendices 7.1-B and 7.1-C address only those design requirements that are specific in nature. For example, paragraph 4.9 of ANSI/IEEE Std 279 requires that the design include the means for checking the availability of each system

input sensor during operation. Appendix 7.1-B outlines a procedure that can be used to determine whether or not this requirement is met.

Appendices 7.1-B and 7.1-C discuss the requirements of ANSI/IEEE Std 279 and IEEE Std 603, and how they are used in the review of the RTS. Although the primary emphasis is on the equipment comprising the RTS, the reviewer must consider the overall protective functions on a system level. The RTS design should be compatible with the accident analysis. It is not sufficient to judge the adequacy of the RTS only on the basis of the design meeting the specific requirements of ANSI/IEEE Std 279 or IEEE Std 603.

The RTS review should address all topics identified as applicable by Table 7-1. Appendix 7.1-A describes review methods for each topic. Major design considerations that should be emphasized in the review of the RTS are identified below.

- Design basis — See Appendix 7.1-B item 1 or Appendix 7.1-C item 4.
- Single-failure criterion — See Appendix 7.1-B item 3 or Appendix 7.1-C item 6.
- Quality of components and modules — See Appendix 7.1-B item 4 or Appendix 7.1-C item 8.
- Independence — See Appendix 7.1-B items 7 and 8 or Appendix 7.1-C items 11 and 24.
- Defense-in-depth and diversity — RTS systems should incorporate multiple means for response to each event discussed in Chapter 15 of the SAR. At least one pair of these means for each event should have the property of signal diversity, i.e., the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters are sensed incorrectly (see NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"). The diverse means may actuate the same protective function or different protective functions, and may be automatically or manually activated, consistent with the response time requirements of the function. For digital computer-based RTS systems, the applicant/licensee should have performed a defense-in-depth and diversity analysis. Additionally, for advanced reactor design under 10 CFR 52, the design should provide for manual, system-level actuation of critical safety functions. BTP HICB-19 provides guidance for the review of defense-in-depth and diversity.
- System testing and inoperable surveillance — See Appendix 7.1-B items 10 and 11 or Appendix 7.1-C items 12, 13, and 27.
- Use of digital systems — See Appendix 7.0-A.
- Setpoint determination — See Draft Reg. Guide DG-1045 (proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems"), and BTP HICB-12.

In certain instances, it will be the reviewer's judgment that, for a specific case under review, emphasis should be placed on specific aspects of the design, while other aspects of the design need not receive the same emphasis and in-depth review. Typical reasons for such a non-uniform emphasis are the introduction of new

design features or the utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the NRC's regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the SER:

The NRC staff concludes that the design of the reactor trip system (RTS) and the RTS initiation of the essential auxiliary support (EAS) systems are acceptable and meet the relevant requirements of General Design Criteria (GDC) 1, 2, 4, 13, 19-25, and 29, and 10 CFR 50.34(f), 50.55a(a)(1), and 50.55a(h).

The Staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The Staff concluded that the applicant/licensee adequately identified the guidelines applicable to these systems. Based upon the review of the system design for conformance to the guidelines, the Staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore the Staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included the identification of those systems and components for the RTS designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based upon the review, the Staff concludes that the applicant/licensee has identified those systems and components consistent with the design bases for those systems. Sections 3.10 and 3.11 of the SER address the qualification programs to demonstrate the capability of these systems and components to survive these events. Therefore, the Staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

Based on the review of RTS system status information, manual initiation capabilities, and provisions to support safe shutdown, the Staff concludes that information is provided to monitor the RTS over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for manual initiation of reactor trip. The RTS appropriately supports actions to operate the nuclear power unit safety under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the Staff finds that the RTS design satisfies the requirements of GDC 13 and 19.

Based on the review of system functions, the Staff concludes that the RTS conforms to the design bases requirements of [ANSI/IEEE Std 279 OR IEEE Std 603] and 10 CFR 50.34(f). The RTS conforms to the guidance of Draft Reg. Guide DG-1045. Based upon this review and coordination with those having primary review responsibility for the accident analysis, the Staff concludes that the RTS includes the provision to sense accident conditions and anticipated operational occurrences in order to initiate reactor shutdown consistent with the accident analysis presented in Chapter 15 of the SAR and evaluated in the SER. Therefore, the Staff finds that the RTS satisfies the requirements of GDC 20.

The RTS conforms to the guidelines for periodic testing in Reg. Guide 1.22 and Reg. Guide 1.118. The bypassed and inoperable status indication conforms to the guidelines of Reg. Guide 1.47. The RTS conforms to the guidelines on the application of the single-failure criterion in ANSI/IEEE Std 379 as supplemented by Reg. Guide 1.53. Based on the review, the Staff concludes that the RTS satisfies the requirement of [ANSI/IEEE Std 279 OR IEEE Std 603] with regard to the system

reliability and testability. Therefore the Staff finds that the RTS satisfies these requirements of GDC 21.

The RTS conforms to the guidelines in Reg. Guide 1.75 for the protection system independence. Based on the review, the Staff concludes that the RTS satisfies the requirement of ANSI/IEEE Std 279 or IEEE Std 603 with regard to the systems independence. Therefore, the Staff finds that the RTS satisfies the requirements of GDC 22.

Based on the review of the failure modes and effects analysis for the RTS, the Staff concludes that the system is designed to fail into a safe mode if conditions such as disconnection of the system, loss of energy, or postulated adverse environment are experienced. Therefore, the Staff finds that the RTS satisfies the requirements of GDC 23.

Based on the review of the interfaces between the RTS and plant operating control systems, the Staff concludes that the system satisfies the requirements of [ANSI/IEEE Std 279 OR IEEE Std 603] with regard to control and protection system interactions. Therefore the Staff finds the RTS satisfies the requirements of GDC 24.

Based on the review of the RTS, the Staff concludes that the system satisfies the protection system requirements for malfunctions of the reactivity control system such as accidental withdrawal of control rods. Section 15 of the SAR and SER address the capability of the system to ensure that fuel design limits are not exceeded for such events. Therefore, the Staff finds that the RTS satisfies the requirements of GDC 25.

Based on the review of all the above GDCs, the Staff concludes that the RTS satisfies the requirements of GDC 29.

The Staff's conclusions noted above are based upon the requirements of [ANSI/IEEE Std 279 OR IEEE Std 603] with respect to the design of the RTS. Therefore, the Staff finds that the RTS satisfies the requirement of 10 CFR 50.55a(h) with regard to ANSI/IEEE Std 279.

The applicant/licensee has also incorporated in the system design the recommendations of task action plan items [identify item number and how implemented] that the Staff has reviewed and found acceptable.

In the review of the RTS, the Staff examined the dependence of this system on the availability of essential auxiliary systems. Based on this review and coordination with those having primary review responsibility of EAS systems, the Staff concludes that the design of the RTS is compatible with the functional requirements of EAS systems.

Note: the following finding applies only to systems involving computer-based components.

Based on the review of software development plans and the inspections of the computer development process and design outputs, the Staff concludes that the computer systems meet the guidance of Reg. Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the Staff finds that the RTS satisfies the requirements of GDC 1 and 21.

Based on the review of the applicant/licensee's defense-in-depth and diversity analysis, the Staff concludes that the RTS complies with the criteria for defense against common-mode failure in digital instrumentation and control systems. Therefore, the Staff finds that adequate diversity and defense against common-mode failure has been provided to satisfy these requirements of GDC 21 and 22, and Item II.Q of the Staff Requirements Memorandum on SECY-93-087.

Note: the following findings apply only to applications under 10 CFR 52.

The RTS design appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the RTS satisfies the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the RTS examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the RTS satisfies the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the RTS [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the RTS design satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

The RTS contains the following elements that differ significantly from evolutionary changes from light water reactor designs of plants that have been licensed in commercial operation before April 18, 1989. [Insert list.] Based upon the review of [analysis OR test programs OR operating experience] the Staff concludes that the performance of these features have been demonstrated; interdependent effects among the safety features are acceptable; sufficient data exist to assess the analytical tools used for safety analysis; and the scope of the design is complete except for site-specific elements. Therefore, the Staff finds that the RTS satisfies the requirements of 10 CFR 52.47(b)(2)(i).

Based upon an initial review of the scope and content of the material submitted by the applicant, and a completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the RTS design to satisfy the requirements of 10 CFR 52.47(a)(2).

Note: the following conclusion is applicable to all applications.

The conclusions noted above for the RTS are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted [List applicable system or topics and identify references].

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

VI. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

NUREG/CR-6303. "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems." December 1994.

Regulatory Guide 1.22. "Periodic Testing of Protection System Actuation Functions," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.53. "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

Regulatory Guide 1.118. "Periodic Testing of Electric Power and Protection Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1995.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.168. "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.169. "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.170. "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.171. "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.172. "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.173. "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs." July 15, 1993.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Section 7.3. Engineered Safety Features Systems

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

This SRP section describes the review process and acceptance criteria for the engineered safety features actuation system (ESFAS), which is a portion of the protection system used to initiate the engineered safety features (ESF) systems and essential auxiliary supporting (EAS) systems. The ESFAS provides both automatic and manual initiation of these systems. This SRP section also includes the review criteria for control systems that regulate the ESF systems. The ESF control systems include both the automatic and manual features.

The review of instrumentation and control systems that regulate the operation of EAS systems is included in the SRP section that addresses each EAS system. SRP Section 7.5 provides the review criteria for the information systems important to safety, which includes instrumentation that indicates the need for manual initiation and control of ESF systems.

Typical ESF systems are:

- Containment and reactor vessel isolation systems.

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

- Emergency core cooling systems.
- Containment heat removal and depressurization systems.
- Pressurized water reactor auxiliary feedwater systems.
- Boiling water reactor standby gas treatment systems.
- Containment air purification and cleanup systems.
- Containment combustible gas control systems.
- Control room isolation and emergency heating, ventilating, and air conditioning (HVAC).

Typical EAS systems are:

- Electric power systems.
- Diesel generator fuel storage and transfer systems.
- Instrument air systems.
- HVAC systems for ESF areas.
- Essential service water and component cooling water systems.

The objective of the review is to confirm that the ESFAS and ESF control systems satisfy regulatory acceptance criteria, guidelines, and performance requirements.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

II. Acceptance Criteria

Acceptance criteria and guidelines applicable to the ESFAS and ESF control systems are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified for these systems. The review of the ESFAS and ESF control systems confirms that these systems conform to the requirements of the acceptance criteria and guidelines.

Acceptance criteria for the review of ESFAS and ESF control systems are the relevant requirements of the following regulations:

1. Acceptance criteria applicable to any ESFAS and ESF control systems

10 CFR 50.55a(a)(1), "Quality Standards."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 2, "Design Basis for Protection Against Natural Phenomena."

General Design Criterion 4, "Environmental and Missile Design Basis."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs."

2. Additional acceptance criteria applicable to the ESFAS

10 CFR 50.55a(h), "Protection Systems," which requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations."

10 CFR 50.34(f), "Additional TMI-Related Requirements," or equivalent TMI action requirements imposed by Generic Letters.

(2)(v), "Bypass and Inoperable Status Indication."

(2)(xii), "Auxiliary Feedwater System Automatic Initiation and Flow Indication."

(2)(xiv), "Containment Isolation Systems."

General Design Criterion 20, "Protection System Function."

General Design Criterion 21, "Protection System Reliability and Testability."

General Design Criterion 22, "Protection System Independence."

General Design Criterion 23, "Protection System Failure Modes."

General Design Criterion 24, "Separation of Protection and Control Systems."

General Design Criterion 29, "Protection against Anticipated Operational Occurrences."

3. Additional acceptance criteria applicable to ESF control systems

General Design Criterion 34, "Residual Heat Removal."

General Design Criterion 35, "Emergency Core Cooling."

General Design Criterion 38, "Containment Heat Removal."

General Design Criterion 41, "Containment Atmosphere Cleanup."

4. Additional acceptance criteria applicable to ESFAS and ESF control systems proposed for design certification under 10 CFR 52

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

10 CFR 52.47(b)(2)(i), "Innovative Means of Accomplishing Safety Function."

5. Additional acceptance criteria applicable to ESFAS and ESF control systems proposed as part of combined license applications under 10 CFR 52

10 CFR 52.79(c), "ITAAC in Combined License Applications."

As described in Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," compliance with IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as modified and supplemented by the regulatory guide, is considered by the NRC staff to satisfy the provisions of ANSI/IEEE Std 279.

Section 7.1, Table 7-1 and Appendix 7.1-A list standards, regulatory guides, and branch technical positions that provide information, recommendations, and guidance that describe a basis acceptable to the NRC staff for implementing the relevant requirements of the NRC regulations identified above for the ESFAS and ESF control systems.

III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any instrumentation and control system. Section 7.3 highlights specific topics that should be emphasized in the ESFAS review.

The review should include an evaluation of the ESFAS design against the requirements of ANSI/IEEE Std 279, or Reg. Guide 1.153 (which endorses IEEE Std 603), depending upon the applicant/licensee's commitment regarding these design criteria. This procedure is detailed in Appendix 7.1-B for ANSI/IEEE Std 279 and in Appendix 7.1-C for IEEE Std 603. The procedures in Appendices 7.1-B and 7.1-C address specific design requirements only. For example, paragraph 4.9 of ANSI/IEEE Std 279 requires that the design include the means for checking the availability of each system input sensor during operation. Appendix 7.1-B outlines a procedure that can be used to determine whether or not this requirement is met.

Appendices 7.1-B and 7.1-C discuss the requirements of ANSI/IEEE Std 279 and IEEE Std 603, and how they are used in the review of the ESFAS. Although the primary emphasis is on the equipment comprising the ESFAS, the reviewer must consider the overall ESF functions on a system level. The ESFAS design should be compatible with the SAR Chapter 15 design bases accident analyses. It is not sufficient to evaluate the adequacy of the ESFAS only on the basis of the design meeting the specific requirements of ANSI/IEEE Std 279 or IEEE Std 603.

The ESFAS review should address the applicable topics identified in Table 7-1. Appendix 7.1-A describes review methods for each topic. Major design considerations that should be emphasized in the review of the ESFAS are identified below.

- Design basis — See Appendix 7.1-B item 1 or Appendix 7.1-C item 4.
- Single-failure criterion — See Appendix 7.1-B item 3 or Appendix 7.1-C item 6.
- Quality of components and modules — See Appendix 7.1-B item 4 or Appendix 7.1-C item 8.
- Independence — See Appendix 7.1-B items 7 and 8 or Appendix 7.1-C items 11 and 24.
- Completion of protective action — See Appendix 7.1-B item 17 or Appendix 7.1-C item 25.
- Defense-in-depth and diversity — ESFAS systems should incorporate multiple means for response to each event discussed in Chapter 15 of the SAR. At least one pair of these means for each event should have the property of signal diversity, i.e., the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters are sensed incorrectly (see NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"). The diverse means may actuate the same protective function or different protective functions, and may be automatically or manually activated, consistent with the response time requirements of the function. For digital computer-based ESFAS systems the applicant/licensee should have performed a defense-in-depth and diversity analysis. Additionally, for advanced reactor design under 10 CFR 52, the design should provide for manual, system-level actuation of critical safety functions. BTP HICB-19 provides guidance for the review of defense-in-depth and diversity.
- System testing and inoperable surveillance — See Appendix 7.1-B items 10 and 11 or Appendix 7.1-C item 12, 13, and 27.
- Use of digital systems — See Appendix 7.0-A.
- Setpoint determination — See Draft Reg. Guide DG-1045 (the proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems"), and BTP HICB-12.
- ESF control systems — Conformance to the single-failure criterion on a system basis, and operability from onsite and offsite electrical power as required by GDC 34, 35, 38, and 41.

In each safety review, the Staff should determine the elements of the design that require additional review emphasis. Typical reasons for such a non-uniform emphasis are the introduction of new design features or the

utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the Code of Federal Regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the SER:

The review of the instrumentation and control aspects of the engineered safety feature (ESF) systems includes the engineered safety features actuation systems (ESFAS) and the ESF control systems. The ESFAS detects a plant condition requiring the operation of an ESF system and/or essential auxiliary supporting (EAS) system and initiates operation of these systems. The ESF control systems regulate the operation of the ESF systems following automatic initiation by the protection system or manual initiation by the plant operator.

The NRC staff concludes that the design of the ESFAS is acceptable and meets the relevant requirements of General Design Criteria (GDC) 1, 2, 4, 13, 19-24, 29, 34, 35, 38, and 41 and 10 CFR 50.34(f), 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h).

The Staff conducted a review of these systems for conformance to the guidelines in the regulatory guides, industry standards and branch technical positions applicable to these systems. The Staff concludes that the applicant/licensee acceptably identified the guidelines applicable to these systems. Based upon the review of the system design for conformance to the guidelines, the Staff concludes that the systems conform to the guidelines applicable to these systems. Therefore the Staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included the identification of those systems and components of the ESFAS and ESF control systems that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based upon the review, the Staff concludes that the applicant/licensee has identified those systems and components consistent with the design bases for those systems. Sections 3.10 and 3.11 of the SER address the acceptability of the qualification programs to demonstrate the capability of these systems and components to survive the above effects. Therefore, the Staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

Based on the review of ESFAS and ESF control system status information, manual initiation capabilities, control capabilities, and provisions to support safe shutdown, the Staff concludes that information is provided to monitor the system over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for manual initiation and control of ESF functions. ESF controls appropriately support actions to operate the nuclear power unit safely under normal conditions, and to achieve and maintain a safe condition under accident conditions. Therefore, the Staff finds that the ESFAS and ESF control design satisfies the requirements of GDC 13 and 19.

Based on the review of system functions, the Staff concludes that the ESFAS conforms to the requirements of [ANSI/IEEE Std 279 OR IEEE Std 603] and 10 CFR 50.34(f). The ESFAS setpoint methodology conforms to the guidance of Draft Reg. Guide DG-1045. Based upon this review and coordination with those having primary review responsibility for the accident analysis, the Staff concludes that the ESFAS includes the provision to sense accident conditions and anticipated operational occurrences consistent with the accident analysis presented in Chapter 15 of the SAR and evaluated in the SER. Therefore, the Staff finds that the ESFAS satisfies the requirements of GDC 20.

The ESFAS conforms to the guidelines for periodic testing in Reg. Guide 1.22 and Reg. Guide 1.118. The bypassed and inoperable status indication conforms to the guidelines of Reg. Guide 1.47. The ESFAS conforms to the guidelines on the application of the single-failure criterion in ANSI/IEEE Std 379 as supplemented by Reg. Guide 1.53. Based on the review, the Staff concludes that the ESFAS satisfies the requirement of [ANSI/IEEE Std 279 OR IEEE Std 603] with regard to system reliability and testability. Therefore, the Staff finds that the ESFAS satisfies these requirements of GDC 21.

The ESFAS conforms to the guidelines in Reg. Guide 1.75 for protection system independence. Based on the review, the Staff concludes that the ESFAS satisfies the requirement of [ANSI/IEEE Std 279 OR IEEE Std 603] with regard to the system's independence. Therefore, the Staff finds that the ESFAS satisfies the requirements of GDC 22.

Based on the review of the failure modes and effects analysis for the ESFAS, the Staff concludes that the system is designed to fail into a safe state if conditions such as disconnection of the system, loss of energy, or a postulated adverse environments are experienced. Therefore, the Staff finds that the ESFAS satisfies the requirements of GDC 23.

Based on the review of the interfaces between the ESFAS and plant control systems, the Staff concludes that the system satisfies the requirements of [ANSI/IEEE Std 279 OR IEEE Std 603] with regard to control and protection system interactions. Therefore, the Staff finds the ESFAS satisfies the requirements of GDC 24.

The Staff conducted a review of the ESF control systems for conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures. The Staff concludes that the ESF control systems are testable and are operable using either onsite or offsite power (assuming only one source is available). Additionally, the controls associated with redundant ESF systems are independent and satisfy the single-failure criterion and, therefore, meet the relevant requirements of GDC 34, 35, 38, and 41.

The conclusions noted above are based upon the requirements of [ANSI/IEEE Std 279 OR IEEE Std 603] with respect to the design of the ESFAS. Therefore, the Staff finds that the ESFAS satisfies the requirements of 10 CFR 50.55a(h).

The applicant/licensee has also incorporated in the system design the [recommendations of the TMI task action plan items OR the requirements of 10 CFR 50.34(f)], [identify item number and how implemented] which the Staff has reviewed and found acceptable.

In the review of the ESFAS, the Staff examined the dependence of this system on the availability of essential auxiliary systems. Based on this review and coordination with those having primary review responsibility of EAS systems, the Staff concludes that the design of the ESFAS is compatible with the functional requirements of EAS systems.

Note: the following finding applies only to systems involving digital computer-based components.

Based on the review of software development plans and the inspections of the computer development process and design outputs, the Staff concludes that the computer systems meet the guidance of Reg. Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the Staff finds that the ESFAS satisfies these requirements of GDC 1 and 21.

Based on the review of the applicant/licensee's defense-in-depth and diversity analysis, the Staff concludes that the ESFAS complies with the criteria for defense against common-mode failure in digital instrumentation and control systems. Therefore, the Staff finds that adequate diversity and

defense against common-mode failure has been provided to satisfy these requirements of GDC 21, GDC 22, and the Staff Requirements Memorandum on SECY-93-087.

Note: the following findings apply only to applications under 10 CFR 52.

The ESFAS design appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the ESFAS satisfies the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the ESFAS examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria are met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the ESFAS satisfies the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the ESFAS [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the ESFAS design satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

The ESFAS contains the following features which differ significantly from plant designs that have been licensed for commercial operation before April 18, 1989. [Insert list.] Based upon the review of [analysis OR test programs OR operating experience], the Staff concludes that the performance of these features has been demonstrated; interdependent effects among the safety features are acceptable; sufficient data exist to assess the analytical tools used for safety analysis; and the scope of the design is complete except for site-specific elements. Therefore, the Staff finds that the ESFAS satisfies the requirements of 10 CFR 52.47(b)(2)(i).

Based upon the review of the scope and content of the material submitted by the applicant, and the completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the ESFAS design to satisfy the requirements of 10 CFR 52.47(a)(2).

Note: the following conclusion is applicable to all applications.

The conclusions noted above for the ESFAS are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted [List applicable system or topics and identify references].

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

VI. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

NUREG/CR-6303. "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems." December 1994.

Regulatory Guide 1.118. "Periodic Testing of Electric Power and Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1995.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.22. "Periodic Testing of Protection System Actuation Functions." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs." July 15, 1993.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Section 7.4. Safe Shutdown Systems

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

This SRP section describes the review process and acceptance criteria for those instrumentation and control systems used to achieve and maintain a safe shutdown condition of the plant as required by 10 CFR 50 Appendix A, General Design Criteria (GDC) 13, "Instrumentation and Control," and GDC 19, "Control Room." To the extent that the engineered safety feature (ESF) systems are used to achieve and maintain safe shutdown, the review of these systems in this section is limited to those features which are unique to safe shutdown and not directly related to accident mitigation. The features within the scope of Section 7.4 may involve individual component control for safe shutdown versus system-level actuation for accident mitigation, or system-level controls used to achieve and maintain safe shutdown but not used for accident mitigation. System-level controls used for accident mitigation may also need to be reviewed using Section 7.4 if the safe shutdown functions of these controls involve features or operating modes that are unique to their safe shutdown functions. This SRP section also addresses the review of those systems required for safe shutdown which are not classified as ESF systems. The specific arrangement of these systems depends on (1) the type of plant (pressurized water reactor, boiling water reactor, etc.), (2) individual plant design features, and (3) the conditions under which the safe shutdown has to be achieved and maintained. The functional performance requirements of safe shutdown systems and essential auxiliary supporting systems are reviewed by other branches in accordance with the SRP sections which address these systems.

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

There are two kinds of shutdown conditions: hot shutdown and cold shutdown. In either case, reactivity control systems must maintain a subcritical condition of the core, and residual heat removal systems must operate to maintain adequate cooling of the core. For definitions of both shutdown conditions for a specific plant, see Chapter 16, "Technical Specifications," in the applicant/licensee's SAR. Section 7.5 of the SRP addresses the information systems important to safety that provide information to the operator for the manual control of systems required for safe shutdown. Section 9.5.1 of the SRP includes the instrumentation and controls provided as part of an alternative or dedicated shutdown capability needed for compliance with GDC 3, "Fire Protection."

The objectives of the review are to confirm that the safe shutdown systems satisfy the requirements of the acceptance criteria and guidelines applicable to safety systems, and that they will perform their safety functions during all plant conditions for which they are required.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

Typical systems required for safe shutdown are:

- Auxiliary feedwater systems,
- Residual heat removal systems, and
- Boric acid transfer systems.

Typical essential auxiliary supporting (EAS) systems are:

- Electric power systems,
- Diesel generator fuel storage and transfer systems,
- Instrument air systems,
- Heating, ventilation, and air conditioning (HVAC) systems for areas containing systems required for safe shutdown, and
- Essential service water and component cooling water systems.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

Voice communication between safe shutdown control areas is reviewed by HICB as part of its primary review responsibility for SRP Section 9.5.2.

II. Acceptance Criteria

The acceptance criteria and guidelines applicable to the I&C systems required for safe shutdown are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified as applicable to these systems. The review of the systems required for safe shutdown confirms that these systems conform to the requirements of the acceptance criteria and guidelines.

1. Acceptance criteria for the review of the safe shutdown I&C systems are based on meeting the relevant requirements of the following regulations

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For post-accident monitoring systems isolated from the protection system, the only applicable requirement from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

10 CFR 50.34(f), "Additional TMI-Related Requirements," or equivalent TMI action plan requirements imposed by Generic Letters.

(2)(xx), "Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 2, "Design Bases for Protection Against Natural Phenomena."

General Design Criterion 4, "Environmental and Missile Design Bases."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

General Design Criterion 34, "Residual Heat Removal."

General Design Criterion 35, "Emergency Core Cooling."

General Design Criterion 38, "Containment Heat Removal."

2. Additional acceptance criteria applicable to safe shutdown systems proposed for design certification under 10 CFR 52 include

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

10 CFR 52.47(b)(2)(i), "Innovative Means of Accomplishing Safety Function."

3. Additional acceptance criteria applicable to safe shutdown systems proposed as part of combined license applications under 10 CFR 52 include

10 CFR 52.79(c), "ITAAC in Combined License Applications."

Section 7.1, Table 7-1 and Appendix 7.1-A list the requirements, standards, regulatory guides, and branch technical positions (BTP) that provide information, recommendations, and guidance that describe a basis acceptable to the NRC staff to implement the relevant requirements of the NRC regulations identified above.

III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any instrumentation and control system. This part of section 7.4 highlights specific topics that should be emphasized in the review of safe shutdown systems.

The review should include an evaluation of the safe shutdown systems design against the guidance of ANSI/IEEE Std 279, or Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems" (which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"), depending upon the applicant/licensee's commitment regarding these design criteria. This procedure is detailed in Appendix 7.1-B for ANSI/IEEE Std 279 and in Appendix 7.1-C for IEEE Std 603. The procedures in Appendices 7.1-B and 7.1-C address specific design requirements.

Appendices 7.1-B and 7.1-C discuss ANSI/IEEE Std 279 and IEEE Std 603, respectively, and how they are used in the review of safe shutdown systems. Although the primary emphasis is on the equipment comprising the safe shutdown systems, the reviewer should consider the safe shutdown functions on a system level. The safe shutdown systems design should be compatible with the SAR Chapter 15 design bases accident analyses. It is not sufficient to evaluate the adequacy of the safe shutdown systems only on the basis of the design meeting the specific requirements of ANSI/IEEE Std 279 or IEEE Std 603.

Major portions of the systems required for safe shutdown are also used as ESF systems, as discussed in SRP Section 7.3. Therefore, the review under this SRP section includes those aspects of ESF systems which are unique to safe shutdown, in addition to those systems required for safe shutdown which are not classified as ESF systems.

The safe shutdown systems review should address the topics identified as applicable by Table 7-1. Appendix 7.1-A describes review methods for each topic. Major design considerations that should be emphasized in the review of I&C for the safe shutdown systems are identified below.

- The review confirms that I&C required for safe shutdown (where appropriate based on their safety function):
 - Provides the required redundancy,
 - Meets the single-failure criterion,
 - Provides the required capacity and reliability to perform intended safety functions on demand,
 - Provides the capability to function during and after design-basis events such as earthquakes and anticipated operational occurrences,
 - Provides the capability to operate with onsite electric power available (assuming offsite power is not available) and with offsite electric power available (assuming onsite power is not available), and
 - Provides the capability to be tested during reactor operation.
- Single-failure criterion — The remote control stations and the equipment used to maintain safe shutdown should be designed to accommodate a single failure. See Appendix 7.1-B item 3 or Appendix 7.1-C item 4.¹
- Independence — See Appendix 7.1-B item 7 and 8 and Appendix 7.1-C item 11 and 24.
- Use of digital systems — See Appendix 7.0-A.
- Periodic testing — See Appendix 7.1-B item 11 or see Appendix 7.1-C items 12 and 27.
- Remote shutdown capability — Plant designs should provide for control in locations removed from the main control room that may be used for manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown. This control equipment should be capable of operating independently of (without interaction with) the equipment in the main control room. This equipment may include the remote shutdown station and other local controls.

The design of remote shutdown stations should provide appropriate displays so that the operator can monitor the status of the shutdown. Typical parameters for PWR displays are steam generator level, steam generator pressure, pressurizer pressure, pressurizer level, reactor coolant temperature, and

¹Shutdown remote from the control room is not an event analyzed in the accident analysis in Chapter 15 of the SAR. Specific scenarios have not been specified upon which the adequacy of shutdown capability remote from the control room is evaluated. However, smoke due to a fire in the control room has long been recognized as the type of event which could force the evacuation of the control room and result in a need to effect safe shutdown remote from the control room. Branch Technical Position CMEB 9.5.-1 establishes the bases for safe shutdown with respect to fire protection. Specifically, fire damage limits as they impact on safe shutdown have been established therein. These limits do not require consideration of an additional random single failure in the evaluation of the capability to safely shut down as a consequence to fires. The evaluation of conformance to the BTP is addressed in SRP Section 9.5.1. Therefore, the application of the single-failure criterion to remote shutdown is only applicable for other events which could cause the control room to become uninhabitable. These events would not result in consequential damage or unavailability of systems required for safe shutdown.

auxiliary feedwater flow. Typical parameters for BWR displays are reactor vessel water level and pressure and high pressure core injection system flow.

The remote shutdown capability should be capable of accommodating expected plant response following a reactor trip, including protective system actions which could occur as a result of plant cooldown. For example, in the cooldown of a PWR, reactor cooling system pressure will eventually drop below the safety injection initiation setpoint. Since the control room is not available, it may be impossible to block this trip. Therefore, the remote shutdown capability must be able to accommodate this condition.

Access to remote shutdown stations should be under strict administrative controls.

The equipment in the remote shutdown stations should be designed to the same standards as the corresponding equipment in the main control room.

Remote shutdown station control transfer devices should be located remote from the main control room and their use should initiate an alarm in the control room. The location should be consistent with the procedures for remote, alternative, and dedicated shutdown, as appropriate.

Where the control functions are transferred between the control room and the remote shutdown station, the design should maintain parameter indications such that the operators at the control room and the remote shutdown station both have access to the same parameters that are being relied upon.

- Safe shutdown — System conformance to the single-failure criterion on a system basis and operability from onsite and offsite electrical power as required by GDC 34, 35, and 38.

In certain instances, it will be the Staff's judgment that, for a specific case under review, emphasis should be placed on specific aspects of the design, while other aspects of the design need not receive the same emphasis and in-depth review. Typical reasons for such a non-uniform emphasis are the introduction of new design features or the utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the NRC's regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the safety evaluation report (SER):

The NRC staff concludes that the design of the safe shutdown systems and the safe shutdown initiation of the essential auxiliary support (EAS) systems are acceptable and meet the relevant requirements of General Design Criteria (GDC) 1, 2, 4, 13, 19, 34, 35 and 38, and 10 CFR 50.55a(a)(1).

The Staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and standards applicable to these systems. The Staff concludes that the applicant/licensee adequately identified the guidelines applicable to these systems. Based upon the review of the system design for conformance to the guidelines, the Staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore, the Staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The non-safety portions of information systems important to safety are appropriately isolated from safety systems, including the safety portions of the information systems. Therefore, the Staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 5.55a(h) and the requirements of GDC 24.

The review included the identification of those systems and components for the safe shutdown systems which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based upon the review, the Staff concludes that the applicant/licensee has identified those systems and components consistent with the design bases for those systems. Sections 3.10 and 3.11 of the SER address the qualification programs to demonstrate the capability of these systems and components to survive these events. Therefore, the Staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

Based on the review, the Staff concludes that instrumentation and controls have been provided to maintain variables and systems which can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems within prescribed operating ranges during plant shutdown. Therefore, the Staff finds that the systems required for safe shutdown satisfy the requirements of GDC 13.

Instrumentation and controls have been provided within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including a shutdown following an accident. Equipment at appropriate locations outside the control room has been provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures. Therefore, the Staff concludes that the systems required for safe shutdown satisfy the requirements of GDC 19.

The review of the instrumentation and control systems required for safe shutdown includes conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures as appropriate based on their safety function consistent with the General Design Criteria applicable to safe shutdown systems. The Staff concludes that these systems are testable, and are operable on either onsite or offsite electrical power, and that the controls associated with redundant safe shutdown systems are independent and satisfy the requirements of the single-failure criterion and, therefore, meet the relevant requirements of GDC 34, 35, and 38.

In the review of the safe shutdown systems, the Staff examined the dependence of these systems on the available essential auxiliary systems. Based on this review and coordination with those having primary review responsibility of EAS systems, the Staff concludes that the design of the safe shutdown systems is compatible with the functional requirements of EAS systems.

Note: the following finding applies only to systems involving digital computer-based components.

Based on the review of software development plans and the inspections of the computer development process and design outputs, the Staff concludes that the computer systems meet the guidance of Reg. Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the Staff finds that the computer-based safe shutdown systems satisfy the requirements of GDC 1.

Note: the following findings apply only to applications under 10 CFR 52.

The safe shutdown systems design appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the safe shutdown systems satisfy the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the safe shutdown systems examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria are met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the safe shutdown systems satisfy the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the safe shutdown systems [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the design of the safe shutdown systems satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

The safe shutdown systems contain the following elements which differ significantly from evolutionary changes from light water reactor designs of plants which have been licensed in commercial operation before April 18, 1989. [Insert list.] Based upon the review of [analysis OR test programs OR operating experience] the Staff concludes that the performance of these features has been demonstrated; interdependent effects among the safety features are acceptable; sufficient data exist to assess the analytical tools used for safety analysis; and the scope of the design is complete except for site-specific elements. Therefore, the Staff finds that the safe shutdown systems satisfy the requirements of 10 CFR 52.47(b)(2)(i).

Based upon an initial review of the scope and content of the material submitted by the applicant/licensee, and completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the safe shutdown systems design to satisfy the requirements of 10 CFR 52.47(a)(2).

Note: the following conclusion is applicable to all applications.

The conclusions noted above for the safe shutdown systems are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted [List applicable system or topics and identify references].

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

VI. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Section 7.5. Information Systems Important to Safety

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

This SRP section describes the review process and acceptance criteria for those instrumentation and control (I&C) systems that provide information to the plant operators for: (1) assessing plant conditions, safety system performance and making decisions related to plant responses to abnormal events; and (2) preplanned manual operator action related to accident mitigation. The information systems reviewed using this section also provide the necessary information from which appropriate actions can be taken to mitigate the consequences of anticipated operational occurrences. The systems reviewed using Section 7.5 of the SRP include the following:

- Post-accident monitoring (PAM) systems.
- Bypassed or inoperable status indication (BISI) for safety systems.

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

- Plant annunciator (alarm)¹ systems
- Safety parameter display system (SPDS).
- Information systems associated with the emergency response facilities (ERF) and nuclear data link (NDL).

For SPDS, ERF, and NDL, the HICB review is limited to the system interface with the plant control and protection systems. Functional performance of those systems, as well as functional aspects of other I&C systems — such as radiation monitoring, fire detection, and the information systems for environs conditions during and following an accident — are addressed in the review of other sections of the safety analysis report (SAR).

The objectives of the review are to confirm that the information systems important to safety satisfy the requirements of the acceptance criteria and guidelines applicable to these systems, and that they will provide the information to ensure plant safety during all plant conditions for which they are required.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

II. Acceptance Criteria

The acceptance criteria and guidelines applicable to information systems important to safety are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified for these systems. The review of the information systems important to safety in this section of the SAR confirms that these systems conform to the requirements of the acceptance criteria and guidelines.

Acceptance criteria for the review of the information systems important to safety are based on meeting the relevant requirements of the following regulations.

1. Acceptance criteria applicable to post-accident monitoring systems

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For post-accident monitoring systems isolated from the protection system, the only applicable requirement from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

¹For the purposes of this section, the annunciator system is considered to consist of sets of alarms (which may be displayed on tiles, video display units, or other devices) and sound equipment; logic and processing support, and functions to enable operators to silence, acknowledge, reset, and test alarms.

10 CFR 50.34(f), "Additional TMI-Related Requirements," or equivalent TMI action plan requirements imposed by Generic Letters. The following portions of this part apply to PAM systems.

(2)(xii), "Auxiliary Feedwater System Flow Indication" (applicable to PWRs only).

(2)(xvii), "Accident Monitoring Instrumentation."

(2)(xviii), "Inadequate Core Cooling Instrumentation."

(2)(xix), "Instruments for Monitoring Plant Conditions Following Core Damage."

(2)(xx), "Power for Pressurizer Level Indication" (applicable to PWRs only).

(2)(xxiv), "Central Reactor Vessel Water Level Recording" (applicable to BWRs only).

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 2, "Design Basis for Protection Against Natural Phenomena" (applicable only to channels classified as Category 1 or 2 in Reg. Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident").

General Design Criterion 4, "Environmental and Missile Design Basis" (applicable only to channels classified as Category 1 or 2 in Reg. Guide 1.97).

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

2. Acceptance criteria applicable to bypassed and inoperable status indication

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For BISI that are isolated from the protection system, the only applicable requirements from ANSI/IEEE Std 279 are item 4.7.2, "Isolation Devices," and 4.13, "Indication of Bypasses."

10 CFR 50.34(f)(2)(v), "Additional TMI-Related Requirements" - bypass and inoperable status indication, or equivalent TMI action plan requirements imposed by Generic Letters.

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 24, "Separation of Protection and Control Systems."

3. Acceptance criteria applicable to annunciator systems

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For annunciators that are isolated from the protection system, the only applicable requirements from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

Additional acceptance criteria applicable to ALWR annunciator systems

Staff Requirements Memorandum (SRM), "SECY-93-087 — Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," Item II.T, "Control Room Annunciator (Alarm) Reliability." This SRM states:

"... the alarm system for ALWRs should meet the applicable EPRI requirements for redundancy, independence, and separation. In addition, alarms that are 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, shall meet the applicable requirements for Class 1E equipment and circuits."

4. Acceptance criteria applicable to the HICB review of SPDS, ERF information systems, and NDL information systems

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279. For SPDS, ERF information systems, and NDL information systems isolated from the protection system, the only applicable requirement from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 24, "Separation of Protection and Control Systems."

5. Additional criteria applicable to information systems important to safety proposed for design certification under 10 CFR 52

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

10 CFR 52.47(b)(2)(i), "Innovative Means of Accomplishing Safety Functions."

6. Additional acceptance criteria applicable to information systems important to safety proposed as part of combined license applications under 10 CFR 52

10 CFR 52.79(c), "ITAAC in Combined License Applications."

Section 7.1, Table 7-1, and Appendix 7.1-A list standards, regulatory guides, and branch technical positions that provide information, recommendations, and guidance that describe a basis acceptable to the NRC staff for implementing the relevant requirements of the NRC regulations identified above.

III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any I&C system. Section 7.5 highlights specific topics that should be emphasized in the review of information systems important to safety.

The systems addressed below may be implemented either as stand alone systems or integrated as part of other systems. If the information systems are not isolated from the protection systems, they should also be evaluated according to the criteria in Section 7.2 or 7.3, as appropriate.

Other information systems (for example, plant computer and severe accident monitoring) may be included in the review. The acceptance criteria for such systems depend on the function of the system and the applicable design criteria.

Any exceptions or deviations to a post-accident monitoring system designed to satisfy Reg. Guide 1.97 should be identified in the SAR. This includes acceptable deviations and clarifications identified in BTP HICB-10.

The review should include an evaluation of the information systems design against the guidance of ANSI/IEEE Std 279, or Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems" (which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"), depending upon the applicant/licensee's commitment regarding these design criteria. This procedure is detailed in Appendix 7.1-B for ANSI/IEEE Std 279 and in Appendix 7.1-C for IEEE Std 603. The procedures in Appendices 7.1-B and 7.1-C address specific design requirements.

The reviewer should consider the overall information system functions on a system level. The design should be compatible with the SAR Chapter 15 design bases accident analyses, and operating procedures as well as applicable guidance of ANSI/IEEE Std 279 or IEEE Std 603.

The review should also consider the guidance provided in NUREG-0737, Supplement 1, "Clarification of TMI Action Plan Requirements — Requirements for Emergency Response Capability," with respect to PAM, ERF, and SPDS.

The information systems review should address the topics identified as applicable in Table 7-1. Appendix 7.1-A describes review methods for each topic. Certain guidance documents identified in Parts 3 and 4 of Table 7-1 apply only to BISI or PAM, but not both. The guidance documents that are not applicable to a specific system are identified below.

Major design considerations that should be emphasized in the review of the information systems important to safety are identified below.

1. Recommended review emphasis for PAM

- Conformance with Reg. Guide 1.97 and BTP HICB-10.
- Use of digital systems — See Appendix 7.0-A.
- Emergency operating procedures (EOP) action points — A basis should be provided for EOP action points that accounts for measurement uncertainties. Draft Reg. Guide DG-1045, the proposed revision 3 to Reg. Guide 1.105, "Instrument Spans and Setpoints," provides acceptable guidance for establishing these uncertainties.
- Monitoring for severe accidents — The accident monitoring instrumentation should be demonstrated to perform their intended function for severe accident protection. They need not be subject to additional 10 CFR 50.49 environmental qualification requirements. However, they should be designed so there is reasonable assurance that they will operate in the severe-accident environment for which they are intended and over the time span for which they are needed.

2. Recommended review emphasis for BISI

- Scope of BISI indications — As a minimum BISI should be provided for the following systems:
 - RTS and ESFAS — See Appendix 7.1-B item 14 and Appendix 7.1-C item 13.
 - Interlocks for isolation of low-pressure systems from the reactor coolant system — See BTP HICB-1.
 - ECCS accumulator isolation valves — See BTP HICB-2.
 - Controls for changeover of RHR from injection to recirculation mode — See BTP HICB-6.
- Conformance with Reg. Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

- Independence — See Appendix 7.1-B item 8 and Appendix 7.1-C item 24. The indication system should be designed and installed in a manner which precludes the possibility of adverse effects on plant safety systems. Failure or bypass of a protective function should not be a credible consequence of failures occurring in the indication equipment, and the bypass indication should not reduce the required independence between redundant safety systems.
- Use of digital systems — See Appendix 7.0-A.

3. Recommended review emphasis for annunciator systems

- Reliability — The applicant/licensee should justify that the degree of redundancy, diversity, testability, and quality provided in annunciator systems is adequate to support normal and emergency operations. Appendix 7.1-C item 20 provides guidance on the evaluation of safety system reliability that may be used in evaluating the reliability of annunciator systems.
- Use of digital systems — See Appendix 7.0-A.
- Independence (isolation between safety systems and other systems) — See Appendix 7.1-B item 8 and Appendix 7.1-C item 24.

Additional items for emphasis for ALWR annunciator systems

- Redundancy — Redundant alarm systems should be provided. These redundant systems need not comply with the single failure criterion, but independence between the redundant systems should be equivalent to that provided between redundant channels of the protection systems. See Appendix 7.1-B item 7 and Appendix 7.1-C item 11.
- Self-test provisions — See BTP HICB-17. The surveillance test portions of this BTP are not applicable.
- Compliance with IEEE Std 279 — Alarms that are 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 should be reviewed against the guidance of Reg. Guide 1.153. See Appendix 7.1-C.

4. Recommended review emphasis for SPDS, ERF information systems, and NDL information systems

- Independence (isolation between safety systems and other systems) — See Appendix 7.1-B item 8 and Appendix 7.1-C item 24.

In each safety review, the reviewer should determine the elements of the design that require additional review emphasis. Typical reasons for such a non-uniform emphasis are the introduction of new design features or the utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the Code of Federal Regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the SER:

The NRC staff concludes that the designs of the information systems important to safety are acceptable and meet the relevant requirements of General Design Criteria (GDC) 1, 2, 4, 13, 19, and 24, and 10 CFR 50.34(f), 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h).

The Staff conducted a review of the information systems important to safety for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The Staff concluded that the applicant/licensee adequately classified and identified the guidelines applicable to these systems. Based upon the review of the system design for conformance to the guidelines, the Staff finds that the systems conform to the guidelines applicable to these systems. Therefore, the Staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included the identification of those systems and components for the information systems important to safety that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based upon the review, the Staff concludes that the applicant/licensee has identified those systems and components consistent with the design bases for those systems. Sections 3.10 and 3.11 of the SER address the qualification programs to demonstrate the capability of these systems and components to survive these events. Therefore, the Staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

The non-safety portions of information systems important to safety are appropriately isolated from safety systems, including the safety portions of the information systems. Therefore, the Staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and the requirements of GDC 24.

The instrumentation provided for monitoring severe accident conditions has been designed to operate in the severe-accident environment for which they are intended and over the time span for which they are needed. Therefore, the Staff finds that the severe accident monitoring instrumentation satisfies the requirements of GDC 2 and 4.

The post-accident monitoring system conforms to the guidelines for the instrumentation to access plant conditions during and following an accident provided in Reg. Guide 1.97. The redundant information systems conform to the guidelines for the physical independence of electrical systems provided in Reg. Guide 1.75. The instrument spans and EOP action points were established in accordance with the guidelines of Draft Reg. Guide DG-1045. The environmental monitoring system provided to protect the safety instrument sensing lines from freezing conforms to the guidelines of Reg. Guide 1.151, position 5. The post-accident monitoring system includes appropriate variables. The range and accuracy of the instrument channels for these variables are consistent with the plant safety analysis. The post-accident monitoring system includes appropriate variables for monitoring severe accident conditions. The variables monitored and the range and accuracy of instrumentation provided to monitor these variables is consistent with the severe accident analysis. Therefore, the staff finds that the post-accident monitoring system meets the requirements of GDC 13 and 19.

The post-accident monitoring system includes the following functions required by 10 CFR 50.34(f): [feedwater system flow indication²], accident monitoring instrumentation, inadequate core cooling instrumentation, instruments for monitoring plant conditions following core damage, [central reactor vessel water level recording³]. Additionally, the power supply for the PAM pressurizer level indication complies with the requirements of 10 CFR 50.34(f)(xx) [applicable to PWRs only]. Therefore, the Staff concludes that the instrumentation systems important to safety satisfy the requirements of 10 CFR 50.34(f), Subparts xii, xvii, xviii, xix, xx, and xxiv.

The Staff reviewed the systems for which a bypassed or inoperable status is indicated in the control room. The Staff finds that the bypass indications will give the operators timely information and status reports so the operators can mitigate the effects of unexpected system unavailability. The bypass indications satisfy the guidelines of Reg. Guide 1.47. Therefore, the Staff concludes that the BISI functions satisfy the applicable requirements of 10 CFR 50.55a(h) and 10 CFR 50.34(f)(2)(v).

The Staff reviewed the control room annunciator systems and finds that these systems are sufficiently reliable to support normal and emergency plant operations. [Redundant annunciator systems are provided and the independence of these redundant systems complies with the independence requirements of IEEE Std 279 Section 4.6 OR IEEE Std 603 Section 5.6. Alarms 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 comply with the guidance of IEEE Std 603.] Therefore, the Staff concludes that the annunciator systems satisfy the requirements of [the SRM on SECY-93-087 item II.T,] GDC 13 and 19.

Based upon the above items, the Staff finds that the information systems satisfy the requirements of GDC 13 for monitoring variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions. Further, the Staff finds that conformance to GDC 13 and the applicable guidelines satisfies the requirements of GDC 19 with respect to information systems provided in the control room from which actions can be taken to operate the unit safely under normal conditions and to maintain it in a safe condition under accident conditions.

The safety parameter display system, the information systems associated with the emergency response facilities, and the nuclear data link, non-safety portions of PAM, non-safety portions of BISI, and non-safety portions of the annunciator systems are appropriately isolated from safety systems. Electrical isolation devices were qualified in accordance with the guidance of BTP HICB-11. Therefore, the staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and GDC 24.

The applicant/licensee has also incorporated in the system design the recommendations of TMI task action plan items [identify item number and how implemented] that the Staff has reviewed and found acceptable.

In the review of the information systems important to safety, the Staff examined the dependence of these systems on the availability of essential auxiliary systems. Based on this review and coordination with those having primary review responsibility of EAS systems, the Staff concludes that the design of the information systems important to safety is compatible with the functional requirements of EAS systems.

²Applicable to PWRs only.

³Applicable to BWRs only.

Note: the following finding applies only to systems involving digital computer-based components.

Based on the review of software development plans and the inspections of the computer development process and design outputs, the Staff concludes that the computer systems meet the guidance of Reg. Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the Staff finds that the information systems important to safety satisfy these requirements of GDC 1.

Note: the following findings apply only to applications under 10 CFR 52.

The design of the information systems important to safety appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the information systems important to safety satisfy the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the information systems important to safety examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria are met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the information systems important to safety satisfy the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the information systems important to safety [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the design of the information systems important to safety satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

The information systems important to safety contain the following elements that differ significantly from evolutionary changes from light water reactor designs of plants that have been licensed in commercial operation before April 18, 1989. [Insert list.] Based upon the review of [analysis OR test programs OR operating experience] the Staff concludes that the performance of these features has been demonstrated; interdependent effects among the safety features are acceptable; sufficient data exist to assess the analytical tools used for safety analysis; and the scope of the design is complete except for site-specific elements. Therefore, the Staff finds that the information systems important to safety satisfy the requirements of 10 CFR 52.47(b)(2)(i).

Based upon an initial review of the scope and content of the material submitted by the applicant, and completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the information systems important to safety design to satisfy the requirements of 10 CFR 52.47(a)(2).

Note: the following conclusion is applicable to all applications.

The conclusions noted above for the information systems important to safety are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted. [List applicable system or topics and identify references.]

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

VI. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

NUREG-0737 Supplement 1. "Clarification of TMI Action Plan Requirements — Requirements for Emergency Response Capability." January 1983.

Regulatory Guide 1.151. "Instrument Sensing Lines." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1983.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

Regulatory Guide 1.97. "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1983.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Section 7.6. Interlock Systems Important to Safety

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

This SRP section describes the review process and acceptance criteria for those interlock systems important to safety that operate to reduce the probability of occurrence of specific events, or to maintain safety systems in a state that ensures their availability in an accident. These systems include interlock systems to prevent overpressurization of low-pressure systems (for example, residual heat removal (RHR)) when these systems are connected to high-pressure systems (for example, primary coolant), interlocks to prevent overpressure of the primary coolant system during low-temperature operation of the reactor vessel, valve interlocks to ensure the availability of emergency core cooling system (ECCS) accumulators, interlocks to isolate safety systems from non-safety systems (for example, seismic and non-seismic portions of auxiliary supporting systems), and interlocks to preclude inadvertent inter-ties between redundant or diverse safety systems where such inter-ties exist for the purposes of testing or maintenance.

The objective of the review is to confirm that design considerations such as redundancy, independence, single failures, qualification, bypasses, status indication, and testing are consistent with the design bases of these systems and commensurate with the importance of the safety functions to be performed.

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

II. Acceptance Criteria

The acceptance criteria and guidelines applicable to interlock systems are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified for these systems. The review in this section of the SAR confirms that these systems conform to the requirements of the acceptance criteria and guidelines.

1. Acceptance criteria applicable to any interlock system important to safety

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For interlock systems isolated from the protection system, the only applicable requirement from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

2. In addition to the acceptance criteria indicated above, safety system interlocks are reviewed for conformance to the following acceptance criteria

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations."

10 CFR 50.34(f)(2)(v), "Additional TMI-Related Requirements, Bypass and Inoperable Status Indication," or equivalent TMI action requirements imposed by Generic Letters.

General Design Criterion 2, "Design Bases for Protection Against Natural Phenomena."

General Design Criterion 4, "Environmental and Missile Design Bases."

3. The following acceptance criteria are applicable to safety systems with which interlock systems may interact. These criteria are used as guidance, where applicable, in establishing the importance to safety for functions performed by interlock systems

General Design Criterion 10, "Reactor Design."

General Design Criterion 15, "Reactor Coolant System Design."

General Design Criterion 16, "Containment Design."

General Design Criterion 28, "Reactivity Limits."

General Design Criterion 33, "Reactor Coolant Makeup."

General Design Criterion 34, "Residual Heat Removal."

General Design Criterion 35, "Emergency Core Cooling."

General Design Criterion 38, "Containment Heat Removal."

General Design Criterion 41, "Containment Atmosphere Cleanup."

General Design Criterion 44, "Cooling Water."

4. Additional acceptance criteria applicable to interlock systems important to safety proposed for design certification under 10 CFR 52

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

10 CFR 52.47(b)(2)(i), "Innovative Means of Accomplishing Safety Functions."

5. Additional acceptance criteria applicable to interlock systems important to safety proposed as part of combined license applications under 10 CFR 52

10 CFR 52.79(c), "ITAAC in Combined License Applications."

Section 7.1, Table 7-1 and Appendix 7.1-A list standards, regulatory guides, and branch technical positions that provide information, recommendations, and guidance that describe a basis acceptable to the NRC staff for implementing the relevant requirements of the NRC regulations identified above for interlock systems important to safety.

III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any instrumentation and control system. This part of section 7.6 highlights specific topics that should be emphasized in the interlock systems review.

The review should include an evaluation of the interlock system design against the guidance of ANSI/IEEE Std 279, or Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems" (which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"), depending upon the applicant/licensee's commitment regarding these design criteria. This procedure is detailed in Appendix 7.1-B for ANSI/IEEE Std 279 and in Appendix 7.1-C for IEEE Std 603. The procedures in Appendices 7.1-B and 7.1-C address specific design requirements.

Appendices 7.1-B and 7.1-C discuss ANSI/IEEE Std 279 and IEEE Std 603, respectively, and how they are used in the review of the interlock systems. Although the primary emphasis is on the equipment comprising the interlock systems, the reviewer should consider the interlock functions on a system level. The interlock systems design should be compatible with the SAR Chapter 15 design bases accident analyses. It is not sufficient to evaluate the adequacy of the interlock systems only on the basis of the design meeting the specific requirements of ANSI/IEEE Std 279 or IEEE Std 603.

The interlock systems review should address the applicable topics identified in Table 7-1. Appendix 7.1-A describes review methods for each topic. Major design considerations that should be emphasized in the review of the interlock systems are identified below.

- Single-failure criterion — See Appendix 7.1-B item 3 or Appendix 7.1-C item 6.
- Quality of components and modules — See Appendix 7.1-B item 4 or Appendix 7.1-C item 8.
- Independence — See Appendix 7.1-B items 7 and 8 or Appendix 7.1-C item 11 and 24.
- System testing and inoperable surveillance — See Appendix 7.1-B items 10 and 11 or Appendix 7.1-C item 12, 13, and 27.
- Use of digital systems — See Appendix 7.0-A.
- Interlocks to prevent overpressurization of low pressure systems — See BTP HICB-1.
- Interlocks to prevent overpressure of the primary coolant system during low-temperature operations of the reactor vessel — See BTP RSB 5-2.
- Interlocks for ECCS accumulator valves — See BTP HICB-2.
- Interlocks required to isolate safety systems from non-safety systems and interlocks required to preclude inadvertent inter-ties between redundant or diverse safety systems.

In each safety review, the Staff should determine the elements of the design that require additional review emphasis. Typical reasons for such a non-uniform emphasis are the introduction of new design features or the

utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the Code of Federal Regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the SER:

The NRC staff concludes that the design of the interlock systems is established in accordance with its safety function, is acceptable, and meets the relevant requirements of General Design Criteria (GDC) 1, 2, 4, 10, 13, 15, 16, 19, 24, 28, 33-35, 38, 41 and 44, 10 CFR 50.55a(a)(1) and 10 CFR 50.55a(h).

The Staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The Staff concluded that the applicant/licensee adequately identified the guidelines applicable to these systems and has properly classified them. Based upon the review of the system design for conformance to the guidelines, the Staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore the Staff finds that these requirements of GDC 1, 15, 16, 33-35, 38, 41, and 44, and 10 CFR 50.55a(a)(1) have been met.

Based upon the review of interlock system functions, the Staff concludes that appropriate interlocks are provided to maintain an appropriate design margin to assure that acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences. Therefore, the Staff finds that the interlock systems satisfy the requirements of GDC 10, 15, 16, 28, 33-35, 38, 41, and 44.

Based on the review of interlock system status information, initiation capabilities, and provisions to support safe shutdown, the Staff concludes that information is provided to monitor interlocks over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for interlock initiation and bypass. The interlocks appropriately support actions to operate the nuclear power unit safety under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the Staff finds that the interlock systems satisfy the requirements of GDC 13 and 19.

The Staff conducted a review of these systems and finds that they comply with the reliability guidance of [IEEE Std. 279 or Reg. Guide 1.153]. Based upon this review, the Staff finds that the redundancy requirements of GDC 34, 35, 38, 41, and 44 have been met.

The review included the identification of those systems and components for the interlock systems that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based upon the review, the Staff concludes that the applicant/licensee has identified those systems and components consistent with the design bases for those systems. Sections 3.10 and 3.11 of the SER address the qualification programs to demonstrate the capability of these systems and components to survive these events. Therefore, the Staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

The Staff reviewed the bypassed or inoperable status indication of safety interlocks. The Staff finds that appropriate bypass indications are provided to give the operators timely information and status reports so the operators can mitigate the effects of unexpected system unavailability. The bypass

indications satisfy the guidelines of Reg. Guide 1.47. Therefore, the Staff concludes that the safety interlock systems satisfy the applicable requirements of 10 CFR 50.55a(h) and 10 CFR 50.34(f)(2)(v).

The non-safety interlock systems are appropriately isolated from safety systems. Therefore, the staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and the requirements of GDC 24.

Based on the review of interlock safety system design, the Staff concludes that the safety portions of the interlock systems comply with the requirements of [ANSI/IEEE Std 279 OR IEEE Std 603]. Therefore, the Staff finds that the interlock safety systems satisfy the requirements of 10 CFR 50.55a(h).

In the review of the interlock systems, the Staff examined the dependence of this system on the availability of essential auxiliary systems. Based on this review and coordination with those having primary review responsibility of essential auxiliary supporting (EAS) systems, the Staff concludes that the design of the interlock systems is compatible with the functional requirements of EAS systems.

Note: the following finding applies only to systems involving digital computer-based components.

Based on the review of software development plans and the inspections of the computer development process and design outputs, the Staff concludes that the computer systems meet the guidance of Reg. Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the Staff finds that the interlock systems satisfy these requirements of 10 CFR 50.55a(a)(1), GDC 1, 13, and 19.

Note: the following findings apply only to applications under 10 CFR 52.

The interlock systems design appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the interlock systems satisfy the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the interlock systems examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria are met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the interlock systems satisfy the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the interlock systems [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the interlock systems satisfy the requirements of 10 CFR 52.47(a)(1)(vii).

The interlock systems contain the following elements that differ significantly from evolutionary changes from light water reactor designs of plants that have been licensed in commercial operation before April 18, 1989. [Insert list.] Based upon the review of [analysis OR test programs OR operating experience] the Staff concludes that the performance of these features has been demonstrated; interdependent effects among the safety features are acceptable; sufficient data exist to assess the analytical tools used for safety analysis; and the scope of the design is complete

except for site-specific elements. Therefore, the Staff finds that the interlock systems satisfy the requirements of 10 CFR 52.47(b)(2)(i).

Based upon an initial review of the scope and content of the material submitted by the applicant, and completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the interlock systems design to satisfy the requirements of 10 CFR 52.47(a)(2).

Note: the following conclusion is applicable to all applications.

The conclusions noted above for the interlock systems are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted [List applicable system or topics and identify references].

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

VI. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Section 7.7. Control Systems

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

This SRP section describes the review process and acceptance criteria for those control systems used for normal operation that are not relied upon to perform safety functions following anticipated operational occurrences or accidents, but those that control plant processes having a significant impact on plant safety. These control systems are those systems that can, through normal operation, system failure or inadvertent operation, affect the performance of critical safety functions. Table 7.7-1 lists examples of control system functions that may be included in the scope of Section 7.7 for boiling water and pressurized water reactors. The actual list of system functions and systems included in the scope of Section 7.7 will be plant specific. A specific plant may not necessarily incorporate all of the functions listed in Table 7.7-1, may require functions beyond those listed in Table 7.7-1, or may group functions into systems differently than indicated in Table 7.7-1.

These systems are reviewed to ensure that they conform to the acceptance criteria and guidelines, that the controlled variables can be maintained within prescribed operating ranges, and that effects of operation or failure of these systems are bounded by the accident analyses in Chapter 15 of the SAR.

HICB also has secondary review responsibility for instrumentation and control systems which are reviewed by the Staff as part of the controlled system. These systems include I&C for support systems and plant

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

process systems. The acceptance criteria and review procedures of Section 7.7 are also applicable to these other I&C systems. Table 7.7-2 lists examples of control system functions for which HICB may have secondary review responsibility. Table 7.7-2 is not grouped according to plant type. The actual list of system functions and systems within the scope of HICB's secondary review responsibility will be plant-specific. A specific plant may not necessarily incorporate all of the functions listed in Table 7.7-2, may require functions beyond those listed in Table 7.7-2, or may group functions into systems differently than indicated in Table 7.7-2.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

In addition to the coordinated reviews discussed in SRP Section 7.0, the review of Section 7.7 should be coordinated with the Reactor Systems Branch (SRXB) and Plant Systems Branch (SPLB) to confirm the adequacy of control systems with respect to maintaining variables within operational limits during plant operation and to confirm that the impact of control system failures are appropriately included in the design basis accident analyses.

For those areas being reviewed as part of the primary review responsibility of other branches, the acceptance criteria necessary for the review, and their methods of application, are contained in the SRP sections identified in Appendix 7.1-A item 2.d.

II. Acceptance Criteria

Acceptance criteria and guidelines applicable to control systems are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified for these systems. The review of the control systems confirms that these systems conform to the requirements of the acceptance criteria and guidelines.

Acceptance criteria for the review of control systems are based on meeting the relevant requirements of the following regulations:

1. Acceptance criteria applicable to any control systems

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For control systems isolated from the protection system, the only applicable requirement from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

10 CFR 50.34(f), "Additional TMI-Related Requirements," or equivalent TMI action plan requirements imposed by Generic Letters.

(2)(xxii), "Failure Mode and Effect Analysis of Integrated Control System" (applies only to B&W plants).

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs."

2. Additional acceptance criteria applicable to control systems proposed for design certification under 10 CFR 52

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

3. Additional acceptance criteria applicable to control systems proposed as part of combined license applications under 10 CFR 52

10 CFR 52.79(c), "ITAAC in Combined Operating License Applications."

Section 7.1, Table 7-1 and Appendix 7.1-A list standards, regulatory guides, and branch technical positions that provide information, recommendations, and guidance that describe a basis acceptable to the NRC staff for implementing the relevant requirements of the NRC regulations identified above for control systems.

III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any instrumentation and control system. This part of Section 7.7 highlights specific topics that should be emphasized in the control systems review.

The control systems review should address the applicable topics identified in Table 7-1. Appendix 7.1-A describes review methods for each topic. Major design considerations that should be emphasized in the review of the control systems are identified below.

- Design bases — The review should confirm that the control systems include the necessary features for manual and automatic control of process variables within prescribed normal operating limits.
- Safety classification — The review should confirm that the plant accident analysis in Chapter 15 of the SAR does not rely on the operability of any control system function to assure safety.
- Effects of control system operation upon accidents — The review should confirm that the safety analysis includes consideration of the effects of both control systems action and inaction in assessing the transient response of the plant for accidents and anticipated operational occurrences.
- Effects of control system failures — The review should confirm that the failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the SAR. This evaluation should address failure modes that can be associated with digital systems such as software design errors as well as random hardware failures. (The evaluation of multiple independent failures is not intended.)
- Effects of control system failures caused by accidents — The review should confirm that the consequential effects of anticipated operational occurrences and accidents do not lead to control systems failures that would result in consequences more severe than those described in the analysis in Chapter 15 of the SAR.
- Environmental control system — The review should confirm that I&C systems include environmental control as necessary to protect equipment from environmental extremes. This would include, for example, heat tracing of safety instruments and instrument sensing lines as discussed in Reg. Guide 1.151, "Instrument Sensing Lines" and cabinet cooling fans.
- Use of digital systems — To minimize the potential for control system failures that could challenge safety systems, control system software should be developed using a structured process similar to that applied to safety system software. Elements of the process may be tailored to account for the lower safety significance of control system software. Refer to Appendix 7.0-A for guidance on digital system review.
- Independence — The independence of safety system functions from the control system should be verified. See Appendix 7.1-B item 8 or Appendix 7.1-C item 24.
- Defense-in-depth and diversity — Control system elements credited in the Defense-in-Depth and Diversity Analysis (see BTP HICB-19) should be reviewed using the criteria for Diverse I&C systems described in Section 7.8.
- Potential for inadvertent actuation — The control systems design should limit the potential for inadvertent actuation and challenges to safety systems.

- Control of access — Physical and electronic access to digital computer-based control system software and data should be controlled to prevent changes by unauthorized personnel. Control should address access via network connections and via maintenance equipment.

In certain instances, it will be the Staff's judgment that, for a specific case under review, emphasis should be placed on specific aspects of the design, while other aspects of the design need not receive the same emphasis and in-depth review. Typical reasons for such a non-uniform emphasis are the introduction of new design features or the utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the NRC's regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the SER:

The NRC staff concludes that the design of the control systems is acceptable and meet the relevant requirements of General Design Criteria (GDC) 1, 13, 19, and 24, and 10 CFR 50.34(f), 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h).

The Staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The Staff concluded that the applicant/licensee adequately classified and identified the guidelines applicable to these systems. The Staff finds that the control systems are appropriately designed and are of sufficient quality to minimize the potential for challenges to safety systems. Based upon the review of the system design for conformance to the guidelines, the Staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore the Staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The Staff conducted a review of the plant transient response to normal load changes and anticipated operational occurrences such as reactor trip, turbine trip, upsets in the feedwater and steam bypass systems. The Staff concludes that the control systems are capable of maintaining system variables within prescribed operating limits. The applicant has also provided an environmental control system to protect safety instruments and instrument sensing lines from freezing. This system meets the guidelines of Reg. Guide 1.151, position 5; therefore, the Staff finds that the control systems satisfy this aspect of the requirements of GDC 13.

The Staff review of control systems considered the features of these systems for both manual and automatic control of the process systems. The Staff finds that the features for manual and automatic control facilitate the capability to maintain plant variables within prescribed operating limits. The Staff finds that the control systems permit actions to be taken to operate the plant safely during normal operation, including anticipated operational occurrences, and therefore the control systems satisfy the requirements of GDC 19 with regard to normal plant operations.

The control systems are appropriately isolated from safety systems. Therefore, the staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and the requirements of GDC 24.

Based on the review of the applicant/licensee's defense-in-depth and diversity analysis and the quality of control system functions credited in this analysis, the Staff concludes that the control system complies with the criteria for defense against common-mode failure in digital

instrumentation and control systems. Therefore, the Staff finds that the control system functions credited as diverse means for performing safety functions satisfy the requirements of Item II.Q of the Staff Requirements Memorandum on SECY-93-087.

The Staff confirmed that the consequential effects of anticipated operational occurrences and accidents do not result in control system failures that would cause plant conditions more severe than those bounded by the analysis of the events.

The conclusions of the analysis of anticipated operational occurrences and accidents as presented in Chapter 15 of the SAR have been used to confirm that plant safety is not dependent upon the response of the control systems. The Staff also confirmed that failure of the control systems themselves or as a consequence of supporting system failures, such as loss of power sources, does not result in plant conditions more severe than those described in the analysis of design basis accidents and anticipated operational occurrences.

Note: the following findings apply only to applications under 10 CFR 52.

The control systems design appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the control systems satisfy the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the control systems examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the control systems satisfy the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the control system [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the control system design satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

Based upon an initial review of the scope and content of the material submitted by the applicant, and completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the control systems design to satisfy the requirements of 10 CFR 52.47(a)(2).

Note: the following conclusion is applicable to all applications.

The conclusions noted above for the control systems are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted [List applicable system or topics and identify references].

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

VI. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.151. "Instrument Sensing Lines." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1983.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.

Table 7.7-1. Examples of Control Systems Typically Included in Section 7.7

Boiling Water Reactor	Pressurized Water Reactor
Nuclear boiler control and instrumentation Rod control Rod position instrumentation Neutron monitoring system Recirculation flow control system Pressure regulator and turbine generator control system Feedwater control system Internals vibration monitoring system Acoustic leak monitoring system Loose parts monitoring system Process computer system Safety system & sense line environmental control	Reactivity control system Boron control system Reactor power cutback system Rod position instrumentation In-core neutron monitoring system Ex-core neutron monitoring system Pressurizer pressure and level control system Feedwater control system In-core temperature monitoring system Steam generator water level control system Steam dump control system Steam bypass control system Internals vibration monitoring system Acoustic leak monitoring system Loose parts monitoring system Process computer system Safety system and sensing line environmental control

Table 7.7-2. Examples of Control Systems Typically Included in the Review of Other SAR Sections

Containment / drywell cooling system controls Heating, ventilating, and air conditioning controls Atmospheric control system controls Reactor water cleanup system controls Service water system controls Chilled water system controls Make-up water system controls Instrument air system controls	Fire protection systems Fire suppression system controls Security systems Spent fuel storage instrumentation and control Gaseous radioactive waste system controls Liquid radioactive waste system controls Solid radioactive waste system controls
---	---



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

NEW

Section 7.8. Diverse Instrumentation and Control Systems

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

This SRP section describes the review process and acceptance criteria for the diverse instrumentation and control (I&C) systems and equipment provided for the express purpose of protecting against potential common-mode failures of protection systems. The following systems are covered by this section:

1. Anticipated transient without scram (ATWS) mitigation systems required for compliance with 10 CFR 50.62. As defined in 10 CFR 50.62, an ATWS event is an anticipated operational occurrence followed by failure of the reactor trip portion of the protection system. 10 CFR 50.62 identifies design requirements for ATWS mitigation systems and equipment.
2. Diverse manual controls and displays provided to comply with the NRC position on defense-in-depth and diversity (D-in-D&D) as described in the Staff Requirements Memorandum (SRM) regarding SECY-93-087. These systems are to be independent and diverse from the safety computer system, and are to be located in the main control room for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

3. Diverse actuation systems (DAS) are those automatic systems provided solely for the purpose of meeting the NRC position on D-in-D&D. DAS and ATWS mitigation system functions may be combined into a single system. The reactor trip system (RTS), engineered safety features actuation system (ESFAS), control system, or other diverse I&C systems may perform DAS functions to meet the NRC position on D-in-D&D. Diverse I&C system functions performed by these other systems are not within the scope of this section. The diverse I&C functions of these systems should meet the criteria applicable to the systems as a whole. The requirements for these systems and the Staff's review are found in the SRP sections for the individual systems.

The objectives of this review are to ensure that the ATWS mitigation systems and equipment are designed and installed in accordance with the requirements of 10 CFR 50.62, and that other diverse I&C systems within the scope of this section comply with the guidance of the NRC position on D-in-D&D.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

In addition to the coordination described in SRP Section 7.0, the Reactor Systems Branch (SRXB) evaluates the following aspects of the diverse I&C systems:

1. The ATWS mitigation protective functions are reviewed to confirm that they meet the requirements of 10 CFR 50.62. The thermal/hydraulic analytical basis for ATWS is reviewed to verify that the ATWS analysis is consistent with the analyses presented or referenced in the safety analysis report (SAR) Chapter 15 for anticipated operational occurrences, and to verify the adequacy of the design of mechanical systems used to mitigate ATWS.
2. The adequacy of the set of manual control and display functions is reviewed to confirm it is sufficient to monitor the plant states and to actuate systems required by the control room operators to place the nuclear plant in a hot-shutdown condition and to control the following critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.
3. For plants with a digital computer-based RTS or ESFAS, DAS functions are reviewed to confirm that they are consistent with the portions of the accident analysis that support the D-in-D&D analysis.

II. Acceptance Criteria

Acceptance criteria and guidelines applicable to diverse I&C systems are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified for these systems. The review of the diverse I&C systems confirms that these systems conform to the requirements of the acceptance criteria and guidelines.

Acceptance criteria for the review of diverse I&C systems are the relevant requirements of the following regulations:

1. Acceptance criteria applicable to all diverse I&C system functions

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Station." For diverse I&C systems, the only applicable requirement from ANSI/IEEE 279 is item 4.7.2, "Isolation Devices."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

Note that the design of the diverse I&C systems must be such that the protection system continues to meet the requirements of 10 CFR 50 Appendix A, "General Design Criteria for Nuclear Power Plants," Section III, "Protection and Reactivity Control Systems." Review of the reactor protection system for these areas of conformance is addressed in SRP Sections 7.2 and 7.3.

2. Acceptance criteria applicable to all diverse I&C systems proposed for design certification under 10 CFR 52, in addition to those listed in 1 above

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

3. Acceptance criteria applicable to all diverse I&C systems proposed as part of combined license applications under 10 CFR 52.79(c), in addition to those listed in 1 above

10 CFR 52.79(c), "ITAAC in Combined Operating License Applications."

4. Acceptance criteria applicable to ATWS mitigation functions, in addition to the applicable criteria listed in 1 above

10 CFR 50.62, "Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants."

5. Acceptance criteria applicable to manual control and display functions, in addition to those listed in 1 above

Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." SRM requirements applicable to diverse I&C system manual control and display functions are as follows:

"A set of displays and controls located in the main control room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.

"The displays and controls shall be independent and diverse from the safety computer systems."

6. Acceptance criteria applicable to DAS functions, in addition to those listed in 1 above

Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." SRM requirements applicable to DAS functions are as follows:

"If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure [as the safety system]¹ shall be required to perform either the same function [as the safety system function that is vulnerable to common mode failure] or a different function.

"The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions."

III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any I&C system. Procedures for reviewing each acceptance criterion of 10 CFR 50 and 10 CFR 52 are provided in Appendix 7.1-A. Therefore, review procedures specific to any given diverse I&C system can be synthesized from Appendix 7.1-A. Note that while compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," is required only for protection systems, the criteria of ANSI/IEEE Std 279 and Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems" (which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations") address considerations that may be used as guidance, where appropriate, for reviewing any diverse I&C application.

This part of Section 7.8 provides a review procedure for conformance of diverse I&C systems with the requirements of 10 CFR 50.62 and the SRM regarding SECY-93-087. This part of Section 7.8 highlights specific topics that should be emphasized in the application of the Appendix 7.1-A review procedures to diverse I&C systems.

Major design considerations that should be emphasized in the review of any diverse I&C system are identified below.

- Design basis — Design bases should be described in the SAR for each diverse I&C system. The design basis should, as a minimum, address the following topics:
 - The specific design requirements identified in 10 CFR 50.62.

¹Bracketed phrases added for clarity.

- Identification of conditions which require protective action by the diverse I&C systems. For DAS these events are identified in the applicant/licensee's D-in-D&D analysis. For ATWS mitigation systems these events are limited to anticipated operational occurrences, defined in the Definitions and Explanations section of 10 CFR 50 Appendix A as those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit, and include but are not limited to loss of power to all recirculation pumps, tripping of the turbine generator, isolation of the main condenser, and loss of all offsite power.
 - Identification by the applicant/licensee of the bounding events and their bases in the analyses that are presented or referenced in SAR Chapter 15. The reviewer should confirm with SRXB that the analytical basis for each diverse I&C system is acceptable and consistent with the Chapter 15 analysis, and should confirm with SRXB and Plant Systems Branch (SPLB) that the design of the mechanical systems used for ATWS mitigation is acceptable.
 - Identification of the range of transient and steady-state conditions for both the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform. The environmental qualification basis for the ATWS mitigating equipment should be derived from the analysis of the effects of the anticipated operational occurrences.
 - Identification of the performance requirements. The submittal should identify performance requirements for which credit is taken in the mitigation of design basis events (e.g., dynamic response and accuracy). The review should confirm that the applicant/licensee verifies conformance to these requirements by validation testing and surveillance.
- Quality of components and modules — Generic Letter 85-06 provides acceptable guidance for the quality assurance of diverse I&C systems and components.
 - System testing and surveillance — The applicant/licensee should have identified the test, maintenance, surveillance, and calibration procedures. These provisions should be consistent with the guidance of Generic Letter 85-06. The ATWS mitigation system should be testable at power (up to, but not necessarily including, the final actuation device).
 - Defense-in-depth and diversity analysis — The diverse I&C system designs should be consistent with the assumptions of the applicant/licensee's D-in-D&D analysis, if one has been performed. For example, diverse I&C system equipment should be environmentally qualified for the environments in which the D-in-D&D analysis assumes they will operate.
 - Use of digital systems — See Appendix 7.0-A.
 - Power supply availability — The reviewer should confirm with EELB that power sources will be available during and following a loss of offsite power.
 - Environmental qualification — The diverse I&C system equipment as installed should be qualified for the environment that could exist during the events for which the equipment is assumed to respond.
 - System status — Information should be available in the control room to indicate the operation of the diverse I&C systems. This review may involve the considerations included in emergency operating procedures.

- Potential for inadvertent actuation — The diverse I&C systems design should limit the potential for inadvertent actuation and challenges to safety systems. Diverse I&C systems should be designed to initiate after the primary protection system actuation conditions are exceeded. (The use of a primary protection signal sensor to simultaneously initiate diverse I&C functions is acceptable.)

Additional major design considerations that should be emphasized in the review of ATWS mitigation systems are identified below.

- Independence from the RTS — The ATWS mitigation equipment should be independent and diverse from the RTS from the sensor output to the final actuation device. See Appendix 7.1-B item 8 or Appendix 7.1-C item 24.
- Manual initiation capability — The ATWS mitigation systems should include the capability for initiation from the control room.
- Completion of protective action — The ATWS mitigation logic should be designed such that once ATWS mitigation is initiated the mitigation will go to completion.

If the applicant/licensee has provided a D-in-D&D analysis, the diversity provided in the ATWS mitigation system design should be consistent with the assumptions of that analysis.

Where a D-in-D&D analysis is not provided the following diversity criteria should be met:

- Equipment diversity should be provided to the extent reasonable and practicable to minimize the potential for common-mode failures.
- Equipment diversity is required from the sensors/transmitters to and including the components used to interrupt control rod power or vent the scram air header.
- For interruption of control rod power, obtaining circuit breakers from different manufacturers is not, in and of itself, sufficient to provide the required diversity.
- For mitigating systems other than diverse reactor trip systems (e.g., auxiliary feedwater) diversity is required from the sensors to, but not including, the final actuation device.
- Sensors need not be of a diverse design or manufacturer.
- Existing RTS sensing lines may be used for ATWS mitigation instruments.
- Sensors/transmitters and sensing lines should be selected such that adverse interactions with existing control systems are avoided.
- Logic and actuation device power for the ATWS mitigation system must be from an instrument power supply independent from the power supplies for the existing RTS; existing RTS sensor and instrument channel power supplies may be used provided the possibility of common-mode failure is prevented.

If the ATWS system is explicitly addressed as part of a D-in-D&D analysis, then that analysis provides the basis for the assessing the adequacy of diversity between the ATWS mitigation system and the RTS.

Therefore, separate evaluation of the ATWS mitigation system against the above eight diversity criteria is unnecessary if the D-in-D&D analysis is provided.

Additional major design considerations that should be emphasized in the review of manual controls and displays are identified below.

- The manual controls and displays should meet the criteria outlined in BTP HICB-19.

In each safety review, the Staff should determine the elements of the design that require additional review emphasis. Typical reasons for such a non-uniform emphasis are the introduction of new design features or the utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the Code of Federal Regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the SER:

Evaluation findings applicable to any diverse I&C system:

The NRC staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The Staff concluded that the applicant/licensee adequately identified the guidelines applicable to these systems. Based upon the review of the system design for conformance to the guidelines, the Staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore, the Staff finds that these requirements of General Design Criteria (GDC) 1 and 10 CFR 50.55a(a)1 have been met.

The diverse I&C systems are appropriately isolated from safety systems. Therefore, the Staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and the requirements of GDC 24.

Based on the applicant/licensee's commitment to the quality assurance guidance of Generic Letter 85-06, the Staff finds that the quality assurance requirements of GDC 1 have been met.

Based on the review of diverse I&C system status information, manual initiation capabilities, and provisions to support safe shutdown, the Staff concludes that information is provided to monitor the system over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for manual initiation of diverse I&C functions. The diverse I&C systems appropriately support actions to operate the nuclear power unit safety under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the Staff finds that the design of the diverse I&C systems satisfies the requirements of GDC 13 and 19.

Based on the licensee's commitment to periodically test the diverse I&C systems from end-to-end [summarize the specific commitment], the Staff concludes that an acceptable level of availability for the system can be maintained.

Note: the following finding applies only to systems involving digital computer-based components.

Based on the review of software development plans and the inspections of the computer development process and design outputs, the Staff concludes that the computer systems meet the

guidance of Reg. Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the Staff finds that the diverse I&C systems satisfy these requirements of GDC 1.

Additional evaluation findings applicable to all diverse I&C systems proposed in design certification applications under 10 CFR 52:

The diverse I&C systems design appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the diverse I&C systems satisfy the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the diverse I&C systems examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the diverse I&C systems satisfy the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the diverse I&C systems [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the design of the diverse I&C systems satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

Based upon an initial review of the scope and content of the material submitted by the applicant, and completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the diverse I&C systems design to satisfy the requirements of 10 CFR 52.47(a)(2).

Additional evaluation findings applicable to ATWS mitigation systems:

The ATWS mitigation system instrumentation includes [summarize the basic functions and elements of the I&C system design submitted for review]. Based on the review of these functions and the design bases submitted by the applicant, the Staff concluded that the ATWS mitigation design includes an appropriate set of functions.

Based on review of the interfaces of the ATWS mitigation system and equipment with the RTS, the Staff concludes that the separation and independence of the RTS is not compromised by the ATWS mitigation system design. Where isolation devices are provided in the RTS to support ATWS mitigation interfaces, the isolation devices are applied and qualified to the guidelines of BTP HICB-11.

Based upon the above items, the Staff concludes that the design of the ATWS mitigation system is acceptable and satisfies the specific design requirements identified in 10 CFR 50.62 for [identify reactor type].

Additional evaluation findings applicable to diverse I&C system manual controls and displays:

Based on review of the design bases submitted by the applicant, the Staff concludes that the manual controls and displays are acceptable, independent and diverse from the safety computer system, and sufficient for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. Therefore, the Staff concludes that the manual controls and displays fulfill the requirements of the Staff Requirements Memorandum on SECY 93-087, item II.Q.

Additional evaluation findings applicable to DAS:

Based on review of the design bases submitted by the applicant, the Staff concludes that the DAS is acceptable. The functional requirements, independence requirements, and diversity requirements for this system are consistent with the applicant's defense-in-depth and diversity analysis, and fulfill the applicable requirements of the SRM on SECY-93-087, item II.Q.

Note: the following conclusion is applicable to all applications.

The conclusions noted above for the diverse I&C systems are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted [List applicable system or topics and identify references].

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

Implementation schedules for conformance to the method discussed herein are contained in 10 CFR 50.62, the 10 CFR 50.62 considerations identified in the Federal Register Notice (FR Vol. 49, No. 124), and Generic Letter 85-06.

VI. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

Federal Register 49 FR 26042. "Statement of Considerations for the ATWS Rule," 10 CFR 50.62.

Generic Letter 85-06. "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related," April 16, 1986.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

NEW

Section 7.9. Data Communication Systems

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

This SRP section describes the review process and acceptance criteria for data communication systems (DCSs) that are part of or support the systems described in Sections 7.2 through 7.8 of the applicant's safety analysis report (SAR). The scope and depth of the review and the acceptance criteria will vary according to the importance to safety of the system that the DCS is supporting.

The objectives of the review are to confirm that DCSs (1) conform to applicable acceptance criteria and guidelines, (2) will perform the safety functions assigned to them, (3) will meet the reliability and availability goals assumed for the system, and (4) will tolerate the effects of random transmission failures. A particular concern is that the transmission of multiple signals over a single path may constitute a single point of failure that may have a larger impact on plant safety than would occur in previous analog systems.

DCSs may include multiplexers and more general communication systems. The distinction between multiplexers and more general data communication systems is often blurred. For the purposes of this section, a multiplexer is equipment that transmits (or receives) or connects in turn several different signals over an electrical conductor or optical-fiber medium on a fixed schedule or rotation. Internal computer buses are specifically excluded from the definition of DCSs used in this section. Multiplexers may be analog or digital.

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

More generally, a data communication system transmits one or more signals on one or more electrical or optical media according to some analog or digital encoding. The schedule for transmission of the various signals may not be fixed, and particular signals or data may be transmitted at unpredictable intervals. Communications via media other than electrical conductors or optical fiber are not addressed by Section 7.9.

The review described in this section includes communication between systems and communication between computers within a system. This section addresses both safety and non-safety communication systems.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

II. Acceptance Criteria

Acceptance criteria for DCSs derive from the acceptance criteria for the system(s) supported by the DCS. The acceptance criteria for a specific DCS are the union of those criteria applicable to the systems supported by that DCS. These criteria are summarized below. A given plant design may contain more than one DCS. In this case, the criteria applicable to each DCS may be different. These acceptance criteria are summarized in the following tables:

1. Acceptance criteria applicable to any DCS

10 CFR 50.55a(a)(1), "Quality Standards for Systems Important to Safety."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." The only requirement from ANSI/IEEE 279 that is applicable to all DCS is item 4.7.2, "Isolation Devices."

General Design Criteria 1, "Quality Standards and Records."

General Design Criterion 24, "Separation of Protection and Control Systems."

2. Acceptance criteria applicable to all DCSs proposed for design certification under 10 CFR 52, in addition to those listed in item 1 above

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.42(a)(2), "Level of Detail."

10 CFR 52.47(b)(2)(i), "Innovative Means of Accomplishing Safety Functions."

3. Acceptance criteria applicable to all DCSs proposed as part of combined license applications under 10 CFR 52, in addition to those listed in item 1 above

10 CFR 52.79(c), "ITAAC in Combined Operating License Applications."

4. Acceptance criteria applicable to all DCSs that support protection system functions (reactor trip system (RTS) — Section 7.2 or engineered safety features actuation system (ESFAS) — Section 7.3), in addition to those listed in item 1 above

10 CFR 50.34(f)(2)(v), "Automatic Indication of Bypassed and Inoperable Status of Safety System Equipment."

10 CFR 50.55a(h), "Protection Systems," which requires compliance with ANSI/IEEE Std 279.

General Design Criterion 2, "Design Basis for Protection Against Natural Phenomena."

General Design Criterion 4, "Environmental and Missile Design Basis."

General Design Criterion 21, "Protection System Reliability and Testability."

General Design Criterion 22, "Protection System Independence."

General Design Criterion 23, "Protection System Failure Modes."

General Design Criterion 29, "Protection Against Anticipated Operational Occurrences."

Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs."

5. Acceptance criteria applicable to all DCSs that support these functions: safe shutdown systems (Section 7.4), information systems important to safety (Section 7.5), or interlock systems important to safety (Section 7.6), in addition to those listed in item 1 above

General Design Criterion 2, "Design Basis for Protection Against Natural Phenomena."

General Design Criterion 4, "Environmental and Missile Design Basis."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

Item II.T, "Control Room Annunciator (Alarm) Reliability," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs."

6. Acceptance criteria applicable to all DCSs that support control system functions (Section 7.7), in addition to those listed in item 1 above

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

7. Acceptance criteria applicable to all DCSs that support diverse instrumentation and control (I&C) systems functions (Section 7.8), in addition to those listed in item 1 above

10 CFR 50.62, "Requirements for the Reduction of Risk from Anticipated Transients without Scram."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs."

Section 7.1, Table 7-1, and Appendix 7.1-A list 10 CFR requirements, industry-endorsed standards, regulatory guides, and branch technical positions that provide information, recommendations, and guidance that describe a basis acceptable to the NRC staff. This basis may be used to implement the relevant requirements of NRC's regulations identified above.

III. Review Procedures

The review procedures of Section 7.1 describe the general procedures to be followed in reviewing any I&C system. Procedures for reviewing each acceptance criterion of 10 CFR 50 and 10 CFR 52 are provided in Appendix 7.1-A. Therefore, review procedures specific to any given DCS can be synthesized from Appendix 7.1-A. Note that while compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," is required only for protection systems, the criteria of ANSI/IEEE 279 and Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," address considerations that may be used as guidance, where appropriate, for reviewing any DCS application.

This part of Section 7.9 highlights specific topics that should be emphasized in the DCS review. NUREG/CR-6082, "Data Communications," discusses data communication technology, the technical rationale for review issues specific to data communication, and includes background information to assist the reviewer in identifying critical technical features.

Major design considerations that should be emphasized in the review of all DCS are identified below.

- Quality of components and modules — See Appendix 7.1-B item 4 or Appendix 7.1-C item 8.
- DCS software quality — See BTP HICB-14.
- Performance — The review should verify that the protocol selected for the DCS meets the performance requirements of all supported systems. The real-time performance should be reviewed with BTP

HICB-21. This should include verification that DCS safety system timing is deterministic. Time delays within the DCS and measurement inaccuracies introduced by the DCS should be considered when reviewing the instrumentation setpoints (refer to Draft Reg. Guide DG-1045, the proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems," and BTP HICB-12). Data rates, data bandwidths, and data precision requirements for normal and off-normal operation should be reviewed. The error performance should be specified. Vendor test data and in-situ test results should be reviewed to verify the performance. The interfaces with other DCSs or other parts of the I&C system should be reviewed to verify compatibility.

- Reliability — The potential hazards to the DCS and from the DCS should be reviewed. Unneeded but included DCS functions should be reviewed to ensure that they cannot be inadvertently activated and thereby prevent operation of the safety functions. The effects of error recovery should be reviewed. The reviewer should determine that the operating history of the DCS in similar applications is known and that it has been satisfactory. The reviewer should verify the existence and quality of maintenance and operator documentation and ensure that appropriate training has been or will be performed. The review should verify that any DCS safety system is deterministic. The DCS should be designed to support self-testing and surveillance testing (refer to BTP HICB-17).
- Control of access — The review should confirm that the DCS does not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators. If computers or equipment outside of the control of the plant staff may be connected to the DCS (e.g., connections to remote data displays off-site) the connections should be through gateways that prevent unauthorized transactions originating from off-site. Such connections should be one-way communication paths as discussed in Annex G of IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

Additional major design considerations that should be emphasized in the review of DCS safety systems are identified below.

- Single-failure criterion — See Appendix 7.1-B item 3 or Appendix 7.1-C item 6. The use of DCSs as single paths for multiple signals or data raises particular concerns regarding extensive consequential failures as the result of a single failure. This review should confirm that channel assignments to individual communication subsystems are appropriate to ensure that both redundancy and diversity requirements (refer to BTP HICB-19) within the supported systems are met. NUREG/CR-6082 provides additional discussion of independence and failure modes.
- Independence — See Appendix 7.1-B items 7 and 8 or Appendix 7.1-C items 11 and 24.
- Failure modes — See Appendix 7.1-A item 2.i. RTS and ESFAS functions of the DCS should be reviewed to determine whether the selected protection system design strategy (fail-safe or fail-as-is) is carried through consistently from detection of DCS failures to final actuation devices. With regard to power supply requirements, the RTS functions of the DCS should be designed such that failure of a DCS power supply will result in reactor trip for that redundant protective channel (fail-safe design). The design of ESFAS functions of the DCS should ensure that failure of a DCS power supply will result in failure as-is of the related actuation channel (fail-as-is design) unless it is determined by analysis that a more appropriate strategy for the safety function in question is fail-safe.
- System testing and inoperable surveillance — See Appendix 7.1-B items 10 and 11 or Appendix 7.1-C items 12 and 27. Insofar as bypass or deliberate inoperability of a DCS may induce the same condition

upon the system of which it is a part, the review should confirm that the bypassed and inoperable indications for DCSs are consistent with those of the systems of which they are parts.

- EMI/RFI susceptibility — See Appendix 7.1-B item 5 or Appendix 7.1-C item 9. The review should confirm that data communication media do not present a fault propagation path for environmental effects, such as high-energy electrical faults or lightning, from one redundant portion of a system to another or from another system to a safety system. Fiber optics typically offer resistance to such effects, but have other attributes that prevent universal acceptability. For example, if the fiber-optic medium may be subject to radiation, fiber that does not become opaque or brittle under irradiation should be specified, or there should be a defined replacement schedule. NUREG/CR-6082 compares the qualities of optical and conductive media and provides guidance regarding environmental and performance criteria.
- Defense-in-depth and diversity (D-in-D&D) analysis — If one or more DCSs are parts of systems (RTS, ESFAS, anticipated transient without scram (ATWS), diverse I&C) for which a D-in-D&D analysis is required, the analysis should be performed by the applicant and the vulnerabilities to common-mode failure of all similar DCSs should be evaluated. Based upon the credibility of postulated failures, potential consequences, availability of diverse preventive or mitigatory responses, and the NRC's diversity requirements (see the Staff Requirements Memorandum (SRM) "SECY-93-087 — Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"), the reviewer should determine that the design, including DCSs, has sufficient defense-in-depth and diversity. See BTP HICB-19 for guidance on reviewing D-in-D&D analyses.
- DCSs exposed to seismic hazard — The reviewer should determine whether the subject DCS equipment is located in seismic Category I structures. In certain designs, some connected data communication or multiplexer equipment may be located in non-seismic Category I structures. For these cases, the reviewer must assure that simultaneous seismic destruction or perturbation of the exposed equipment does not simultaneously render redundant DCSs ineffective.

It may be the reviewer's judgment that, for a specific case under review, emphasis should be placed on specific aspects of the design, while other aspects of the design need not receive the same emphasis and in-depth review. Typical reasons for such a non-uniform placement of emphasis are the introduction of new DCS designs, or the utilization in the design of DCSs previously found acceptable in similar circumstances. However, in all cases, the review must be sufficient to conclude conformance to the requirements of the NRC's regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the SER. For any particular system, the evaluation findings should include the union of those findings below that are applicable to the system under review.

Evaluation findings applicable to any DCS:

The Staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The Staff concluded that the applicant/licensee adequately identified the guidelines applicable to these systems. Based upon the review of the system design for conformance to the guidelines, the Staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems.

Therefore, the Staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

Additional evaluation findings applicable to all DCSs proposed in applications under 10 CFR 52:

The DCS design appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the DCS satisfies the requirements of 10 CFR 52.47(a)(1)(iv).

The application for design certification does not seek certification for the following portions of the DCS [insert list]. Based upon review of the completed safety analysis and DCS, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the design of the DCS satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

The review of the DCS examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria met, the plant will operate in accordance with the (design certification OR combined license). Therefore, the Staff finds that the DCS satisfies the requirements of (10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)).

The DCS contains the following elements which differ significantly from evolutionary changes in light water reactor designs of plants which have been licensed in commercial operation before April 18, 1989. [Insert list.] Based upon the review of [analysis OR test programs OR operating experience], the Staff concludes that the performance of these features has been demonstrated; interdependent effects among the safety features are acceptable; sufficient data exist to assess the analytical tools used for safety analysis; and the scope of the design is complete except for site-specific elements. Therefore, the Staff finds that the DCS satisfies the requirements of 10 CFR 52.47(b)(2)(i).

Based upon an initial review of the scope and content of the material submitted by the applicant, and completed review with respect to the technical items above, the Staff finds that the application contains appropriate detail about the DCS design to satisfy the requirements of 10 CFR 52.47(a)(2).

Additional evaluation findings applicable to all DCSs that support protection system functions (RTS — Section 7.2 or ESFAS — Section 7.3):

The review included the identification of those systems and components for the DCS which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based upon the review, the Staff concludes that the applicant/licensee has identified those systems and components consistent with the design bases for those systems. Sections 3.10 and 3.11 of the SER address the qualification programs to demonstrate the capability of these systems and components to survive these events. Therefore, the Staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

Based on the review of system functions, the Staff concludes that the DCS conforms to the design basis requirements of IEEE Std 279 and 10 CFR 50.34(f). Setpoint analyses account for measurement inaccuracies attributable to the DCS in accordance with the guidance of Draft Reg. Guide 1.105. The Staff concludes that the DCS adequately supports RTS and ESFAS functions as necessary to sense accident conditions and anticipated operational occurrences in order to initiate protective actions consistent with the accident analysis presented in Chapter 15 of the SAR and evaluated in the SER. Therefore, the Staff finds that the DCS appropriately supports RTS and ESFAS compliance with the requirements of GDC 20.

The DCS conforms to the guidelines for periodic testing in Reg. Guide 1.22 and Reg. Guide 1.118. The bypassed and inoperable status indication conforms to the guidelines of Reg. Guide 1.47. The DCS conforms to the guidelines on the application for the single-failure criterion in IEEE Std 379 as supplemented by Reg. Guide 1.53. Based on the review, the Staff concludes that the DCS satisfies the requirement of IEEE Std 279 with regard to the system reliability and testability. Therefore, the Staff finds that the DCS satisfies these requirements of GDC 21.

Based on the review of software development plans and the inspections of the computer development process and design outputs, the Staff concludes that the computer systems conform to the guidance of Reg. Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the Staff finds that the DCS satisfies these requirements of GDC 21.

DCS functions were included in the Staff's review of defense-in-depth and diversity analysis for RTS and ESFAS. Based upon this review, the Staff concludes that the protection systems, including the DCS functions, comply with the criteria for defense against common-mode failure in digital I&C systems. Therefore, the Staff finds that adequate diversity and defense against common-mode failure has been provided to satisfy the diversity requirements of GDC 22 and the Staff Requirements Memorandum on SECY-93-087, item II.Q.

The staff has reviewed EMI/RFI susceptibility and seismically exposed portions of the DCS. Based upon this review and the finding that the requirements of GDC 2 are satisfied, the staff concludes that the DCS satisfies the requirement for independence from the effects of natural phenomena. The DCS conforms to the guidelines in Reg. Guide 1.75 for protection system independence. Based on the review of system independence and separation, the Staff concludes that the DCS satisfies the requirement of IEEE Std 279 or IEEE Std 603 with regard to systems independence. Therefore, the Staff finds that the DCS satisfies the requirements of GDC 22.

DCS failure modes were accounted for in the failure modes and effects analysis for the RTS and ESFAS. Based upon the Staff's review of these analyses, the Staff concludes that the protection systems, including the DCS, are designed to fail into a safe mode if a condition such as disconnection of the system, loss of energy, or postulated adverse environment is experienced. Therefore, the Staff finds that the DCS satisfies the requirements of GDC 23.

Based on the review of the interfaces between the DCS and plant operating control systems, the Staff concludes that the system satisfies the requirements of IEEE Std 279 or IEEE Std 603 with regard to control and protection system interactions. Therefore, the Staff finds that the DCS satisfies the requirements of GDC 24.

Based on the review of all the above, the Staff concludes that the DCS satisfies the requirements of GDC 29.

The Staff's conclusions noted above are based upon the requirements of IEEE Std 279 or IEEE Std 603 with respect to the design of the DCS. Therefore, the Staff finds that the DCS satisfies the requirement of 10 CFR 50.55a(h) with regard to IEEE Std 279.

Additional evaluation findings applicable to all DCSs that support the following functions: safe shutdown systems (Section 7.4), information systems important to safety (Section 7.5), or interlock systems important to safety (Section 7.6):

The review included the identification of those systems and components for the DCS which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based upon the review, the Staff concludes that the applicant/licensee has identified those systems and components consistent with the design bases for those systems. Sections 3.10

and 3.11 of the SER address the qualification programs to demonstrate the capability of these systems and components to survive these events. Therefore, the Staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

Based on our review, we conclude that DCSs used in the [safe shutdown system, information systems important to safety, and interlock systems important to safety], taken in context with other provisions of the design, transmit the variables and commands necessary to maintain the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems within prescribed operating ranges during plant shutdown. Therefore, we find that the DCSs employed by the (safe shutdown system, information systems important to safety, or interlock systems important to safety) satisfy the requirements of GDC 13 and the Staff Requirements Memorandum on SECY-93-087 item II.T.

DCSs have been provided to support instruments and controls within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including shutdown following an accident. Equipment at appropriate locations outside the control room is also supported by the DCS design to achieve (1) prompt, hot shutdown of the reactor, and (2) subsequent cold shutdown of the reactor. Therefore, we conclude that the DCSs employed by the (safe shutdown system, information systems important to safety, or interlock systems important to safety) satisfy the requirements of GDC 19.

Additional evaluation findings applicable to all DCSs that support control system functions (Section 7.7):

Based on our review, we conclude that DCSs used in the reactor control system, taken in context with other provisions of the design, transmit the variables and commands necessary to maintain the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems within prescribed operating ranges during plant shutdown. Therefore, we find that the DCSs employed by the reactor control system satisfy the requirements of GDC 13.

DCSs have been provided to support instruments and controls within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including shutdown following an accident. Therefore, we conclude that the DCSs employed by the reactor control system satisfy the requirements of GDC 19.

Additional evaluation findings applicable to all DCSs that support diverse I&C systems functions (Section 7.8):

Based upon our review of DCS performance and diversity between the DCSs that support ATWS mitigation functions and DCSs that support RTS functions, the Staff finds that the DCS meets the requirements of 10 CFR 50.62.

Based on our review, we conclude that DCSs used in the diverse I&C system, taken in context with other provisions of the design, transmit the variables and commands necessary to maintain the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems within prescribed operating ranges during plant shutdown. Therefore, we find that the DCSs employed by the diverse I&C system satisfy the requirements of GDC 13.

DCSs have been provided to support instruments and controls within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including shutdown following an accident. Equipment at appropriate locations outside the control room is also supported by the DCS design to achieve (1) prompt, hot shutdown of the reactor, and

(2) subsequent cold shutdown of the reactor. Therefore, we conclude that the DCSs employed by the diverse I&C system satisfy the requirements of GDC 19.

Note: the following conclusion is applicable to all applications.

The conclusions noted above for the DCS are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted [List applicable system or topics and identify references].

V. Implementation

Except in those cases in which the applicant proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, as they regard the DCS, the method described herein will be used by the Staff in its evaluation of conformance with NRC regulations.

For implementation of a DCS via the design acceptance criteria (DAC) and ITAAC approach to design certification, see Chapter 14 of the SRP.

VI. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

NUREG/CR-6082. "Data Communications." August 1993.

Regulatory Guide 1.22. "Periodic Testing of Protection System Actuation Functions." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.53. "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

Regulatory Guide 1.118. "Periodic Testing of Electric Power and Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1995.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Appendix 7-A

Branch Technical Positions

The HICB branch technical positions (BTPs) represent guidelines intended to supplement the acceptance criteria established in Commission regulations and the guidelines provided in regulatory guides and applicable industry standards. The BTPs are written to resolve technical problems or questions of interpretation that arise in the detailed reviews of plant designs. The Staff must make a judgment in each such case, in order to complete its review of the particular application. Where the same technical problem or question of interpretation arises in several cases, the Staff's judgment on the point at issue is formalized in a BTP. A BTP is primarily an instruction to Staff reviewers that outlines an acceptable approach to the particular issue and ensures a uniform treatment of the issue by Staff reviewers. The approaches taken in the BTPs, like the recommendations of regulatory guides, are not mandatory, but do provide defined, acceptable, and immediate solutions to some of the technical problems and questions of interpretation that arise in the review process. In some instances, regulatory guides may be developed from BTPs after a sufficient experience in their use has accumulated.

All HICB BTPs applicable to the SRP sections in Chapter 7 have been collected in this appendix for convenience.

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

Table 7-A-1. Branch Technical Positions of the Instrumentation and Control Systems Branch

BTP number	Title
1	Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System
2	Guidance on Requirements on Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines
3	Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service
4	Guidance on Design Criteria for Auxiliary Feedwater Systems
5	Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors
6	Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode
7	Not used
8	Guidance on Application of Regulatory Guide 1.22
9	Guidance on Requirements for Reactor Protection System Anticipatory Trips
10	Guidance on Application of Regulatory Guide 1.97
11	Guidance on Application and Qualification of Isolation Devices
12	Guidance on Establishing and Maintaining Instrument Setpoints
13	Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
14	Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
15	Not used
16	Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
17	Guidance on Self-Test and Surveillance Test Provisions
18	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
19	Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems
20	Not used
21	Guidance on Digital Computer Real-Time Performance

Branch Technical Position HICB-1

Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System

A. Background

During normal and emergency conditions, it is necessary to keep low-pressure systems that are connected to the high-pressure reactor coolant system properly isolated in order to avoid either damage by overpressurization or the loss of integrity of the low-pressure system and possible radioactive releases. The residual heat removal system used for cold shutdown conditions when in service becomes an extension of the reactor coolant pressure boundary. General Design Criterion 15 requires that reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences. There have been a number of recommendations for accomplishing this aim. Until a more definitive guide is published, the criteria in Part B, below, provide an adequate and acceptable design solution for this concern.

B. Branch Technical Position

The following measures should be incorporated in designs of the interfaces between low-pressure systems and the high-pressure reactor coolant system:

1. At least two valves in series should be provided to isolate any subsystem whenever the primary system pressure is above the pressure rating of the subsystem.
2. For system interfaces where both valves are motor-operated, the valves should have independent and diverse interlocks to prevent both from opening unless the primary system pressure is below the subsystem design pressure. Also, the valve operators should receive a signal to close automatically whenever the primary system pressure exceeds the subsystem design pressure.
3. For those system interfaces where one check valve and one motor-operated valve are provided, the motor-operated valve should be interlocked to prevent the valve from opening whenever the primary pressure is above the subsystem design pressure, and to close automatically whenever the primary system pressure exceeds the subsystem design pressure.
4. Suitable valve position indication should be provided in the control room for the interface valves.
5. For those interfaces where the subsystem is required for emergency core cooling system operation, the above recommendations need not be implemented. System interfaces of this type should be evaluated on an individual basis.
6. The system should satisfy the requirements of the General Design Criteria and Section 50.55a(h) of 10 CFR Part 50 with regard to the protection system requirements (ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations"). As described in Reg. Guide 1.153, "Criteria

for Power, Instrumentation, and Control Portions of Safety Systems," compliance with IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as modified and supplemented by the regulatory guide, is considered by the NRC staff to satisfy the provisions of ANSI/IEEE Std 279. Appendices 7.1-B and 7.1-C provide procedures for reviewing systems against ANSI/IEEE 279 and Reg. Guide 1.153.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems."
Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Branch Technical Position HICB-2

Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines

A. Background

For many postulated loss-of-coolant accidents, the performance of the emergency core cooling system (ECCS) in pressurized water reactor plants depends upon proper functioning of the safety injection tanks (also referred to as "accumulators" or "flooding tanks" in some applications). In these plants, a motor-operated isolation valve (MOIV) and two check valves are provided in series between each safety injection tank and the reactor coolant (primary) system.

The MOIVs must be considered to be "operating bypasses" because, when closed, they prevent the safety injection tanks from performing the intended protective function. ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," has a requirement for "operating bypasses" which states that the bypasses of a protective function will be removed automatically whenever permissive conditions are not met. IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," contains a similar requirement. This branch technical position provides specific guidance in meeting the intent of ANSI/IEEE Std 279 or IEEE Std 603 for safety injection tank MOIVs.

It should be noted that BTP ICSB-18 (PSB), "Application of the Single-Failure Criterion to Manually Controlled Electrically Operated Valves," also applies to these isolation valves and should be used in conjunction with this position.

B. Branch Technical Position

The following features should be incorporated into the design of MOIV systems for safety injection tanks to meet the intent of ANSI/IEEE Std 279:

1. Automatic opening of the valves when either primary coolant system pressure exceeds a preselected value (to be specified in the technical specifications), or a safety injection signal is present. Both primary coolant system pressure and safety injection signals should be provided to the valve operator.
2. Visual indication in the control room of the open or closed status of the valve.
3. Bypassed and inoperable status indication in accordance to Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System."
4. Utilization of a safety injection signal to remove automatically (override) any bypass feature that may be provided to allow an isolation valve to be closed for short periods of time when the reactor coolant system is at pressure (in accordance with provisions of the technical specifications).

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." |

Branch Technical Position HICB-3

Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service

A. Background

For the past several years and before the development of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," the Staff has required automatic adjustment to more restrictive settings of trips affecting reactor safety by means of circuits satisfying the single-failure criterion. IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" contains a similar requirement. The basis for this requirement is that the function can be accomplished more reliably by automatic circuitry than by a human operator. This design practice, which has also been adopted independently by the national laboratories and by much of industry, served as the basis for paragraph 4.15, "Multiple Set Points," of ANSI/IEEE Std 279.

More recently, all applicants have stated that their protection systems were designed to meet ANSI/IEEE Std 279. Paragraph 4.15 of ANSI/IEEE Std 279 specified that where a mode of reactor operation requires a more restrictive set point, the means for ensuring use of the more restrictive set point shall be positive and must meet the other requirements of ANSI/IEEE Std 279. A number of designs have been proposed and accepted which reliably and simply satisfy this requirement. During the review of some applications, however, certain design deficiencies have been found. The purpose of this position is to provide additional guidance on the application of Section 4.15 of ANSI/IEEE Std 279 and Section 6.8.2 of IEEE Std 603.

B. Branch Technical Position

1. If more restrictive safety trip points are required for operation with a reactor coolant pump out of service, and if operation with a reactor coolant pump out of service is of sufficient likelihood to be a planned mode of operation, the change to the more restrictive trip points should be accomplished automatically.
2. Plants with designs not in accordance with the above should have included in the plant technical specifications a requirement that the reactor be shut down prior to changing the set points manually.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

Branch Technical Position HICB-4

Guidance on Design Criteria for Auxiliary Feedwater Systems

A. Background

The function of the auxiliary feedwater system in pressurized water reactors is to provide an emergency source of feedwater supply to the steam generators. It is required to ensure safe shutdown in the event of a main turbine trip with loss of offsite power. The system is also started on a safety injection signal. Feedwater is pumped to each steam generator through normally open control valves. It was found that in some plant designs the auxiliary feedwater system did not meet the single-failure criterion. 10 CFR 50.54(f)(2)(xii) requires automatic and manual auxiliary feedwater initiation. The purpose of this branch technical position is to provide guidance and to establish uniform requirements for acceptable designs of auxiliary feedwater systems.

B. Branch Technical Position

The auxiliary feedwater system should be capable of satisfying the system functional requirements after a postulated break in the auxiliary feedwater piping inside containment together with a single electrical failure. The basis for the position is that an auxiliary feedwater piping break would result in tripping the unit and, in turn, might cause loss of offsite power. Standard Staff assumptions for analyzing postulated accidents include the assumption of loss of offsite power if the affected unit generator is tripped by the accident. Such a circumstance would leave the plant without adequate means for removal of afterheat even though the reactor coolant pressure boundary was intact — an unacceptable result. Plant heat removal systems must, in any postulated piping break, be capable of removing afterheat to the ultimate heat sink assuming a single electrical (active) failure anywhere in the auxiliary feedwater system or in the onsite power system.

Branch Technical Position HICB-5

Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors

A. Background

Operating experience with pressurized water reactors (PWRs) and subsequent reviews of PWR designs with regard to the requirements of 10 CFR 50 Appendix A, General Design Criteria (GDC) 20 and 25 have shown that single failures can cause inadvertent single-rod withdrawals. The intent of this branch technical position is to provide specific guidance toward an acceptable interpretation and application of GDC 20 and 25.

B. Branch Technical Position

GDC 20 requires that the protection system shall be designed to initiate automatically the operation of appropriate systems, including the reactivity control systems, to ensure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences. GDC 25 requires that these limits shall not be exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection) of control rods. Within the context of GDC 20 the Staff considers operator error to be an anticipated operational occurrence, in addition to the consideration of single malfunction requirements of GDC 25, for which conformance to these requirements is to be evaluated. The applicant should perform analyses of the reactivity control systems¹ and analyze the consequences of operator error to assess the impact of these events on fuel design limits. If the results of these analyses show that specified acceptable fuel design limits may be exceeded for these events, the protection system must be designed to detect and terminate these events prior to exceeding these limits.

With regard to the evaluation of malfunctions within the reactivity control systems, consideration should be given to failures that cause actions as well as prevent actions, such that all possible effects are examined. Further, failures that could lead to single or multiple rod position changes or out-of-sequence rod patterns should be analyzed, as well as failures that could lead to reactivity changes by boron control systems.

¹Reactivity control systems include interlocks within the system that limit the consequences of control system failures.

Branch Technical Position HICB-6

Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

A. Background

Designs are reviewed with regard to the automatic and manual initiation of protective actions, as set forth in paragraph 4.17 of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," or paragraphs 6.2 and 7.2 of IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." For some designs, the Staff concluded that the proposed design of the circuits used to change over to the recirculation mode of operation following a loss-of-coolant accident did not conform to ANSI/IEEE Std 279, and the complexity of the proposed changeover procedure raised questions as to whether the operator could be expected to perform correctly the required actions within the time allotted and based on the information available to him or her.

B. Branch Technical Position

1. A design that provides manual initiation at the system level of the transfer to the recirculation mode, while not ideal, is sufficient and satisfies the intent of ANSI/IEEE Std 279, provided that adequate instrumentation and information display are available to the operator so that he or she can make the correct decision at the correct time. Furthermore, it should be shown that, in case of operator error, sufficient time and information are available so that the operator can correct the error, and that the consequences of such an error are acceptable.
2. Automatic transfer to the recirculation mode is preferable to manual transfer, for the reasons cited above, and should be provided for standard plant designs submitted for review on a generic basis under the Commission's standardization policy.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

Branch Technical Position HICB-7

Not used.

Branch Technical Position HICB-8

Guidance for Application of Regulatory Guide 1.22

A. Background

A recent application listed eight functions that are not tested while the reactor is operating at power. The applicant claimed that the periodic testing complied with Reg. Guide 1.22, "Periodic Testing of Protection System Actuation Functions." Reg. Guide 1.22 does make provisions for actuated equipment that is not tested during reactor operation, but it does not have provisions for excluding any portion of the protection system from the requirements of paragraphs 4.9 and 4.10 of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations."

B. Branch Technical Position

All portions of the protection systems should be designed in accordance with ANSI/IEEE Std 279, as required by 10 CFR Part 50, 50.55a(h). All actuated equipment that is not tested during reactor operation should be identified, and a discussion of how each conforms to the provisions of paragraph D.4 of Reg. Guide 1.22 should be submitted. In addition to compliance with the Reg. Guide, the review of this topic should also confirm that the proposed design and the justification for test intervals are consistent with the surveillance testing proposed as part of the plant technical specifications.

Note that IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," incorporates the guidance of this branch technical position; therefore, reviews conducted against Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," do not need separate consideration of this branch technical position.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems."
Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.22. "Periodic Testing of Protection System Actuation Functions." Office of Nuclear
Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

Branch Technical Position HICB-9

Guidance on Requirements for Reactor Protection System Anticipatory Trips

A. Background

Several reactor designs have incorporated a number of anticipatory or "back-up" trips for which no credit was taken in the accident analyses. These trips, as a rule, were not designed to the requirements of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," and therefore introduced non-safety-grade equipment into the reactor protection system. It was determined by the Staff that this was not an acceptable practice, because of possible degradation of the reactor protection system.

B. Branch Technical Position

All reactor trips incorporated in the reactor protection system should be designed to meet the requirements of ANSI/IEEE Std 279, or Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." This position applies to the entire trip function, from the sensor to the final actuated device. For sensors located in non-seismic areas, the installation (including circuit routing) and design should be such that the effects of credible faults (i.e., grounding, shorting, application of high voltage, or electromagnetic interference) or failures in these areas could not be propagated back to the reactor protection system and degrade the reactor protection system performance or reliability. The sensors should be qualified to operate in a seismic event, i.e., not fail to initiate a trip for conditions which would cause a trip.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems."
Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Branch Technical Position HICB-10

Guidance on Application of Regulatory Guide 1.97

A. Background

This branch technical position (BTP) provides additional guidelines for reviewing an applicant/licensee's post-accident monitoring system. These guidelines are based on reviews of applicant/licensee design submittals that contained approved interpretations and alternatives for the guidance identified in Reg. Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident."

1. Regulatory Basis

10 CFR 50.34(f)(2)(xvii), "Accident Monitoring Instrumentation," requires in part that instrumentation be provided to measure, record, and read out in the control room: containment pressure, containment water level, containment hydrogen concentration, containment radiation intensity (high-level), and noble gas effluents.

10 CFR 50 Appendix A, General Design Criterion (GDC) 13, "Instrumentation and Control," requires in part that instrumentation be provided to monitor variables and systems over their anticipated ranges for accident conditions, as appropriate, to ensure adequate safety.

10 CFR 50 Appendix A, GDC 19, "Control Room," requires in part that a control room be provided from which actions can be taken to maintain the nuclear power unit in a safe condition under accident conditions, including loss-of-coolant accidents. It also requires that equipment, including the necessary instrumentation, be provided at appropriate locations outside the control room; such equipment must have a design capability for prompt, hot shutdown of the reactor.

10 CFR 50, Appendix A, GDC 64, "Monitoring Radioactivity Releases," requires in part that means be provided to monitor (1) the reactor containment atmosphere, (2) spaces containing components for recirculation of loss-of-coolant accident fluid, (3) effluent discharge paths, and (4) the plant environs for radioactivity that may be released from postulated accidents.

2. Relevant Guidance

Reg. Guide 1.97 describes a method acceptable to the NRC staff for complying with the NRC's regulations to provide instrumentation to monitor plant variables and systems during and following an accident in a light-water-cooled nuclear power plant.

Applicant/licensees may base design submittals upon Reg. Guide 1.97, Revision 2 or Revision 3.

3. Purpose

The purpose of this BTP is to provide additional guidance for NRC reviewers to verify that the previously cited regulatory bases are met by an applicant/licensee's submittal. This BTP has one objective:

- Provide supplemental guidance that clarifies the Staff position and identifies alternatives acceptable to the Staff for satisfying the guidelines identified in Reg. Guide 1.97.

B. Branch Technical Position

1. Introduction

Applicant/licensees have provided design submittals to the Staff containing interpretations of guidelines identified in Reg. Guide 1.97. In some cases, applicant/licensees have requested relief from selected guidelines. Where the applicant/licensee provided adequate justification, the Staff has accepted alternatives to implementing specific provisions of Reg. Guide 1.97. The Staff documented the basis for this acceptance in various safety evaluation reports. Staff positions and clarifications applicable to various classes of plant designs emerged from these applicant/licensee-specific safety evaluations. These positions included identification of specific designs acceptable to the Staff for instrumentation to assess plant and environs conditions during and following an accident.

2. Information to be Reviewed

The information to be reviewed for post-accident monitoring systems is in the SRP Section 7.5.

3. Acceptance Criteria

The design and qualification criteria identified in Reg. Guide 1.97 should be supplemented by the considerations outlined below:

Environmental Qualification of Category 1 and 2 Instrumentation

10 CFR 50.49(b)(3) has been interpreted by the Staff to require that all post-accident monitoring equipment that falls within the scope of Category 1 or 2 equipment (as defined in Revision 2 of Reg. Guide 1.97) be environmentally qualified as required by 10 CFR 50.49, or the applicant/licensee should provide an acceptable alternative for complying with 10 CFR 50.49(b)(3).

10 CFR 50.49 provides an acceptable basis for environmental qualification of Category 1 and Category 2 instrumentation as defined in Reg. Guide 1.97 Revision 2 or Revision 3. In addition, the use of Reg. Guide 1.97 Revision 3 in lieu of Revision 2 in itself does not exempt the applicant/licensee from addressing environmental qualification of Category 1 and 2 equipment.

Seismic Qualification of Category 1 Instrumentation

If a reactor licensing basis does not include commitment to Reg. Guide 1.100, "Seismic Qualification of Electric Equipment for Nuclear Power Plants," and credit is taken for original equipment in meeting the guidelines identified in Reg. Guide 1.97, then installation of the original equipment in conformance with the licensing basis for seismic qualification is acceptable, provided the other guidelines identified in Reg. Guide 1.97 and this BTP are satisfied. However, for all reactors, new instrumentation that is installed for the purpose of satisfying Reg. Guide 1.97, or new instrumentation that is installed to replace original equipment for which credit was taken in satisfying Reg. Guide 1.97, should satisfy the seismic qualification guidelines identified in Reg. Guide 1.97.

Independence of Redundant Category 1 Instrumentation

If a reactor licensing basis does not include a commitment to Reg. Guide 1.75, "Physical Independence of Electric Systems," and credit is taken for original equipment in meeting the guidelines identified in Reg. Guide 1.97, then installation of the original equipment in conformance with the licensing basis requirements for separation and independence is acceptable, provided the other guidelines identified in Reg. Guide 1.97 and this BTP are satisfied. However, for all reactors, new instrumentation that is installed for the purpose of satisfying Reg. Guide 1.97, or new instrumentation that is installed to replace original equipment for which credit was taken in satisfying Reg. Guide 1.97, should satisfy the separation and isolation guidelines identified in Reg. Guide 1.97.

Display and Recording

Reg. Guide 1.97 states in part that if direct or immediate trend or transient information is essential for operator information or action, the recording should be continuously available on dedicated recorders. Otherwise, the information may be continuously updated, stored in computer memory, and displayed on demand. For the latter non-essential applications, the use of Category 2 computers or dedicated Category 2 recorders is acceptable for recording Category 1 information, provided the Category 1 instrumentation is isolated from the Category 2 instrumentation using qualified isolation devices.

Range

Deviations from the range values identified by Reg. Guide 1.97 may be acceptable if supported by analyses demonstrating that the indication would remain on scale with appropriate margins for any design basis event or accident for which the instrumentation might be required for operator information. An appropriate margin should include allowance for analytical uncertainties and instrumentation uncertainties. However, Reg. Guide 1.97 identifies that, for a limited number of functionally significant variables (e.g., containment pressure or primary system pressure), instrument ranges should extend beyond those values that the selected variables can attain under limiting conditions.

Alternate Instrumentation

The use of alternate instrumentation to monitor variables different than those identified in Reg. Guide 1.97 is acceptable, provided that:

- a. The alternate instrumentation fulfills the purpose of the variables identified in Reg. Guide 1.97;
- b. The alternate instrumentation conforms to the design and qualification criteria for the variables identified in Reg. Guide 1.97; and
- c. No credit is taken by the applicant/licensee in post-accident procedures, emergency operating procedures, or functional recovery guidelines for indication of the variables identified in Reg. Guide 1.97 for which the alternative instrumentation is proposed.

Guidance for Boiling Water Reactor (BWR) and Pressurized Water Reactor (PWR) Variables

Table 1 ("BWR Variables") and Table 2 ("PWR Variables") of Reg. Guide 1.97, Revision 2, and Table 2 ("BWR Variables") and Table 3 ("PWR Variables") of Reg. Guide 1.97, Revision 3, identify guidelines for the range, the design/qualification category, and the purpose for specific BWR and PWR variables. Acceptable deviations from or clarifications to Reg. Guide 1.97 for selected BWR and PWR variables

identified in those tables are identified on Table 1 and Table 2 (respectively) of this BTP. Presented in Tables 1 and 2 are identification of the Reg. Guide 1.97 variable, the type of deviation from Reg. Guide 1.97 guidelines (e.g., deviation with respect to category, redundancy, range, direct measurement), and a summary of the acceptance guidelines or clarification associated with the deviation.

4. Review Procedures

The review procedure for post-accident monitoring systems is described in part III of SRP Section 7.5.

Table 1. Acceptable Deviations and Clarifications to Reg. Guide 1.97 for BWRs

Variable	Deviation	Acceptance Guidelines/Clarification
Neutron flux	Category, Equipment qualification, Redundancy, Power source, Quality assurance, Range	Except for applications submitted after January 13, 1993 (which should satisfy the guidelines identified in Reg. Guide 1.97), the design criteria identified in NEDO-31558, "Position on NRC Regulatory Guide 1.97, Revision 3, Requirement for Post-Accident Neutron Monitoring System," are an acceptable alternative to Category 1 criteria. Pursuant to these alternate criteria, the applicant/licensee should perform a plant-specific evaluation of the electrical power distribution to the neutron monitoring system (including the recorders) to verify that the instrument power is not lost during design basis events.
Coolant level in reactor vessel	Range, Redundancy	If redundant channels of Category 1 instrumentation cover the fuel zone and the wide range (i.e., all manual and automatic trip functions), then a single channel of Category 3 upset range instrumentation (from the upper end of the wide range to the top of the vessel or centerline of the main steamline) is acceptable for detection of water carryover.
Core temperature	N/A	This variable is not necessary for satisfying the guidelines identified in Reg. Guide 1.97, per NUREG 0737 Supplement 1, "Clarification of TMI Action Plan Requirements-Requirements for Emergency Response Capability."

Table 1. Acceptable Deviations and Clarifications to Reg. Guide 1.97 for BWRs, cont.

Variable	Deviation	Acceptance Guidelines/Clarification
Drywell sump and drywell drain sumps level	Category, Direct measurement	<p>Category 3 instrumentation (e.g., flow instrumentation) is an acceptable alternative to Category 1 instrumentation for this variable if it can be shown that:</p> <ul style="list-style-type: none"> a. For small leaks, the alternate instrumentation will not experience a harsh environment; and b. For larger leaks, the sumps fill promptly and the sump drain lines isolate due to the increase in drywell pressure, negating the need for the measurement; and c. Drywell pressure and temperature indication can be used to detect leakage into the drywell; and d. The instrumentation neither automatically initiates nor alerts the operator to initiate operation of a safety system in a post-accident situation.
Primary containment isolation valve position	Redundancy	Redundant position indication for each active containment isolation valve is not necessary, because the valves are redundant. Likewise, position indication is not necessary for valves within the operator's cognizance that are normally closed and remain closed after an accident, and that are administratively controlled.
Radioactivity concentration or radiation level in circulating primary coolant	N/A	A continuous post-accident monitor is not necessary.
Containment & drywell hydrogen concentration	Range	For plants where credit is taken for Class 1E hydrogen ignitors, the range recommendations may be relaxed if analysis shows that the instrumentation will remain on scale through all design basis events with adequate margin for uncertainties.
Containment & drywell oxygen Concentration (inerted containment)	Range	As an alternative to total conformance to Category 1 criteria, qualified instrumentation up to 5 volume percent (v/o) and redundancy up to 10 v/o is acceptable if it can be shown that the instrumentation will perform adequately during all accident and post-accident conditions.

Table 1. Acceptable Deviations and Clarifications to Reg. Guide 1.97 for BWRs, cont.

Variable	Deviation	Acceptance Guidelines/Clarification
Suppression chamber & drywell spray flows	Direct measurement	The use of RHR flow, suppression chamber temperature and pressure, and drywell temperature and pressure are acceptable alternatives if it can be shown that (1) use of these variables can accurately and reliably measure the effectiveness of the drywell and suppression chamber spray in a timely manner, and (2) that the position of the spray throttling valves can be monitored and the sprays adequately controlled from the control room using the alternate variables.
SLCS flow	Direct measurement	Measurement of SLCS pump discharge pressure and SLCS storage tank level may be acceptable as an alternate indication that the SLCS pump is operating and that SLCS flow is occurring.
Reactor building or secondary containment area radiation	Category	<p>Area radiation monitors located in Mark III containments and in primary containments of other BWRs may be Category 2 as an alternative to Category 1 monitors.</p> <p>Area radiation monitors located in reactor building secondary containments for Mark I and Mark II plants and in other plant areas may be Category 3 in lieu of Category 2.</p>
Radiation exposure rate/variables used to monitor airborne radioactive materials released from plant	Category	If the instrument is located in a mild environment and is not part of a safety system, Category 3 instrumentation is acceptable in place of Category 2 instrumentation.

Table 2. Acceptable Deviations and Clarifications to Reg. Guide 1.97 for PWRs

Variable	Deviation	Acceptance Guidelines/Clarification
Neutron flux	Environmental qualification	A non-environmentally qualified instrument is acceptable if qualified core exit thermocouples and RCS hot and cold leg temperature indications are provided in conjunction with directions in emergency procedures for operator action to ensure that boric acid injection is occurring.
RCS pressure (CE reactors)	Range	A range of 0-3,000 psig is an adequate alternative to 0-4,000 psig if analysis is presented or referenced in the FSAR that shows that pressure will remain on scale for all design basis transients and accidents. However, if ATWS analysis indicates that pressures exceeding FSAR values are possible, an expanded range of the Category 1 instrumentation should be provided.
Containment sump level	Range	Separate narrow-range instrumentation is not required if the wide-range instrumentation satisfies the guidelines of Reg. Guide 1.97 and is of sufficient range and accuracy to monitor the sump operation for all design basis conditions.
Containment isolation valve position	Redundancy	Redundant position indication for each active containment isolation valve is not necessary, because the valves are redundant. Likewise, position indication is not necessary for valves within the operator's cognizance that are normally closed and remain closed after an accident, and that are administratively controlled.
Radioactivity concentration or radiation level in circulating primary coolant	N/A	A continuous post-accident monitor is not necessary.
Containment hydrogen concentration	Range	For plants where credit is taken for Class 1E hydrogen ignitors, the range recommendations may be relaxed if analysis shows the instrumentation will remain on scale through all design basis events with adequate margin for uncertainties.
Accumulator tank level and pressure	Category	The safety function of the accumulator is performed passively by opening the discharge check valve when RCS pressure is lower than the tank pressure. Therefore, Category 3 instrumentation is an acceptable alternative to Category 2 if there are no operator actions that depend on use of this instrumentation for accident mitigation.
Accumulator isolation valve position	Category	Category 3 position indication is acceptable if the accumulator isolation valves are locked open motor operated valves (i.e., power to the motor operators is disabled during normal operation) and cannot change position during an accident.
Pressurizer heater status	Indication	At a minimum, status indication should be provided for pressurizer heaters governed by the technical specification (i.e., those heaters required to be served by emergency power).

Table 2. Acceptable Deviations and Clarifications to Reg. Guide 1.97 for PWRs, cont.

Variable	Deviation	Acceptance Guidelines/Clarification
Quench tank temperature and pressure	Range	Pressure relief of the tank via rupture disk limits the temperature of the tank contents to saturated steam conditions (less than 750°F). Therefore, it is acceptable if the upper-range value includes (with adequate margin) the saturation temperature corresponding to the tank rupture disk relief pressure (e.g., a rupture disk relief pressure of 100 psig corresponds to 328°F saturation temperature). Likewise, an upper-range value less than the design pressure of the tank is acceptable if the upper range value covers (with adequate margin) the rupture disk relief pressure.
Steam generator level (wide-range)	Redundancy	For the wide-range level, two-loop plants should have two channels of instrumentation per loop, but three- and four-loop plants may have one channel of instrumentation per loop
Steam generator pressure	Redundancy	If steam generator pressure is identified as a Type A variable, two-loop plants should have two channels of instrumentation per loop, but three- and four-loop plants may have one channel of instrumentation per loop.
Containment atmosphere temperature	Category, Direct measurement	Category 3 instrumentation is an acceptable alternative to Category 1 if it is shown that this instrumentation is considered to be backup instrumentation, i.e., if containment atmosphere temperature is not used in any post-accident procedures, emergency procedures, or functional recovery guidelines, and Category 1 containment pressure instrumentation is available as primary instrumentation.
Containment sump water temperature	Direct measurement	As an alternative to Category 2 containment sump water temperature instrumentation, either Category 2 residual heat removal heat exchanger inlet or outlet temperature instrumentation is an acceptable alternative for determining containment cooling status. In plants where the containment cooling function is provided by the recirculation spray system, either Category 2 recirculation spray system heat exchanger inlet or outlet temperature instrumentation is an acceptable alternative.
Makeup flow/letdown flow/VCT level	Category, Direct measurement	Category 3 instrumentation is an acceptable alternative to Category 2 instrumentation if the charging and letdown lines are isolated with an accident signal and no credit is taken for indication of these variables in post-accident procedures, emergency procedures, or functional recovery guidelines.
Radiation exposure rate & variables used to monitor airborne radioactive materials released from plant	Category	If the instrument is located in a mild environment and is not part of a safety system, Category 3 instrumentation is an acceptable alternative to Category 2 instrumentation.

C. References

- General Electric Report NEDO-31558-A. "Position on NRC Regulatory Guide 1.97, Revision 3, Requirement for Post-Accident Neutron Monitoring System." March 1993.
- NUREG 0737 Supplement 1. "Clarification of TMI Action Plan Requirements-Requirements for Emergency Response Capability." January 1983.
- Regulatory Guide 1.100. "Seismic Qualification of Electric Equipment for Nuclear Power Plants." Revision 2, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, June 1988
- Regulatory Guide 1.75. "Physical Independence of Electric Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.
- Regulatory Guide 1.97. "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident." Revision 3, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, May 1983.
- Regulatory Guide 1.97. "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident." Revision 2, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, December 1980.
- Safety Evaluation by the Office of Nuclear Reactor Regulation. "Boiling Water Reactors, Regulatory Guide 1.97, Post-Accident Neutron Flux Monitoring Instrumentation." January 13, 1993.
- Safety Evaluation by the Office of Nuclear Reactor Regulation. "Pressurized Water Reactors Accumulator Pressure and Volume Instrumentation-Relaxation of Regulatory Guide 1.97 Environmental Qualification Requirements." January 21, 1992.
- Safety Evaluation by the Office of Nuclear Reactor Regulation. "Pressurized Water Reactors Containment Sump Water Temperature Instrumentation Regulatory Guide 1.97." November 22, 1993.

Branch Technical Position HICB-11

Guidance on Application and Qualification of Isolation Devices

A. Background

This branch technical position (BTP) provides guidelines for reviewing the use of isolation devices in instrumentation and control systems. These acceptance guidelines are based on experience in the review of applicant/licensee submittals for electrical qualification and application of isolation devices in safety systems. The devices that provide isolation between safety and non-safety portions of power distribution systems are addressed in SRP Chapter 8.

1. Regulatory Basis

10 CFR 50.55a(h) requires in part that protection systems satisfy the criteria of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," paragraph 4.7.2, "Isolation Devices." These criteria state that "the transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system....," and that "no credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified in the design bases."

10 CFR 50 Appendix A, General Design Criterion (GDC) 1, "Quality Standards and Records," requires in part that "structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed." GDC 1 also requires that "where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be modified as necessary to assure a quality product in keeping with the required safety function."

10 CFR 50 Appendix B, Criterion III, "Design Control," requires in part that, "where a test program is used to verify the adequacy of a specific feature in lieu of other verifying or checking processes, it shall include suitable qualification testing of a prototype unit under the most adverse design conditions.

2. Relevant Guidance

Reg. Guide 1.75, "Physical Independence of Electrical Systems," endorses IEEE Std 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," which identifies specific electrical isolation criteria for isolation devices used in instrumentation and control circuits. These isolation criteria form part of the basis for this BTP.

Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." Section 5.6.3.2 of IEEE Std 603 provides guidance on the requirements for isolation devices.

The following industry standards should be considered, as appropriate to the technology, application, and configuration of the isolation device being qualified:

ANSI Std C37.90.a/IEEE Std 472, "IEEE Guide for Surge Withstand Capability (SWC) Tests," identifies acceptable guidance for testing the surge withstand capability of static relays used as isolation devices, provided that the electrical environment at the device installation is shown to be adequately bounded by the waveform characteristics. This standard has been redesignated as ANSI Std C37.90.1, "IEEE Standard Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems," and its scope is currently intended for electrical protective relaying applications.

ANSI Std C62.41, "IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits," (Formerly IEEE Std 587) provides acceptable guidance for describing and characterizing the surge environment in low-voltage AC power circuits for low, medium, and high exposure levels.

ANSI Std C62.45, "IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits," provides acceptable guidance for surge testing of equipment connected to low-voltage AC power circuits.

ANSI Std C62.36, "IEEE Standard Test Methods for Surge Protectors Used in Low-Voltage Data, Communications, and Signaling Circuits," provides guidance for test methods for surge protectors used in low-voltage data, communications, and signaling circuits. This guidance is acceptable where credit is taken for surge protection in these types of circuits.

The standards above address electrical surges to the device. EMI/RFI considerations are addressed in SRP Section 7.1.

3. Purpose

The purpose of this BTP is to provide guidance to address the application and qualification of isolation devices through the application of maximum credible fault and surge withstand capability. This BTP has three objectives:

- Confirm that the design of isolation devices conform to the guidance of Reg. Guides 1.75 and 1.153.
- Confirm that the qualification basis for isolation devices is consistent with accepted industry standards and use in the plant.
- Confirm that qualification testing demonstrates that the isolation devices meet the acceptance criteria of ANSI/IEEE Std 279 and the guidance of Reg. Guide 1.153.

B. Branch Technical Position

1. Introduction

This BTP addresses the electrical qualification and application of isolation devices. Other qualification requirements (such as those that pertain to environmental conditions, EMI/RFI, and seismic events) are addressed in Section 7.1.

The following types of isolation devices are examples of devices that have been found to be acceptable, provided that the guidelines of this BTP are satisfied:

- Isolation amplifiers.
- Isolation transformers.
- Fiber optic couplers.
- Fiber optic cable.
- Photo-optical couplers.
- Relays (coil to contact isolation).

Qualification of isolation devices should be based upon a combination of design analysis and qualification testing. The analysis should demonstrate the adequacy of the design, considering the range of possible fault conditions and variability between individual units. The qualification testing should validate the results of the analysis at the extremes of fault conditions.

2. Information to be Reviewed

The information to be reviewed includes the applicant/licensee's description of the (1) device application, (2) device design, (3) test method, and (4) test results.

3. Acceptance Criteria

General acceptance guidelines for application and qualification are provided in ANSI/IEEE Std 279 and Reg. Guides 1.75 and 1.153. Acceptance criteria for the descriptions of the device application, device design, test methods, and test results are as follows:

Description of Device Application

Isolation devices should be classified as part of the safety system and powered in accordance with the guidelines of Reg. Guides 1.75 and 1.153. If non-safety power sources interface to the isolation device, the applicant/licensee should verify that the non-safety power is not required for the device to perform its isolation function.

Maximum credible fault (MCF)¹ requirements should be established by analysis of proximate circuits that are credible sources of the fault, either through inadvertent application through human error or through a fault or failure postulated to occur that involves proximate circuits, cabling, or terminations (for example, a "hot short" from an adjacent conductor). The determination of specific MCF characteristics is plant-specific.

¹IEEE Std 384 defines a maximum credible voltage or current transient as that voltage or current transient that may exist in circuits, as determined by test or analysis, taking into consideration the circuit location, routing, and interconnections combined with failures that the circuits may credibly experience.

The surge waveforms and characteristics should be defined for the worst-case conditions expected at the installation.

The acceptable leakage current into the safety system should be identified for specified MCF.

Description of Device Design

The design of isolation devices should conform to ANSI/IEEE Std 279 and Reg. Guides 1.75 and 1.153 guidelines for: (1) independence of redundant safety divisions, and (2) independence between protection (safety) and control (non-safety) systems.

The isolation device should include design features for which credit is taken (e.g., surge protectors or barriers) and identification of the application limits of the device.

The device should be designed for postulated electrical faults or failures, including open circuits, short circuits, ground, and application of an MCF. The specified MCF should equal or exceed the application requirements. Reg. Guides 1.75 and 1.153 suggest that the MCF include the levels and duration of the fault current on the non-safety side of the device. ANSI Std C84.1, "American National Standard for Electric Power Systems and Equipment — Voltage Ratings (60 Hz)," Table 1, "Standard Nominal System Voltages and Voltage Ranges," provides an acceptable basis for identifying nominal voltages and guidelines for steady-state tolerances.

The device design should accommodate the surge waveforms and characteristics defined for the application. Appropriate industry standards should be used as a basis for establishing the surge exposure level (for example, ANSI Std C62.41).

The physical arrangement of components in the isolation device should be configured to prevent, in the event of failure, the effects of shattered parts or material (for example, solder spatter), fire, and smoke on breaching the isolation barrier.

Description of Test Method

A description of the specific testing performed for each type of isolation device should be provided. This should include elementary or schematic diagrams as necessary to describe the test configuration, and to describe how the MCF and surges will be applied to the devices during the test.

The basis for the set of postulated electrical faults and failures should be included in the test program.

A specific definition of pass/fail acceptance criteria for each type of device should be provided. This should include justification that the pass/fail acceptance criterion is sufficient to demonstrate that the tested device meets the requirements of ANSI/IEEE Std 279 Section 4.7.2.

Reg. Guide 1.75 recommends that:

- The maximum credible voltage or current transient applied to the device output should not degrade below an acceptable level the operation of the circuit connected to the device input.
- Shorts, grounds, or open circuits occurring in the output will not degrade below an acceptable level the circuit connected to the device input.

- Transient voltages that may appear in the output circuit (for example, surges) must also be considered.
- The qualification should consider the levels and duration of the fault current on the non-safety side of the device.

For safety/non-safety isolation, during and following the application of the MCF or surge test, there should be no degradation or distortion of the isolation device input that would have a detrimental effect on the performance of the safety system. For isolation of redundant safety circuits, there should be no degradation or distortion of the redundant channel that would have a detrimental effect on the performance of the safety system.

Applicable industry standards should be used as the basis for performing the qualification testing (for example, ANSI Std C62.45).

Devices might be used either for isolation of safety circuits from non-safety circuits or for isolation of redundant safety divisions. For qualification testing, the detailed device configuration will depend upon the objective of the isolation and the specific type and configuration of the isolation device (e.g., relay, isolation amplifier, optical-electronic device).

The MCF represents the application of the maximum credible AC and DC voltages and currents that are applied to the device in common and transverse modes (as defined by IEEE Std 100, "The New IEEE Standard Dictionary of Electrical and Electronic Terms") as installed. The mode of application should satisfy the following guidelines for test configurations.

For isolation of safety circuits from non-safety circuits:

- MCFs and surges should be applied to the output (non-safety) in the transverse mode and between any output terminal and ground (common mode).
- Surges should be applied to power terminals. The guidance of ANSI Std C62.45 is acceptable for surge testing at the power input.
- The input terminals should be monitored to assure that no unacceptable interactions (degradations or distortions) between the safety and non-safety circuits would occur.

For isolation between redundant safety circuits:

- MCFs should be applied to the input in the transverse mode and between any input terminal and ground (common mode); the output should be monitored to assure that no unacceptable interactions (degradations or distortions) between redundant safety circuits will occur.
- Surges should be applied to power terminals. The guidance of ANSI Std C62.45 is acceptable for surge testing at the power input.
- MCFs should also be applied to the output terminals in the transverse mode and between any output terminal and ground (common mode); the input should be monitored to assure that no unacceptable interactions (degradations or distortions) between redundant safety circuits will occur.

MCFs should be applied to the isolation device for a sufficient duration to allow any measurable effects to occur on the isolation device and to allow monitored values or effects to reach steady-state.

Description of Test Results

Test data and results should verify that the design basis faults, including short circuits, open circuits, grounds, MCF, and surge were applied to the device in all of the applicable connection modes (i.e., applicable input, output, power, and ground connection modes).

Test data and results should verify that the test acceptance criteria are met.

4. Review Procedures

Confirm that the device design conforms to the guidance of Reg. Guides 1.75 and 1.153.

Confirm that the applicant/licensee has established an acceptable test method and that the specified testing addresses the conditions of the intended applications.

Confirm that the applicant/licensee's testing properly applied the MCF and surges to devices under test.

Confirm that the acceptance criteria of ANSI/IEEE Std 279 and Reg. Guides 1.75 and 1.153 were met during the tests.

C. References

ANSI Std C37.90.1-1989 (R 1991). "IEEE Standard Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems."

ANSI Std C37.90a-1974/IEEE Std 472-1974. "IEEE Guide for Surge Withstand Capability (SWC) Tests."

ANSI Std C62.45-1987. "IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits."

ANSI Std C84.1-1989. "American National Standard for Electric Power Systems and Equipment-Voltage Ratings (60 Hz)."

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std C62.36-1991. "IEEE Standard Test Methods for Surge Protectors Used in Low-Voltage Data, Communications, and Signaling Circuits."

ANSI/IEEE Std C62.41-1991. "IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits."

IEEE Std 100-1992. "The New IEEE Standard Dictionary of Electrical and Electronic Terms."

IEEE Std 384-1992. "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems."
Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory
Research, U.S. Nuclear Regulatory Commission, 1978.

Branch Technical Position HICB-12

Guidance on Establishing and Maintaining Instrument Setpoints

A. Background

This branch technical position (BTP) provides guidelines for reviewing the process an applicant/licensee follows to establish and maintain instrument setpoints. These guidelines are based on reviews of applicant/licensee submittals and vendor topical submittals describing setpoint assumptions, terminology, and methodology and experience gained from NRC inspections of operating plants.

1. Regulatory Basis

10 CFR 50.55a(h), "Protection Systems," requires in part that protection systems satisfy the criteria of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." Section 3(6) requires identification of the levels that, when reached, will require protective action.

10 CFR 50 Appendix B, Criterion XI, "Test Control," and XII, "Control of Measuring and Test Equipment," provide requirements for tests and test equipment used in maintaining instrument setpoints.

10 CFR 50 Appendix A, General Design Criterion (GDC) 13, "Instrumentation and Control," requires in part that instrumentation be provided to monitor variables and systems, and that controls be provided to maintain these variables and systems within prescribed operating ranges.

10 CFR 50 Appendix A, GDC 20, "Protection System Functions," requires in part that the protection system be designed to initiate operation of appropriate systems to ensure that specified acceptable fuel design limits are not exceeded.

10 CFR 50.36(c)(1)(ii)(A), "Technical Specifications," requires that, where a limiting safety system setting is specified for a variable on which a safety limit has been placed, the setting be so chosen that automatic protective action will correct the most severe abnormal situation anticipated without exceeding a safety limit. Limiting safety system settings are settings for automatic protective devices related to those variables having significant safety functions. Setpoints found to exceed technical specification limits are considered a malfunction of an automatic safety system. Such an occurrence could challenge the integrity of the reactor core, reactor coolant pressure boundary, containment, and associated systems.

2. Relevant Guidance

Draft Reg. Guide DG-1045, proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems," provides guidance for ensuring that instrument setpoints are initially within and remain within the technical specification limits. The guidance of this Reg. Guide is referenced to ISA-S67.04 Part I, "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants."

ISA-S67.04, Part II, provides additional background information.

Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as an alternative to ANSI/IEEE Std 279. Section 4.4 requires the identification of functional requirements pertinent to establishing instrument setpoints. Section 6.8 requires that setpoints be determined using a documented methodology, such as that described in ISA-S67.04. While IEEE Std 603 references ISA-S67.04-1988 for setpoint methodology, the Staff has not endorsed this version of the standard. The Staff is endorsing ISA-S67.04, Part I, via revision 3 of Reg. Guide 1.105. Draft Reg. Guide DG-1045 contains this proposed revision.

IEEE Std 498 (Withdrawn), "IEEE Standard Supplementary Requirements for the Calibration and Control of Measurement and Test Equipment Used in the Construction and Maintenance of Nuclear Power Generating Stations," and ANSI/NCSL Std Z540, "General Requirements for Calibration Laboratories and Measuring and Test Equipment," provide guidance for the calibration and control of measuring and test equipment used in the maintenance of instrument setpoints.

Generic letter 91-04, "Guidance on Preparation of a Licensee Amendment Request for Changes in Surveillance Intervals to Accommodate a 24-Month Fuel Cycle," provides guidance on issues that should be addressed by the setpoint analysis when calibration intervals are extended from 18 months to 24 months.

The Staff has reviewed setpoint methodologies submitted as either topical reports or as support for amendments to technical specifications, and found that they met the requirements of the above regulations.

3. Definitions

Section 3 and Figure 1 of ISA-S67.04, Part I, provide acceptable definitions (except as noted by Draft Reg. Guide DG-1045) of setpoint terminology and relationships between trip setpoint, allowable value, analytical limit, limiting safety system setting (LSSS) and safety limit.

4. Purpose

The purpose of this BTP is to provide guidance for NRC staff to verify conformance with the previously cited regulatory bases and standards for instrument setpoints. This BTP has three objectives:

- To verify that setpoint calculation methods are adequate to ensure that protective actions are initiated before the associated plant process parameters exceed their analytical limits.
- To verify that setpoint calculation methods are adequate to ensure that control and monitoring setpoints are consistent with their requirements.
- To confirm that calibration intervals and methods established are consistent with safety analysis assumptions.

B. Branch Technical Position

1. Introduction

Instrumentation and control (I&C) safety systems control plant parameters to ensure that safety limits will not be exceeded under the most severe design basis accident or transients. Instrument setpoints and allowable

values for these I&C safety system functions are chosen so that potentially unsafe or damaging process excursions (transients) can be avoided and/or terminated before plant conditions exceed safety limits. Accident analyses establish the limits for critical process parameters. These analytical limits, as established by accident analyses, do not normally include considerations for the accuracy (uncertainty) of installed instrumentation. Additional analyses and procedures are necessary to ensure that the actual trip setpoint of each safety control function is appropriate.

Instrument channel uncertainties in these analyses are based upon the characteristics of installed instrumentation, the environmental conditions present at the instruments' installed locations, and process conditions. A properly established setpoint will initiate a plant protective action before the process parameter exceeds its analytical limit. This, in turn, ensures that the transient will be avoided and/or terminated before the process parameters exceed the established safety limits.

Similar calculations and reviews are performed as necessary to verify the setpoints for non-safety systems or procedural action points for safety and non-safety systems.

2. Information to be Reviewed

The information to be reviewed consists of (1) a description of the setpoint program, procedures, and analytical results, (2) engineering information for the installed instrumentation, (3) supporting analyses, and (4) requirements and operating history for the instrument maintenance and calibration program.

3. Acceptance Criteria

Setpoint Documentation

The following information on the licensee/applicant's setpoint program should be provided for review:

- The facility setpoint list identifying safety and non-safety setpoints.
- A description of the setpoint methodology and procedures used in determining setpoints, including information sources, scope, assumptions, interface reviews, and statistical methods used.
- Terminology used to describe limits, allowances, tolerances, and environmental or other effects used to support setpoint calculations.
- The technical specifications and the basis for limiting safety system settings (LSSS).
- The basis for calibration intervals.
- The basis for assumptions regarding instrument uncertainties and a discussion of the method used to determine uncertainty values.
- A description of the provisions for control of measuring and test equipment used for calibration of the instrument.
- A description of the program and methodology used to monitor and manage instrument uncertainties, including drift.

A documented basis for safety system setpoint should be available for Staff review. Documentation should conform with the guidance of Draft Reg. Guide DG-1045.

The description of the instrument channel required by ISA-S67.04 Part I should include:

- A description of the functional and performance requirements for the initiation and execution of the safety functions initiated at the setpoints.
- Instrument specifications, including range, accuracy, repeatability, hysteresis, dynamic response, environmental qualification, calibration reference, and calibration intervals should be listed for each instrument type.
- Instrument loop diagrams showing all hardware elements of the instrument loop(s).
- Instrument and tubing layout drawings and installation details showing locations and elevations of instruments and tubing relative to a reference datum, as well as the points where the instrument interfaces with the monitored process.
- For digital instrumentation, the configuration database for the instrumentation functions, and identification of digital elements (hardware and software) where error could be introduced in the measurement. (For example, errors that could result from analog-to-digital or digital-to-analog conversion or from numerical methods used in the software (e.g., curve fitting).)

The description of assumptions required by ISA-S67.04 Part I should include the environmental allowances (temperature, pressure, humidity, radiation, vibration, seismic, and electrical) for the instruments.

Analysis Supporting Establishment of Setpoints and Instrumentation Tolerances

The applicant/licensee should document the bases and the calculations of measurement uncertainties. The methods by which setpoints are calculated should conform to the guidance of Draft Reg. Guide DG-1045.

Statistical Guidelines for Instrument Uncertainty

In the review of uncertainties in determining a trip setpoint and its allowable values, the NRC staff typically uses 95/95 tolerance limits as an acceptable criterion. That is, there is a 95% probability that the constructed limits contain 95% of the population of interest for the surveillance interval selected.

Guidelines for Graded Approach

Section 4 of ISA-S67.04 Part I states that the safety significance of various types of setpoints important to safety may differ, and thus one may apply a less rigorous setpoint determination method for certain functional units and limiting conditions of operation. The use of a graded approach allows a less-rigorous setpoint determination method based on the safety significance of the instrument function. However, the grading technique chosen by the applicant/licensee should be consistent with the standard and should consider all known applicable uncertainties regardless of setpoint application. Additionally, the application of the standard, using a "graded" approach, is also appropriate for non-safety system instrumentation maintaining design limits in the technical specifications.

Basis for Instrument Calibration Intervals

The applicant/licensee should evaluate the effects of extended calibration intervals on instrument uncertainties, equipment qualification, and vendor maintenance requirements to ensure that an extended surveillance interval does not result in exceeding the assumptions stated in the safety analysis. Generic Letter 91-04 Enclosure 2, "Guidance for Addressing the Effect of Increased Surveillance Intervals on Instrument Drift and Safety Analysis Assumptions," provides acceptable guidance for justifying extended calibration intervals through the use of data analysis, monitoring and assessment.

4. Review Procedures

The setpoint analysis methodology and assumptions should be reviewed to confirm that an acceptable analysis method is used and that the analysis parameters and assumptions are consistent with the safety analysis, system design basis, technical specifications, plant design, and expected maintenance practices. The following factors should be emphasized in the review:

- The relationships between the safety limit, analytical limit, the allowable value, the setpoint, the as-found limit and the as-left limit.
- The basis for selection of the trip setpoint.
- The uncertainty terms that are addressed.
- The method used to combine uncertainty terms.
- Justification of statistical combination.
- The relationship between instrument and process measurement units.
- Data used to select the trip setpoint, including the source of the data.
- Assumptions used to select the trip setpoint (e.g., ambient temperature limits for equipment calibration and operation, potential for harsh accident environment).
- Instrument installation details and bias values that could affect the setpoint.
- Correction factors used to determine the setpoint, e.g., pressure compensation to account for elevation difference between the trip measurement point and the sensor physical location.
- Instrument test, calibration or vendor data, as-found and as-left; each instrument should be demonstrated to have random drift by empirical and field data. Evaluation results should be reflected appropriately in the uncertainty terms, including the setpoint methodology.

The design, installation, calibration procedures, and calibration activities for specific channels may be inspected to gain further confidence that setpoint calculations are consistent with plant equipment and calibration procedures. NRC Inspection Manual Chapter 93807, "Systems Based Instrumentation and Control Inspection," provides guidance for such inspections.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/NCSL Std Z540-1-1994. "Calibration Laboratories and Measuring and Test Equipment - General Requirements."

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Generic Letter 91-04. "Guidance on Preparation of a Licensee Amendment Request for Changes in Surveillance Intervals to Accommodate a 24-Month Fuel Cycle." April 2, 1991.

IEEE Std 498. "IEEE Standard Supplementary Requirements for the Calibration and Control of Measurement and Test Equipment Used in the Construction and Maintenance of Nuclear Power Generating Stations."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

ISA-S67.04-1994, Parts I and II. "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants."

NRC Inspection Manual, Chapter 93807. "Systems Based Instrumentation and Control Inspection." May 31, 1994.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Branch Technical Position HICB-13

Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

A. Background

The purpose of this branch technical position (BTP) is to identify the information and methods acceptable to the Staff for using cross-calibration techniques for surveying the performance of resistance temperature detectors (RTDs). These guidelines are based on experience in the detailed reviews of applicant/licensee submittals describing the application of in-situ cross-calibration procedures for reactor coolant RTDs, as well as NRC research activities. In addition, the Staff has completed reviews of applicant/licensee submittals and found that they met the requirements of the regulations identified.

Other methods, such as using a diverse parameter to provide a cross-correlation reference, can be used if adequate justification is provided.

1. Regulatory Basis

10 CFR 50.55a(h) requires in part that protection systems satisfy the criteria of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," including the following:

- Section 3(9) regarding the bases for minimum performance requirements, including response times and accuracies.
- Section 4.9, "Capability for Sensor Checks."
- Section 4.10, "Capability for Test and Calibration."

10 CFR 50 Appendix A, General Design Criterion (GDC) 13, "Instrumentation and Control" requires in part that instrumentation be provided to monitor variables and systems, and that controls be provided to maintain these variables and systems within prescribed operating ranges.

10 CFR 50 Appendix A, GDC 20, "Protection System Functions," requires in part that the protection system be designed to initiate operation of appropriate systems to ensure that specified acceptable fuel design limits are not exceeded.

10 CFR 50 Appendix A, GDC 21, "Protection System Reliability and Testability," requires in part that the protection system be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.

10 CFR 50 Appendix A, GDC 24, "Separation of Protection and Control Systems," requires in part that the protection system be separated from the 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 protection system, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system.

10 CFR 50 Appendix A, GDC 29, "Protection against Anticipated Operational Occurrences," requires in part that protection and reactivity control systems be designed to ensure an extremely high probability of accomplishing their safety function in the event of an anticipated operational occurrence.

2. Relevant Guidance

Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," endorses IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" as an alternative to ANSI/IEEE Std. 279. IEEE Std 603 requires in part that the safety system design basis include the following:

- The increment allotted for inaccuracies, calibration uncertainties, and errors.
- The overall response times of the safety system used in establishing the setpoint allowable value.
- The basis to demonstrate that the assumed values used for instrumentation inaccuracy, calibration uncertainties and error, and time response are acceptable and reasonable.

Performance of an RTD is characterized by its accuracy and response time. Accuracy is a measure of how well the RTD indicates a static temperature, and response time indicates how quickly the RTD can sense a temperature change. NUREG/CR-5560, "Aging of Nuclear Plant Resistance Temperature Detectors," asserts that the calibration and response time of RTDs are affected by aging even within design conditions, but that the aging is manageable by periodic tests performed at each refueling interval. EPRI TR-106453-3925, "Temperature Sensor Evaluation," provides additional information on RTD performance.

3. Purpose

The purpose of this BTP is to provide guidance for NRC reviewers to verify that the previously cited regulatory bases and standards are met by an applicant's submittal. This BTP has two objectives:

- Confirm that calibration inaccuracies, uncertainties, and errors associated with a proposed cross-calibration method are consistent with design basis and setpoint analysis assumptions, and
- Confirm that a proposed cross-calibration method is adequate to confirm that RTD response times are consistent with accident analysis assumptions.

B. Branch Technical Position

1. Introduction

To ensure adequate performance of the RTD, its accuracy and response time should be verified at appropriate intervals. For reactor coolant system (RCS) RTD sensors, practical considerations may limit the extent and methods prudent for in-situ calibration and testing. Periodic removal and re-installation of RTDs solely to support verification of calibration or response time could potentially introduce errors due to installation and increasing personnel exposure. In addition, it may not be feasible or prudent to achieve the range of

isothermal conditions in the RCS for in-situ verification of the complete calibration range of the RTDs. Nevertheless, the applicant/licensee should provide assurance that the calibration and response time for each RTD has not significantly changed due to aging or degradation of the sensor and its installation.

One method acceptable to the Staff is to periodically provide an installed reference RTD that has been recently calibrated and response-time tested. The remaining "similar" RTDs may be cross-correlated to the reference RTD to identify any significant degradation in performance. The "similar" RTDs are those which can be shown to be subject to sufficiently similar temperature and flow conditions in the RCS. While this method does not provide for complete calibration verification of each RTD over its range, the Staff has found the method adequate for timely detection of drift or degradation of RTDs, provided that the guidance herein is applied. This guidance addresses the following topics:

- Traceability of the installed reference RTD to laboratory calibration data.
- Acceptable methods for in-situ testing of RTDs.
- Response time testing.
- "As-found" and "as-left" surveillance data.
- Control/protection interaction or common-mode failure during in-situ testing.

2. Information to be Reviewed

The information to be reviewed consists of specifications, drawings, and analyses of the proposed RTD cross-calibration program.

3. Acceptance Criteria

Supporting Analysis

Analyses, and information on the instrument maintenance and calibration program should be provided to support the adequacy of the cross-calibration program. The analysis should, as a minimum, address the following topics.

- Justification that the cross-calibration program is consistent with the characteristics of the RTD sensors, including RTD specifications, range, accuracy, repeatability, dynamic response, installed configuration, environmental qualification, calibration reference, calibration history, and calibration intervals.
- The specific methods or analyses used for signal conditioning or processing (for example, averaging, biasing, failure detection, data quality determination, and error compensation).
- The planned process for cross-calibration and response time determination.
- Justification that the performance requirements and failure criteria assumed in the plant accident/event analyses are satisfied by the cross-calibration process and testing results.
- The technical basis for the acceptance criteria and values of cross-calibration points monitored in-situ throughout the RTD range, to ensure that the data are adequate for detecting degradation or systematic drift.

Traceability of the Installed Reference RTD to Laboratory Calibration Data

Laboratory calibration involves measuring the RTD's resistance at several known temperatures. The data are then used to provide a calibration curve for the device. In addition, the RTD response time can be determined under laboratory conditions using controlled temperature baths and a methodology to calculate the RTD response time over the measuring temperature range.

The installation of a calibrated RTD should include a test procedure to demonstrate the response time applicability of the laboratory test results. Loop current step response (LCSR) testing is an acceptable way to verify that the conditions of the installed RTD are adequately correlated to the laboratory test data.

Response time testing of the installed RTDs using LCSR should use an analytical technique such as the LCSR transformation identified in NUREG-0809, "Review of Resistance Temperature Detector Time Response Characteristics," to correlate the in-situ results with the results of a laboratory-type temperature test.

Acceptable Methods for In-Situ Testing

Verification of RTD calibrations should be accomplished by installing a newly calibrated reference RTD sensor and then cross-correlating with the measurements of the other RTDs subject to the same temperature and flow environment. A critical element in this approach is providing assurance that all sensor elements are subject to sufficiently similar temperature and flow environments. Other methods, such as using a diverse parameter to provide a cross-correlation reference, can be used if adequate justification is provided.

Before installing a reference or new RTD, the sensor should either be calibrated in a laboratory or, if the manufacturer's calibration data are to be used, the applicant/licensee should perform an analysis or test to verify the RTD has retained its calibration. The application temperatures should be within the manufacturer's highest calibration range.

All data should be taken at isothermal plant conditions and all loops (hot legs and cold legs) should be at similar temperatures. If this condition can not be assured then the applicant/licensee should provide for removal of one or more of the RTDs at each representative location and for replacement with a newly calibrated RTD.

The applicant/licensee should provide an analysis which states the limits of acceptable calibration, response times, and in-situ testing of the RTDs. Test procedures, with acceptance criteria, should state the limits of the calibration, particularly the dependency of the data on uniform coolant temperature and flow.

Correction factors or bias values should be established to compensate for non-isothermal conditions. Because plant temperatures cannot be perfectly controlled, fluctuations and drift in the primary coolant temperature might occur during in-situ testing. The test data should be corrected for the fluctuations and drift in the coolant temperature. If during the testing incomplete mixing of the reactor coolant should occur, the test data should be corrected for the temperature differences. Reactor coolant temperatures should be stable and uniform. In the event this is not the case the data should be corrected to account for these effects.

Equipment used in the test should be accurate to within the necessary tolerance and have stable performance. See BTP HICB-12 for guidance on determining plant instrumentation tolerances.

Response Time Testing

Even though response time testing is independent from the cross-calibration test, it should be performed for the existing and the newly installed reference sensors to account for installation effects and to identify degradation.

The resulting test data and analysis should support correlation of each of the existing sensors in the common flow path to its laboratory response time test data, and also to the laboratory response time test data for the reference sensor. Correlation between LCSR test results for the existing sensors and LCSR test results for the reference sensor may be used to establish the correlation with the reference RTD laboratory test data.

As-Found/As-Left Surveillance Data

The applicant/licensee should maintain a database of the "as-left" and "as-found" calibration and response time tests for each sensor.

To monitor systematic drift or degradation, at each refueling cycle a newly calibrated RTD or a new RTD with recent calibration data should be installed at representative location(s) determined by analysis. The cross-correlation to the reference RTD(s) should be monitored using "as found" and "as left" data records.

Test data and analysis should identify and account for differences in isothermal conditions and demonstrate that the drift is random and is within an acceptable band as determined by setpoint analyses, and that systematic drift is not exhibited. If historical data reveals potential drift problems which would exceed the allowable values of temperature drift in testing for any sensor then the applicant/licensee should verify the calibration of the deviating sensor(s) and identify appropriate corrective action. Analysis to project RTD drift should be available for all RTDs within the protection system.

Control/Protection Interaction and Common-Mode Failure During In-Situ Testing

If the applicant/licensee uses test equipment common to redundant channels, qualified isolation should be provided to preclude single-failure effects on redundant channels or unacceptable protection/control interactions.

4. Review Procedures

The protection system design basis should be examined to identify the requirements for RTD accuracy and time response.

The cross-calibration method and calibration and response time data should be examined to identify calibration inaccuracies, uncertainties, and errors, and to confirm that the cross-calibration method is adequate.

The programmatic documentation of the cross-calibration process should be reviewed with respect to the acceptance criteria above. This review should confirm that the calibration process is consistent with all setpoint analysis assumptions and design basis requirements.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

EPRI Topical Report TR-106453-3925. "Temperature Sensor Evaluation.." Electric Power Research Institute, June 1996.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

NUREG-0809. "Review of Resistance Temperature Detector Time Response Characteristics." August 1981.

NUREG/CR-5560. "Aging of Nuclear Plant Resistance Temperature Detectors." June 1990.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Branch Technical Position HICB-14

Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

A. Background

The Staff's acceptance of software for safety system functions is based upon (1) confirmation that acceptable plans were prepared to control software development activities, (2) evidence that the plans were followed in an acceptable software life cycle, and (3) evidence that the process produced acceptable design outputs. This branch technical position (BTP) provides guidelines for evaluating software life-cycle processes for digital computer-based instrumentation and control (I&C) systems. These guidelines are based on reviews of licensee submittals, EPRI's requirements for advanced reactor designs, and the analysis of standards and practices documented in NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems." The structure of this BTP is derived from the review process described in Appendix 7.0-A.

1. Regulatory Basis

10 CFR 50.55a(h) requires in part that protection systems satisfy the criteria of ANSI/IEEE Std 279, "IEEE Standard Criteria for Protection Systems for Nuclear Power Generating Stations." Paragraph 4.3 of ANSI/IEEE Std 279 states in part that quality of components is to be achieved through the specification of requirements known to promote high quality, such as requirements for design, inspection, and test. Similar criteria for the quality of components are identified in IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

10 CFR 50, Appendix A, General Design Criterion (GDC) 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they should be identified and evaluated to determine their applicability, adequacy, and sufficiency, and should be supplemented or modified as necessary to ensure a quality product consistent with the required safety function.

10 CFR 50 Appendix A, GDC 21, "Protection System Reliability and Testability," requires in part that protection systems be designed for high functional reliability commensurate with the safety function to be performed.

10 CFR 50, Appendix B, Criterion III, "Design Control," requires in part that quality standards be specified and that design control measures be provided for verifying or checking the adequacy of design. Criterion V, "Instructions, Procedures, and Drawings," requires in part that activities affecting quality should be prescribed by "documented. . . procedures. . . of a type appropriate to the circumstances. . . ." This BTP outlines such procedures for software. Further, Criterion VI, "Document Control," requires in part that "measures should be established to control the issuance of documents. . . which prescribe all activities affecting quality. . . . These measures should ensure that documents, including changes, are reviewed for adequacy and approved for release by authorized personnel. . . ."

2. Relevant Guidance

Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," provides guidance for complying with requirements for safety systems that use digital computer systems. Other applicable regulatory guides are discussed in the acceptance criteria sections below.

Many standards exist that can be used to develop software for safety systems. The information in this BTP is generally based on the standards and reports referred to in Section C below, supplemented and modified as appropriate for attaining the required safety functions.

This BTP presents specific acceptance criteria for the elements of software reviews; however, important context information is found in the concepts contained in the referenced standards and reports. The reviewer should also understand the specific provisions of applicable regulatory guides.

3. Definitions

Activity group — A collection of software life cycle activities, all of which are related to a specific life-cycle topic. Eight activity groups are recognized in this BTP: planning, requirements, design, implementation, integration, validation, installation, and operations and maintenance (see Figure 7-A-1).

Design output — Documents, such as drawings and specifications, that define technical requirements of structures, systems, and components (ASME Std NQA-1, "Quality Assurance Requirements for Nuclear Facility Applications"). For software, design outputs are the products of the development process that describe the end product that will be installed in the plant. The design outputs of a software development process include software requirements specifications, software design specifications, hardware and software architecture designs, code listings, system build documents, installation configuration tables, operations manuals, maintenance manuals, and training manuals.

Deterministic timing — Timing is deterministic if the time delay between stimulus and response has a guaranteed maximum and minimum.

Documentation — Information recorded about a specific life cycle activity. Forty-one activities are recognized in this BTP (see Figure 7-A-1). Documentation includes software life-cycle design outputs and software life-cycle process documentation. A document may be in written or electronic format, and may contain text, illustrations, tables, computer files, program listings, binary images, and other forms of expression. A document for an activity may be packaged with documents for other activities, or documents for non-software life-cycle activities. A document for an activity may be divided into several individual entities.

The following paragraphs define the software planning characteristics important to safety system software. The definitions given are specific to software. The planning characteristics can be divided into three sets: management, implementation, and resource characteristics.

Planning Characteristics

- **Management** — Those characteristics of planning documents that are primarily significant to the managing of the project activities described in the planning document.

- Purpose — A description of the reasons for the existence of the planning document, and the objectives which are to be satisfied by the planning document.
- Organization — The organizational structure used to achieve the purpose of the planning document, including organizational boundaries and interfaces to other organizations.
- Oversight — A specification of the methods used to oversee the work covered by the planning document.
- Responsibilities — The duties of the organization covered by the planning document, and of the individuals within that organization.
- Risks — The method used to identify, assess and manage risks that may interfere with achieving the purpose of the planning document.
- Security — The methods used to protect the information created by or reviewed by the organization covered by the planning document from inadvertent or malicious alteration.
- Implementation — Those characteristics of planning documents that describe the work necessary to achieve the purpose of the planning documents.
 - Measurement — A set of indicators used to determine the success or failure of the activities and tasks defined in the planning document.
 - Procedures — The work necessary in order to achieve the purpose of the planning document,
 - Record keeping — Identification of the documentation required in order to demonstrate that the purpose of the planning document has been achieved, and the tasks necessary to store, handle, retain and ship that documentation have been accomplished.
 - Schedule — The time order of events necessary to achieve the purpose of the planning document, given either as absolute dates, ranges of dates, or offsets from other dates.
- Resources — The material resources necessary to carry out the work defined in the planning document.
 - Budget — The financial resources necessary to carry out the work.
 - Methods/tools — The methods and techniques by which the work will be carried out, and the tools used to implement those methods.
 - Personnel — The numbers, qualification, and training of personnel required to carry out the work defined in the planning document.
 - Standards — The international, national, industry and company standards and guidelines to be followed in the work defined in the planning document.

The following paragraphs define the software characteristics important to safety system software. The definitions given are specific to software. Software characteristics can be divided into two sets: functional characteristics and software development process characteristics. The first set includes those characteristics that directly relate to the actions that the safety system software must take, while the second includes those characteristics of the software development process that contribute to assurance that the software will perform the required actions. Both sets are important in safety system software. The sets, and the definitions of the characteristics, are listed below.

Functional Characteristics

- Accuracy — The degree of freedom from error of sensor and operator input, the degree of exactness exhibited by an approximation or measurement, and the degree of freedom from error of actuator output.
- Functionality — The operations which must be carried out by the software. Functions generally transform input information into output information in order to affect the reactor operation. Inputs may be obtained from sensors, operators, other equipment, or other software. Outputs may be directed to actuators, operators, other equipment, or other software.
- Reliability — The degree to which a software system or component operates without failure. This definition does not consider the consequences of failure, only the existence of failure.
- Robustness — The ability of a software system or component to function correctly in the presence of invalid inputs or stressful environmental conditions. This includes the ability to function correctly despite some violation of the assumptions in its specification.
- Safety — Those properties and characteristics of the software system that directly affect or interact with system safety considerations. The other characteristics discussed in this BTP are important contributors to the overall safety of the software-controlled safety system, but are primarily concerned with the internal operation of the software. The safety characteristic, however, is primarily concerned with the effect of the software on system hazards and the measures taken to control those hazards.
- Security — The ability to prevent unauthorized, undesired, and unsafe intrusions. Security is a safety concern insofar as such intrusions can affect the safety-related functions of the software.
- Timing — The ability of the software system to achieve its timing objectives within the hardware constraints imposed by the computing system being used.

Software Development Process Characteristics

- Completeness — Those attributes of the planning documents, implementation process documents and design outputs that provide full implementation of the functions required of the software. The functions which the software is required to perform are derived from the general functional requirements of the safety system, and the assignment of functional requirements to the software in the overall system design.

- Consistency — The degree of freedom from contradiction among the different documents and components of a software system. There are two aspects to consistency. Internal consistency denotes the consistency within the different parts of a component for example, a software design is internally consistent if no set of design elements are mutually contradictory. External consistency denotes the consistency between one component and another for example, software requirements and the resulting code are consistent with one another if there are no contradictions between the requirements and the code.
- Correctness — The degree to which a design output is free from faults in its specification, design, and implementation. There is considerable overlap between correctness properties and properties of other characteristics such as accuracy and completeness.
- Style — The form and structure of a planning document, implementation process document or design output. Document style refers to the structure and form of a document. This has connotations of understandability, readability, and modifiability. Programming style refers to the programming language characteristics of the software and programming techniques which are mandated, encouraged, discouraged, or prohibited in a given implementation.
- Traceability — The degree to which each element of one life cycle product can be traced forward to one or more elements of a successor life cycle product, and can be traced backwards to one or more elements of a predecessor life cycle product.
- Unambiguity — The degree to which each element of a product, and of all elements taken together, have only one interpretation.
- Verifiability — The degree to which a software planning document, implementation process document or design output is stated or provided in such a way as to facilitate the establishment of verification criteria and the performance of analyses, reviews, or tests to determine whether those criteria have been met.

4. Purpose

The purpose of this BTP is to provide guidance for NRC staff to verify conformance with the previously cited regulatory bases and standards in the design of digital computer systems. This BTP has three objectives:

- To confirm that plans exist that will provide a high-quality software life cycle process, and that these plans commit to documentation of life cycle activities that permit the NRC staff to evaluate the quality of the design features upon which the safety determination is based.
- To verify that implementation of the software life cycle process meets the criteria expected for high-quality software.
- To assess the adequacy of the design outputs.

B. Branch Technical Position

1. Introduction

Digital I&C safety systems must be designed, fabricated, installed, and tested to quality standards commensurate with the importance of the safety functions to be performed. Implementation of an acceptable software life cycle provides the necessary software quality.

Digital I&C systems may share code, data transmission, data, and process equipment to a greater degree than analog systems. Although this sharing is the basis for many of the advantages of digital systems, it also raises a key concern: a design using shared data or code has the potential to propagate a common-cause or common-mode failure via software errors, thus defeating the redundancy achieved by the hardware architectural structure. Greater sharing of process equipment among functions within a channel increases the consequences of the failure of a single hardware module and reduces the amount of diversity available within a single safety channel.

Because of these concerns, the Staff review of digital I&C systems emphasizes quality, defense-in-depth, and diversity as protection against common-mode failures within and between channels. Software quality is an important element in preventing the propagation of common-mode failures.

Commercial-off-the-shelf software and software embedded in commercial-off-the-shelf components, such as meters, circuit breakers, or alarm modules should be appropriately evaluated to confirm that required characteristics are met. EPRI Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," describes an acceptable method for performing this evaluation. NUREG/CR-6421, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications," provides additional background information. The guidelines of this BTP may be used as appropriate in assessing the software engineering processes used to develop commercial software. See the discussion of the commercial dedication of predeveloped software (PDS) in Appendix 7.0-A.

The development of safety system software should progress according to a formally defined life cycle. Many life cycles have been defined in the technical literature and in national and international standards. These differ in the definitions of life cycle activity groups and in the order in which life cycle activities are performed. An appropriate set of life cycle activities is provided in Reg. Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 1074, "Standard for Developing Life Cycle Processes." The software developer should select and document the software life cycle, and specify the products that will be produced by that life cycle. The software developer may be the applicant/licensee, the vendor, a company working on behalf of either, or a commercial software development company.

All software development life cycles share certain characteristics. The activities that will be performed can be grouped into a number of categories (termed activity groups here); the activity groups are common to all life cycles. Life cycle activities produce process documents and design outputs which can be reviewed and assessed. The documents to be provided for each life cycle activity group are shown in Figure 7-A-1. It is acceptable to package documents differently than shown in the figure. For example, information which is assumed to be provided in two or more documents could be combined by the software developer into a single document, and information which is assumed to be provided in a single document could be provided in two or more documents. Further information on life cycles, activity groups, and document contents can be found in NUREG/CR-6101.

2. Information to be Reviewed

The information to be reviewed is subdivided into three topic areas: software life cycle process planning, listed in Section 2.1; software life cycle process implementation, listed in Section 2.2; and software life cycle process design outputs, listed in Section 2.3.

The applicant/licensee need not develop a separate document for each of the topics identified below; however, project documentation should encompass all of the topics. The information reviewed need not be in separate documents. It is acceptable to package the information with other engineering project information, provided that the required information exists. This is particularly true of software life cycle planning information. For example, the software safety plan may be included in a general project safety plan.

2.1 Software Life Cycle Process Planning

The information to be reviewed is contained in the following documents:

- Software management plan.
- Software development plan.
- Software quality assurance plan.
- Integration plan.
- Installation plan.
- Maintenance plan.
- Training plan.
- Operations plan.
- Software safety plan.
- Software verification and validation plan.
- Software configuration management plan.

2.2 Software Life Cycle Process Implementation

The information to be reviewed is contained in the following:

- Safety analyses.
- Verification and validation analysis and test reports.
- Configuration management reports.

One or more sets of these reports should be available for each of the following activity groups:

- Requirements.
- Design.
- Implementation.
- Integration.
- Validation.
- Installation.
- Operations and maintenance.

2.3 Software Life Cycle Process Design Outputs

The information to be reviewed is contained in the following:

- Software requirements specifications (SRS).
- Hardware and software architecture descriptions (SAD).
- Software design specifications (SDS).
- Code listings.
- Build documents.
- Installation configuration tables.
- Operations manuals.
- Maintenance manuals.
- Training manuals.

System requirements documents should also be examined to provide context for this review.

3. Acceptance Criteria

The acceptance criteria are subdivided into three areas matching the information to be reviewed listed in Section 2: software life cycle process planning criteria, enumerated in Section 3.1; software life cycle process implementation criteria, enumerated in Section 3.2; and software life cycle process design output criteria, listed in Section 3.3. The topic areas and documentation groups arise naturally from a disciplined engineering process that has three major stages: planning, design process implementation, and design output.

3.1 Acceptance Criteria for Software Life Cycle Process Planning

This section addresses acceptance criteria for planning activities. The acceptance criteria address specific software development planning activities and products. These products, when found to be acceptable, provide the reviewer with additional criteria for reviewing the processes and products of subsequent life cycle activities, as discussed in Sections 3.2 and 3.3 below.

Acceptance criteria are divided into three sets: management characteristics, implementation characteristics, and resource characteristics. Each of these is further divided into specific characteristics, as shown in the following table. Not all specific characteristics occur for every plan.

Management Characteristics	Implementation Characteristics	Resource Characteristics
Purpose	Measurement	Budget
Organization	Procedures	Methods/tools
Oversight	Record keeping	Personnel
Responsibilities	Schedule	Standards
Risks		
Security		

Software development process characteristics are defined in Section A.3 above. All planning documents should be evaluated for the following process characteristics: consistency, style, traceability, unambiguity and verifiability. Each plan should be internally consistent, and the complete set of plans should be mutually consistent. Plans should be documented so that they can be understood both by the users of the plan and by the reviewers. The software management plan should be traceable back to system management planning; the remaining software plans should be traceable back to the software management plan; and the various process implementation documents and the design outputs should be traceable back to the relevant plans. The set of plans should not be ambiguous. It should be possible to verify that the plans have been followed during the software project. The review and assessment of the quality of the plans provide a means of judging the competency of the development organization and management.

It may be the case, particularly when the applicant/licensee is planning for future plants, that the software plans are created in stages as information becomes available. For example, budget and schedule information may not be available when the initial plans are created. This is acceptable, provided that the information is added to the plans prior to the time the information is needed to carry out the plans.

a. Software Management Plan

The software management plan describes the management aspects of the software development project. It may be part of a general company software management plan, a project engineering management plan, or may be split among various management plans and company procedures. The software management plan should exhibit the management, implementation and resource characteristics listed below.

Management Characteristics

The management characteristics that the software management plan should exhibit include purpose, organization, oversight, responsibilities, and security.

Purpose requires that the intent of the software project be defined in the software management plan. The plan should list the general functions the software will be expected to provide, and should provide an overview of the system within which the software will reside. A general overview of the project should be provided. The assumptions upon which the project is based should be stated. The scope of work for the software project, and the product and process goals, should be discussed.

Organization requires a description of the software project planning organization. The plan should describe the software project organizational structure, and should describe the interfaces and boundaries between the project organization and other company organizations. Management reporting channels should be described. The methods by which subcontractors and suppliers will be managed should be described.

The plan should ensure that the quality assurance organization, the software safety organization and the software verification and validation (V&V) organization maintain independence from the development organization. In particular, the plan should ensure that these assurance organizations not report to the development organization, and not be subject to the financial control of the development organization.

Oversight requires that the strategy for managing the software project be specified. Project priorities should be listed. A method should be described to monitor progress against the software management plan and to document progress at regular intervals in progress reports. A method should exist to identify any deviations from the software management plan in time to take corrective action.

Responsibilities requires a definition of the duties of each member of the project's management and technical teams. The plan should include a policy statement that the development personnel who produce each design output required by the software development plan have the primary responsibility for the quality of that output.

Security requires a description of the methods to be used to prevent contamination of the developed software by viruses, Trojan horses or other nefarious intrusions. The required security level for each project phase should be given.

Implementation Characteristics

The implementation characteristics that the software management plan should exhibit include measurement and procedures.

Measurement requires the definition of a set of management indicators which will be used to monitor and control the project. The plan should require that data associated with project management be systematically collected and analyzed to determine the effectiveness of project management.

Procedures requires a description of the process by which the project will be managed. The plan should describe project priorities, project assumptions, and monitoring and control methods. It should describe the approach to be followed for recording the rationale for key decisions made in specifying, designing, implementing, procuring and assessing the software. A list of all deliverable software, test software, support software and associated documentation should be included. Project management reviews should

be specified. The means for performing corrective action and process improvement should be described. Management reports should be described, and reporting channels should be described. Periodic progress reports should be required.

The software management plan should define the means by which the remaining plans will be produced. It should provide a means of managing externally and internally generated changes in any of the plans. The people responsible for reviewing the various project plans and any changes to those plans should be listed, by name or by title. A means should exist for generating changes to the plans and for evaluating suggested changes. The plans should be under configuration management control.

Resource Characteristics

The resource characteristics that the software management plan should exhibit include budget, methods/tools and personnel.

Budget requires a project budget for all project activities. A means should exist to track and report resource expenditures. Sufficient resources should exist to carry out the defined tasks. The plan should ensure that quality assurance budgets, safety budgets, and V&V budgets not be subject to expropriation by the software development organization, in order to maintain financial independence of these assurance activities.

Methods/tools requires a description of the means used to manage the project. The plan should identify the methods, techniques and tools required to carry out the project management, including office equipment, computer hardware, and computer software.

Personnel requires a specification of the numbers, qualifications, training and types of personnel required to conduct the project. Personnel resources for each project phase should be listed.

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.

b. Software Development Plan

The software development plan describes the plan for technical project development. It may be part of a general company software management plan, may be project specific, or may be split among various management plans. The software development plan should exhibit the management, implementation and resource characteristics listed below.

Management Characteristics

The management characteristics that the software development plan should exhibit include purpose, organization, oversight, and risks.

Purpose requires a description of the objectives of each life cycle phase and its context within the overall project.

Organization describes the software life cycle that will be used in the project. The life cycle should include uniquely identifiable development, verification and support processes with well-defined inputs

and outputs. The life cycle model should be documented in the plan. Reg. Guide 1.173, "Development Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1074, "IEEE Standard for Developing Life Cycle Processes," describes acceptable methods of organizing the software life cycle.

Oversight requires that the strategy for managing the technical development effort be specified. Project priorities should be listed. Required software quality factors should be identified and ordered by importance. A method should be provided to monitor progress against the software development plan and to document progress at regular intervals in progress reports. A method should exist to identify any deviations from the software development plan in time to take corrective action.

Risks requires that project risks be identified, assessed and managed. The plan should describe the method to be used for risk identification, assessment and management, with particular attention to risks that have the potential for compromising safety. The plan should describe the method to be used to identify and assess the risk factors associated with product engineering, development environment and program constraints. It should describe the mechanisms for tracking the risk factors and implementing contingency plans. Risk factors that should be included include system risks, mechanical/electrical hardware integration, risks due to size and complexity of the product, the use of predeveloped software, cost and schedule, technological risk, and risks from program interfaces (maintenance, user, associate contractors, subcontractors, etc.). The plan should identify key design and implementation issues, and the preliminary studies, simulation modeling, and prototyping required to resolve them.

Implementation Characteristics

The implementation characteristics that the software development plan should exhibit include measurement, procedures, and schedule.

Measurement requires a set of indicators used to determine the success or failure of the technical aspects of the development process and the resulting design outputs. The plan should require data associated with the technical development of the design outputs to be collected and analyzed to determine software quality. The error rate found during the development phases should be measured, recorded, analyzed and reported.

Procedures requires the division of each life cycle activity into well-defined tasks. The inputs to each activity and each task should be provided, and the sources of those inputs should be identified. The conditions that must be satisfied before each activity can begin should be described. The outputs from each activity and each task should be provided, and the destination of those outputs should be identified. The plan should include a review at the end of each life cycle activity. Reports on the technical development work should be described. Reg. Guide 1.173 describes acceptable methods for defining the inputs and outputs of the life cycle activities.

Schedule requires a project schedule. The plan should identify key work packages, milestones and hold points. Sufficient intermediate milestones should be identified to avoid unexpected schedule delays. Reviews and audits should be included in the schedule as project milestones. The schedule should justify the time anticipated to complete each task. A single schedule that includes both management and technical activities is acceptable.

Resource Characteristics

The resource characteristics that the software development plan should exhibit include methods/tools and standards.

Methods/tools requires a description of the software development methods, techniques and tools to be used. The approach to be followed for reusing software should be described. The plan should identify suitable facilities, tools and aids to facilitate the production, management and publication of appropriate and consistent documentation and for the development of the software. It should describe the software development environment, including software design aids, compilers, loaders, and subroutine libraries. The plan should require that tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be developed using the tools. Methods, techniques and tools that produce results that cannot be verified to an acceptable degree or that are not compatible with safety requirements should be prohibited, unless analysis shows that the alternative would be less safe.

Standards requires a list the international, national, industry, and company standards and guidelines (including Reg. Guides) to be followed in the project. This should include software requirements standards, software design standards and software coding standards and internal standards and engineering and physical standards that form the basis for the plant safety analysis. The Reg. Guides listed in Table 7-1 should be considered for inclusion in the list of standards.

c. *Software Quality Assurance Plan*

The software quality assurance (QA) plan should exhibit the management, implementation and resource characteristics listed below. It is acceptable to include the software QA plan in a more general project QA plan if the required content exists. The software QA plan should conform with the requirements of 10 CFR 50, Appendix B, and the applicant/licensee's overall quality assurance program.

Management Characteristics

The management characteristics that the software quality assurance plan should exhibit include purpose, organization, and responsibilities.

Purpose requires a general description of the quality assurance process, and the goals of that process. The plan should list the general functions the software QA organization will be expected to perform and specific objectives for this project, if applicable.

Organization requires a description of the software QA organization. The plan should describe the boundaries between the software QA organization and other company organizations. Reporting channels should be described.

Responsibilities requires a definition of the responsibilities and authority of the software QA organization. The plan should require the software QA organization to assess and evaluate system safety, reliability and maintainability characteristics of the software.

Implementation Characteristics

The implementation characteristics that the software quality assurance plan should exhibit include measurement, procedures, and record keeping.

Measurement requires a set of indicators used to determine the success or failure of the software QA effort. The plan should require quality assurance data to be systematically collected and analyzed to determine software quality.

Procedures requires a description of the software QA procedures for the entire software life cycle. The plan should provide for QA participation in the assessment and review of project-specific standards, methods and tools. The plan should describe the methods, procedures and controls used to ensure that technical, quality and other requirements are accurately stated in project documentation. Procedures should exist to identify, track and resolve project conditions adverse to quality. The plan should ensure that traceability is maintained through all phases of the software life cycle. Required software quality factors (listed in Section B.3.3 below) should be identified. Software QA reports should be described.

The software QA organization should participate in formal reviews and audits of the software development activity. Required reviews and audits should be listed in the plan, including review documentation requirements, evaluation criteria, anomaly reporting and anomaly resolution procedures. Reg. Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 1028, "IEEE Standard for Software Reviews and Audits," describes acceptable methods for QA software reviews and audits.

Record keeping requires a description of the software QA record keeping requirements and procedures. A list of the documents subject to software quality assurance oversight should be included. The plan should describe storage, handling, retention and shipping procedures for these documents and for project quality records. Document structures (such as an annotated table of contents) should be provided. The document control mechanism should be specified.

Resource Characteristics

The resource characteristics that the software quality assurance plan should exhibit include methods/tools and standards.

Methods/tools requires a description of the means that will be used to accomplish the quality assurance function. The plan should identify suitable facilities, equipment, methods, techniques and tools to facilitate the performance of the QA work. Computer equipment and software used to perform the QA work should be specified.

Standards requires a method to ensure that approved standards, methods and tools are applied throughout the software life cycle. The plan should provide a method to establish and maintain the standards and methods for software QA, software V&V and software configuration management (CM).

d. Software Integration Plan

The software integration plan should exhibit the management, implementation, and resource characteristics listed below.

Management Characteristics

The management characteristics that the software integration plan should exhibit include purpose, organization and responsibilities.

Purpose requires a general description of the software integration process, the hardware/software integration process and the goals of those processes. The plan should include a general description of the software integration process and of the hardware/software integration process.

Organization requires a description of the software integration organization. The plan should describe the boundaries between the software integration organization and other company organizations. Reporting channels should be described. It is acceptable for the integration organization to report to the development organization, or to be part of the development organization.

Responsibilities requires a definition of the responsibilities and authority of the software integration organization.

Implementation Characteristics

The implementation characteristics that the software integration plan should exhibit include measurement and procedures.

Measurement requires a set of indicators used to determine the success or failure of the integration effort. The plan should require that data associated with the integration of the software, and of the hardware/software combination, be collected and analyzed to determine the adequacy of the integration effort. The error rate found during integration activities should be measured, recorded, analyzed and reported.

Procedures requires an integration strategy. The plan should include methods, procedures and controls for software integration, and for combined hardware/software integration. Integration design outputs and reports should be described. The plan should require documentation describing the software integration tests to be performed, the hardware/software integration tests to be performed, and the expected results of those tests.

Resource Characteristics

The resource characteristics that the software integration plan should exhibit include methods/tools.

Methods/tools requires 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 level of detail appropriate to the safety significance of the software which is to be created using the tools.

e. Software Installation Plan

The software installation plan should exhibit the management, implementation, and resource characteristics listed below.

Management Characteristics

The management characteristics that the software installation plan should exhibit include purpose, organization and responsibilities.

Purpose requires a general description of the installation process, and the goals of that process. A general description of the environment (such as temperature, humidity, vibration, and rack space) within which the computer system and software system is qualified to operate should be included in the plan.

Organization requires a description of the software installation organization. The plan should describe the boundaries between the software installation organization and the broader safety system installation organization. Reporting channels should be described. It is acceptable for the installation to be performed by the development organization or by the customer.

Responsibilities requires a definition of the responsibilities and authority of the software installation organization. If installation is performed by the customer, then the delineation of responsibility between the development organization and the customer should be defined in such a way that misunderstandings in communications between the two organizations are kept to a minimum.

Implementation Characteristics

The implementation characteristics that the software installation plan should exhibit include measurement and procedures.

Measurement requires a set of indicators used to determine the success or failure of the installation effort. The plan should require that data associated with the installation be collected and analyzed. The error rate found during installation activities should be measured, recorded, analyzed and reported.

Procedures requires a description of the installation strategy. The plan should describe procedures for software installation, and for combined hardware/software installation. The plan should describe the methods, procedures and controls used to ensure that the success or failure of the installation effort can be reliably determined. Checks should be required to ensure that the computer system is functional, that the sensors and actuators are functional, that all cards are present and installed in the correct slots, and that the communication system is correctly installed. A check should be required to ensure that the correct software versions are installed on the correct computers. Installation reports should be described. The plan should require that anomalies discovered during installation be reported to the developer and resolved prior to placing the software into operation. Either this plan, or the software V&V plan, should require adequate testing to provide confidence that the installed system will perform its safety function.

Plans for installation of software on installed systems in operating plants should recognize the need to declare all affected functions inoperable according to the plant's technical specifications before proceeding with installation, and to conduct appropriate return-to-service testing before declaring the modified function operable.

Resource Characteristics

The resource characteristics that the software installation plan should exhibit include methods/tools.

Methods/tools requires a description of the methods, techniques and tools that will be used to accomplish the installation function. The plan should require that installation tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be installed using the tools.

f. Software Maintenance Plan

The software maintenance plan should exhibit the management, implementation and resource characteristics listed below.

Management Characteristics

The management characteristics that the software maintenance plan should exhibit include purpose, organization, responsibilities, risks, and security.

Purpose requires a general description of the software maintenance process and the goals of that process. The plan should list the general functions that the software maintenance organization will be expected to perform, and provide general information on obtaining field trouble reports. Maintenance should be limited to the process of modifying a software design output to repair nonconforming items or to implement pre-planned actions necessary to maintain performance. Modifications to improve performance or other attributes, or to adapt the design outputs to a modified environment should be considered design changes.

Organization requires a description of the software maintenance organization. The plan should describe the boundaries between the software maintenance organization and other company organizations. Reporting channels should be described. Formal communication channels between the maintenance organization and the customers using the software should be provided, so that incorrect behavior of the software during operation can be identified, isolated and corrected. This communication structure should provide assurance that software failures during operation will not be ignored.

Responsibilities requires a definition of the responsibilities and authority of the software maintenance organization.

Risks requires a description of the method used for software risk management during maintenance, with particular attention to risks that have the potential for compromising safety.

Security requires a description of the methods to be used to prevent contamination of the corrected software by viruses, Trojan horses or other nefarious additions. The required security level for each maintenance project phase should be provided.

The plan should identify the controls needed over maintenance activities and maintenance and test equipment to prevent unauthorized changes to hardware, software and system parameters. At a minimum, the potential for introducing unauthorized changes during repair, testing and calibration should be addressed.

Implementation Characteristics

The implementation characteristics that the software maintenance plan should exhibit include measurement and procedures.

Measurement requires a set of indicators used to determine the success or failure of the maintenance effort. The plan should require that data associated with maintenance activities be collected and analyzed

to determine the effectiveness of the maintenance effort. The error rate found during maintenance activities should be measured, recorded, analyzed and reported.

Procedures requires a description of the maintenance strategy. The plan should include procedures for problem reporting by customers, and for resolution of those problem reports. The problem reporting procedure should give time and date of occurrence, a brief description of the problem (including the state of the system at the beginning of the occurrence) and a description as to what was done to correct the problem. It should require that reported problems be evaluated to allow the identification of nonconforming items and the performance of corrective actions as described in Sections XV and XVI of 10 CFR 50 Appendix B. The plan should describe the process for identification, documentation, evaluation, segregation where practical, and disposition of nonconforming items, and for notification to affected organizations. Evaluation of nonconforming items and corrective actions should include as appropriate evaluation with respect to the requirements of 10 CFR 50.59 and reporting per the requirements of 10 CFR 21. Nonconformances to design requirements dispositioned "use-as-is" or "repair" should be subject to design control (including verification and validation, quality assurance, safety analysis, and configuration management) measures commensurate with those applied to the original design. The plan should require that as-built records reflect any accepted deviations and justification for that acceptance.

Because any error in safety system software presents the potential for common-mode failure of redundant functions, the maintenance plan should require timely evaluation of the effects of reported problems to support equipment operability determinations as required by plant technical specifications.

Periodic analysis and reporting of problems and their resolution should be required along with recommendations for improving operation. There should be a requirement for reporting what actions were taken regarding these recommendations.

Resource Characteristics

The resource characteristics that the software maintenance plan should exhibit include methods/tools.

Methods/tools requires a description of the methods, techniques and tools that will be used to accomplish the maintenance function. The plan should describe the facilities required to maintain the delivered software. It should list and describe the software, hardware and associated documentation required to maintain the delivered software. The plan should require that maintenance tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be created using the tools.

g. Software Training Plan

The software training plan should exhibit the management, implementation, and resource characteristics listed below.

Management Characteristics

The management characteristics that the software training plan should exhibit include purpose, organization, and responsibilities.

Purpose requires a description of the means necessary to ensure that training needs of appropriate plant staff, including operators and I&C engineers and technicians, are fully achieved. The plan should include a general description of the training facilities.

Organization requires a description of the software training organization. The interfaces between the training organization and the project management organization should be described. Reporting channels should be described. Trainers should have the necessary knowledge of the software operation to ensure that trainees understand its operating and maintenance requirements.

Responsibilities requires a definition of the responsibilities and authority of the training organization and training by customers.

Implementation Characteristics

The implementation characteristics that the software training plan should exhibit include measurement and procedures.

Measurement requires a set of indicators used to determine the success or failure of the training effort. The plan should require that training data be collected and analyzed to determine the effectiveness of the training effort. The trainee error rate found at the end of training activities should be measured, recorded, analyzed and reported.

Procedures requires a description of the training procedures. The plan should list any documentation required to support the training effort. The training program should be described. The plan should require that training be specific to different job functions. Training products and reports should be described. Reporting requirements should be specified.

Resource Characteristics

The resource characteristics that the software training plan should exhibit include methods/tools.

Methods/tools requires a description of the methods, techniques and tools that will be used to accomplish the training function. Training should be carried out on a training system which is equivalent to the actual hardware/software system.

h. Software Operations Plan

The software operations plan should exhibit the management, implementation and resource characteristics listed below.

Management Characteristics

The management characteristics that the software operations plan should exhibit include purpose, organization, responsibilities and security.

Purpose requires a general description of the operation of the software. The plan should include a general description of the functions that the software is to perform, and a general discussion of the means of carrying out those functions.

Organization requires a description of the organizational structure necessary to control the software operation. The plan should specify operator interface stations and actions required to support operation.

Responsibilities requires a description of the responsibilities and authority of the operators.

Security requires a description of the security requirements for operating the software system. The operations plan should identify the controls needed over operation activities to prevent unauthorized changes to hardware, software and system parameters, the monitoring activities needed to detect penetration or attempted penetration of the system, and contingency plans needed to ensure appropriate response to penetration.

Implementation Characteristics

The implementation characteristics that the software operations plan should exhibit include measurement and procedures.

Measurement requires a set of indicators used to determine the success or failure of the operating procedures. The error rate found during operation activities should be measured, recorded, analyzed and reported.

Procedures requires a description of the procedures necessary to start, operate and stop the software system. The plan should require a description of procedures for executing the software in all operating modes, and procedures for ensuring that the software state is consistent with the plant operating mode at all times. The plan should require a description of backup procedures for data and code, and the intervals at which backup should occur. The plan should require a list of error messages, giving a description of the error indication, the probable interpretation of the error indication, and steps to be taken to resolve the situation.

Resource Characteristics

The resource characteristics that the software operations plan should exhibit include methods/tools.

Methods/tools requires a description of the methods, techniques and tools that will be used to operate the software system. The plan should describe the facilities required to operate the delivered software. It should list and describe the software, hardware and associated documentation required to operate the delivered software.

i. Software Safety Plan

The software safety plan should exhibit the management, implementation and resource characteristics listed below. It is acceptable to include the software safety plan in a more general project safety plan if the required content exists. The software safety plan should conform with the requirements of the design basis for the software applications involved.

Management Characteristics

The management characteristics that the software safety plan should exhibit include purpose, organization, responsibilities and risks.

Purpose requires a specification of the purpose and scope of the software safety activities. The 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.

Organization requires a description of the software safety organization. The 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 with the system safety activities, how the software safety activities are coordinated with the development activities, and the interactions between the software safety organization and the software V&V organization. The plan should designate a single safety officer that has clear responsibility for the safety qualities of the software being constructed.

Responsibilities requires a definition of the responsibilities and authority of the software safety organization. The plan should specify the person or group responsible for each software safety task. A designated safety officer should have clear authority for enforcing safety requirements in the software requirements specification, the design, and the implementation of the software. The safety officer should have the authority to reject the use of predeveloped software if the software cannot be shown to be adequately safe or if, in using a tool, it cannot be shown that the tool will not impact the safety of the final software system. The plan should require that safety personnel be aware of the safety implications of hardware, software and interfaces between them.

Risks requires a description of the methods to be used to reduce safety risks caused by software failures to an acceptable level. The plan should describe the method to be used to ensure that hazards which software is expected to control are resolved in an acceptable manner. The plan should include a requirement that a safety analysis be performed and documented on each of the principal design documents: requirements, design descriptions, and source code. Hazards, including abnormal events and conditions and malicious modifications, should be analyzed and documented. Hazard reduction efforts should be documented.

Implementation Characteristics

The implementation characteristics that the software safety plan should exhibit include measurement and procedures.

Measurement requires a set of indicators used to determine the success or failure of the software safety effort. The plan should require that software safety data be systematically collected and analyzed to determine the effectiveness of the software safety effort.

Procedures requires a description of the software safety strategy. The plan should describe the management of the software safety activities within the development organization. It should provide procedures for resolving safety issues. The plan should require that problems encountered in implementing the safety program be brought to the attention of the project manager. A procedure should exist for assuring resolution of identified unacceptable risks. The plan should describe methods to be used to implement each safety task. A method should exist to identify hazards caused by software, and to identify hazards whose resolution will be under the control of software.

The plan should require that appropriate safety requirements be included in the software requirements specification. It should define the safety-related activities to be carried out for each set of life cycle activities, from requirements through operation and maintenance. The plan should identify all

documentation required for the proper and safe operation of the software. Procedures should require monitoring the software safety function performance during operation of the system.

The plan should require that hazards identified by plant safety analysis, system safety analysis and security vulnerability assessment be traceable to the software safety analysis whenever these hazards can affect software operability or whenever software has a role in controlling the hazard.

Resource Characteristics

The resource characteristics that the software safety plan should exhibit include methods/tools and standards.

Methods/tools requires a description of the methods and tools used to carry out the safety activities. The plan should specify a process for selecting tools. It should describe a method for preventing the inadvertent introduction of hazards by the use of project tools.

Standards requires a list of the international, national, industry and company standards and guidelines to be followed by the safety organization.

j. Software Verification and Validation Plan

The software verification and validation (V&V) plan should exhibit the management, implementation and resource characteristics listed below. Reg. Guide 1.168, which endorses ANSI/IEEE Std 1012, "Software Verification and Validation Plans," shows an acceptable organization and content for this plan.

Management Characteristics

The management characteristics that the software V&V plan should exhibit include organization, oversight, responsibilities, and risks.

Purpose requires a definition of the purpose and scope of the software V&V activities. The plan should include a general description of the software V&V process.

Organization requires a description of the V&V organization. The plan should describe the boundaries and interfaces between the V&V organization and other company organizations. Reporting channels should be described. The relationship among the different V&V tasks should be specified. The plan should require that the V&V organization be independent of the development organization. It should require that formal communication between the V&V and design organizations be documented.

Responsibilities requires a definition of the responsibilities and authority of the software V&V organization. The plan should specify the person or group responsible for the successful completion of each V&V task. It should specify the person with authority to approve the successful completion of each V&V task. It should specify the person with authority to approve the release of the reviewed and tested software design outputs.

Risks requires a specification of the methods used to identify and manage risks associated with the V&V process. The plan should specify a method for evaluating the risk to safety associated with each software item. It should describe a method for identifying the risk associated with each V&V task. A contingency

plan should be included to identify risk factors that may cause the V&V task to fail to perform its functions, and to recover from any such failure.

Implementation Characteristics

The implementation characteristics that the software V&V plan should exhibit include measurement and procedures.

Measurement requires a set of indicators used to determine the success or failure of the software V&V effort. The plan should specify the criteria to be used to verify the completion of each V&V task. Evaluation criteria should be provided for test plans, test specifications, test procedures and test cases. Evaluation criteria should be provided for review plans, review specifications and review procedures. The plan should require that V&V analysis, review and testing data be systematically collected and analyzed to determine the effectiveness of the V&V effort. The error rate found during software reviews and software testing should be measured, recorded, analyzed and reported.

Procedures requires a description of the software review and testing strategy. The plan should describe the management of the software V&V activities. It should specify the V&V tasks which will be carried out, including the planning assumptions for each task. It should establish the procedures and methods by which each V&V task will be performed, including the activities required to evaluate each software design output and each development activity in order to demonstrate that the system and software requirements have been met. It should establish procedures to ensure that systems in which errors are detected are appropriately analyzed, reported, corrected and reassessed. The plan should provide procedures for evaluating the risks associated with each project development activity. It should include a procedure for evaluating the effect of proposed software changes on planned reviews and tests.

Anomaly reports should be generated and disseminated. A method should be specified for resolving discrepancies identified during the verification of each V&V task. Procedures should be specified for selecting test cases, and for software review activities.

The plan should describe V&V 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.

The plan should include a description of all required testing plans, specifications, procedures and cases. This includes unit testing, integration (subsystem) testing, system validation testing, installation (acceptance) testing, and the regression testing of modifications. The description should also include test documentation requirements, readiness and evaluation criteria, error reporting, and anomaly resolution procedures. Testing documentation should include test item descriptions, test data, test logs, the identities of testers, types of observations, results and acceptability, and actions taken in connection with any deficiencies. Test case documentation should specify expected results and actual results. Reg. Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 829, "IEEE Standard for Software Test Documentation," describes acceptable methods for documenting test plans, test specifications, test procedures, test cases, and test reports. Reg. Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety

Systems of Nuclear Power Plants," which endorses ANSI/IEEE Std 1008, "IEEE Standard for Software Unit Testing," describes acceptable methods for performing unit tests.

Resource Characteristics

The resource characteristics that the software V&V plan should exhibit include methods/tools and standards.

Methods/tools requires a description of the methods, equipment, instrumentation and tools used to carry out each V&V task. Test methods should be specified for unit, integration, validation, installation and regression testing. The plan should specify a process for selecting tools. The hardware and software environment within which the V&V tools are to be applied and any necessary controls should be described.

Standards requires a list of the international, national, industry and company standards and guidelines to be followed by the V&V organization.

k. Software Configuration Management Plan

The software configuration management (CM) plan should exhibit the management, implementation and resource characteristics listed below. Reg. Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 828, "IEEE Standard for Software Configuration Management Plans," provides an acceptable organization for this plan. It is acceptable for the software configuration management plan to be included in a more general system configuration management plan if the required content exists.

Management Characteristics

The management characteristics that the software CM plan should exhibit include purpose, organization, and responsibilities.

Purpose requires a definition of the purpose and scope of the software CM activities. The plan should list the general functions the software CM organization will be expected to perform.

Organization requires a description of the software CM organization. The plan should describe the boundaries and interfaces between the CM organization and other company organizations. Reporting channels should be described. It is acceptable for the software configuration management organization to be a part of, or to report to, the development organization or a project CM organization.

Responsibilities requires a definition of the responsibilities and authority of the software CM organization. The plan should specify the person or group responsible for the successful completion of each CM task. It should define the duties of the configuration control board. It should specify the person who has the authority to release any software, data or documents for revision, and the person who has the authority to release any software, data or documents for operation after revision has been completed.

Implementation Characteristics

The implementation characteristics that the software CM plan should exhibit include measurement, procedures, and record keeping.

Measurement requires a set of indicators used to determine the success or failure of the software CM activity. The plan should require that data associated with configuration management be systematically collected and analyzed to determine the effectiveness of the CM effort. The plan should specify the criteria to be used to verify the completion of each CM task.

Procedures requires a description of the software configuration management strategy. The plan should specify procedures for identifying and naming configuration items. It should specify procedures for placing items under configuration control. It should describe the method for keeping data files and tables synchronized with the software that uses them, and for keeping software and its associated documentation synchronized. It should specify the procedure for associating source code with the derived object code and executable modules. Procedures should exist for managing software libraries. The plan should ensure the control and retrieval of qualification information associated with the software designs and code, software confirmation audits, and status accounting.

Items to be controlled should include: software requirements, designs, and code; support software used in development (exact versions); libraries of software components essential to safety; software plans that could affect quality; test 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; predeveloped software items that are safety system software; software change documentation; and tools used in the software project for management, development or assurance tasks.

The plan should specify procedures for tracking problem reports, and for ensuring that each problem reported has been correctly resolved. The plan should describe the information required to approve a change request, and should ensure control of all software design changes. The relationship of software CM to other change control procedures, such as V&V anomaly handling and maintenance, should be described.

The plan should require periodic reviews and audits of the configuration baseline, including physical audits of the baseline.

The plan should include a description of the process used to maintain and track purchased items, such as software tools used to make the final product. A qualification procedure should be provided, and a method of tracking tool history, buglists, and errata sheets should enable the applicant/licensee to track which design outputs may be affected by discovered tool or purchased item deficiencies. The plan should describe procedures to control vendors supplying safety system software.

Record keeping requires a description of the software CM record keeping requirements. The plan should identify required CM records. Record structures (such as an annotated table of contents) should be provided. Procedures should exist for protecting configuration items. The plan should describe how configuration items will be stored, handled, retained and shipped. A tracking system should exist for managing configuration items, so that the revision history of each configuration item may be retrieved, and so that the latest revision of each configuration item may be easily identified. Procedures should exist for backup and disaster recovery.

Resource Characteristics

The resource characteristics that the software CM plan should exhibit include methods/tools and standards.

Methods/tools requires a description of the means that will be used to carry out each CM task. The plan should identify suitable facilities, methods, techniques and tools to facilitate the performance of the CM work. The plan should specify a process for selecting configuration management tools. The hardware and software environment within which the CM tools are to be applied and any necessary controls should be described.

Standards requires a list of the international, national, industry and company standards and guidelines to be followed by the software CM organization.

3.2. Acceptance Criteria for Software Life Cycle Process Implementation

This section addresses acceptance criteria for implementation activities. The acceptance criteria address specific software life cycle process implementation activities and documentation. These activities and products, when found to be acceptable, provide the reviewer with confidence that the plans listed in Section 2.1 above have been carried out.

The NRC staff reviewer confirms that the plans described in Section 3.1 have been followed by the software developer. The detailed acceptance criteria are provided by the software developer and evaluated by the NRC staff in its acceptance of the plans. In addition to verifying that plans have been followed, the reviewer should pay particular attention to the three areas discussed below. These activities are depicted in Figure 7-A-1 as process implementation.

a. Safety Analysis Activities

The software safety plan describes the safety analysis implementation tasks that are to be carried out by the applicant/licensee. The acceptance criterion for software safety analysis implementation is that the tasks in that plan have been carried out in their entirety. Documentation should exist that shows that the safety analysis activities have been successfully accomplished for each life cycle activity group. In particular, the documentation should show that the system safety requirements have been adequately addressed for each activity group; that no new hazards have been introduced; that the software requirements, design elements, and code elements that can affect safety have been identified; and that all other software requirements, design, and code elements will not adversely affect safety.

b. Software Verification and Validation Activities

The software V&V plan describes the V&V implementation tasks that are to be carried out by the applicant/licensee. The acceptance criterion for software V&V implementation is that the tasks in the plans have been carried out in their entirety. Documentation should exist that shows that the V&V tasks have been successfully accomplished for each life cycle activity group. In particular, the documentation should show that the requirements, design, code, integration, and installation design outputs satisfy the appropriate software development functional and process characteristics (as described in Section B.3.3 below).

Problems identified by the verification effort should be documented, together with any action items required to mitigate or eliminate each problem. A record should be kept of actions taken in response to the action items and the appropriate CM activities should be performed.

As part of the software V&V effort, a traceability matrix should be produced. This traceability matrix should clearly show the linkage between each requirement imposed on the software by the system requirements document and system design documents, and one or more requirements in the SRS. The matrix should allow traceability in both directions. It should be organized so that as design, implementation, and validation take place, traceability information can be added for these activities. It should be updated at the completion of each life cycle activity group. The final matrix should permit tracing from the system requirements and design through the software requirements, design, implementation, integration, validation, and installation.

The integration V&V activities should demonstrate that all unit and subsystem tests required by the V&V plan were successfully completed. Any anomalies or errors found during the tests should be resolved and documented. Final integration tests should be completed and documented. Reports should be written for each test run. These reports should include any anomalies found and actions recommended. The final integration V&V report should describe the procedures followed and the tests performed during integration. This report should be consistent with the integration plan.

The software validation activities should demonstrate that all validation tests required by the V&V plan were successfully completed. The testing process should contain one or more tests for each requirement in the SRS, as well as the acceptance criteria for each test. The result of each test should clearly show that the associated requirement has been met. Each test procedure should contain detailed information for the test setup, input data requirements, output data expectations, and completion time. Documentation should be produced for each test. Procedures should be included for handling errors and anomalies that are encountered during the testing. These procedures should include correction procedures (including configuration management), and provision for re-test until such time as the problems are resolved. A final report summarizing the validation testing should be provided. The report should contain a summary of problems and errors encountered during testing, and the actions taken to correct the problems encountered. The report should contain a statement that the validation testing was successful and that the software tested met all of the requirements of the SRS.

The installation (acceptance) test activities should document the test configuration, the required inputs, expected outputs, the steps necessary to execute the test, and the acceptance criteria for each test. The procedure should require that problems identified during the test activity, and any action items required to mitigate or eliminate each problem, be documented. Installation problems and their resolution should be documented. An acceptance test report should be produced describing the execution of the plan and summarizing the results. This report should contain a statement that the plan was successfully executed, and the system is ready for operation. The acceptance test report should demonstrate that the system operates correctly and is identical to the system that was validated during the validation phase. The report should summarize the test results after all problems have been satisfactorily resolved. The report should demonstrate that acceptance testing was executed according to the acceptance test procedure.

c. Software Configuration Management Activities

The software development plan describes the documents that will be created and placed under configuration management control. The configuration management plan describes the implementation tasks that are to be carried out by the applicant/licensee. The acceptance criterion for software CM implementation is that the tasks in that plan have been carried out in their entirety. Documentation should exist that shows that the configuration management tasks for that activity group have been successfully accomplished. In particular, the documentation should show that configuration items have been appropriately identified; that configuration baselines have been established for the activity group; that an adequate change control process has been used for changes to the product baseline; and that appropriate configuration audits have been held for the configuration items created or modified for the activity group.

Each configuration item should be labeled unambiguously so that a basis can be established for the control and reference of the configuration items defined in the software CM plan. Configuration baselines should be established for each life cycle activity group, to define the basis for further development, allow control of configuration items, and permit traceability between configuration items. The baseline should be established before the set of activities can be considered complete. Once a baseline is established, it should be protected from change. Change control activities should be followed whenever a derivative baseline is developed from an established baseline. A baseline should be traceable to the baseline from which it was established, and to the design outputs it identified or to the activity with which it is associated.

Configuration control actions should be used to control and document changes to configuration baselines. A configuration control board (CCB) should exist with the authority to authorize all changes to baselines. Problem reports should be prepared to describe anomalous and inconsistent software and documentation. Problem reports that require corrective action should invoke the change control activity. Change control should preserve the integrity of configuration items and baselines by providing protection against their change. Any change to a configuration item should cause a change to its configuration identification. This can be done via a version number or attached change date. Changes to baselines and to configuration items under change control should be recorded, approved and tracked. If the change is due to a problem report, traceability should exist between the problem report and the change. Software changes should be traced to their point of origin, and the software processes affected by the change should be repeated from the point of change to the point of discovery. Proposed changes should be reviewed by the CCB for their impact on system safety.

Status accounting should take place for each set of life cycle activities prior to the completion of those activities. The status accounting should document configuration item identifications, baselines, problem report status, change history and release status.

The configuration management organization should audit life cycle activities to confirm that configuration management procedures were carried out in the life cycle process implementation.

3.3. Acceptance Criteria for Software Life Cycle Process Design Outputs

This section describes the criteria to be used to determine whether the software has each of the characteristics important to safety system software. Criteria are organized first by life cycle activity group, then by design output, and then by characteristic.

Formal or semiformal methods are available for use in preparing some of the design outputs described in this section. Section C.3 of Appendix 7.0-A describes the benefits of using such methods and the precautions that should be observed when reviewing design outputs prepared with such methods.

Acceptance criteria are divided into two sets: functional characteristics and process characteristics, as shown in the following table. Not all characteristics occur for every design output.

Functional Characteristics	Process Characteristics
Accuracy	Completeness
Functionality	Consistency
Reliability	Correctness
Robustness	Style
Safety	Traceability
Security	Unambiguity
Timing	Verifiability

a. Requirements Activities — Software Requirements Specification

An SRS that exhibits the functional and the software development process characteristics listed below should be produced. Reg. Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 830, "IEEE Recommended Practice for Software Requirements Specifications," describes an acceptable approach for describing software requirements.

Functional Characteristics

For each of the functional characteristics, the requirements imposed by the system requirements and system design on the software for that characteristic should be contained in the SRS. Functional characteristics addressed by the SRS include accuracy, functionality, reliability, robustness, safety, security, and timing.

Accuracy requirements should be provided for each input and each output variable. Accuracy requirements should be stated numerically, and appropriate physical units and error bounds should be supplied. Accuracy requirements should include a description of data type and data size for each input and output variable.

Functionality requires that the operations that must be performed for each mode of operation be completely specified. Functions should be specified in terms of inputs to the function, transformations to be carried out by the function, and outputs generated by the function.

Reliability requires that all requirements for fault tolerance and failure modes be fully specified for each operating mode. Software requirements for handling both hardware and software failures should be provided, including requirements for analysis of and recovery from computer system failures. Requirements for on-line in-service testing and diagnostics should be provided.

Robustness requires that the behavior of the software in the presence of unexpected, incorrect, anomalous and improper (1) input, (2) hardware behavior, or (3) software behavior be fully specified. Of particular

concern is the behavior of the software in the presence of unexpectedly high or low rates of message traffic.

Safety requires that the software functions, operating procedures, input, and output be classified according to their importance to safety. Requirements important to safety should be identified as such in the SRS. The identification of safety items should include safety analysis report requirements, as well as abnormal conditions and events as described in Reg. Guide 1.152.

Security requires that security threats to the computer system be identified and classified according to severity and likelihood. Actions required of the software to detect, prevent, or mitigate such security threats should be specified, including access control restrictions.

Timing requires that functions that must operate within specific timing constraints be identified, and that timing criteria be specified for each. Timing criteria should be provided for each mode of operation. Timing requirements should distinguish between goals and requirements. Timing requirements should be stated in such a way that the time delay between stimulus and response for safety actions is deterministic under normal and anticipated failure conditions. BTP HICB-21 provides additional guidance on real-time performance.

Software Development Process Characteristics

Software development process characteristics exhibited by the SRS should include completeness, consistency, correctness, style, traceability, unambiguity and verifiability.

Completeness requires that all actions required of the computer system be fully described for all operating modes and all possible values of input variables (for example, the complete span of instrument inputs or clock/calendar time)*. The SRS should describe any actions that the software is prohibited from executing. The operational environment within which the software will operate should be described. All variables in the physical environment that the software must monitor and control shall be fully specified. Functional requirements should describe (1) how each function is initiated; (2) the input and output variables required of the function; (3) the task sequences, actions, and events required to carry out the function; and (4) the termination conditions and system status at the conclusion of the function. User interfaces should be fully described for each category of user.

Consistency requires that the contents of the SRS be consistent with the safety system requirements, the safety system design, and documented descriptions and known properties of the operational environment within which the safety system software will operate. Individual requirements should not contradict other requirements. Timing requirements should be consistent with thermohydraulic analyses performed in the system safety analysis. Uniform and consistent terminology, notation, and definitions should be used throughout the SRS.

Correctness requires that the description of actions required of the computer system be free from faults and that no other requirements be stated. The operational environment within which the software will operate should be accurately described. All variables in the physical environment that the software must monitor and control should be properly specified. Functional requirements should accurately describe (1) how each function is initiated; (2) the input and output variables required of the function; (3) the task

*Implementation of safety functions should not rely upon a date (calendar time). Actions depending upon calendar time should account for concerns such as those identified with the year 2000 (two-digit 00).

sequences, actions and events required to carry out the function; and (4) the termination conditions and system status at the conclusion of the function.

Style requires that the contents of the SRS be understandable. The SRS should differentiate between requirements placed on the software and other supplementary information, such as design constraints, hardware platforms, and coding standards. A precise definition of each technical term should exist, either in the SRS or in a separate dictionary or glossary. Each requirement should be uniquely and completely defined in a single location in the SRS.

Traceability requires that a two-way trace exist between each requirement in the SRS, and the safety system requirements and design. There should be a two-way trace between each requirement in the SRS and the software design, as well as a forward trace from each requirement in the SRS to the specific inspections, analyses, or tests used to confirm that the requirement has been met.

Unambiguity requires that each requirement, and all requirements taken together, have one and only one interpretation.

Verifiability requires that it be possible to construct a specific analysis, review, or test to determine whether each requirement has been met.

b. Design Activities — Software Architecture Description

A SAD should be produced. The SAD should include all of the functional and software development process characteristics listed below.

Functional Characteristics

For each of the functional characteristics, the requirements imposed on the software for that characteristic should be satisfied by the software architecture. A review of the software architecture requires a concurrent review of the hardware architecture. Functional characteristics addressed by the SAD should include reliability, safety, security, and timing.

Reliability requires that the combined hardware and software architecture be such that individual software element failure will not compromise safety. The software architecture should identify actions to be taken in the event of error detection. The hardware and software architecture should be reviewed to verify that the propagation of errors is controlled via a well-structured modular design.

Safety requires that the software architecture introduce no new hazards into the safety system. The safety functions should be separated from normal operating and overhead functions, with well-defined and strictly controlled interfaces between them. Any online maintenance features should be included. The hardware and software architecture should be reviewed to verify that there is no violation of other criteria such as single failure, channel separation, and separation between Class 1E and non-1E systems. The review should verify that no new hazards are introduced into the safety system as a result of the architecture configuration.

Security requires that the architecture correctly handle identified security threats, and introduce no new security threats.

Timing requires that the architectural design describe all timing limitations, the strategy for handling each, the required margins, and the method of measuring those margins. A timing specification should exist for each architectural element, in terms of minimum and maximum times for execution. Scheduling mechanisms and interprocess communication methods should be described. The architecture should be such that operations are performed in the correct sequence. BTP HICB-21 provides additional guidance on real-time performance. SRP Section 7.9 provides additional guidance on digital data communications systems.

Software Development Process Characteristics

The software development process characteristics that the SAD must exhibit include completeness, consistency, style, traceability, and verifiability.

Completeness requires that all the software requirements be satisfied in the architecture. The SAD should address all operating modes specified in the SRS, including initialization, operational, shut-down, maintenance, and test modes.

Consistency requires that each software architectural element be compatible with the SRS, the hardware architecture, documented descriptions and known properties of the operational and hardware environment, and other software elements. Timing specifications of each software element should be consistent with the specifications of the other elements with which it interacts and with the expected performance of the system as a whole. Uniform and consistent terminology, notation, and definitions should be used.

Style requires that the contents of the SAD be understandable. The architecture description should conform to the developer's style guide. The architecture specification should contain the rationale for architectural decisions.

Traceability requires that a two-way trace exist between the requirements in the SRS and the elements in the architecture. A two-way trace should exist between the architectural elements and the detailed design elements. There should be a forward trace from each architectural element to the specific inspections, analyses, or tests that will be used to confirm that the element has been correctly designed.

Verifiability requires that it be possible to construct specific analyses, reviews, and tests to verify that the architecture satisfies the software requirements.

c. *Design Activities — Software Design Specification*

An SDS should be produced. The SDS should include all of the functional and software development process characteristics listed below.

Functional Characteristics

For each of the functional characteristics, the requirements imposed on the software for that characteristic should be satisfied by the software design. Product functional characteristics addressed by the SDS should include accuracy, reliability, robustness, safety, security, and timing.

Accuracy requires that all calculations be specified in such a way that the accuracy requirements for the calculations will be satisfied. In particular, floating point arithmetic should be avoided; if that is not possible, special care must be taken to maintain the accuracy of the calculations. The design should specify the method for determining that the values of input variables are within the proper range, the

method by which the software will detect that the values of input variables are not within their proper range, and the actions to be taken in the latter case. All calculations should be analyzed for convergence, round-off error, precision, and accuracy as appropriate.

Reliability requires that the detailed software design be such that single failures of individual elements will not cause safety system failure.

Robustness requires that the design be such that the software will operate correctly in the presence of unexpected, incorrect, anomalous and improper (1) input, (2) hardware behavior, or (3) software behavior. In particular, the software should not fail, and should not provide incorrect outputs, in the presence of these conditions. Attention should be paid to those values of input variables that are physically possible to the device, even if logically impossible in the application (to account for sensor errors, communication line noise, and similar concerns).

Safety requires that the detailed design introduce no new safety hazards into the safety system.

Security requires that unauthorized changes be prevented, detected, or mitigated as appropriate.

Timing requires that the time delay between stimulus and response be deterministic. BTP HICB-21 provides additional guidance on real-time performance.

Software Development Process Characteristics

The SDS should exhibit each of the following software development process characteristics: completeness, consistency, correctness, style, traceability, and verifiability.

Completeness requires that the detailed design specify the actions of each software unit for the entire domain of each input variable (for example, the complete span of instrument inputs or clock/calendar time). The design should be sufficiently complete to permit implementation to take place. Actions should be specified for all situations anticipated in the SRS. Equipment, human, hardware, and software interfaces should be correctly and fully specified. Equations, algorithms, and control logic should be correctly and fully specified.

Consistency requires that the detailed design be consistent with the architectural design, and that the detailed design elements be mutually consistent. Design elements should be consistent with documented descriptions and known properties of the operational environment within which the software will execute. Input and output specifications specified in the software design should be consistent with interface requirements imposed by the hardware or predeveloped software products. Timing specifications of each detailed design element should be consistent with the timing specifications of the architectural element of which it is a part. Models, algorithms, and numerical techniques specified in the software design should agree with standard references where such are applicable. A uniform and consistent terminology, notation, and definitions should be used. Models, algorithms, and numerical techniques specified in the software design should be mathematically mutually compatible.

Correctness requires that all equations, algorithms, and control logic be evaluated for potential errors. All equations and algorithms should be defined to a sufficient level of detail to permit coding. Data structure design should ensure that the code elements will correctly initialize data, correctly access stored data, and correctly scale and dimension data. The detailed design should ensure that no data item can be used before it is initialized, can have its value changed in an unanticipated manner, or can have its value

changed by an unanticipated design element. The detailed design should ensure that no data item can be changed in an unanticipated manner.

Style requires that the detailed design documents description should conform to the developer's style guide. Each element of the detailed design should be specified. The detailed design documentation should contain the rationale for design decisions. Programming language standards should be identified. The detailed design documentation should identify those language features which will not be used without justification.

Traceability requires that a two-way trace exist between the elements of the detailed design and the elements in the architecture. A two-way trace should exist between the detailed design elements and the code elements. There should be a forward trace from each detailed design element to the specific inspections, analyses, or tests that will be used to confirm that the element has been correctly designed.

Verifiability requires that it be possible to construct specific analyses, reviews, and tests to verify that the design satisfies the software architecture.

d. Implementation Activities — Code Listings

A software implementation (code) should be produced. The code should include all of the functional and software development process characteristics listed below.

Functional Characteristics

For each of the functional characteristics, the requirements imposed on the software for that characteristic should be satisfied by the code. Functional characteristics addressed by the code documents should include accuracy, robustness, safety, and timing.

Accuracy requires that the actual source code be written so that the accuracy requirements and accuracy design specifications are met. In particular, special care should be taken for floating point arithmetic, round-off errors, and the retention of precision during numerical operations. If mathematical subroutine libraries are used, the accuracy characteristics of the subroutines should be known and documented, and shown to meet the accuracy requirements and accuracy design specifications.

Robustness requires that the system be coded in such a way that corrupted data will not cause the safety system to fail. Data corruption should be avoided. All input data should be checked to ensure that the correct data is being read and that the data is in the correct format. All messages should be checked to ensure that the correct message is being read and that the message contents are in the correct format. Appropriate corrective actions should take place if any of these criteria are violated.

Safety requires that the code introduce no new hazards into the safety system.

Security requires that the code introduce no new security threats into the safety system software.

Timing requires that the execution time be deterministic. BTP HICB-21 provides additional guidance on real-time performance.

Software Development Process Characteristics

Software development process characteristics exhibited by the code documents should include completeness, consistency, correctness, style, traceability, and verifiability.

Completeness requires that the code meet all the specifications of the design and all implementation constraints. The software implementation should be compatible with the hardware environment.

Consistency requires that all variable names, types, locations, and array sizes be defined consistently throughout the software units. The code should use mathematical equations which correspond to the mathematical models, algorithms, and numerical techniques described in or derived from the SDS. All parameters passed between software units should be consistent with respect to number, type, structure, physical units, and direction. Minimum and maximum execution times should be consistent with expected overall performance.

Correctness requires that the code be correctly implemented.

Style requires that the programming style constraints specified in the design documents be followed. NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," provides guidance on coding practices to be avoided. In particular, data structures should be protected so that they cannot be changed simultaneously. Arrays should have a fixed, predefined length. Global variables and dynamic memory allocation should not be used.

Traceability requires that a two-way trace exist between the elements of the detailed design and the elements in code. A two-way trace should exist between the code elements and the specific software subsystem or system which contains that element during factory build and test. There should be a forward trace from each detailed design element to the specific inspections, analyses, or tests that will be used to confirm that the element has been correctly implemented.

Verifiability requires that it be possible to construct specific analyses, reviews, and tests to verify that the code correctly implements the detailed design.

*e. **Integration Activities — System Build Documents***

One or more system build documents should be produced. The build documents should include all of the functional and software development process characteristics listed below.

Functional Characteristics

For each of the functional characteristics, the requirements imposed on the build documents for that characteristic should be satisfied. Functional characteristics addressed by the build documents should include robustness, safety, and security.

Robustness requires that the software build documents specify methods to detect incorrectly built software releases. The software build documents should identify all errors and anomalies discovered during software build activities.

Safety requires that the software build activity introduce no new hazards into the safety system.

Security requires that the software build activity introduce no new security threats into the safety system software.

Software Development Process Characteristics

The system build documents must exhibit each of the following software development process characteristics: completeness, consistency, correctness, style, traceability, and verifiability.

Completeness requires that all build procedures be fully specified. The software build documents should include all required software units, including code and data, that are part of the build.

Consistency requires that the software build documents be consistent with the software specifications, as described in the SRS, software design description, and software code. A consistent and uniform set of terminology, notation, and definitions should be used throughout the software build document.

Correctness requires that the software build documents identify the correct versions of all required software elements and all required software documents. It should be verified that the correct elements have actually been used in the build, including proper units from software libraries.

Style requires that the software build documents conform to applicable standards imposed by the developer. A precise definition of each technical term used in the build documents should be included in the document, or in a separate dictionary or glossary.

Traceability requires that it be possible to trace each element of the integrated builds (software subsystem or software system) backward to the code elements contained in the build. It should be possible to trace each element of the integrated build forward to the software field installation.

Verifiability requires that it be possible to analyze, review, or test each integrated software build for the product functional requirements. The system build documents should specify methods to detect incorrectly built software releases. The build documents should identify all errors and anomalies discovered during software build activities.

f. Installation Activities — Installation Configuration Tables

Installation configuration tables should be produced. They should include all of the functional characteristics listed below to ensure that the software will be correctly configured in the operating safety system. The software development process characteristics listed below should be exhibited by the installation configuration tables themselves.

Functional Characteristics

For each of the functional characteristics, the requirements imposed on the configuration tables for that characteristic should be satisfied. Functional characteristics addressed by the configuration tables should include functionality, safety, and security.

Functionality requires that the installation tables configure the installed system to have the functionality that is required for the plant.

Safety requires that the installation tables introduce no new hazards into the safety system.

Security requires that the installation tables introduce no new security threats into the installed system, and that the installation tables be protected from unauthorized change.

Software Development Process Characteristics

The configuration tables must exhibit each of the specified software development process characteristics: completeness, consistency, correctness, traceability, and verifiability.

Completeness requires that the software configuration tables include all information necessary for the correct operation of the system.

Consistency requires that the installation configuration tables be consistent with the software specifications, as described in the SRS, software design description, software code, and software build documents.

Correctness requires that the software configuration tables contain all plant-specific data.

Traceability requires that it be possible to trace each installed program element backward to the integrated software elements that created that installed program element.

Verifiability requires that it be possible to analyze, review, or test each installed software system on initial software installation, all subsequent installations, and periodically during operation.

g. Installation Activities — Operations Manuals

One or more software operations manuals should be produced. They may be incorporated into a system operations manual. Because operations manuals do not impose requirements on the software itself, the functional characteristics described in other sections of this BTP are not directly relevant. However, the software development process characteristics listed below should be exhibited by software operations manuals.

Completeness requires that all actions available to the system operator be fully described for all operating modes, including error recovery and backup. Operator actions should be specified in terms of inputs supplied by the operator or equipment, actions initiated by the operation, and responses to the operator. The purpose and operation of each function should be described, including interfaces with other functions. The operations manual should describe the operational environment within which the software will operate, including precautions and limitations that must be observed during operations to avoid exposing personnel or the plant to hazards or security vulnerabilities. All variables in the physical environment that the software must monitor and control should be fully described. User interfaces should be fully described for each category of user.

Consistency requires that the operations manual be consistent with the system operations, safety system requirements, the safety system design, the SRSs, the SDS, and documented descriptions and known properties of the operational environment within which the safety system will operate. Individual user instructions should not contradict other instructions. Uniform and consistent terminology, notation, and definitions should be used throughout the operations manuals.

Style requires that the operations manual be understandable by the users of the manual. A precise definition of each technical term should exist, either in the operations manual or in a separate dictionary or glossary. The operations manual may be organized in the style of a reference manual, with the assumption that its users are well trained.

Traceability requires that a forward trace exist between the SRS, the operations plan, and the operations manual, which shows how each requirement is to be carried out by the operators, or carried out automatically by the safety system without operator action, and how the results of each requirement are displayed to the operators. A forward trace should also exist from all error messages generated by the code to a description of the error messages in the operations manual.

Unambiguity requires that instructions to users have only one interpretation by the users.

h. Installation Activities — Maintenance Manuals

One or more software maintenance manuals should be produced. They may be incorporated into a system maintenance manual. Because maintenance manuals do not impose requirements on the software itself, the functional characteristics described in other sections of this BTP are not directly relevant. However, the software development process characteristics listed below should be possessed by software maintenance manuals.

Completeness requires that maintenance procedures be fully defined. This should include identification of precautions and limitations that must be observed during maintenance to avoid exposing personnel or the plant to hazards or security vulnerabilities. Trouble reports should be collected from field installations and analyzed to determine if changes to the software are required. Configuration management procedures should be described in or referenced by the maintenance manual. Procedures should exist to (1) verify that changes have been carried out correctly and that no faults have been introduced in the software by the changes, and (2) ensure that software is correctly returned to service. Field upgrade procedures should be described.

Style requires that the maintenance manual be understandable by the users. A precise definition of each technical term should exist, either in the maintenance manual or in a separate dictionary or glossary. The maintenance manual may be organized in the style of a reference manual, with the assumption that its users are well trained.

Traceability requires that a forward trace exist between the maintenance plan and the maintenance manual, which shows how each requirement is carried out by the maintenance organization.

i. Installation Activities — Training Manuals

One or more software training manuals should be produced. They may be incorporated into a system training manual. Because training manuals do not impose requirements on the software itself, the functional characteristics described in other sections of this BTP are not directly relevant. However, the software development process characteristics listed below should be exhibited by software training manuals.

Completeness requires that all actions available to the operator be fully described for all operating modes, including error recovery. Operator actions should be specified in terms of inputs supplied by users and equipment, actions initiated by the operation, and responses to the user. The training manual should describe the operational environment within which the software will operate, including precautions and limitations that must be observed during operations to avoid exposing personnel or the plant to hazards. All variables in the physical environment that the software must monitor and control should be fully described. User interfaces should be fully described for each category of user.

Consistency requires that the training manual be consistent with the safety system requirements, the safety system design, the SRSs, the SDS, and documented descriptions and known properties of the operational environment within which the safety system will operate. Individual user instructions should not contradict other instructions. Uniform and consistent terminology, notation, and definitions should be used throughout the training manuals.

Style requires that the training manual be understandable by the users. A precise definition of each technical term should exist, either in the training manual or in a separate dictionary or glossary. The operations manual may be organized in the style of a tutorial guide, with the assumption that the users also have access to the operations manual.

Traceability requires that a forward trace exist between the SRS, the training plan, and the training manual, which shows how each requirement is to be carried out by the users, or carried out automatically by the safety system without user action, and how the results of each requirement are displayed to the users.

4. Review Procedures

Reviews are carried out by a combination of inspection and analysis of documents. The adequacy of the computer development process should be reviewed to confirm that software life cycle plans incorporate appropriate commitments, as described in Section 3.1 above. New software, or an unproven development team, will require greater emphasis on the adequacy of the planning phase. A sample of V&V, safety analysis, and configuration management documentation for various life cycle activity groups should be audited to confirm that the developer's life cycle activities have been properly implemented. Section 3.2 above presents specific criteria from which the inspection activities for each specific life cycle activity may be derived. A sample of software design outputs should be reviewed to confirm that they address the functional requirements allocated to the software, and that the expected software development process characteristics are evident in the design outputs. Section 3.3 above describes functional characteristics and software development process characteristics from which the inspection activities for each specific design output may be derived. SRP Appendix 7.0-A contains additional detail on the software review process and the relationship between software reviews and system reviews.

C. References

ANSI/IEEE Std 1008-1987. "IEEE Standard for Software Unit Testing."

ANSI/IEEE Std 1012-1986. "IEEE Standard for Software Verification and Validation Plans."

ANSI/IEEE Std 1058.1-1987. "IEEE Standard for Software Project Management Plans."

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std 829-1983. "IEEE Standard for Software Test Documentation."

ASME Std NQA-1-1994. "Quality Assurance Requirements for Nuclear Facility Applications."

EPRI Topical Report TR-106439. "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." Electric Power Research Institute, October 1996.

IEEE Std 1028-1988. "IEEE Standard for Software Reviews and Audits."

IEEE Std 1042-1987. "IEEE Guide to Software Configuration Management."

IEEE Std 1074-1995. "IEEE Standard for Developing Software Life Cycle Processes."

IEEE Std 1219-1992. "IEEE Standard for Software Maintenance."

IEEE Std 1228-1994. "IEEE Standard for Software Safety Plans."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

IEEE Std 730.1-1989. "IEEE Standard for Quality Assurance Plans."

IEEE Std 828-1990. "IEEE Standard for Software Configuration Management Plans."

IEEE Std 830-1993. "IEEE Recommended Practice for Software Requirements Specifications."

NUREG/CR-6421. "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications." March 1996.

NUREG/CR-6101. "Software Reliability and Safety in Nuclear Reactor Protection Systems." 1993.

NUREG/CR-6463. "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems." June 1996.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Regulatory Guide 1.168. "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.169. "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

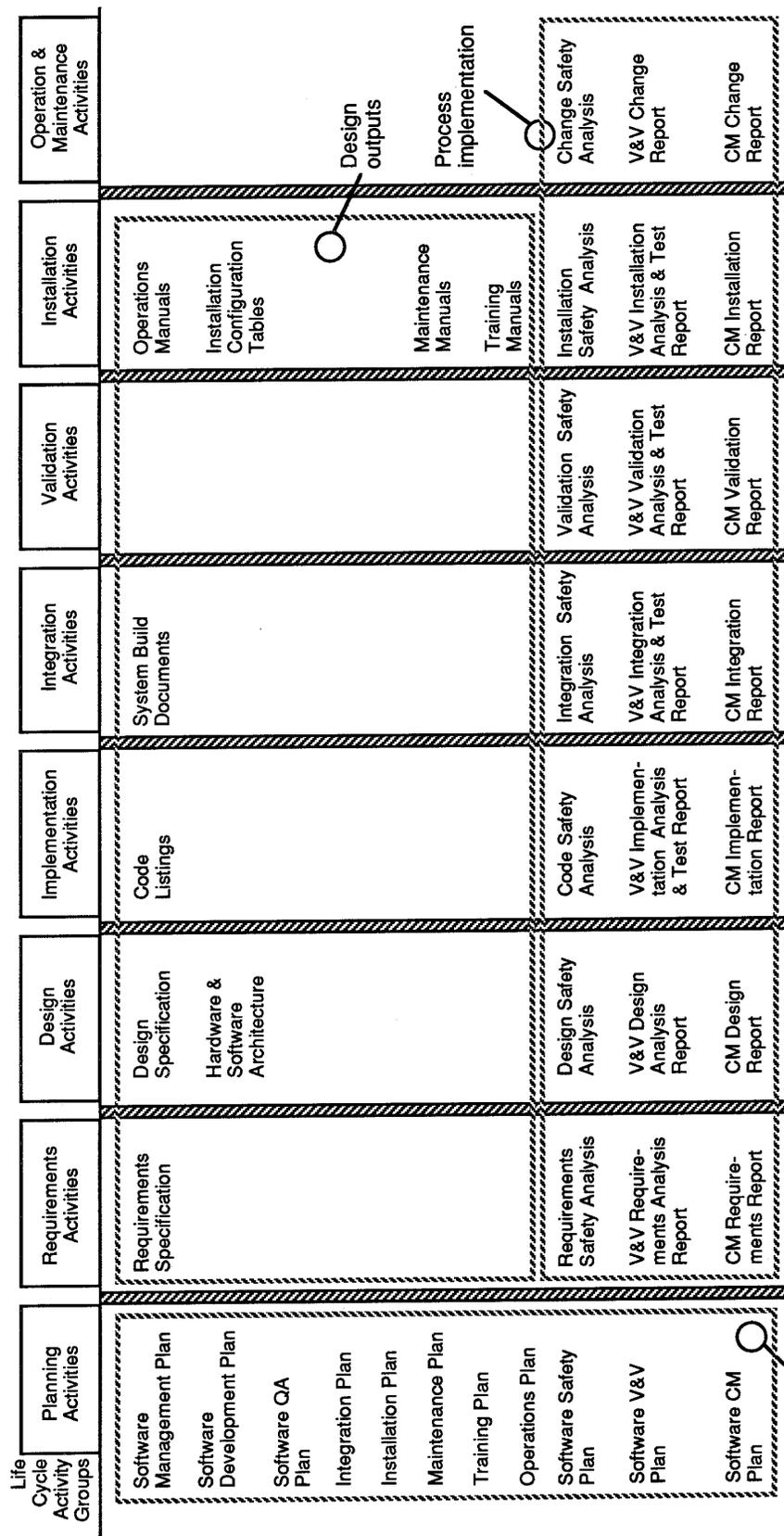
Regulatory Guide 1.170. "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.171. "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.172. "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.173. "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Safety Evaluation by the Office of Nuclear Reactor Regulation. "EPRI Topical Report TR-106439." May 1997.



Note: A separate document is not required for each topic identified; however, project documentation should encompass all of the topics.

Figure 7-A-1. Flow of Documents Through the Software Life Cycle

Branch Technical Position HICB-15

Not used.

Branch Technical Position HICB-16

Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

A. Background

This branch technical position (BTP) identifies (1) the level of detail of the approach and (2) information the Staff needs in order to review digital computer-based instrumentation and control (I&C) systems for design certification in accordance with 10 CFR 52. This guidance supplements and modifies the guidance of Reg. Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants."

1. Regulatory Basis

10 CFR 52.47 requires in part that applications for design certification include the non-site-specific technical information required of applicants for construction permits and operating licenses by 10 CFR 50 and its appendices. The applicant shall also provide information regarding the TMI-related requirements (10 CFR 50.34(f)), the resolution of unresolved safety issues, the technical resolution of medium- and high-priority generic safety issues, a design-specific probabilistic risk assessment, and inspections, test, analyses, and acceptance criteria (ITAAC). The application shall contain a level of design information sufficient to enable the NRC staff to reach a final conclusion on all safety questions associated with the design, and to judge the applicant's proposed means of ensuring that construction conforms to the design.

The NRC staff's conclusions are documented in a safety evaluation report (SER) and a standardized design certification, which is a rule describing the certified design. However, incorporating all safety analysis report (SAR) material directly into the rule would prevent combined license (CL) applicants from incorporating advancements in technology and equipment into the plant when it is eventually built. Therefore, to maintain necessary flexibility in the detailed design, the SAR is composed of Tier 1, Tier 2, and Tier 2* material as defined below.

2. Definitions

The *design certification document (DCD)* is the master document that contains the information that is referenced by the design certification rule. The DCD includes both the Tier 1 information that is certified by the design certification rule and the Tier 2 information that is approved by and supports the rule. The DCD is composed of the certified design material and the non-proprietary version of the SAR, including all material incorporated by reference.

Tier 1 is the design-related information contained in the DCD that constitutes the certified standard design. This information identifies the scope of the standard design and consists of the certified design descriptions, the ITAAC, the site parameters, and the interface requirements. Tier 1 material becomes part of the design certification rule and may be changed only by rule-making.

Tier 2 consists of the remainder of the design-related information contained in the DCD. It supports the certification of a standard design by providing additional details about the proposed implementation. The Tier 2 information generally consists of the SAR with the proprietary information removed for purposes of rule-making. Although Tier 2 information is not certified by the design certification rule, it consists of "those matters resolved in connection with the issuance or renewal of a design certification" within the meaning of 10 CFR 52.63(a)(4). Tier 2 material is approved by the design certification rule, but is not part of the rule. Tier 2 material may be changed by a process similar to that described in 10 CFR 50.59, unless designated as Tier 2* in the SER.

*Tier 2** is a subset of Tier 2 material that the NRC SER and DCD for the standardized plant design approval identifies as requiring NRC approval prior to modification or change by the applicant/licensee.

Design acceptance criteria (DAC) are a set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies in making a final safety determination to support design certification when detailed design information is not available. The DAC are part of the Tier 1 information. The DAC may be used to compensate for the lack of design detail in areas of rapidly changing technology where it would be detrimental to freeze design details many years before an actual plant is ready to be constructed. Computer-based I&C systems typically meet this criterion. The DAC are objective and are verified as a part of the ITAAC performed to demonstrate that the as-built facility conforms to the certified design. Using DAC will result in less detail about the design, but more detail regarding how the design will be accomplished. Conformance review points are specified for the Staff to assess the design development process at various stages of detailed design and subsequent construction and testing. The CL applicant is required to develop the procedures and test programs necessary to demonstrate that the DAC requirements are met at each conformance review point.

Certified design material (CDM) aggregates all Tier 1 material for reference by the design certification rule. It includes general provisions, ITAAC, certified design descriptions, interface requirements, and site parameters for the design.

3. Purpose

The purpose of this BTP is to provide guidance for NRC reviewers to verify that the previously cited regulatory basis and standards are met by a design certification applicant's submittal. This BTP has the following objectives:

- Confirm that the documentation that supports design certification applications contains sufficient information about I&C systems important to safety to support an evaluation of whether a plant constructed to the certified design can be operated without undue risk to the health and safety of the public.
- Confirm that appropriate design details and commitments are identified for certification and approval by the standard design certification rule (Tier 1 material).
- Confirm that appropriate design details supporting the standard design certification rule are identified in the SAR as unchangeable without NRC approval (Tier 2* material).
- Confirm that appropriate additional design details supporting the standard design certification rule are included in the SAR either directly or by reference (Tier 2 material).

B. Branch Technical Position

1. Introduction

During the review of design certification applications, the Staff developed a two-tier review approach to allow a CL applicant some flexibility in the implementation of a certified design. A variation of Tier 2 was also added (Tier 2*). (The development of Staff policy is discussed in a memorandum from W. T. Russell to B. A. Boger, et al.; Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants;" SECY-90-241; SECY-90-377; SECY-92-053; SECY-92-087; and SECY-93-087.)

The use of DAC allows approval of fundamental design requirements and commitments to an effective detailed design process in lieu of detailed design information for design certification. ITAAC will be provided to verify that DAC have been satisfied. The ITAAC for the DAC will be performed by the CL applicant, and reviewed by the NRC throughout the design implementation and construction process. Refer to SRP Chapter 14 for guidance on ITAAC.

2. Information to be Reviewed

The information to be reviewed is the SAR (including information incorporated by reference), CDM, and detailed design information available for audit.

3. Acceptance Criteria

3.1 Content of Design Certification Applications

In addition to the material identified in Reg. Guide 1.70, the SAR should include the information described below. Detailed documentation that supports the summary information described below should be available for audit.

3.2 Section 7.1

In addition to the material identified by Reg. Guide 1.70, Section 7.1 should (1) describe the resolution of unresolved and generic safety issues applicable to the I&C systems, (2) describe the interface requirements to be met by portions of the plant for which the application does not seek certification and which are necessary to ensure proper functioning of the I&C systems, and (3) identify and describe the validation of innovative means of accomplishing I&C system safety functions. Furthermore, applications that propose the use of computers for systems important to safety should describe the computer system development process. Applications that propose the use of computers for reactor trip system (RTS) or engineered safety features actuation system (ESFAS) functions should also describe the design of the overall I&C systems with respect to defense-in-depth and diversity (D-in-D&D) requirements. Since the discussion of these topics will apply to several I&C systems, these topics will normally be located in Section 7.1. Details on the content expected in these discussions are described below.

Computer Development Process

The software and hardware development process used or planned for use to ensure that computer systems have the necessary quality and functionality should be discussed. This discussion should include a commitment to a design process compatible with that described in Reg. Guide 1.152 and BTP HICB-14.

Plans addressing the review topics described in Section B.2.1 of BTP HICB-14 should be available for review at the time of design certification. The process and acceptance criteria for qualifying predeveloped software (including tools) should be described.

For completed designs, documentation of development process implementation as described in Section B.2.2 of BTP HICB-14, and design output documents as described in Section B.2.3 of BTP HICB-14, should be available for inspection. An applicant may choose not to request design certification of a completed design, in which case the information described in Sections B.2.2 and B.2.3 of BTP HICB-14 will be unavailable. In such cases applicants may commit to DAC to compensate for the lack of design detail. In this case, the DAC will be accompanied by ITAAC proposed to demonstrate that the as-built system conforms to the certified design. Chapter 14 of the SRP describes the review of ITAAC submitted in conjunction with DAC.

The provisions to ensure that computer systems maintain necessary functional capability under conditions described in the SAR should be discussed. This discussion should include a description of design, analysis, and test techniques used or planned to be used, to ensure that computer systems will have acceptable real-time performance. BTP HICB-21 describes the review of real-time performance.

Defense-in-Depth and Diversity

Analyses should be provided to demonstrate compliance of the overall I&C system design with defense-in-depth and diversity guidance. BTP HICB-19 describes the characteristics of such analyses. Provisions for ensuring appropriate diversity should be described in the applicable section of the SAR. Primary backup systems should be described to a level of detail commensurate with that described below for Sections 7.2 and 7.3.

3.3 Section 7.2 through 7.7

A complete set of final system drawings may not be available for computer-based systems at the design certification stage. In this case, system-specific DAC may be substituted for the final system drawings requested by Reg. Guide 1.70.

Regardless of whether complete final system drawings or DAC are provided, the application should include a description of the overall system architecture and the functional block diagrams for each system. Additionally, system features provided to meet the requirements of 10 CFR 50.34(f) should be identified. The functional block diagrams should contain the information described below:

- Each block of the block diagram should represent a complete functional unit. That is, there should be inputs from an external source, such as instruments or other functional blocks, and outputs to external plant systems or equipment, such as actuators or other functional blocks.
- The relationship between the inputs and the outputs should be clearly and completely specified for each block.
- Allowable timing for each block should be specified.
- It should be possible to specify from these numbers the maximum allowable total cycle time of the system and the processing time from primary input to primary output.

- For multi-processor functional blocks, the method of communication between the processors of the block should be specified (e.g., shared memory).
- The inputs and outputs of each functional block may be binary signals (0/1), analog signals, or serial synchronous or asynchronous communication lines.
- The character of each signal line and its function and name should be completely described, with the exception that voltage and current levels need not be specified.

Computer-Based Systems

For computer-based systems, the application should describe the system characteristics that the self-diagnostics and on-line testing will detect to indicate computer system failures. The application should also describe the interconnections of test and diagnostics with the system functional hardware and software. Specific machine-dependent items that may not be available during design certification should be included in the DAC. Overall maximum system reaction time should be specified for each input from the sensor to major plant systems or equipment such as actuators or pump controllers (e.g., the plant control system).

The mechanisms available to modify software (including programming, calibration data, or configuration data) in the installed systems, either directly or via network connections, should be identified. Design provisions that enable applicants to prevent unauthorized changes should be described.

The material identified above should be discussed in sufficient detail to allow Staff determination that the applicant has met the requirements related to postulated single failures, common-mode failures, appropriate signal isolation (both electrical and logic isolation), and other aspects of the Staff's review as described in Appendices 7.1-A and 7.1-C.

3.4 Section 7.8

In addition to the systems described in Reg. Guide 1.70, advanced light-water reactors (ALWRs) should include systems to mitigate the consequences of anticipated transients without scram (ATWS).

Description

The SAR should describe the I&C systems provided for ATWS mitigation and their compliance with the ATWS rule, 10 CFR 50.62. For plants that have computer-based protection systems (RTS or ESFAS), Section 7.8 should discuss the systems provided specifically to comply with the defense-in-depth and diversity criteria. These systems include the hardwired backup controls and instrumentation credited for compliance with the manual means of component actuation, and any automatic systems provided specifically to achieve the necessary level of defense-in-depth and diversity. (See BTP HICB-19.)

Section 7.8 should include design basis information for the diverse actuation systems. The ATWS, hardwired displays and controls, and automatic diverse actuation systems may have different design bases. Section 4 of IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," outlines a set of design basis information that would be acceptable. Any supporting systems should be identified and described (reference may be made to other sections of the SAR).

Diverse I&C systems should be described to a level of detail commensurate with those described for Sections 7.2 and 7.3.

Analysis

Analysis should be provided to demonstrate how the requirements of 10 CFR 50.62, General Design Criteria 1, 13, and 19, applicable regulatory guides, and other appropriate criteria and standards are satisfied. For applications involving computer-based RTS or ESFAS, the analysis should also demonstrate that the design is consistent with the assumptions of the D-in-D&D analysis described above.

3.5 Section 7.9

I&C systems utilizing digital computers may also use data communication.

Description

The SAR should describe the data communication systems provided to support the I&C systems identified in Section 7.1. For data communication systems that support I&C functions in systems important to safety, Section 7.9 should provide the design basis information recommended by Section 4 of IEEE Std 603. Design basis requirements should also be provided for data communication systems that support other I&C functions identified in Section 4 of IEEE Std 603. IEEE Std 603 outlines a set of design basis information that would be acceptable for these systems. Any supporting systems should be identified and described (reference may be made to other sections of the SAR).

Final system drawings or DAC/ITAAC should be provided as described for the supported systems above. The DAC should describe the criteria that an acceptable design will meet for the following subjects, or the final design should address the following subjects:

- All data communication protocols used should be identified and described. This description should include discussion of error handling together with the method for dealing with the indeterminacy and extra traffic that error handling might engender.
- The provisions for bypassed or inoperable status should be described, along with the coordination of communication system bypass or inoperable status with the bypass and inoperable status of the safety system of which the communication system is part.
- Timing and data rate requirements should be included. Message formats and the approximate frequency at which each type of message appears on each data link should be included.
- The maximum traffic rate (messages per second and bytes per second) on each line should be specified, and the conditions under which these rates will occur should be identified.
- The method for establishing communication independence between redundant channels of a communication system and between safety and non-safety systems should be described.

Final system drawings may not be available at the design certification stage. In that case, the minimum set of information described above for Sections 7.2 through 7.7 will be acceptable for Section 7.9.

Analysis

Analysis of each data communication system should be provided to demonstrate that the requirements applicable to the I&C functions supported by the data communication systems are satisfied. For data

communication systems this analysis should demonstrate that the system design, including error handling performance, supports the timing and reliability requirements of the supported systems.

Data communication system failure modes should be identified, and the effect of these failures on supported systems should be analyzed. Such analysis may be incorporated into the failure mode and effects analysis of each supported system.

The immunity of the data communication system to design basis EMI/RFI should be demonstrated. This analysis should address both resistance to noise and prevention of fault propagation between redundant channels or systems.

For data communication systems that support RTS or ESFAS functions, the analysis should demonstrate that the design is consistent with the assumptions of the D-in-D&D analysis.

3.6 *Standardized Safety Analysis Report*

The Staff's safety determination for design certification of a standardized design is based upon the material in the SAR. To the extent that design detail or other information reviewed in the course of inspections or audits is necessary for the Staff to reach a safety conclusion, that design detail or other information should be available to the Staff. The design detail may be an amendment to or reference in the SAR.

3.7 *Tier 1, Tier 2, and Tier 2* Material*

Material identified as Tier 1 should be that information necessary to ensure that significant features of the certified design application which the Staff is relying upon to make a safety determination are captured in the DCD. Two important factors should be balanced when identifying Tier 1 material:

- The safety significance of the design feature or commitment to the Staff's safety determination.
- The likelihood that the design feature or commitment will have to be changed in the future.

If the reviewer concludes that the details of a particular design feature or commitment are likely to change (the applicant may suggest such candidates), then it is appropriate to limit the amount of detail included in Tier 1. DAC that describe the necessary design acceptance criteria for such features should be provided in lieu of the design detail. Sufficient additional detail, however, should be specified in the SAR Tier 2 material in order for the Staff to make a final safety determination for certification. If the Staff believes these additional Tier 2 details are critical to the safety determination, they should be identified as Tier 2* material in the SER and DCD, thereby requiring prior NRC staff approval if changed.

For I&C systems, Tier 1 material consists of the certified design description, ITAAC, and interface requirements as defined in 10 CFR 52.47(a)(1)(ii) and (vii). The certified design description is composed of narrative descriptions and schematic drawings needed to describe the significant design features certified by the Staff.

Design details and commitments that are important to the NRC's safety determination, but are subject to change (e.g., technology advancement and standard revisions), should be identified as Tier 2* material in the SER and the DCD. For I&C systems, Tier 2* information will normally be limited to computer design, data communication design, setpoint methodology, commercial-grade item dedication, and equipment qualification, including electromagnetic compatibility.

4. Review Procedures

The reviewer should confirm early in the review that the basic types of information outlined above are available to support the review.

The review should confirm that the CDM contains an appropriate set of Tier 1 material, and that appropriate Tier 2* material is identified.

C. References

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

Memorandum from W. T. Russell to B. A. Boger, et al. "Reviewer Guidance for Design Certification Reviews — Certified Design Descriptions; Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC); Applicant SAR Level of Detail; and Staff SER Documentation." December 28, 1992.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Regulatory Guide 1.70. "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants." Office of Standards Development, U.S. Nuclear Regulatory Commission, November 1978.

SECY-90-241. "Level of Detail Required for Design Certification Under Part 52." July 11, 1990.

SECY-90-377. "Requirements for Design Certification under 10 CFR 52." November 8, 1990.

SECY-92-053. "Use of Design Acceptance Criteria During 10 CFR 52 Design Certification Reviews." February 19, 1992.

SECY-92-287. "Form and Content of a Design Certification Rule." August 18, 1992.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.

Branch Technical Position HICB-17

Guidance on Self-Test and Surveillance Test Provisions

A. Background

This branch technical position (BTP) provides guidelines for reviewing the design of the self-test and surveillance test provisions. These guidelines are based on reviews of applicant/licensee submittals and vendor topical submittals describing self-test and surveillance test assumptions, terminology, methodology, and experience gained from NRC inspections of operating plants.

1. Regulatory Basis

10 CFR 50.55a(h), "Protection Systems," requires in part that protection systems satisfy the criteria of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." Section 4.10 of ANSI/IEEE Std 279 requires the capability to test and calibrate protection system channels and devices. Section 4.21 states that protection systems must be designed to facilitate the recognition and location of malfunctioning components or modules. Additionally, Section 4.2 requires that any single failure within the protection system shall not prevent proper protective action at the system level. Reg Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," which endorses IEEE Std 603, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," contains similar requirements. Reg. Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Protection Systems," which endorses ANSI/IEEE Std 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," amplifies this requirement by noting that the protection system must be capable of accomplishing the required protective function in the presence of any single detectable failure concurrent with all identifiable, but non-detectable failures. Consequently, self-testing and periodic testing are important elements in a design's ability to meet the single-failure criterion.

10 CFR 50 Appendix A, General Design Criterion (GDC) 21, "Protection System Reliability and Testability," requires in part that the protection system be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. It also requires a design that permits periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

10 CFR 50 Appendix A, GDC 22, "Protection System Independence," requires in part that the protection system be designed to ensure that the effects of natural phenomena, and of normal operating, maintenance and testing do not result in loss of protection function.

10 CFR 50 Appendix B, Criterion 12, "Control of Measuring and Test Equipment," requires in part that measures be established to ensure that measuring and testing devices used in activities affecting quality are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy within necessary limits.

2. Relevant Guidance

Reg. Guide 1.22, "Periodic Testing of Protection System Actuation Functions," describes acceptable methods of including actuation devices in the periodic tests of the protection system during reactor operations.

Reg. Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," describes an acceptable method of complying with the requirements of ANSI/IEEE Std 279 with regard to indicating the inoperable status of a portion of the protection system, systems actuated or controlled by the safety system, or essential auxiliary support systems.

Reg. Guide 1.53 "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," clarifies the application of the single-failure criterion and endorses ANSI/IEEE Std 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems." ANSI/IEEE Std 379 discusses the credit taken for testing in the application of the single-failure criterion.

Reg. Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," states that the requirements and recommendations of IEEE Std 338, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," are considered acceptable methods for the periodic testing of protection systems (subject to the specific exceptions discussed in Reg. Guide 1.118). IEEE Std 338 provides design and operational criteria for the performance of periodic and automatic testing; its requirements and criteria are supplementary to ANSI/IEEE Std 279 and IEEE Std 603.

Reg. Guide 1.152, . "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and IEC Std 880, "Software for Computers in the Safety Systems of Nuclear Power Stations," recommend characteristics for self-testing in digital computer-based protection systems.

Reg. Guide 1.153 "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as an alternative to ANSI/IEEE Std 279.

3. Definitions

Periodic tests are tests performed at scheduled intervals to detect failures and verify operability (IEEE Std 338). Periodic tests include surveillance tests.

A *self-test* is a test or series of tests, performed by a device upon itself. Self-test includes on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics.

Surveillance tests are tests conducted specifically to confirm compliance with technical specification surveillance requirements.

A *watchdog timer* is a form of interval timer that is used to detect a possible malfunction (ANSI/IEEE Std C37.1, "Standard Definitions, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control").

4. Purpose

The purpose of this BTP is to provide guidance for NRC staff to verify that the previously cited regulatory basis and standards are met by an applicant/licensee's submittal. The objectives of this BTP are to confirm that:

- The safety system (including self-test) is designed for in-service testability commensurate with the safety functions to be performed through all modes of plant operation.
- The positive aspects of self-test features are not compromised by the additional complexity that may be added to the safety system by the self-test features.
- Hardware and software design support the required periodic testing.
- Failure modes assumed to be detectable by the single-failure analysis are in fact detectable. Failures may be detectable by observing operational characteristics as well as other methods.

B. Branch Technical Position

1. Introduction

Digital computer-based instrumentation and control systems are prone to different kinds of failures than are traditional analog systems. Self-testing and watchdog timers may reduce the time to detect and identify failures, but are not a guarantee of hardware or software error detection. Computer self-testing is most effective at detecting random hardware failures.

Surveillance testing taken together with automatic self-testing should provide a mechanism for detecting all detectable failures.

The characteristics of digital systems must be considered in the review of technical specification surveillance features. Architectural differences between digital and analog systems warrant careful consideration during the review of surveillance test provisions. Furthermore, the concepts used to determine test intervals for hardware-based systems do not directly apply to the software used in digital computer-based instrumentation and control systems. Therefore, previous reliability analysis used to establish test intervals may not apply.

Similar reviews are performed as necessary to verify the self-test and periodic test provisions for non-safety systems.

2. Information to be Reviewed

Applicant/licensee's technical description of surveillance and self-test features, single-failure analyses, failure mode and effect analyses, and plant technical specifications should be considered in the review.

3. Acceptance Criteria

Surveillance test and self-test features for digital computer-based protection systems should conform to the guidance of Reg. Guide 1.22, Reg. Guide 1.118, and Reg. Guide 1.153, "Criteria for Power, Instrumentation,

and Control Portions of Safety Systems." Bypasses necessary to enable testing should conform with the guidance of Reg. Guide 1.47.

Failure Detection

Failures detected by hardware, software, and surveillance testing should be consistent with the failure detectability assumptions of the single-failure analysis and the failure modes and effects analysis.

Self-Test Features

Digital computer-based instrumentation and control systems should include self-test features to confirm computer system operation upon system initialization.

Digital computer-based instrumentation and control systems should generally include continuous self-testing. Some small, stand-alone, embedded digital computers may not need self-testing. Typical self-tests include monitoring memory and memory reference integrity, using watch-dog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity.

Other self-testing features that are candidates for incorporation into digital computer-based I&C systems include: plausibility checks for intermediate results, evaluation using different methods, ranges of variables, array bound checking, well-defined outputs for detected failures, reporting of errors for which error recovery techniques are used, use of counters and reasonableness traps, correctness verification of transferred parameters, and the use of assertions (see IEC Std 880). BTP HICB-14 discusses a number of functional characteristics for software design outputs, such as robustness and timing, which could give rise to self-testing features.

Hardware and software used to perform automatic self-testing should be of equivalent safety classification, quality, and reliability as the tested system. The design should maintain channel independence, maintain system integrity, and meet the single-failure criterion during testing. The scope and extent of interfaces between software that performs protection functions and software for other functions such as testing should be designed to minimize the complexity of the software logic and data structures. The hardware and software used to perform automatic self-testing should be of equivalent safety classification of the tested system, unless physical, electrical, and communications independence are maintained such that no failure of the test function can inhibit the performance of the safety function.

The positive aspects of self-test features should not be compromised by the additional complexity that may be added to the safety system by the self-test features. The improved ability to detect failures provided by the self-test features should outweigh the increased probability of failure associated with the self-test feature.

Self-test functions should be verified during periodic functional tests.

Periodic Testing

Systems should provide the ability to conduct periodic testing consistent with the technical specifications and plant procedures.

As required by ANSI/IEEE Std 279, Section 4.13 and Reg. Guide 1.47, if the protective action of some part of a protection system is bypassed or deliberately rendered inoperative for testing, that fact should be

continuously indicated in the control room. Provisions should also be made to allow operations staff to confirm that the system has been properly returned to service.

Reg. Guide 1.118 states in part that test procedures for periodic tests should not require makeshift test setups. For digital computer-based systems, makeshift test setups, including temporary modification of code or data that must be appropriately removed to restore the system to service, should be avoided.

If automatic self-test features are credited with automatically performing surveillance test functions, provisions must be made to confirm the execution of the automatic tests during plant operation. The capability to periodically test and calibrate the automatic test equipment must also be provided.

Hardware and software used to perform periodic self-testing should be of equivalent safety classification and quality as the tested system. The design should maintain channel independence, maintain system integrity, and meet the single-failure criterion during testing. Commercial digital computer-based equipment used to perform periodic testing should be appropriately qualified for its function.

Actions on Failure Detection

The design should have either the automatic or manual capability to take compensatory action upon detection of any failed or inoperable component. The design capability and plant technical specifications, operating procedures, and maintenance procedures should be consistent with each other.

Plant procedures should specify manual compensatory actions and mechanisms for recovery from automatic compensatory actions.

Mechanisms for operator notification of detected failures should comply with the system status indication provisions of IEEE Std 603 and should be consistent with, and support, plant technical specifications, operating procedures, and maintenance procedures.

4. Review Procedures

The surveillance test and self-test features of each digital computer-based module, as well as each system incorporating digital computers, are reviewed to verify conformance with acceptance criteria.

The review of surveillance test provisions should confirm that these provisions are adequate to fulfill the fundamental intent of each surveillance test. Because of design and architectural differences between analog and digital systems, traditional provisions for analog systems may not be adequate for digital computer-based systems.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

ANSI/IEEE Std C37.1-1987. "Standard Definitions, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control."

IEC Std 880. "Software for Computers in the Safety Systems of Nuclear Power Stations." IEC Publication 1986.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

Regulatory Guide 1.22. "Periodic Testing of Protection System Actuation Functions." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.53. "Application of the Single-Failure Criterion to Nuclear Power Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.118. "Periodic Testing of Electric Power and Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1995.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Branch Technical Position HICB-18

Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

A. Background

This branch technical position (BTP) provides guidelines for reviewing the use of programmable logic controllers (PLCs) in instrumentation and control (I&C) systems. These guidelines are based on reviews of licensee submittals and the analysis of PLC-related issues documented in NUREG/CR-6090, "The PLC and Its Application in Nuclear Reactor Protection Systems."

1. Regulatory Basis

10 CFR 50 Appendix A, General Design Criterion 1, "Quality Standards and Records," requires in part that "structures, systems, and components important to safety shall be designed, fabricated, and tested to quality standards commensurate with the importance of the safety functions to be performed."

10 CFR 50 Appendix A, General Design Criterion 21, "Protection System Reliability and Testability," requires in part that "the protection system shall be designed for high functional reliability . . . commensurate with the safety functions to be performed."

2. Relevant Guidance

Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," provides guidance for complying with the requirements for safety systems that use digital computer systems. The guidance in Reg. Guide 1.152 refers to IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

NUREG/CR-6090 covers the application of PLCs to nuclear reactors. The guidance in this NUREG will aid the reviewer in the evaluation of an I&C system containing one or more PLCs.

NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," describes recommended practices in the use of common PLC programming languages.

EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," provides more detail on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors.

NUREG/CR-6421 discusses graded acceptance processes for commercial off-the-shelf software used in reactor applications. The guidance in this NUREG will aid the reviewer in the evaluation of acceptance processes that are part of commercial dedications of PLC embedded, operating system, and programming tools software.

3. Purpose

The purpose of this BTP is to provide guidance for NRC staff to verify conformance with the previously cited regulatory bases and standards in the design of digital computer systems using PLCs. This BTP has two objectives:

- To ensure that embedded and operating system software and programming tools are reviewed, and the appropriate acceptance criteria are applied.
- To ensure that the PLC application programs (e.g., ladder-logic programs) are developed using an appropriate software development process.

B. Branch Technical Position

1. Introduction

The PLC is typically a commercial-grade computer system that employs a particular high-level language, such as ladder logic, for the purpose of monitoring and controlling industrial processes. The PLC is a computer system, and as such, the software used on it should be designed and implemented using a process that conforms with the guidance in BTP HICB-14. The detailed design and implementation activities of such a process, however, may be easier to implement for applications produced using the high-level languages typical of PLCs.

PLC applications are usually coded using ladder logic or sequential function charts. The resulting programs can be expected to use standard functions provided by the PLC vendor. Standard functions may have considerable industrial experience. This experience may supplement other methods of evaluating the quality of the PLC program, provided that the experience is commensurate with the reactor application, and that field trouble reports are generated, available, and reviewed. If existing industrial experience cannot be shown to be applicable to the safety system application, it is of limited use.

Appendix 7.0-A, Section C.3 describes the advantages of using high-level languages such as ladder logic and function charts. It also describes precautions that should be observed when reviewing systems specified or designed using such languages.

Many vendors of PLCs allow programming languages other than ladder-logic to be used (e.g., C). The reviewer should take this possibility into account and assess the impact of using programming languages on the design of the PLC and on the application.

An I&C system built using PLCs contains a number of purchased components: the hardware, including the processor, memory, I/O equipment, communications equipment, terminals, etc.; and the software, consisting of one or more operating systems, interpreters, compilers, libraries, configuration software, tools, and variations thereof. This purchased equipment should be of a quality appropriate to the proposed application.

Other issues associated with the application of digital computers to I&C systems (e.g., maintenance, verification and validation, EMI, and calibration) apply and should be reviewed. The Staff should not accept an argument that the PLC is somehow simpler or different from a computer and hence does not require the rigorous review that a computer system would receive.

2. Information to be Reviewed

Information to be reviewed is contained in the safety analysis report (SAR), revisions to the SAR, license amendment requests, topical reports, or other applicant/licensee documentation. Inspections, tests, analyses, and acceptance criteria (ITAAC) or detailed design documents describe designs, tests, analyses, or other methods of demonstrating that design commitments have been satisfied. Information that is not contained in the licensee/applicant's submittal should be available for review.

3. Acceptance Criteria

Purchased PLC hardware, embedded, programming, and operating system software, and peripheral components should be qualified to a level commensurate with the system they are designed to support. EPRI TR-106439 describes an acceptable process for qualifying commercial systems. NUREG/CR-6421 provides more detail on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors for purchased PLC software. See the discussion of the commercial dedication of predeveloped software (PDS) in Appendix 7.0-A.

PLC hardware, embedded and operating system software, and peripheral components built specifically for nuclear power plant applications should meet the appropriate quality criteria. The embedded and operating system software should meet the acceptance criteria contained in BTP HICB-14, appropriately graded for the application in which the PLC will be used.

The application software (ladder logic or other) should meet the acceptance criteria contained in BTP HICB-14 commensurate with the system it is designed to support. Application software should conform with the recommended practices of NUREG/CR-6463.

Tools for developing application software or loading it into the PLC should be qualified to a level commensurate with the system they are designed to support.

PLC-based functions should conform with the guidance regarding real-time performance and testing outlined in BTP HICB-21 and BTP HICB-17.

Administrative or hardware lockout controls that prevent casual modification of the PLC program should be in place. This is particularly important because many PLCs are designed so that their programming is easy to modify. All program changes must be under configuration management control. In particular, administrative procedures for maintaining control of the software implemented in the PLC should be detailed in the configuration management plan.

4. Review Procedures

PLC applications should be reviewed in the same manner as other digital computer instrument and control system applications. SRP Appendix 7.0-A, Section 7.1 and BTPs HICB-14 and HICB-17 describe these review procedures.

C. References

EPRI Topical Report TR-106439. "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." Electric Power Research Institute, October 1996.

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

NUREG/CR-6090. "The PLC and Its Application in Nuclear Reactor Protection Systems." September 1993.

NUREG/CR-6421. "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications." June 1996

NUREG/CR-6463. "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems." June 1996.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Safety Evaluation by the Office of Nuclear Reactor Regulation. "EPRI Topical Report TR-106439." May 1997.

Branch Technical Position HICB-19

Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems

A. Background

Digital instrumentation and control (I&C) systems are vulnerable to common-mode failure caused by software error, which defeats the redundancy achieved by hardware architecture. In NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," the Staff documented a defense-in-depth and diversity (D-in-D&D) analysis of a digital computer-based reactor protection system, in which defense against common-mode failures was based upon an approach using a specified degree of system separation between echelons of defense. Subsequently, in SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors," the Staff included discussion of its concerns about common-mode failures in digital systems used in nuclear power plants. As a result of the reviews of ALWR design certification applications that used digital protection systems, the Staff documented its position with respect to common-mode failures in digital systems and defense-in-depth. This position was documented as Item II.Q in SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," and was subsequently modified in the associated Staff Requirements Memorandum. Based on experience in the detailed reviews, the NRC staff has established acceptance guidelines for D-in-D&D assessments as described in this branch technical position.

1. Regulatory Basis

10 CFR 50.55a(h), "Protection Systems," requires in part that protection systems satisfy the criteria of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." Section 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," requires in part various diverse methods of responding to anticipated transients without scram (ATWS).

10 CFR 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."

10 CFR 50 Appendix A, GDC 22, "Protection System Independence," requires in part that the effects of natural phenomena, postulated accident conditions, normal operating, maintenance, and testing not result in the loss of protective 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."

10 CFR 50 Appendix A, GDC 24, "Separation of Protection and Control Systems," requires in part that "Interaction of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

10 CFR 50 Appendix A, 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."

2. Relevant Guidance

Reg. Guide 1.53 "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," clarifies the application of the single-failure criterion (GDC 21) and endorses ANSI/IEEE Std 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," providing supplements and an interpretation.

Reg. Guide 1.153 "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as an alternative to ANSI/IEEE Std 279.

NUREG-0493 is the first formal defense-in-depth and diversity assessment of a reactor protection system, the RESAR-414.

NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," documents several D-in-D&D analyses performed after 1990, and presents a method for performing such analyses.

The Staff Requirements Memorandum on SECY 93-087 describes the NRC position on defense-in-depth and diversity.

3. Purpose

The purpose of this branch technical position is to provide guidance for review of an applicant/licensee's D-in-D&D assessment and design of manual controls and displays to ensure that the requirements of the NRC position on D-in-D&D for I&C systems incorporating digital computer-based reactor trip systems (RTS) or engineered safety features actuation systems (ESFAS) are followed. This branch technical position has three objectives:

- To verify that adequate diversity has been provided in a design to meet the criteria established by the NRC's requirements.
- To verify that adequate defense-in-depth has been provided in a design to meet the criteria established by the NRC's requirements.
- To verify that the displays and manual controls for critical safety functions initiated by operator action are diverse from computer systems used in the automatic portion of the reactor protection system and ESFAS.

B. Branch Technical Position

1. Introduction

Based on experience in detailed reviews, the Staff has established acceptance guidelines for D-in-D&D assessments. The Staff has identified four echelons of defense against common-mode failures:

- Control system — The control echelon consists of that non-safety equipment which routinely prevents reactor excursions toward unsafe regimes of operation, and is used for normal operation of the reactor.
- RTS — The reactor trip echelon consists of that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.
- ESFAS — The ESFAS echelon consists of that safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment).
- Monitoring and indicators — The monitoring and indication echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

As a result of the reviews of ALWR design certification applications that used digital protection systems, the NRC established the following position on D-in-D&D for the advanced reactors. Points 1, 2, and 3 of this position apply to digital system modifications to operating plants.

1. The applicant/licensee should assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.
2. In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.
3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, should be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
4. A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.

The above position is based on the NRC concern that software design errors are a credible source of common-mode failures. Software cannot be proven to be error-free, and therefore is considered susceptible to common-mode failures because identical copies of the software are present in redundant channels of safety-related systems. To defend against potential common-mode failures, the Staff considers high quality,

defense-in-depth, and diversity to be key elements in digital system design. High-quality software and hardware reduces failure probability. However, despite high quality of design, software errors may still defeat safety functions in redundant, safety-related channels. Therefore, as set forth in points 1, 2, and 3 above, the Staff requires that the applicant/licensee perform a D-in-D&D assessment of the proposed digital I&C system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed. In this assessment, the applicant/licensee should analyze design basis events (as identified in the safety analysis report). If a postulated common-mode failure could disable a safety function that is required to respond to the design basis event being analyzed, then a diverse means of effective response (with documented basis) is necessary. The diverse means may be a non-safety system, automatic, or manual if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time.

The methods and results of D-in-D&D assessments used in ALWR design certification submissions are documented in NUREG/CR-6303. This document describes an acceptable method for performing such assessments.

In those cases where the RTS or ATWS mitigation system in an operating plant is modified, the requirements of the ATWS rule, 10 CFR 50.62, must be met. 10 CFR 50.62 requires that the ATWS mitigation system be composed of diverse equipment from the RTS. Therefore implementation of RTS digital modifications by a different manufacturer from the ATWS mitigation system satisfies the diversity requirements of 10 CFR 50.62. This is also true in the complementary case in which an existing ATWS system is modified by the inclusion of digital equipment and the RTS is already digital. If "sufficient" difference in manufacturer cannot be demonstrated, then a case-by-case assessment of the RTS and ATWS mitigation system designs should be conducted. This analysis should include differences such as manufacturing division (within a corporate entity), software (including implementation language), equipment (including CPU architecture), function, people (design and verification/validation team), and initiating events.

2. Information to be Reviewed

The information to be reviewed is the D-in-D&D assessment conducted by the applicant/licensee.

3. Acceptance Criteria

The D-in-D&D assessment submitted by the applicant/licensee should demonstrate compliance with the four-point position described above. To reach a conclusion of acceptability, the following four conclusions should be reached and supported by summation of the results of the analyses:

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.
2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant/licensee should either (1)

demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

3. When a failure of a common element or signal source shared between the control system and the RTS is postulated, and (1) this common-mode failure results in a plant response that requires reactor trip, and (2) the common-mode failure also impairs the trip function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the RTS function. The diverse means should ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.

When a failure of a common element or signal source shared between the control system and the ESFAS is postulated, and (1) this common-mode failure results in a plant response that requires ESF, and (2) the common-mode failure also impairs the ESF function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the ESF function. The diverse means should ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.

Interconnections between reactor trip and ESFAS (for interlocks providing for (1) reactor trip if certain ESFs are initiated, (2) ESF initiation when a reactor trip occurs, or (3) operating bypass functions) are permitted provided that it can be demonstrated that functions required by the ATWS rule (10 CFR 50.62) are not impaired.

4. No failure of monitoring or display systems should influence the functioning of the reactor trip system or the ESFAS. If plant monitoring system failure induces operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation, the analysis should demonstrate that such operator-induced transients will be compensated by protection system function.

The adequacy of the diversity provided with respect to the above criteria must be justified. NUREG/CR-6303, in Section 3.2, describes six types of diversity and describes how instances of different types of diversity might be combined into an overall case for the sufficiency of the diversity provided. Typically, several types of diversity should exist, some of which should exhibit one or more of the stronger attributes listed in NUREG/CR-6303 for the diversity type. Functional diversity and signal diversity are considered to be particularly effective. The following cautions should be noted where applicable:

- The justification for equipment diversity, or for the diversity of related system software such as a real-time operating system, must extend to the equipment's components to ensure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby incorporating common failure modes. Claims for diversity based just on difference in manufacturer name are insufficient without consideration of the above.
- With respect to software diversity, experience indicates that independence of failure modes may not be achieved in cases where multiple versions of software are developed to the same software requirements. Other considerations, such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity.

Manual displays and controls provided for compliance with the fourth point of the NRC position on D-in-D&D should be sufficient to both monitor the plant states and to actuate systems required by the control room operators to place the nuclear plant in a hot-shutdown condition. In addition, the displays and controls should monitor and control the following critical safety functions: reactivity level, core heat removal, reactor coolant inventory, containment isolation, and containment integrity. This additional manual capability is necessary in advanced reactors because all of the protection and control systems are digital-computer-based, and thus vulnerable to common-mode failure. The manual capability should consist of hardwired, system-level controls and displays. These controls provide plant operators with information and control capabilities that are not subject to common-mode failures caused by software errors in the plant's automatic digital I&C safety system.

The point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs, but should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. To achieve system-level actuation at the lowest possible level in the safety system architecture, the controls may be hardwired either to analog components or to simple (e.g., the component function can be completely demonstrated by test), dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic.

These displays may include digital components that are exclusively dedicated to the display function. The functional characteristics (e.g., range, accuracy, time response) of the displays provided should be sufficient to provide operators with the information needed to place and maintain the plant in a hot-shutdown condition.

Human-factors engineering principles and criteria should be applied to the selection and design of the displays and controls. The human-performance requirements should be described and related to the plant safety criteria. Recognized human-factors standards and design techniques should be employed to support the described human-performance requirements.

4. Review Procedures

The applicant/licensee's D-in-D&D analysis is reviewed against the above acceptance criteria using the detailed guidance of NUREG/CR-6303. Emphasis should be given to the following topics:

System Representation as Blocks

The system being assessed is represented as a block diagram; the inner workings of the blocks are not necessarily shown. Diversity is determined at the block level.

Documentation of Assumptions

Assumptions made to compensate for missing information in the design description materials or to explain particular interpretations of the analysis guidelines as applied to the system are documented by the applicant/licensee.

Identification of Alternate Trip or Initiation Sequences

Thermal-hydraulic analyses, using best-estimate (realistic assumptions) methods, of the sequence of events that would occur if the primary trip channel were to fail to trip the reactor or actuate ESF are included in the

assessment. (Coordination with the Reactor Systems Branch, the Mechanical Engineering Branch, and the Materials and Chemical Engineering Branch is necessary in reviewing these analyses.)

Identification of Alternative Mitigation Capability

For each design-basis event, alternate mitigation actuation functions are identified that will prevent or mitigate core damage and unacceptable release of radioactivity.

Where a common-mode failure is compensated by a different automatic function, a basis is provided which demonstrates that the different function constitutes adequate mitigation for the conditions of the event.

Where operator action is cited as the diverse means for response to an event, the applicant/licensee should demonstrate that adequate information (indication) and sufficient time is available for operator action.

Justification for Not Correcting Specific Vulnerabilities

If any identified vulnerabilities are not addressed by provision of alternate trip, initiation, or mitigation capability, justification should be provided. Justification may be based upon the availability of systems outside of the scope of the analysis that act to prevent or mitigate the event of concern. For example, I&C system vulnerability to common-mode failure affecting the response to large-break loss-of-coolant accidents and main steam line breaks has been accepted in the past. This acceptance was based upon the provision of primary and secondary coolant system leak detection, and pre-defined operating procedures that together enable operators to detect small leaks and take corrective actions before a large break occurs.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

NUREG-0493. "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System." March 1979.

NUREG/CR-6303. "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems." December 1994.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.53. "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

SECY 91-292. "Digital Computer Systems for Advanced Light-Water Reactors." September 1991.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.

Branch Technical Position HICB-20

Not used.

Branch Technical Position HICB-21

Guidance on Digital Computer Real-Time Performance

A. Background

This branch technical position (BTP) provides guidelines for reviewing digital system real-time performance and system architectures in instrumentation and control (I&C) systems. These guidelines are based on reviews of licensee submittals and the analysis of these issues documented in NUREG/CR-6083, "Reviewing Real-Time Performance of Nuclear Reactor Safety Systems," and NUREG/CR-6082, "Data Communications."

1. Regulatory Basis

10 CFR 50.55a(h), "Protection Systems," requires in part that protection systems satisfy the criteria of IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." Section 3 of the standard requires, in part, specification of the protection system design basis, including system response times. Section 4.1 requires in part that the protection system automatically initiate protective action within the range of performance enumerated in the design basis.

10 CFR 50 Appendix A, General Design Criterion (GDC) 10, "Reactor Design," requires in part that control and protection systems be designed with appropriate margin to ensure that specified acceptable fuel damage limits are not exceeded. This includes timing and performance margins.

10 CFR 50 Appendix A, GDC 12, "Suppression of Reactor Power Oscillations," requires in part that reactor power oscillations are either (1) not possible or (2) detected and suppressed. This requirement places strict real-time constraints on any protection system components that detect and suppress power oscillations.

10 CFR 50 Appendix A, GDC 13, "Instrumentation and Control," requires in part that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operations, for anticipated operational occurrences, and for accident conditions as appropriate to ensure adequate safety. Digital instrumentation must respond quickly enough so that the behavior of variables can be ascertained by operators.

10 CFR 50 Appendix A, GDC 19, "Control Room," requires in part that applicants establish a control room from which actions can be taken to operate the nuclear power unit safely under normal conditions, and to maintain the nuclear power unit in a safe condition during an accident. In addition, a remote shutdown capability is required to permit the reactor to be safely shut down.

10 CFR 50 Appendix A, GDC 20, "Protection System Functions," requires in part that the reactor protection system provide automatic initiation so that fuel design limits are not exceeded and so that accidents are sensed and mitigated. Both of these goals require timely operation of protection system components, thus establishing the timing requirements for detecting parameters exceeding their setpoints, and equipment actuation in the protection system.

10 CFR 50 Appendix A, GDC 21, "Protection System Reliability and Testability," requires in part the high functional reliability of safety systems. Timely operation is necessary for high functional reliability of safety systems.

10 CFR 50 Appendix A, GDC 23, "Protection System Failure Modes," requires in part the protection system to be designed so that if it fails, it fails into a safe state given the anticipated failure modes and conditions in which the failure occurs. This is a design architectural issue aimed at staying within timing limits.

10 CFR 50 Appendix A, GDC 25, "Protection System Requirements for Reactivity Control Malfunctions," requires, in part, reactivity control to prevent fuel design limits from being exceeded. This requires timely operation of the protection features of the reactivity control system.

10 CFR 50 Appendix A, GDC 28, "Reactivity Limits," requires in part a limited reactivity rate-of-change to prevent (1) fuel limits from being exceeded and (2) a non-coolable core geometry. The protection system must meet the timing requirements imposed by this criterion.

10 CFR 50 Appendix A, GDC 29, "Protection Against Anticipated Operational Occurrences," requires in part defense against anticipated operational transients to ensure an extremely high probability of accomplishing safety functions. To ensure this, the protection system must be demonstrated to operate within the time constraints of each anticipated operational transient.

2. Relevant Guidance

Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," which is a system-level standard that contains some requirements related to performance and timing. This standard requires in part that a reactor safety system have a documented design basis consisting of the following:

- Section 4.4 — limits, ranges, and rates of change of variables should be included in the documented design basis.
- Section 4.5 — minimum times should be specified for manual actions, below which such actions cannot be considered to be accomplished.
- Section 4.10 — critical points in time should be specified for:
 - Initiation of protective action.
 - Completion of protective action.
 - Time when automatic control of protective action is required.
 - Time when protective system may be returned to normal.

In addition, timely automatic control action is required when events occur too quickly for operator intervention.

Reg. Guide 1.152, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," endorses the guidance of IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power

Generating Stations," as an acceptable method for complying with the NRC's regulations for safety systems that use digital computers. The main body of IEEE Std 7-4.3.2 does not add to the guidance of IEEE Std 603 regarding timing and performance. However, Annexes E and F, although not endorsed by Reg. Guide 1.152, contain useful guidance on certain timing and architectural requirements.

Annex E E.2.2.1(k) states that timing, response time, and performance requirements must be validated and verified.

E.2.2.8.2 states that sizing and timing analyses are suggested to assess the feasibility of meeting response time and performance requirements mentioned in E.2.2.1(k).

Annex F F.2.3.3(b) states that sizing and timing anomalies in requirements are considered abnormal conditions.

F.2.3.5(g) states that failure of code to run within timing and sizing constraints imposed by validated requirements is considered an abnormal condition.

Draft Reg. Guide DG-1045, proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems," endorses ISA-S67.04, Part 1, "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants," as an acceptable method for initially setting and maintaining instrument calibrations in nuclear reactor I&C systems in order to ensure their proper response on demand. System time delays are an important consideration in establishing instrument setpoints.

In addition to the above, NUREG/CR-6082 describes data communication systems, including aspects related to system performance and timing. NUREG/CR-6083 describes real-time systems with respect to performance, timing, and complexity. These documents include detailed guidance for reviewing such systems, and a glossary of related terms.

3. Purpose

The purpose of this BTP is to provide guidance for NRC staff to verify conformance with the previously cited regulatory bases and standards in the design of digital computer systems. This BTP has three objectives:

- To verify that system timing requirements calculated from the design basis events and other criteria have been allocated to the digital computer portion of the system as appropriate, and have been satisfied in the digital system design.
- To make the reviewer aware that more extensive efforts are required to verify certain timing design and implementation techniques, such as interrupts.
- To assess the technical basis for concluding that the installed plant systems perform as predicted when enlarged from small-scale or partial-system engineering prototypes used in the design phases.

B. Branch Technical Position

1. Introduction

System architecture needs to be considered in evaluating real-time performance.

Digital system architecture affects performance because communication between components of the system takes time, and allocation of functions to various system components affects timing. The architecture may also affect timing because an arrangement of otherwise simple components may have unexpected interactions. Requirements for redundancy and diversity may complicate timing analysis because they result in additional components and interconnections. General guidance on evaluating a system architecture is given in BTP HICB-14.

Specific timing requirements may affect system architecture because it may not be possible to get sufficient computational performance for a specific function or group of functions from a single processor¹, or the locations where functions are performed may be widely separated. Timing requirements may also increase complexity, either by fragmenting the system into multiple processors or by code tuning, which makes the software product harder to understand, verify, or maintain.

The digital instrumentation loop often includes the sensor, transmitter, analog-to-digital converter, multiplexer, data communication equipment, demultiplexer, computers, memory devices, controls, and displays. Timing analysis should consider the entire loop.

2. Information to be Reviewed

Information to be reviewed is contained in the safety analysis report (SAR), revisions to the SAR, license amendment requests, and topical reports or other applicant/licensee documentation. The SAR and referenced documents typically contain the architectural description, the design basis events and analyses, and certain design commitments. Inspections, tests, analyses and acceptance criteria (ITAAC) or detailed design documents describe designs, tests, analyses, or other methods of demonstrating satisfaction of design commitments for applications made under 10 CFR 52.

3. Acceptance Criteria

If the following criteria are met, the Staff may conclude that the design or completed system will meet timing requirements, can be verified as correct and timely, or that a prototype system accurately reflects the performance and correctness expected of the actual plant. Some of the criteria described herein may be met by submissions describing a software development process or verification methods that include real-time concerns.

Limiting Response Times

Limiting response times should be shown to be consistent with safety requirements, e.g., suppress power oscillations, prevent the fuel design limits from being exceeded, prevent a non-coolable core geometry. Setpoint analyses and limiting response times should also be shown to be consistent. The reviewer should verify that limiting response times are acceptable to the Reactor Systems Branch (SRXB), Electrical Engineering Branch (EELB) and the Plant Systems Branch (SPLB) before accepting their use as a basis for timing requirements.

¹In this context, using multiple processors means using separate computer systems assigned to separate functions or groups of functions. Shared-memory multiprocessors are not implied.

Digital Computer Timing Requirements

Digital computer timing should be shown to be consistent with the limiting response times and the characteristics of the computer hardware, software, and data communications systems. Computer system timing requirements that should be addressed in a software requirements specification are described in BTP HICB-14.

Architecture

The level of detail in the architectural description should be sufficient that the Staff can determine the number of message delays and computational delays interposed between the sensor and the actuator. An allocation of time-delays to elements of the system and software architecture should be available. In initial design phases (e.g., at the point of design certification application), an estimated allocation of time-delays to elements of the proposed architecture should be available. Subsequent detailed design should develop refined timing allocations down to unit levels in the software architecture.

A design should be feasible with currently known methods and representative equipment. Design timing feasibility may be demonstrated by allocating a timing budget to components of the system architecture (Annex E of IEEE Std 7-4.3.2) so that the entire system meets its timing requirements. See also Sections 2.2, 2.3.1, and 2.3.2 of NUREG/CR-6083, and NUREG/CR-6082. The timing budget should include internal and external communication delays, with adequate margins.

Any non-deterministic delays should be noted, and a basis provided that such delays are not part of any safety functions, nor can the delays impede any protective action.

Software architectural timing requirements should be addressed in a software architectural description as described in BTP HICB-14. Databases, disk drives, printers, or other equipment or architectural elements subject to halting or failure should not be able to impede protective system action.

Design Commitments

Design basis documents should describe system timing goals.

Timing requirements should be satisfied by design commitments.

Design basis documents should identify design practices that the applicant/licensee will use to avoid timing problems. Risky design practices such as non-deterministic data communications, non-deterministic computation, use of interrupts, multitasking, dynamic scheduling, and event-driven design should be avoided. Where such practices are allowed, the applicant/licensee should describe methods for control of the associated risk. NUREG/CR-6082 and NUREG/CR-6083 describe risky design practices in more detail.

Performance Verification

The means proposed, or used, for verifying a system's timing should be consistent with the design.

Testing should show that the system meets limiting response times for a reasonable, randomly-selected subset of system loads, conditions, and design basis events. The subset should include some limiting load conditions, and should be chosen by persons independent of the persons who designed the system.

Measurement methods should be appropriate to the resolution and detail required.

Timing measurements should meet projections, or the anomalies should be satisfactorily explained (Sections 2.1, 2.3.3, and 2.3.4 of NUREG/CR-6083).

Use of Part-Scale Prototypes

In systems that have not been implemented and tested on a full scale, expected system delays on scale-up should be calculated and shown to be less than limiting system response times (Annex E of IEEE Std 7-4.3.2, and Sections 2.1.3 and 2.1.4 of NUREG/CR-6083).

A basis should be provided that describes the effects of adding sensors, divisions, communication links, controllers, computer nodes, or actuation devices required to scale the test system to full scale.

Test data should confirm scaling as well as performance projections. Exceptions are considered anomalies or abnormal events (Annex F of IEEE Std 7-4.3.2).

Prototypes designed to demonstrate scaling should include all significant architectural elements plus enough additional elements to show the scaling effects to be measured.

4. Review Procedures

Based on review of the available information and applicant/licensee commitments, the reviewer should reach a conclusion appropriate to the level of detail and type of submittal. For certified designs under 10 CFR Part 52, or preliminary SARs or topical reports, the level of detail will typically include only information to verify *limiting response times, digital computer timing requirements, architecture, and design commitments*. For this level of detail, the reviewer verifies that system timing requirements calculated from the design basis events and other criteria have been allocated to the digital computer portion of the system as appropriate, and have been satisfied in the digital system architectural design.

When inspections, tests, analyses and acceptance criteria (ITAAC) or detailed design documents that describe designs, tests, analyses, or other methods of demonstrating satisfaction of design commitments are available, the reviewer verifies that the installed plant systems perform as predicted, and that appropriate measurement and analysis techniques have been used to compensate for the uncertainties introduced by certain design and implementation practices, such as the use of interrupts. This level of review verifies satisfaction of the latter two acceptance criteria groups, *performance verification* and *use of part-scale prototypes*.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

ISA-S67.04-1994. "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants."

NUREG/CR-6082. "Data Communications." August 1993.

NUREG/CR-6083. "Reviewing Real-Time Performance of Nuclear Reactor Safety Systems." August 1993.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Appendix 7-B

General Agenda, Station Site Visits

An important part of the review at the operating license stage is a site visit. It is preferable to have the site visit sometime before the completion of the drawing review. The purpose of the site visit is to supplement the review of the design based on the drawings and to evaluate the actual implementation of the design as installed at the site. The NRC Regional Office, having jurisdiction over the plant under consideration, should be notified in advance of the visit so that the regional inspectors can become familiar on a first-hand basis with findings that may require follow-up action. Since proper implementation of design is the ultimate goal of the technical review process, the importance of a site visit is self-evident. The following is a typical general agenda that may be used as a guide for developing a specific agenda for the plant under review.

1. Preliminary Discussions

- a. Unresolved items
- b. Plant layout for touring
- c. Special interest areas

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

2. Control Room

- a. General layout
- b. Nuclear and reactor protection instrument arrangement, separation, and layout
- c. Rod position indication
- d. Protection system initiation, bypass switch arrangements, and status panels
- e. Engineered safety feature initiation and bypass switch arrangements and status panels
- f. Panel wiring separation and isolation

3. Instrument Rooms

- a. General layout
- b. Protection system racks and panels
- c. Testing features
- d. Component separation and isolation
- e. Panel wiring separation and isolation

4. Local Instrument Racks/Piping

- a. Physical separation and single failure
- b. Potential for damage due to fire, flooding, etc.
- c. Test features

5. Reactor Building and Turbine Building

- a. Protection system instrument arrangement, separation, and layout
- b. Potential for instrument damage due to fire, missiles, etc.
- c. Separation of piping and wiring to redundant instruments
- d. Provisions for testing protection instruments

6. Shutdown Outside Control Room

- a. Remote shutdown panels arrangement, separation, and layout
- b. Local control and indication features



U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

Appendix 7-C

Acronyms, Abbreviations, Glossary, and Index

Version 2.0, July 10, 1997

A. Acronyms and Abbreviations

AFW	auxiliary feedwater
ALWR	advanced light water reactor
ARI	alternate rod injection
ANS	American Nuclear Society
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
ATWS	anticipated transient without scram
B&W	Babcock and Wilcox
BISI	bypassed or inoperable status indication
BTP	branch technical position
BWR	boiling water reactor
CDM	certified design material
CM	configuration management
CE	Combustion Engineering
CFR	Code of Federal Regulations

Rev. 4 — June 1997

USNRC STANDARD REVIEW PLAN

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

CL	combined license
COTS	commercial off-the-shelf
CP	construction permit
D-in-D&D	defense-in-depth and diversity
DAC	design acceptance criteria
DC	design certification
DCD	design certification document
DCS	data communication system
EAS	essential auxiliary support
ECCS	emergency core cooling system
EELB	Electrical Engineering Branch
EEPROM	electrically erasable programmable read-only memory
EMEB	Mechanical Engineering Branch
EMI	electromagnetic interference
EPRI	Electrical Power Research Institute
ERF	emergency response facility
ESF	engineered safety features
ESFAS	engineered safety features actuation system
FR	Federal Register
FSAR	final safety analysis report
GDC	general design criteria(on)
GSI	generic safety issue
HHFB	Human Factors Assessment Branch
HICB	Instrumentation and Controls Branch
HVAC	heating, ventilating, and air conditioning
I/O	Input/output
I&C	instrumentation and control
ICS	integrated control system
IEEE	Institute of Electronic and Electrical Engineers
ISA	International Society for Measurement and Control (formerly Instrument Society of America)
ITAAC	inspections, tests, analyses, and acceptance criteria
LCSR	loop current step response
LSSS	limiting safety system setting
MCF	maximum credible fault
MCR	main control room
MOIV	motor-operated isolation valve
NDL	nuclear data link
NRC	Nuclear Regulatory Commission

NRR	Office of Nuclear Reactor Regulation
OL	operating license
PAM	post-accident monitoring
PDS	pre-developed software
PLC	programmable logic controller
PRA	probabilistic risk assessment
PSAR	preliminary safety analysis report
PWR	pressurized water reactor
QA	quality assurance
RAI	request for additional information
RCS	reactor coolant system
RHR	residual heat removal
RTD	resistance temperature detector
RTS	reactor trip system
SAR	safety analysis report
SCM	software configuration management
SCSB	Containment Systems and Severe Accident Branch
SER	safety evaluation report
SLCS	standby liquid control system
SPDS	safety parameter display system
SPLB	Plant Systems Branch
SRM	Staff Requirements Memorandum
SRP	Standard Review Plan
SRXB	Reactor Systems Branch
SSAR	standardized safety analysis report
Std	standard
SWC	surge withstand capability
TMI	Three Mile Island
TSB	Technical Specifications Branch
USI	unresolved safety issue
V&V	verification and validation
VDU	video display unit

B. Glossary

Accuracy. The degree of freedom from error of sensor and operator input, the degree of exactness exhibited by an approximation or measurement, and the degree of freedom from error of actuator output.

Activity group. A collection of software life cycle activities, all of which are related to a specific life cycle topic. Eight activity groups are recognized in BTP HICB-14: planning, requirements, design, implementation, integration, validation, installation, and operations and maintenance.

Activity. A group of related tasks [IEEE Std 1074].

Completeness. Those attributes of the design outputs that provide full implementation of the functions required of the software. The functions which the software is required to perform are derived from (1) the general functional requirements of the safety system, and (2) the assignment of functional requirements to the software in the overall system design.

Configuration control board. The authority responsible for evaluating and recommending disposition of proposed changes.

Configuration management. A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements [610.12].

Consistency (as a software functional characteristic). The degree of freedom from contradiction among the different documents and components of a software system. Internal consistency denotes the consistency within the different parts of a component; for example, a software design is internally consistent if no set of design elements are mutually contradictory. External consistency denotes the consistency between one component and another; for example, software requirements and the resulting code are consistent with one another if there are no contradictions between the requirements and the code.

Control systems. Those systems used for normal operation that are not relied upon to perform safety functions following anticipated operational occurrences or accidents. The control systems evaluated using SRP Chapter 7 are those which control plant processes having a significant impact on plant safety, but are not wholly incorporated into systems addressed by other SRP chapters.

Correctness. The degree to which a design output is free from faults in its specification, design, and implementation. There is considerable overlap between correctness properties and properties of other characteristics such as accuracy and completeness.

Data communication systems (DCS). Systems that transmit signals between systems and between components of systems. Data communication systems may include analog and digital multiplexers as well as non-multiplexed transmission. Where such systems are included in a design, they support one or more of the I&C systems.

Design acceptance criteria (DAC). A set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies in making a final safety determination to support design certification when detailed design information is not available. The DAC are part of the Tier 1 information.

Design certification document (DCD). The master document that contains the information that is referenced by the design certification rule. The DCD includes both the Tier 1 information that is certified by the design certification rule and the Tier 2 information that is approved by and supports the rule. The DCD is composed of the certified design material and the non-proprietary version of the SAR, including all material incorporated by reference.

Design output. Documents, such as drawings and specifications, that define technical requirements of structures, systems, and components (ASME Std NQA-1, "Quality Assurance Requirements for Nuclear Facility Applications"). For software, design outputs are the products of the development process that describe the end product that will be installed in the plant. The design outputs of a software development process include software requirements specifications, software design specifications, hardware and software architecture designs, code listings, system build documents, installation configuration tables, operations manuals, maintenance manuals, and training manuals.

Deterministic timing. Timing is deterministic if the time delay between stimulus and response has a guaranteed maximum and minimum.

Diverse instrumentation and control systems (diverse I&C). Those systems provided expressly for diverse backup of the reactor trip system and engineered safety features actuation systems. Diverse I&C systems account for the possibility of common-mode failures in the protection systems. Diverse I&C systems include the anticipated transient without scram (ATWS) mitigation system as required by 10 CFR 50.62. For plants with digital computer-based instrumentation and controls, diverse I&C systems may also include hardwired manual controls, diverse displays, and any other systems specifically installed to meet the guidance of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs."

Documentation. Information recorded about a specific life cycle activity. Forty-one activities are recognized in BTP HICB-14. Documentation includes software life cycle design outputs and software life cycle process documentation. A document may be in written or electronic format, and may contain text, illustrations, tables, computer files, program listings, binary images, and other forms of expression. A document for an activity may be divided into several individual entities.

Embedded software or firmware. Software that is built into (stored in read-only memory) a computer dedicated to a pre-defined task. Normally, embedded software cannot be modified by the computer that contains it, nor will power failure erase it; some computers may contain embedded software stored in electrically erasable programmable read-only memory (EEPROM), but changing this memory typically requires a special sequence of actions by maintenance personnel.

Engineered safety features actuation systems (ESFAS). Those I&C systems which initiate and control safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, reactor coolant pressure boundary, and containment).

Essential auxiliary supporting (EAS) systems. Those systems that enable the I&C systems important to safety to perform their functions. Heating, ventilation and air conditioning systems; electrical power systems; and cooling water systems are typical examples of essential auxiliary supporting systems.

Formal methods. Mathematically based methods for the specification, design, and production of software. Also includes a logical inference system for formal proofs of correctness, and a methodological framework for software development in a formally verifiable way [MOD-00-55].

Functional characteristic. A trait or property of a design output that implements a functional requirement, a portion of a functional requirement, or a combination of functional requirements. For software, functional characteristics include accuracy, functionality, reliability, robustness, safety, security, and timing.

Functional requirement. A requirement that specifies a function that a system or system component must be capable of performing [IEEE Std 610.12]. In the SRP, the term functional requirement includes design requirements, interface requirements, performance requirements, and physical requirements.

Functionality (as a software functional characteristic). Those operations which must be carried out by the software. Functions generally transform input information into output information in order to affect the reactor operation. Inputs may be obtained from sensors, operators, other equipment, or other software. Outputs may be directed to actuators, operators, other equipment, or other software.

Handshake. A four-step process of linked acknowledgments between a sender and a receiver used to transmit data or signals reliably. A handshake involves a signal that (1) initiates the transaction (from the initiating member of a pair), (2) accepts the transaction (from the passive member), (3) terminates the transaction (from the initiator), and (4) acknowledges the termination and readiness for another transaction (from the passive member).

Implementation (as a software life cycle process planning characteristic). Those characteristics of planning documents that describe the work necessary to achieve the purpose of the planning documents. The implementation characteristics of software life cycle plans discussed in BTP HICB-14 are: measurement, procedures, record keeping, and schedule.

Information systems important to safety. Those systems which provide information to the operators for the safe operation of the plant during normal operation, anticipated operational occurrences, and accidents. The information systems important to safety include those systems which provide information for manual initiation and control of safety systems. They indicate that plant safety functions are being accomplished and provide information from which appropriate actions can be taken to mitigate the consequences of anticipated operational occurrences and accidents. During normal plant operation, the information systems important to safety provide information on the normal status and the bypassed and inoperable status of safety systems.

Integration. The process of combining system entities into an overall functioning system.

Interface. A shared boundary across which information is passed [IEEE Std 610.12].

Interlock systems important to safety. Those systems which operate to reduce the probability of occurrence of specific events or to maintain safety systems in a state to assure their availability in an accident. These systems differ from protection systems in that interlock system safety action is taken prior to or to prevent accidents.

Interrupt. The suspension of a process to handle an event external to the process.

Management (as a software life cycle process planning characteristic). Those characteristics of planning documents that are primarily significant to the managing of the project activities described in the planning document. The management characteristics of software life cycle plans discussed in BTP HICB-14 are: purpose, organization, oversight, responsibilities, risks, and security.

On-line testing. Testing performed on an operable system.

Operable. A system, subsystem, train, component, or device is operable when it is capable of performing its specified safety function(s) and when all necessary attendant instrumentation, controls, normal or emergency electrical power, cooling and seal water, lubrication, and other auxiliary equipment that are required for the system, subsystem, train, component, or device to perform its specified safety function(s) are also capable of performing their related support function(s).

Performance. The degree to which a system or component accomplishes its designated functions within given constraints, such as speed, accuracy, or memory usage [IEEE Std 610.12].

Periodic tests. Tests performed at scheduled intervals to detect failures and verify operability [IEEE Std 338]. Periodic tests include surveillance tests.

Predeveloped software (PDS). Software that already exists, is available as a commercial or proprietary product, and is being considered for use in a computer-based function [IEC Std 880, Supplement 1 draft]. Commercial off-the-shelf (COTS) software is a subset of PDS.

Protection systems. Those I&C systems which initiate safety actions to mitigate the consequences of design basis events. The protection systems include the reactor trip system (RTS) and the engineered safety features actuation system (ESFAS).

Reactor trip systems (RTS). Those I&C systems that initiate rapid control rod insertion to mitigate the consequences of design basis events.

Reliability (as a software functional characteristic). The degree to which a software system or component operates without failure. This definition does not consider the consequences of failure, only the existence of failure.

Resources (as a software life cycle process planning characteristic). The material resources necessary to carry out the work defined in the planning document. The resource characteristics of software life cycle plans discussed in BTP HICB-14 are: budget, methods/tools, personnel, and standards.

Robustness (as a software functional characteristic). The ability of a software system or component to function correctly in the presence of invalid inputs or stressful environmental conditions. This includes the ability to function correctly despite some violation of the assumptions in its specification.

Safe shutdown systems. Those systems which function to achieve and maintain a safe shutdown condition of the plant. The safe shutdown systems include those I&C systems used to maintain the reactor core in a subcritical condition and provide adequate core cooling to achieve and maintain both hot and cold shutdown conditions.

Safety (as a software functional characteristic). Those properties and characteristics of the software system that directly affect or interact with system safety considerations. The safety characteristic is primarily concerned with the effect of the software on system hazards and the measures taken to control those hazards.

Security. The ability to prevent unauthorized, undesired, and unsafe intrusions.

Self-test. A test or series of tests, performed by a device upon itself. Self-test includes on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics.

Software development process characteristic. A trait or property of a software development process design output that results from the implementation of a design process, including completeness, consistency, correctness, style, traceability, unambiguity, and verifiability.

Software life cycle. A project-specific, time-sequenced mapping of activities [IEEE Std 1074].

Style (as a software functional characteristic). The form and structure of a design output. Document style refers to the structure and form of a document. This has connotations of understandability, readability, and modifiability. Programming style refers to the programming language characteristics of the software.

Surveillance tests. Tests conducted specifically to confirm compliance with technical specification surveillance requirements.

Task. The smallest unit of work subject to management accountability. A task is a well-defined work assignment for one or more project members [IEEE Std 1074].

Testability. (1) The degree to which a requirement is stated in terms that permit establishment of test criteria and performance of tests to determine whether those criteria have been met [610.12]. (2) The degree to which a system or component facilitates the establishment of test criteria and the performance of tests to determine whether those criteria have been met [IEEE Std 610.12].

Tier 1. The design-related information contained in the DCD that constitutes the certified standard design. This information identifies the scope of the standard design and consists of the certified design descriptions, the ITAAC, the site parameters, and the interface requirements. Tier 1 material becomes part of the design certification rule and may be changed only by rule-making.

Tier 2. The design-related information contained in the DCD that is not Tier 1 information. It supports the certification of a standard design by providing additional details about the proposed implementation. The Tier 2 information generally consists of the SAR with the proprietary information removed for purposes of rule-making. Although Tier 2 information is not certified by the design certification rule, it consists of “those matters resolved in connection with the issuance or renewal of a design certification” within the meaning of 10 CFR 52.63(a)(4). Tier 2 material is approved by the design certification rule, but is not part of the rule. Tier 2 material may be changed by a process similar to that described in 10 CFR 50.59, unless designated as Tier 2* in the SER.

Tier 2*. A subset of Tier 2 material that the NRC SER and DCD for the standardized plant design approval identifies as requiring NRC approval prior to modification or change by the applicant/licensee.

Timing (as a software functional characteristic). The ability of the software system to achieve its timing objectives within the hardware constraints imposed by the computing system being used.

Traceability. The degree to which each element of one life cycle product can be traced forward to one or more elements of a successor life cycle product, and can be traced backward to one or more elements of a predecessor life cycle product.

Unambiguity. The degree to which each element of a life cycle product, and of all elements taken together, have only one interpretation.

Unbounded loop. The term used to describe the situation in which a programming language control structure called a loop has no upper limit to the number of times it may execute.

Validation. The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements [IEEE Std 610.12].

Verifiability (as a software functional characteristic). The degree to which a software design output is stated or provided in such a way as to facilitate the establishment of verification criteria and the performance of analyses, reviews, or tests to determine whether those criteria have been met.

Verification and Validation. The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements [IEEE Std 610.12].

Verification. The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase [IEEE Std 610.12].

Walkthrough. A static analysis technique in which a designer or programmer leads members of the development team and other interested parties through a segment of documentation or code, and the participants ask questions and make comments about possible errors, violation or development standards, and other problems. [IEEE Std 610.12]

Watchdog timer. A form of interval timer that is used to detect a possible malfunction and is typically arranged to cause a hardware restart if not reset periodically by software.

C. Index

10 CFR 50, 7-C-5, 7-C-8, 7.0-2, 7.0-5, 7.0-8, 7.0-A-3, 7.0-A-9, 7.0-A-11, 7.0-A-14, 7.1-2, 7.1-4- 7.1-6, 7.1-8, 7.1-9, 7.1-A-1- 7.1-A-5, 7.1-A-7- 7.1-A-9, 7.1-A-11, 7.1-A-24- 7.1-A-27, 7.1-B-2, 7.1-B-5, 7.1-B-6, 7.1-C-5, 7.1-C-7, 7.1-C-10, 7.1-C-11, 7.1-C-16, 7.2-2, 7.2-5, 7.2-6, 7.3-3, 7.3-6, 7.3-7, 7.4-1, 7.4-3, 7.4-7, 7.5-2- 7.5-4, 7.5-6, 7.5-8, 7.5-9, 7.6-2, 7.6-5, 7.6-6, 7.7-2, 7.7-3, 7.7-5, 7.8-1- 7.8-5, 7.8-7- 7.8-9, 7.9-2- 7.9-4, 7.9-7- 7.9-9, BTP-13-1, BTP-13-2, BTP-10-1, BTP-10-2, BTP-11-1, BTP-12-1, BTP-14-1, BTP-14-13, BTP-14-17, BTP-16-1, BTP-16-2, BTP-16-4-6, BTP-17-1, BTP-18-1, BTP-19-1, BTP-19-2, BTP-19-4, BTP-19-5, BTP-21-1, BTP-21-2, BTP-4-1, BTP-5-1, T7.1-1

10 CFR 50.62, 7-C-5, 7.0-A-9, 7.1-2, 7.1-9, 7.1-A-7, 7.8-1- 7.8-5, 7.8-8, 7.8-9, 7.9-4, 7.9-9, BTP-16-5, BTP-16-6, BTP-19-1, BTP-19-4, BTP-19-5

10 CFR 52, 7-C-8, 7.0-2, 7.0-4, 7.0-6, 7.0-8, 7.0-11, 7.0-A-3, 7.0-A-5, 7.1-3, 7.1-11, 7.1-A-2, 7.1-A-7, 7.1-A-9- 7.1-A-11, 7.2-3, 7.2-4, 7.2-7, 7.3-4, 7.3-5, 7.3-8, 7.4-4, 7.4-8, 7.5-5, 7.5-10, 7.6-3, 7.6-6, 7.6-7, 7.7-3, 7.7-6, 7.8-3, 7.8-4, 7.8-8, 7.9-2- 7.9-4, 7.9-7, BTP-16-1, BTP-16-2, BTP-16-7, BTP-16-8, BTP-21-4

49 FR 26042, 7.8-9

Activity group(s), 7-C-4, 7.0-A-1, 7.1-A-26, BTP-14-2, BTP-14-6, BTP-14-26-28, 7-C-4, 7.0-A-1, 7.0-A-5, BTP-14-2, BTP-14-6, BTP-14-7, BTP-14-38

Advanced light water reactor (ALWR), 7-C-1, 7-C-5, 7.0-A-10, 7.0-A-16, 7.1-2, 7.1-14, 7.1-A-20, 7.1-A-21, 7.1-B-11, 7.1-C-10, 7.1-C-19, 7.2-3, 7.2-9, 7.3-3, 7.3-9, 7.5-4, 7.5-7, 7.5-11, 7.7-3, 7.7-7, 7.8-4, 7.8-10, 7.9-3, 7.9-4, 7.9-6, 7.9-11, BTP-16-8, BTP-19-1, BTP-19-3, BTP-19-4, BTP-19-8

AFW (see also auxiliary feedwater), 7-C-1, 7.1-A-3

Alternate rod injection (ARI), 7-C-1, 7.1-A-7

ANS Std 4.5, 7.1-11, 7.1-A-26

ANSI Std C37.90.1, BTP-11-2, BTP-11-6, BTP-11-6

ANSI Std C62.45, BTP-11-2, BTP-11-5, BTP-11-6

ANSI Std C84.1, BTP-11-4, BTP-11-6

ANSI/IEEE Std 1008, 7.1-12, 7.1-A-25, 7.1-A-26, BTP-14-23, BTP-14-38, T7.1-5

ANSI/IEEE Std 1012, 7.1-12, 7.1-A-24, 7.1-A-26, BTP-14-22, BTP-14-38, T7.1-5

ANSI/IEEE Std 1042, 7.1-A-25

ANSI/IEEE Std 1058.1, BTP-14-39

ANSI/IEEE Std 279, 7.0-5, 7.0-11, 7.0-A-3, 7.0-A-14, 7.1-3- 7.1-9, 7.1-11, 7.1-A-1- 7.1-A-3, 7.1-A-15- 7.1-A-19, 7.1-A-21- 7.1-A-24, 7.1-A-26, 7.1-B-1- 7.1-B-4, 7.1-B-7, 7.1-B-10, 7.1-C-5, 7.1-C-18, 7.2- 2- 7.2-4, 7.2-6, 7.2-7, 7.3-3- 7.3-5, 7.3-8, 7.4-3, 7.4-4, 7.4-9, 7.5-2- 7.5-6, 7.5-11, 7.6-2, 7.6-4, 7.6-7, 7.7-2, 7.7-7, 7.8-3, 7.8-4, 7.8-9, 7.9-2- 7.9-4, 7.9-10, BTP-13-1, BTP-13-6, BTP-1-1, BTP-1-2, BTP- 11-1-7, BTP-12-1, BTP-12-2, BTP-12-6, BTP-14-1, BTP-14-39, BTP-17-1, BTP-17-2, BTP-17-5, BTP-19-1, BTP-19-2, BTP-19-7, BTP-2-1, BTP-2-2, BTP-21-6, BTP-3-1, BTP-6-1, BTP-8-1, BTP-9- 1, T7.1-1, T7.1-2

ANSI/IEEE Std 323, 7.1-12, 7.1-B-5, 7.1-B-10, 7.1-C-11, 7.1-C-18

ANSI/IEEE Std 379, 7.1-12, 7.1-A-22, 7.1-A-26, 7.1-B-4, 7.1-B-10, 7.1-C-9, 7.1-C-18, 7.2-5, 7.2-7, 7.3-7, 7.3-9, BTP-17-1, BTP-17-2, BTP-17-5, BTP-19-2, BTP-19-7, T7.1-4

ANSI/IEEE Std 829, 7.1-12, 7.1-A-27, BTP-14-39, T7.1-5

ANSI/IEEE Std C37.1, BTP-17-2, BTP-17-6

ANSI/IEEE Std C62.36, BTP-11-7

ANSI/IEEE Std C62.41, BTP-11-7

Anticipated transient without scram, 7-C-1, 7-C-5, 7.1-2, 7.8-1, 7.9-6

Application types, 7.0-2, 7.0-3

ASME Std NQA-1, 7-C-5

ATWS, 7-C-1, 7-C-5, 7.1-2, 7.1-9, 7.1-A-7- 7.1-A-9, 7.1-A-22, 7.1-A-27, 7.8-1- 7.8-3, 7.8-5- 7.8-9, 7.9-6, 7.9-9, BTP-10-7, BTP-16-5, BTP-19-1, BTP-19-4, BTP-19-5, 7-A-2, 7-C-1

Auxiliary feedwater (see also AFW), 7.1-A-3, 7.1-B-3, 7.1-C-8, 7.3-2, 7.3-3, 7.4-2, 7.4-6, 7.5-3, 7.8-6, BTP-4-1, T7.1-2, T7.1-5

Babcock and Wilcox (B&W), 7-C-1, 7.1-A-6, 7.1-A-7, 7.1-A-27, 7.7-3, T7.1-2

Boiling water reactor (BWR), 7-C-1, 7.1-A-7, 7.3-2, 7.4-1, 7.4-6, 7.7-8, BTP-10-4

Bypassed or inoperable status indication (BISI), 7-C-1, 7.5-1, 7.5-3, 7.5-6, 7.5-9, 7.6-5

Certified design material (CDM), 7-C-1, 7-C-5, 7.0-2, 7.1-11, BTP-16-1, BTP-16-2, BTP-16-3, BTP-16-8

Code of Federal regulations, 7-C-1, 7.3-6, 7.5-8, 7.6-5, 7.8-7

Combined license (CL), 7-C-2, 7.0-2, 7.0-6- 7.0-8, 7.0-11, 7.0-A-13, 7.1-11, 7.1-A-11, 7.2-3, 7.3-4, 7.4-4, 7.5-5, 7.6-3, 7.7-3, 7.8-3, 7.9-3, 7.9-7, BTP-16-1-3

Combustion Engineering (CE), 7-C-1, 7.1-A-7, BTP-10-7

Common-mode failure, 7.1-A-20, 7.7-5, BTP-13-3, BTP-14-18

Completeness, 7-C-4, 7-C-8, 7.0-6, 7.0-A-8, 7.1-8, 7.1-B-2, 7.1-C-7, BTP-14-4, BTP-14-5, BTP-14-28, BTP-14-29, BTP-14-31, BTP-14-32, BTP-14-34-38

Configuration control, 7-C-4 7.0-A-7, BTP-14-24, BTP-14-27

Configuration management, 7-C-1, 7-C-3, 7-C-4, 7.0-6, 7.0-A-5, 7.0-A-8, 7.0-A-9, 7.0-A-15, 7.1-6, 7.1-12, 7.1-13, 7.1-A-25, 7.1-A-27, 7.1-A-28, 7.1-C-15, 7.1-C-18, 7.2-8, BTP-14-7, BTP-14-10, BTP-14-14, BTP-14-17, BTP-14-23-28, BTP-14-37-40, BTP-18-3, T7.1-5

Consistency, 7-C-4, 7-C-8, 7.0-10, 7.0-A-6, 7.0-A-8, 7.1-8, 7.1-B-2, 7.1-C-7, BTP-14-4, BTP-14-9, BTP-14-28-32, BTP-14-34-38

Construction permit (CP), 7-C-2, 7.0-2, 7.0-5, 7.0-7, 7.0-8, 7.1-A-7

Containment Systems and Severe Accident Branch (see also SCSB), 7-C-3, 7.0-10, 7.1-A-5

Control system(s), 7-C-2, 7-C-3, 7.0-4, 7.0-5, 7.0-A-9, 7.0-A-10, 7.1-A-6, 7.1-A-7, 7.1-A-11, 7.1-A-14, 7.1-A-18- 7.1-A-20, 7.1-A-27, 7.1-B-3, 7.1-B-5, 7.1-B-7, 7.1-C-8, 7.1-C-11, 7.1-C-16, 7.2-1, 7.2-3, 7.2-6, 7.3-4, 7.3-6, 7.4-4, 7.6-4, 7.7-1- 7.7-6, 7.7-8, 7.8-2, 7.9-4, 7.9-9, BTP-13-1, BTP-11-1, BTP-16-5, BTP-18-3, BTP-19-3, BTP-19-5, BTP-21-2, BTP-5-1, T7.1-2, 7-A-2, 7-C-4, 7-C-5, 7.0-4, 7.0-5, 7.0-10, 7.0-A-1, 7.0-A-3, 7.0-A-6, 7.0-A-9, 7.0-A-10, 7.0-A-17, 7.0-A-23, 7.1-1, 7.1-2, 7.1-4, 7.1-9, 7.1-A-1, 7.1-A-6, 7.1-A-8, 7.1-A-14, 7.1-A-15, 7.1-A-18- 7.1-A-24, 7.1-B-5- 7.1-B-7, 7.1-C-6, 7.1-C-10, 7.1-C-11, 7.2-2, 7.2-3, 7.2-6, 7.3-1- 7.3-8, 7.4-1- 7.4-3, 7.4-7, 7.5-3, 7.5-4, 7.6-2, 7.7-1- 7.7-6, 7.7-8, 7.8-1, 7.8-3, 7.8-4, 7.8-6, 7.9-2- 7.9-4, 7.9-8, BTP-13-1, BTP-13-2, BTP-11-1, BTP-14-1, BTP-17-3, BTP-17-4, BTP-18-1, BTP-19-1, BTP-19-2, BTP-19-6, BTP-5-1, T7.1-1, T7.1-2, T7.1-4, T7.1-6

Correctness, 7-C-4, 7-C-6, 7-C-8, 7.0-A-8, 7.1-B-2, 7.1-C-7, BTP-14-5, BTP-14-28-30, BTP-14-32-36, BTP-17-4, BTP-21-4

COTS (see also predeveloped software, PDS), 7-C-2, 7-C-7, 7.0-A-2, 7.0-A-13, 7.1-13, 7.1-C-11, 7.1-C-18, BTP-14-6, BTP-14-39, BTP-18-4

D-in-D&D (see also defense-in-depth and diversity), 7-C-2, 7.0-A-4-7.0-A-6, 7.0-A-9, 7.0-A-10, 7.8-1, 7.8-2, 7.8-5, 7.8-6, 7.8-7, 7.9-6, BTP-16-3, BTP-16-6, BTP-16-7, BTP-19-1-4, BTP-19-6

Data communication system(s) (DCS), 7-C-2, 7-C-4, 7.0-A-9, 7.0-2, 7.0-A-10, 7.9-2, BTP-16-7, 7-C-4, 7.0-A-10, 7.1-1, 7.1-2, 7.1-A-2, 7.1-A-3, 7.1-A-7, 7.1-A-12- 7.1-A-24, 7.1-C-6, 7.9-1, 7.9-2, 7.9-4- 7.9-10, BTP-16-6, BTP-16-7, BTP-19-3, BTP-21-3

Defense-in-depth and diversity (see also D-in-D&D), 7-A-2, 7-C-2, 7.0-9, 7.0-A-4, 7.0-A-5, 7.0-A-10, 7.0-A-20, 7.1-2, 7.1-8, 7.1-A-4, 7.1-A-20, 7.1-C-6, 7.1-A-20, 7.2-4, 7.2-6, 7.3-5, 7.3-8, 7.7-4, 7.7-5, 7.8-1, 7.8-5, 7.8-9, 7.9-6, 7.9-8, BTP-16-3-5, BTP-19-1-3

Design acceptance criteria (DAC), 7-C-2, 7-C-5, 7.9-10, BTP-16-2-8

Design certification document (DCD), 7-C-2, 7-C-5, 7-C-8, 7-C-9, BTP-16-1, BTP-16-2, BTP-16-7

Design certification (DC), 7-A-2, 7-C-2, 7-C-5, 7-C-8, 7.0-2, 7.0-5- 7.0-8, 7.0-11, 7.1-3, 7.1-11, 7.1-A-7, 7.1-A-9- 7.1-A-11, 7.2-3, 7.2-7, 7.3-4, 7.3-8, 7.4-4, 7.4-8, 7.5-5, 7.5-10, 7.6-3, 7.6-6, 7.7-3, 7.7-6, 7.8-

3, 7.8-8, 7.9-2, 7.9-7, 7.9-10, BTP-11-5, BTP-16-1-8, BTP-19-1, BTP-19-3, BTP-19-4, BTP-21-5, T7.1-3, T7.1-6

Design criteria, 7-A-2, 7-C-2, 7.0-5, 7.0-10, 7.0-A-1, 7.0-A-3, 7.0-A-5, 7.0-A-8, 7.0-A-11, 7.0-A-13, 7.1-3, 7.1-11, 7.1-A-1, 7.1-A-11, 7.1-A-14, 7.2-3, 7.2-5, 7.3-4, 7.3-6, 7.4-1, 7.4-4, 7.4-7, 7.5-5, 7.5-8, 7.6-4, 7.6-5, 7.7-5, 7.8-3, 7.8-7, 7.9-2, BTP-1-1, BTP-10-4, BTP-16-6, BTP-4-1, BTP-5-1, T7.1-1, T7.1-3, T7.1-5

Design output, 7-C-4-7-C-6, 7-C-8, 7-C-9, 7.0-A-2, 7.0-A-3, 7.0-A-6, 7.0-A-8, BTP-14-2, BTP-14-5, BTP-14-8, BTP-14-10, BTP-14-16, BTP-14-23, BTP-14-28, BTP-14-38, BTP-16-4

Design process, 7-C-8, 7.0-6, 7.0-7, 7.0-A-2-7.0-A-4, 7.0-A-6, 7.0-A-10, 7.0-A-12, BTP-14-8, BTP-16-3

Deterministic timing, 7-C-5, BTP-14-2

Deterministic, 7-C-5, 7.0-A-2, 7.0-A-11, 7.1-7, 7.1-A-20, 7.1-B-4, 7.1-C-8, 7.1-C-9, 7.1-C-16, 7.9-5, BTP-14-2, BTP-14-29, BTP-14-32, BTP-14-34, BTP-21-5

Diverse actuation system(s), 7.1-A-22, 7.1-2, 7.8-2, BTP-16-5

Diverse instrumentation and control system(s), 7.0-A-9, 7.8-2-7.8-5, 7.8-7, 7.8-9, 7.9-9, 7.9-10, 7-C-5, 7.0-A-10, 7.1-1, 7.1-2, 7.1-C-6, 7.7-4, 7.8-1-7.8-9, 7.9-9, BTP-16-6, 7.1-A-20-23

Diversity, 7-A-2, 7-C-2, 7.0-9, 7.0-A-4, 7.0-A-5, 7.0-A-9, 7.0-A-10, 7.0-A-20, 7.1-2, 7.1-8, 7.1-A-4, 7.1-A-17, 7.1-A-20, 7.1-B-4, 7.1-C-10, 7.1-C-15, 7.2-4, 7.2-6, 7.2-8, 7.3-5, 7.3-8, 7.3-9, 7.5-7, 7.7-4, 7.7-5, 7.8-1, 7.8-5-7.8-7, 7.8-9, 7.9-5, 7.9-6, 7.9-8, 7.9-9, BTP-14-6, BTP-16-3-5, BTP-19-1-7, BTP-21-4, T7.1-6

Draft Regulatory Guide DG-1045, 7.1-A-5, 7.1-A-8, 7.1-A-23, 7.1-A-27, 7.1-B-3, 7.1-B-10, 7.1-C-13, 7.1-C-14, 7.2-4, 7.2-5, 7.2-8, 7.3-5, 7.3-6, 7.3-9, 7.5-6, 7.5-8, 7.5-11, 7.9-5, 7.9-10, BTP-12-1, BTP-12-2, BTP-12-4, BTP-12-6, BTP-21-3, BTP-21-7, T7.1-4

Early site permit, 7.0-2

EAS (see also essential auxiliary support), 7-C-2, 7-C-6, 7.0-4, 7.0-10, 7.2-5, 7.2-6, 7.3-1, 7.3-2, 7.3-6, 7.3-7, 7.4-2, 7.4-6, 7.4-7, 7.5-9, 7.6-6

ECCS (see also emergency core cooling system(s)), 7-C-2, 7.5-6, 7.6-1, 7.6-4, BTP-2-1

EELB (see also Electrical Engineering Branch), 7-C-2, 7.0-10, 7.1-A-6, 7.1-A-13, 7.1-B-5-7.1-B-7, 7.1-C-11, 7.1-C-13, 7.1-C-18, 7.8-5, BTP-21-5

EEPROM, 7-C-2, 7-C-5, 7.0-A-2

Electrical Engineering Branch (see also EELB), 7-C-2, 7.0-10, 7.1-A-6, 7.1-B-5, 7.1-C-11, BTP-21-5

Electrical Power Research Institute (see also EPRI), 7-C-2, 7.1-5

Electromagnetic interference (see also EMI), 7-C-2, 7.1-5, 7.1-12, 7.1-B-5, 7.1-B-6, 7.1-B-10, 7.1-C-11, 7.1-C-18, BTP-9-1

Embedded software, 7-C-5, 7.0-A-2, 7.0-A-10, 7.1-5

EMEB (see also Mechanical Engineering Branch), 7-C-2, 7.0-10, 7.1-A-12, 7.1-B-5, 7.1-B-6, 7.1-C-11

Emergency core cooling system(s) (see also ECCS), 7-A-2, 7-C-2, 7.6-1, BTP-1-1, BTP-2-1, T7.1-5, 7.3-2

Emergency response facility (ERF) , 7-C-2, 7.5-2, 7.5-4, 7.5-6, 7.5-7

EMI (see also electromagnetic interference), 7-C-2, 7.1-B-5, 7.1-B-6, 7.1-C-11, 7.9-6, 7.9-8, BTP-11-2, BTP-11-3, BTP-16-7, BTP-18-2

Engineered safety features actuation system (see also ESFAS), 7-C-2, 7-C-7, 7.0-A-5, 7.1-A-2, 7.3-1, 7.8-2, 7.9-3, BTP-16-3

Engineered safety features (see also ESF), 7-C-2, 7-C-5, 7-C-7, 7.0-A-5, 7.1-1, 7.1-2, 7.1-A-2, 7.1-B-1, 7.3-1, 7.3-6, 7.8-2, 7.9-3, BTP-16-3, BTP-19-2

EPRI (see also Electrical Power Research Institute), 7-C-2, 7.0-A-1, 7.0-A-6, 7.0-A-13, 7.0-A-14, 7.0-A-16, 7.1-5, 7.1-6, 7.1-12, 7.1-14, 7.1-A-9, 7.1-A-27, 7.1-B-6, 7.1-B-10, 7.1-C-10, 7.1-C-11, 7.1-C-18, 7.1-C-19, 7.5-4, BTP-13-2, BTP-13-6, BTP-14-6, BTP-14-39, BTP-14-40, BTP-18-1, BTP-18-3, BTP-18-4

EPRI-TR-102323, 7.1-5, 7.1-12, 7.1-14, 7.1-B-6, 7.1-B-10, 7.1-C-7, 7.1-C-14

EPRI-TR-106439, 7.0-A-6, 7.0-A-13, 7.0-A-14, 7.0-A-16, 7.1-5, 7.1-6, 7.1-12, 7.1-14, 7.1-C-6, 7.1-C-14, 7.1-C-15, BTP-14-6, BTP-14-39, BTP-14-40, BTP-18-1, BTP-18-3, BTP-18-4

ESF (see also engineered safety features), 7-C-2, 7.0-4, 7.0-10, 7.1-A-8, 7.1-A-13, 7.1-A-27, 7.3-1- 7.3-7, 7.4-1, 7.4-4, 7.4-5, BTP-19-5, BTP-19-6

ESFAS (see also engineered safety features actuation system), 7-C-2, 7-C-5, 7-C-7, 7.0-A-5, 7.0-A-9, 7.0-A-10, 7.1-1, 7.1-A-2- 7.1-A-4, 7.1-A-10, 7.1-A-15- 7.1-A-18, 7.1-A-20- 7.1-A-22, 7.1-B-1, 7.1-B-7, 7.1-C-12, 7.3-1- 7.3-8, 7.5-6, 7.8-2, 7.9-3, 7.9-5- 7.9-8, BTP-16-3, BTP-16-5-7, BTP-19-2, BTP-19-3, BTP-19-5

Essential auxiliary support (see also EAS), 7-C-2, 7.0-4, 7.2-5, 7.4-6, BTP-17-2

Essential auxiliary supporting systems, 7-C-6, 7.1-1- 7.1-3, 7.4-1

Fault(s), 7-C-2, 7.1-A-21, 7.9-6, BTP-11-2-5, BTP-14-29, BTP-16-7, 7-C-4, 7.1-6, 7.9-6, BTP-11-4, BTP-11-6, BTP-14-5, BTP-14-30, BTP-14-37, BTP-9-1

Federal Register, 7-C-2, 7.8-9

Final safety analysis report (FSAR), 7-C-2, 7.0-2, BTP-10-7

Formal methods, 7-C-6, 7.0-A-7, 7.0-A-8, 7.1-8

Functional characteristic(s), 7-C-4, 7-C-6-7-C-9, 7.0-A-2, 7-C-6, 7.0-A-6, 7.0-A-7, 7.0-A-12, BTP-14-4, BTP-14-28, BTP-14-30, BTP-14-32-38, BTP-17-4, BTP-19-6

Functional requirement(s), 7-C-6, 7.0-A-2, 7-C-4, 7-C-6, 7.0-A-2- 7.0-A-7, 7.0-A-9- 7.0-A-13, 7.0-A-23, 7.1-B-2, 7.1-B-4, 7.1-C-7, 7.1-C-9, 7.1-C-16, 7.2-6, 7.3-7, 7.4-7, 7.5-9, 7.6-6, 7.8-9, BTP-12-2, BTP-14-4, BTP-14-29, BTP-14-30, BTP-14-35, BTP-14-38, BTP-4-1

Functional tests, 7.0-A-11, BTP-17-4

Functionality, 7-C-6, 7.0-A-4, BTP-14-4, BTP-14-28, BTP-14-29, BTP-14-36, BTP-16-3

General Design Criterion(a) (GDC), 7-C-2, 7.0-10, 7.0-A-3, 7.0-A-5, 7.1-3- 7.1-9, 7.1-11, 7.1-A-1, 7.1-A-11- 7.1-A-26, 7.1-B-2, 7.1-B-6, 7.1-C-7, 7.1-C-11, 7.1-C-15, 7.1-C-16, 7.2-2, 7.2-3, 7.2-5, 7.2-6, 7.3-3- 7.3-8, 7.4-1, 7.4-2, 7.4-3, 7.4-6- 7.4-8, 7.5-3, 7.5-4, 7.5-8- 7.5-10, 7.6-2, 7.6-3, 7.6-5, 7.6-6, 7.7-3, 7.7-5, 7.8-3, 7.8-7, 7.8-8, 7.9-2- 7.9-4, 7.9-7- 7.9-10, BTP-1-1, BTP-5-1, BTP-10-1, BTP-11-1, BTP-12-1, BTP-13-1, BTP-13-2, BTP-14-1, BTP-16-6, BTP-17-1, BTP-18-1, BTP-19-1, BTP-19-2, BTP-21-1, BTP-21-2, T7.1-1, T7.1-3, T7.1-4

Generic Letter 83-28, 7.1-A-8, 7.1-A-27 85-06, 7.1-A-9, 7.1-A-27 85-06, 7.8-5, 7.8-7, 7.8-9 91-04, BTP-12-2, BTP-12-5, BTP-12-6

Generic safety issue(s) (GSI), 7-C-2, 7.0-9, 7.0-5, 7.1-10, 7.1-13, 7.1-A-7, 7.2-3, 7.2-7, 7.3-4, 7.3-8, 7.4-4, 7.4-8, 7.5-5, 7.5-10, 7.6-3, 7.6-6, 7.7-3, 7.7-6, 7.8-3, 7.8-8, 7.9-2, 7.9-7, BTP-16-1, BTP-16-3, T7.1-3

Hardware critical characteristics, 7.0-A-2

Heating, ventilating, and air conditioning (HVAC), 7-C-2, 7.3-2, , 7.4-2, 7.7-8

Human Factors Assessment Branch (HHFB), 7-C-2, 7.0-11, 7.1-B-6, 7.1-B-9, 7.1-C-15, 7.1-C-16

Human factors, 7-C-2, 7.0-5, 7.0-11, 7.1-A-17, 7.1-B-6, 7.1-B-9, 7.1-C-15

I/O, 7-C-2, BTP-18-2

ICS (see also integrated control system), 7-C-2, 7.1-A-6

IEC Std 880, 7.0-A-2, 7.0-A-15, BTP-17-2, BTP-17-4, BTP-17-6

IEEE Std 100, BTP-11-5, BTP-11-7

IEEE Std 1028, 7.1-12, 7.1-A-24, 7.1-A-27, BTP-14-14, BTP-14-39, T7.1-5

IEEE Std 1042, 7.1-12, 7.1-A-25, 7.1-A-27, BTP-14-39, T7.1-5

IEEE Std 1074, 7.0-A-3, 7.0-A-15, 7.1-12, 7.1-A-26, 7.1-A-27, BTP-14-6, BTP-14-39, T7.1-5

IEEE Std 1219, BTP-14-39

IEEE Std 1228, BTP-14-39

IEEE Std 323, 7.1-12, 7.1-B-5, 7.1-B-10, 7.1-C-11, 7.1-C-18

IEEE Std 338, 7.1-12, 7.1-A-23, 7.1-A-27, 7.1-B-8, 7.1-B-10, 7.1-C-13, 7.1-C-18, BTP-17-2, T7.1-4

IEEE Std 384, 7.1-12, 7.1-A-21, 7.1-A-22, 7.1-A-27, 7.1-B-7, 7.1-B-10, 7.1-B-11, 7.1-C-13, 7.1-C-14, 7.1-C-18, BTP-11-1, BTP-11-4, BTP-11-7, T7.1-4

IEEE Std 472, BTP-11-2, BTP-11-6

IEEE Std 498, BTP-12-2, BTP-12-6

IEEE Std 603, 7.0-5, 7.0-11, 7.0-A-3, 7.0-A-5, 7.0-A-15, 7.1-4-7.1-9, 7.1-12, 7.1-A-2, 7.1-A-3, 7.1-A-15-7.1-A-19, 7.1-A-24, 7.1-A-28, 7.1-C-5-7.1-C-8, 7.1-C-12, 7.1-C-15, 7.1-C-18, 7.2-3, 7.2-4, 7.2-6, 7.2-8, 7.3-4, 7.3-5, 7.3-9, 7.4-4, 7.4-9, 7.5-5, 7.5-6, 7.5-9, 7.5-11, 7.6-4, 7.6-7, 7.8-4, 7.8-9, 7.9-8, 7.9-10, BTP-13-2, BTP-13-6, BTP-1-2, BTP-11-2, BTP-11-7, BTP-12-2, BTP-12-6, BTP-14-1, BTP-14-39, BTP-16-5, BTP-16-6, BTP-16-8, BTP-17-1, BTP-17-2, BTP-17-5, BTP-17-6, BTP-19-2, BTP-19-7, BTP-2-1, BTP-2-2, BTP-21-2, BTP-21-3, BTP-21-7, BTP-3-1, BTP-6-1, BTP-8-1, T7.1-4

IEEE Std 610.12, 7.0-A-2, 7.0-A-15

IEEE Std 7-4.3.2, 7.0-A-5, 7.0-A-15, 7.0-A-5, 7.0-A-8, 7.1-12, 7.1-4-7.1-7, 7.1-A-24, 7.1-A-28, 7.1-C-1, 7.1-C-2, 7.1-C-4, 7.1-C-6, 7.1-C-8, 7.1-C-9, 7.1-C-14, 7.9-5, 7.9-10, BTP-14-2, BTP-14-39, BTP-17-2, BTP-17-6, BTP-18-1, BTP-18-4, BTP-21-3, BTP-21-5-7, T7.1-4

IEEE Std 730.1, BTP-14-39

IEEE Std 828, 7.1-12, 7.1-A-25, 7.1-A-28, 7.1-C-18, BTP-14-39, T7.1-5

IEEE Std 830, 7.1-12, 7.1-A-26, 7.1-A-28, BTP-14-28, BTP-14-39, T7.1-5

IEEE Std 934, 7.0-A-1, 7.0-A-15

Implementation (as a software process planning characteristic), BTP-14-2-29, BTP-14-32-34, BTP-16-2-4, BTP-18-2, BTP-19-4, BTP-21-3, BTP-21-6, T7.1-1

Independence, 7.0-A-4, 7.0-A-10, 7.0-A-11, 7.1-7, 7.1-12, 7.1-A-4, 7.1-A-16-7.1-A-19, 7.1-A-21, 7.1-A-22, 7.1-A-27, 7.1-A-29, 7.1-B-1, 7.1-B-6, 7.1-B-7, 7.1-B-11, 7.1-C-5, 7.1-C-6, 7.1-C-11-7.1-C-13, 7.1-C-18, 7.1-C-19, 7.2-2, 7.2-4, 7.2-6, 7.2-8, 7.3-3, 7.3-5, 7.3-7, 7.3-9, 7.4-5, 7.5-4, 7.5-7-7.5-9, 7.5-11, 7.6-1, 7.6-4, 7.7-4, 7.8-6, 7.8-8-7.8-10, 7.9-3, 7.9-5, 7.9-8, 7.9-10, BTP-13-2, BTP-10-3, BTP-10-9, BTP-11-1, BTP-11-4, BTP-11-7, BTP-14-10, BTP-14-11, BTP-16-6, BTP-17-1, BTP-17-4, BTP-17-5, BTP-19-1, BTP-19-5, T7.1-4

Information systems important to safety, 7-C-6, 7.1-1, 7.1-2, 7.1-A-2-7.1-A-6, 7.1-A-21, 7.1-A-22, 7.3-1, 7.4-2, 7.4-7, 7.5-1, 7.5-2, 7.5-5, 7.5-6, 7.5-8-7.5-10, 7.9-3, 7.9-8, 7.9-9

Inspections, tests, analyses, and acceptance criteria (see also ITAAC), 7-C-2, 7.0-11, 7.1-A-9, 7.1-A-29, 7.2-7, 7.3-8, 7.4-8, 7.5-10, 7.6-6, 7.7-6, 7.8-8, 7.9-7, BTP-16-8, BTP-18-3

Integrated control system (see also ICS), 7-C-2, 7.1-A-6, 7.1-A-27, 7.7-3, T7.1-2

Integration, 7-C-4, 7-C-6, 7.0-3, 7.0-6, 7.0-7, 7.0-A-1, 7.0-A-3, 7.0-A-11, 7.1-5, 7.1-6, BTP-14-2, BTP-14-7, BTP-14-8, BTP-14-12, BTP-14-14, BTP-14-15, BTP-14-23, BTP-14-26, BTP-14-34

Integrity, 7-C-5, 7.0-A-12, 7.1-1, 7.1-6, 7.1-7, 7.1-A-5, 7.1-A-13, 7.1-A-16, 7.1-A-18, 7.1-B-6, 7.1-C-11, 7.1-C-12, 7.4-7, 7.8-2, 7.9-9, BTP-1-1, BTP-12-1, BTP-14-27, BTP-17-4, BTP-17-5, BTP-19-3-6

Interface, 7-C-6, 7-C-8, 7.0-6, 7.0-7, 7.0-10, 7.0-A-2, 7.1-A-9, 7.1-A-10, 7.2-3, 7.3-4, 7.4-4, 7.5-2, 7.5-5, 7.6-3, 7.7-3, 7.8-3, 7.9-2, BTP-1-1, BTP-11-3, BTP-12-3, BTP-14-19, BTP-14-32, BTP-16-1-3, BTP-16-7, T7.1-3

Interlock, 7-C-6, 7-C-7, 7.0-10, 7.1-1, 7.1-2, 7.1-4, 7.1-A-3, 7.1-A-15, 7.1-A-22, 7.1-A-23, 7.1-B-3, 7.1-C-8, 7.6-1-7.6-7, 7.9-3, 7.9-8, 7.9-9

Interrupt, 7-C-7, 7.8-6

ITAAC (see also inspections, tests, analyses, and acceptance criteria), 7-C-2, 7-C-8, 7.0-2, 7.0-4, 7.0-6-7.0-8, 7.0-11, 7.1-3, 7.1-11, 7.1-A-9, 7.1-A-11, 7.1-A-29, 7.2-3, 7.2-7, 7.3-4, 7.3-8, 7.4-4, 7.4-8, 7.5-5, 7.5-10, 7.6-3, 7.6-6, 7.7-3, 7.7-6, 7.8-3, 7.8-8, 7.9-2, 7.9-3, 7.9-7, 7.9-10, BTP-16-1-4, BTP-16-6-8, BTP-18-3, BTP-21-4, BTP-21-6, T7.1-3

License renewal, 7.0-3

Limiting safety system setting(s) (LSSS), 7-C-2, BTP-12-1, BTP-12-1-3

Loop current step response (LCSR), 7-C-2, BTP-13-4, BTP-13-5

Management (as a software process planning characteristic), BTP-14-2, BTP-14-7, BTP-14-9-28, BTP-14-37-40

Manufacturing license, 7.0-2, 7.0-8, 7.1-13, 7.1-A-2, 7.1-A-28, T7.1-1

Maximum credible fault (MCF), 7-C-2, BTP-11-2, BTP-11-4-6

Mechanical Engineering Branch (see also EMEB), 7-C-2, 7.0-10, 7.1-A-12, 7.1-B-5, 7.1-C-11, BTP-19-7

Motor-operated isolation valve (MOIV), 7-C-2, BTP-2-1

NDL (see also nuclear data link), 7-C-2, 7.5-2, 7.5-4, 7.5-7

NEDO-31558-A, BTP-10-9

NP-5652, 7.0-A-1, 7.0-A-14

NRC Inspection Manual, Chapter 93807, BTP-12-6

Nuclear data link (see also NDL), 7-C-2, 7.5-2, 7.5-9

NUREG-0493, BTP-19-1, BTP-19-2, BTP-19-7

NUREG-0694, 7.1-13, 7.1-A-2, 7.1-A-6, 7.1-A-28, T7.1-1, T7.1-2

NUREG-0718, 7.1-13, 7.1-A-2, 7.1-A-28, T7.1-1, T7.1-2, T7.1-3

NUREG-0737 (including Supplement 1), 7.1-13, 7.1-A-2-7.1-A-6, 7.1-A-28, 7.5-6, , 7.5-11, T7.1-1, T7.1-2, BTP-10-4

NUREG-0809, BTP-13-4, BTP-13-6

NUREG/CR-5560, BTP-13-2, BTP-13-6

NUREG/CR-6082, 7.9-4-7.9-6, 7.9-10, BTP-21-1, BTP-21-3, BTP-21-5, BTP-21-7

NUREG/CR-6083, BTP-21-1, BTP-21-3, BTP-21-5-7

NUREG/CR-6090, BTP-18-1, BTP-18-4

NUREG/CR-6101, BTP-14-1, BTP-14-6, BTP-14-39

NUREG/CR-6303, 7.2-4, 7.2-8, 7.3-5, 7.3-9, BTP-19-2, BTP-19-4, BTP-19-5-7

NUREG/CR-6421, 7.1-13, 7.1-C-6, 7.1-C-14, BTP-14-6, BTP-14-39, BTP-18-1, BTP-18-3, BTP-18-4

NUREG/CR-6463, BTP-14-34, BTP-14-39, BTP-18-1, BTP-18-3, BTP-18-4

Object code, BTP-14-24

Office of Nuclear Reactor Regulation, 7-A-1, 7-B-1, 7-C-1, 7-C-3, 7.0-1, 7.0-A-1, 7.0-A-16, 7.1-1, 7.1-14, 7.1-A-1, 7.1-B-1, 7.1-C-5, 7.1-C-19, 7.2-1, 7.3-1, 7.3-2, 7.4-1, 7.4-2, 7.5-1, 7.5-2, 7.6-1, 7.6-2, 7.7-1, 7.7-2, 7.8-1, 7.8-2, 7.9-1, 7.9-2, BTP-10-9, BTP-14-40, BTP-18-4

Operating license (OL), 7-B-1, 7-C-3, 7.0-2, 7.0-7, 7.0-8, 7.0-A-13, 7.2-3, 7.7-3, 7.8-3, 7.9-3, T7.1-3

PAM (see also Reg. Guide 1.97 and post-accident monitoring), 7-C-3, 7.5-1, 7.5-3, 7.5-6, 7.5-9

PDS (see also predeveloped software), 7.0-A-2, 7.0-A-7, 7.0-A-11, 7.0-A-13, 7.1-5, BTP-14-6, BTP-18-3

Periodic test, 7.0-A-11, 7.1-A-23, BTP-17-3

Plant Systems Branch (see also SPLB), 7-C-3, 7.0-10, 7.1-A-12, 7.1-A-14, 7.1-B-6, 7.1-C-13, 7.1-C-18, 7.7-2, 7.8-5, BTP-21-5

Post-accident monitoring (see also Reg. Guide 1.97 and PAM), 7-C-3, 7.1-A-23, 7.4-3, 7.5-1, 7.5-2, 7.5-5, 7.5-8, 7.5-9, BTP-10-1, BTP-10-2, BTP-10-4

Precision, 7.1-B-4, 7.1-C-9, 7.1-C-16, 7.9-5, BTP-14-32, BTP-14-33

Predeveloped software (see also PDS), 7.0-A-2, 7.1-5, BTP-14-6, BTP-14-12, BTP-14-20, BTP-14-24, BTP-14-33, BTP-16-4, BTP-18-3

PLC (see also programmable logic controller(s)), 7-C-3, 7.0-A-8, 7-A-2, 7.1-6, BTP-18-1-4, T7.1-6

Preliminary safety analysis report (PSAR), 7-C-3, 7.0-2

Pressurized water reactor (see also PWR), 7-C-3, 7.1-A-7, 7.3-2, 7.4-1, 7.7-8, BTP-10-4, BTP-2-1

Programmable logic controller(s) (see also PLC), 7-C-3, 7.0-A-8, 7-A-2, 7.1-6, BTP-18-1-4, T7.1-6

Protocol(s) 7.0-A-10, 7.9-5, BTP-16-6

Prototype(s), 7.1-A-10, 7.1-C-12, BTP-11-1, BTP-21-4, BTP-21-3, BTP-21-6

PSAR (see also preliminary safety analysis report), 7-C-3, 7.0-2

PWR (see also pressurized water reactor), 7-C-3, 7.4-6, BTP-10-4, BTP-5-1

QA, 7-C-3, 7.0-5, BTP-14-13, BTP-14-14

Reactor coolant system (RCS), 7-A-2, 7-C-3, 7.0-4, 7.1-A-5, 7.1-A-14, 7.5-6, 7.6-3, BTP-1-1, BTP-2-1, BTP-10-7, BTP-13-2, BTP-13-3, T7.1-5

Reactor Systems Branch (see also SRXB), 7-C-3, 7.0-10, 7.1-A-14, 7.1-B-5, 7.1-C-9, 7.7-2, 7.8-2, BTP-19-7, BTP-21-5

Reactor trip system(s) (see also RTS), 7-C-3, 7-C-5, 7-C-7, 7.0-A-5, 7.1-A-2, 7.1-A-7, 7.1-A-19, 7.1-C-12, 7.2-1, 7.2-5, 7.8-2, 7.9-3, BTP-16-3, BTP-19-5, 7-C-7, 7.1-1, 7.1-B-1, 7.8-6, BTP-19-2

Regulatory Guide 1.22, 7-A-2, 7.1-A-21, 7.1-A-29, 7.1-B-8, 7.1-B-11, 7.1-C-13, 7.1-C-19, 7.2-5, 7.2-8, 7.3-7, 7.3-9, 7.9-8, 7.9-10, BTP-17-2, BTP-17-3, BTP-17-6, BTP-8-1, T7.1-4, T7.1-6

Regulatory Guide 1.47, 7.1-A-22, 7.1-A-29, 7.1-B-9, 7.1-B-10, 7.1-B-11, 7.1-C-14, 7.1-C-19, 7.2-5, 7.2-8, 7.3-7, 7.3-9, 7.5-7, 7.5-11, 7.5-9, 7.6-6, 7.6-7, 7.9-8, 7.9-10, BTP-17-2, BTP-17-4, BTP-17-5, BTP-17-6, BTP-2-1, BTP-2-2, T7.1-4

Regulatory Guide 1.53, 7.1-A-22, 7.1-A-29, 7.1-B-4, 7.1-B-11, 7.1-C-9, 7.1-C-19, 7.2-5, 7.2-8, 7.3-7, 7.9-8, 7.9-10, BTP-17-1, BTP-17-2, BTP-17-6, BTP-19-2, BTP-19-7, T7.1-4

Regulatory Guide 1.62, 7.1-A-21, 7.1-A-22, 7.1-A-29, 7.1-B-4, 7.1-B-9, 7.1-B-11, 7.1-C-16, 7.1-C-19, T7.1-4

Regulatory Guide 1.70, 7.0-8, 7.0-11, 7.1-11, 7.1-14, 7.1-A-29, BTP-16-1, BTP-16-3-5, BTP-16-8

Regulatory Guide 1.75, 7.1-A-22, 7.1-A-29, 7.1-B-7, 7.1-B-10, 7.1-B-11, 7.1-C-13, 7.1-C-14, 7.1-C-19, 7.2-6, 7.2-8, 7.3-7, 7.3-9, 7.5-8, 7.5-11, 7.8-10, 7.9-8, 7.9-10, BTP-10-3, BTP-10-9, BTP-11-1, BTP-11-5, BTP-11-7, T7.1-4

Regulatory Guide 1.97, 7-A-2, 7.1-14, 7.1-A-8, 7.1-A-22, 7.1-A-29, 7.5-3, 7.5-5, 7.5-6, 7.5-8, 7.5-11, BTP-10-1-9, T7.1-4, T7.1-6

Regulatory Guide 1.100, BTP-10-2, BTP-10-9

Regulatory Guide 1.105 (see also Draft Regulatory Guide DG-1045), 7.1-A-23, 7.1-A-27, 7.1-A-5, 7.1-B-10, 7.1-B-3, 7.1-C-17, 7.1-C-18, 7.2-4, 7.2-8, 7.3-5, 7.3-9, 7.5-11, 7.5-6, 7.9-5, 7.9-7, 7.9-10, BTP-12-1, BTP-12-2, BTP-12-6, BTP-21-3, BTP-21-7, T7.1-4

Regulatory Guide 1.118, 7.1-A-23, 7.1-A-28, 7.1-B-8, 7.1-B-11, 7.1-C-13, 7.1-C-18, 7.2-5, 7.2-8, 7.3-7, 7.3-9, 7.9-8, 7.9-10, BTP-17-2, BTP-17-3, BTP-17-5, BTP-17-6, T7.1-4

Regulatory Guide 1.151, 7.1-A-13, 7.1-A-23, 7.1-A-24, 7.1-A-28, 7.1-A-8, 7.1-B-6, 7.1-C-11, 7.1-C-19, 7.5-8, 7.5-11, 7.7-4, 7.7-5, 7.7-7, T7.1-4

Regulatory Guide 1.152, 7.0-A-5, 7.0-A-6, 7.0-A-8, 7.0-A-13, 7.0-A-15, 7.1-4, 7.1-7, 7.1-13, 7.1-A-24, 7.1-A-28, 7.1-C-6, 7.1-C-15, 7.1-C-19, 7.2-6, 7.2-8, 7.3-7, 7.3-9, 7.4-8, 7.4-9, 7.5-10, 7.5-11, 7.6-6, 7.6-7, 7.8-8, 7.8-9, 7.9-8, 7.9-11, BTP-14-2, BTP-14-29, BTP-14-39, BTP-16-3, BTP-16-8, BTP-17-2, BTP-17-6, BTP-18-1, BTP-18-4, BTP-21-3, BTP-21-7, T7.1-4

Regulatory Guide 1.168, 7.0-A-9, 7.0-A-15, 7.1-13, 7.1-A-24, 7.1-A-28, 7.2-8, BTP-14-14, BTP-14-22, BTP-14-39, T7.1-5

Regulatory Guide 1.169, 7.0-A-9, 7.0-A-15, 7.1-6, 7.1-13, 7.1-A-25, 7.1-A-28, 7.2-8, BTP-14-23, BTP-14-40, T7.1-5

Regulatory Guide 1.170, 7.0-A-9, 7.0-A-15, 7.1-13, 7.1-A-25, 7.1-A-28, 7.2-8, BTP-14-23, BTP-14-40, T7.1-5

Regulatory Guide 1.171, 7.0-A-9, 7.0-A-15, 7.1-13, 7.1-A-25, 7.1-A-28, 7.2-8, BTP-14-23, BTP-14-40, T7.1-5

Regulatory Guide 1.172, 7.0-A-9, 7.0-A-16, 7.1-A-25, 7.1-A-26, 7.1-A-29, 7.2-9, BTP-14-28, BTP-14-40, T7.1-5

Regulatory Guide 1.173, 7.0-A-3, 7.0-A-9, 7.0-A-16, 7.1-5, 7.1-13, 7.1-A-26, 7.1-A-29, 7.2-9, BTP-14-6, BTP-14-11, BTP-14-12, BTP-14-40, T7.1-5

Reliability, 7-C-6, 7-C-7, 7.0-11, 7.0-A-2, 7.0-A-10, 7.1-3-7.1-5, 7.1-7, 7.1-8, 7.1-A-2, 7.1-A-5, 7.1-A-6, 7.1-A-16-7.1-A-18, 7.1-A-20, 7.1-A-21, 7.1-A-27, 7.1-B-4, 7.1-C-8, 7.1-C-9, 7.1-C-15, 7.1-C-16, 7.2-2, 7.2-6, 7.3-3, 7.3-7, 7.4-5, 7.5-4, 7.5-7, 7.6-5, 7.9-1, 7.9-3, 7.9-5, 7.9-8, BTP-13-1, BTP-13-2, BTP-14-1, BTP-14-4, BTP-14-13, BTP-14-28-30, BTP-14-32, BTP-14-39, BTP-16-7, BTP-17-1, BTP-17-3, BTP-17-4, BTP-18-1, BTP-19-1, BTP-21-2, BTP-9-1, T7.1-3, T7.1-4

Remote shutdown, 7-B-2, 7.1-9, 7.1-A-15, 7.4-5, 7.4-6, BTP-21-1

Renewal of standard design certification, 7.0-2

Residual heat removal, (see also RHR), 7-C-3, 7.1-A-14, 7.3-3, 7.4-2, 7.4-3, 7.6-1, 7.6-3, BTP-1-1, BTP-10-8

Resistance temperature detector(s) (see also RTD), 7-C-3, BTP-13-4, BTP-13-6, 7-A-2, BTP-13-1, BTP-13-2, BTP-13-6, T7.1-6

Response time, 7.1-A-9, 7.1-A-27, 7.1-B-8, 7.1-B-9, 7.1-C-12, 7.1-C-16, 7.1-C-17, 7.2-4, 7.3-5, BTP-13-2-5, BTP-21-3

Review of standard designs, 7.0-2

RHR (see also residual heat removal), 7-C-3, 7.5-6, 7.6-1, BTP-10-6

Risk assessment, 7-C-3, 7.0-5, 7.1-A-9, BTP-16-1

Robustness, 7-C-6, 7-C-7, 7.0-A-3, 7.0-A-8, BTP-14-4, BTP-14-28, BTP-14-29, BTP-14-32, BTP-14-33, BTP-14-35, BTP-17-4

RTD (see also resistance temperature detector(s)), 7-C-3, BTP-13-2-5

RTS (see also reactor trip system(s)), 7-C-3, 7-C-7, 7.0-A-5, 7.0-A-9, 7.1-1, 7.1-A-2, 7.1-A-3, 7.1-A-6, 7.1-A-10, 7.1-A-15- 7.1-A-18, 7.1-A-20- 7.1-A-22, 7.1-B-1, 7.1-B-7, 7.1-C-12, 7.2-1- 7.2-7, 7.5-6, 7.8-2, 7.8-6- 7.8-8, 7.9-3, 7.9-5- 7.9-9, BTP-16-3, BTP-16-5-7, BTP-19-2-5

Safe shutdown system(s), 7.4-5, 7.9-9, 7-C-7, 7.1-1, 7.1-2, 7.1-4, 7.1-A-6, 7.4-1, 7.4-2, 7.4-4- 7.4-8, 7.9-3, 7.9-8

Safety analysis report(s) (see also SAR), 7-C-2, 7-C-3, 7.0-2, 7.0-A-6, 7.1-1, 7.1-4, 7.1-A-1, 7.1-B-2, 7.1-C-6, 7.2-1, 7.5-2, 7.8-2, 7.9-1, BTP-14-29, BTP-16-1, BTP-16-7, BTP-18-3, BTP-19-3, BTP-19-4, BTP-21-4, T7.1-1, 7.0-8, 7.0-11, 7.1-11, 7.1-14, 7.1-A-29, BTP-16-1, BTP-16-8

Safety evaluation report (see also SER), 7-C-3, 7.0-3, 7.0-7, 7.0-A-13, 7.1-5, 7.1-11, 7.4-6, BTP-16-1, 7.0-9, BTP-10-2

Safety parameter display system (see also SPDS), 7-C-3, 7.5-2, 7.5-9

SAR (see also safety analysis report(s)), 7-C-3, 7-C-5, 7-C-8, 7.0-2, 7.0-4, 7.0-10, 7.1-1- 7.1-4, 7.1-9- 7.1-11, 7.1-A-1- 7.1-A-7, 7.1-A-9- 7.1-A-12, 7.1-A-14- 7.1-A-20, 7.1-A-22- 7.1-A-24, 7.1-B-2, 7.1-B-3, 7.1-B-5, 7.1-B-8, 7.1-C-6- 7.1-C-8, 7.1-C-10, 7.1-C-15, 7.1-C-17, 7.2-1, 7.2-2, 7.2-4- 7.2-6, 7.3-2, 7.3-5, 7.3-6, 7.4-2-5, 7.5-2, 7.5-5, 7.5-6, 7.6-2, 7.6-4, 7.7-1, 7.7-2, 7.7-4, 7.7-6, 7.7-8, 7.8-2, 7.8-5, 7.9-1, 7.9-8, BTP-16-1-8, BTP-18-3, BTP-19-3, BTP-21-4, T7.1-1

SCSB (see also Containment Systems and Severe Accident Branch), 7-C-3, 7.0-10, 7.1-A-5, 7.1-A-14

Security, 7-C-6-7-C-8, 7.1-3, 7.7-8, BTP-14-3, BTP-14-4, BTP-14-9, BTP-14-10, BTP-14-16, BTP-14-17, BTP-14-19, BTP-14-21, BTP-14-28-32, BTP-14-34-37

SECY-90-241, BTP-16-3, BTP-16-8

SECY-90-377, BTP-16-3, BTP-16-8

SECY-91-178, 7.1-A-29

SECY-91-292, BTP-19-1, BTP-19-7

SECY-92-053, BTP-16-3, BTP-16-8

SECY-92-287, BTP-16-8

SECY-93-087, 7-C-5, 7.0-A-10, 7.0-A-16, 7.1-2, 7.1-4, 7.1-8, 7.1-14, 7.1-A-20, 7.1-A-21, 7.1-B-11, 7.1-C-6, 7.1-C-15, 7.2-3, 7.2-6, 7.2-9, 7.3-3, 7.3-8, 7.3-9, 7.5-4, 7.5-9, 7.5-11, 7.7-3, 7.7-6, 7.7-7, 7.8-1, 7.8-3, 7.8-4, 7.8-9, 7.8-10, 7.9-3, 7.9-4, 7.9-6, 7.9-8, 7.9-9, 7.9-11, BTP-16-3, BTP-16-8, BTP-19-8

Self-test, 7-C-8, 7.1-7, 7.5-7, BTP-17-1-5, T7.1-6

SER (see also safety evaluation report), 7-C-3, 7-C-8, 7-C-9, 7.0-7, 7.0-11, 7.0-A-13, 7.1-11, 7.1-A-9, 7.1-A-11, 7.2-5, 7.2-6, 7.3-6, 7.3-7, 7.4-6, 7.4-7, 7.5-8, 7.6-5, 7.7-5, 7.8-7, 7.9-6, 7.9-9, BTP-16-1, BTP-16-2, BTP-16-7, BTP-16-8

Single-failure criterion, 7.1-A-4, 7.1-A-16, 7.1-A-18, 7.1-A-19, 7.1-A-22, 7.1-A-26, 7.1-A-29, 7.1-B-4, 7.1-B-8, 7.1-B-10, 7.1-B-11, 7.1-C-5, 7.1-C-9, 7.1-C-14, 7.1-C-15, 7.1-12, 7.2-4, 7.2-5, 7.2-7, 7.2-8, 7.3-5, 7.3-7, 7.3-9, 7.4-5-7.4-7, 7.6-4, 7.9-5, 7.9-8, 7.9-10, BTP-17-1, BTP-17-2, BTP-17-4-6, BTP-19-2, BTP-19-7, BTP-2-1, BTP-3-1, BTP-4-1, T7.1-4

Site visits, 7-B-1

SLCS (see also standby liquid control system), 7-C-3, 7.1-A-7, BTP-10-6

Software configuration management, 7-C-3, 7.1-6, 7.1-12, 7.1-A-25, 7.1-A-27, 7.1-A-28, 7.1-C-15, 7.1-C-18, BTP-14-7, BTP-14-14, BTP-14-23, BTP-14-24, BTP-14-27, BTP-14-39

Software critical characteristics, 7.0-A-3

Software development process characteristic(s), 7-C-8, 7.0-A-3, 7.0-A-3, 7.0-A-6, 7.0-A-7, 7.0-A-12, BTP-14-4, BTP-14-9, BTP-14-28-38

Software development process requirement(s), 7.0-A-3, 7.0-A-6, 7.0-A-7, 7.0-A-12

Software life cycle, 7-C-4-7-C-8, 7.0-A-1, 7.0-A-3, 7.0-A-5-7.0-A-7, 7.0-A-9-7.0-A-12, 7.0-A-15, 7.0-A-16, 7.0-A-22, 7.1-5, 7.1-12, 7.1-13, 7.1-A-26, 7.1-A-27, 7.1-A-29, 7.2-9, BTP-14-1, BTP-14-2, BTP-14-5-8, BTP-14-11, BTP-14-13, BTP-14-14, BTP-14-25, BTP-14-28, BTP-14-38-40, T7.1-5

Software product(s), 7.0-A-3, 7.0-A-12, BTP-21-4, BTP-14-33

Software testing, 7.1-A-25, BTP-14-22

Source code, 7.0-A-8, BTP-14-21, BTP-14-24, BTP-14-33

SPDS (see also safety parameter display system), 7-C-3, 7.5-2, 7.5-4, 7.5-6, 7.5-7

SPLB (see also Plant Systems Branch), 7-C-3, 7.0-10, 7.1-A-12, 7.1-A-14, 7.1-B-6, 7.1-B-7, 7.1-C-13, 7.1-C-18, 7.7-2, 7.8-5, BTP-21-5

SRXB (see also Reactor Systems Branch), 7-C-3, 7.0-10, 7.1-A-14, 7.1-B-5, 7.1-B-10, 7.1-C-9, 7.1-C-14, 7.7-2, 7.8-2, 7.8-5, BTP-21-5

Staff Requirements Memorandum (SRM), 7-C-3, 7-C-5, 7.0-A-10, 7.0-A-16, 7.1-2, 7.1-8, 7.1-14, 7.1-A-20, 7.1-A-21, 7.1-B-11, 7.1-C-10, 7.1-C-19, 7.1-2, 7.2-3, 7.2-6, 7.2-9, 7.3-3, 7.3-8, 7.3-9, 7.5-4, 7.5-9, 7.5-11, 7.7-3, 7.7-6, 7.7-7, 7.8-1, 7.8-3, 7.8-4, 7.8-9, 7.8-10, 7.9-3, 7.9-4, 7.9-6, 7.9-8, 7.9-9, 7.9-11, BTP-16-8, BTP-19-1, BTP-19-2, BTP-19-8, T7.1-4

Standard design certification, 7.0-2, 7.0-8, BTP-16-2

Standardized safety analysis report, 7-C-3, BTP-16-7

Standby liquid control system (see also SLCS), 7-C-3, 7.1-A-7

Status accounting, BTP-14-24, BTP-14-28

Style, 7-C-8, BTP-14-5, BTP-14-9, BTP-14-28-35, BTP-14-37, BTP-14-38

Surveillance test, 7-A-2, 7.1-C-17, 7.5-7, BTP-17-1, BTP-17-3, BTP-17-5, T7.1-6, 7.1-7, 7.1-12, 7.1-A-23, 7.1-A-27, 7.1-B-8, 7.1-B-10, 7.1-C-13, 7.1-C-18, 7.9-5, BTP-17-2-4, BTP-8-1, 7-C-7, 7-C-8, BTP-17-2

SWC, 7-C-3, BTP-11-2, BTP-11-6

Technical Specifications Branch (see also TSB), 7-C-3, 7.0-6, 7.1-B-8, 7.1-C-14

Test case(s), BTP-14-23, BTP-14-22, BTP-14-23

Testability, 7-C-8, 7.0-A-2, 7.0-A-3, 7.1-4, 7.1-A-2, 7.1-A-8, 7.1-A-16, 7.1-B-4, 7.1-C-15, 7.2-2, 7.2-6, 7.3-3, 7.3-7, 7.4-7, 7.5-7, 7.9-3, 7.9-8, BTP-13-1, BTP-14-1, BTP-17-1, BTP-17-3, BTP-18-1, BTP-19-1, BTP-21-2, T7.1-3

Three Mile Island, (TMI), 7-C-3, 7.1-4, 7.1-13, 7.1-A-1, 7.1-A-2, 7.1-A-28, 7.2-2, 7.3-3, 7.3-7, 7.4-3, 7.5-3, 7.5-6, 7.5-9, 7.5-11, 7.6-2, 7.7-3, BTP-10-4, BTP-10-9, BTP-16-1, T7.1-1

Tier 1, 7-C-5, 7-C-8, BTP-16-1, BTP-16-2, BTP-16-7, BTP-16-8

Tier 2*, 7-C-8, 7-C-9, BTP-16-1-3, BTP-16-7, BTP-16-8

Tier 2, 7-C-5, 7-C-8, 7-C-9, BTP-16-1-3, BTP-16-7, BTP-16-8

Timing, 7-C-5, 7-C-6, 7-C-9, 7.0-A-8, 7.1-B-3, 7.1-C-8, 7.9-5, BTP-14-2, BTP-14-4, BTP-14-28-34, BTP-16-4, BTP-16-6, BTP-16-7, BTP-17-4, BTP-21-1-6

Topical report(s), 7.0-8, 7.0-A-14, 7.0-A-16, 7.1-5, 7.1-12, 7.1-14, 7.1-A-27, 7.1-B-10, 7.1-C-18, 7.1-C-19, BTP-13-6, BTP-14-6, BTP-14-39, BTP-14-40, BTP-18-4, 7.0-1- 7.0-3, 7.0-8, 7.0-9, 7.1-3, BTP-12-2, BTP-18-3, BTP-21-4, BTP-21-6

Traceability, 7-C-8, 7-C-9, 7.1-B-3, 7.1-C-7, BTP-13-3, BTP-13-4, BTP-14-5, BTP-14-9, BTP-14-13, BTP-14-26-38

TSB (see also Technical Specifications Branch), 7-C-3, 7.0-6, 7.1-B-8, 7.1-C-14, 7.1-C-17

Type testing, 7.0-, 7.0-A-4

Unambiguity, 7-C-8, 7-C-9, 7.1-B-3, 7.1-C-7, BTP-14-5, BTP-14-9, BTP-14-28-30, BTP-14-37

Understandability, 7-C-8, BTP-14-5

Unresolved safety issue(s), 7-C-3, 7.0-5, 7.1-10, 7.1-A-7, BTP-16-1

V&V (see also verification and validation), BTP-14-10, BTP-14-11, BTP-14-14, BTP-14-16, BTP-14-20, BTP-14-22, BTP-14-23, BTP-14-25, BTP-14-26, BTP-14-38

Validation, 7-C-3, 7-C-4, 7-C-9, 7.0-3, 7.0-4, 7.0-6, 7.0-7, 7.0-A-1, 7.0-A-3, 7.0-A-5- 7.0-A-7, 7.0-A-9, 7.0-A-11, 7.0-A-12, 7.0-A-15, 7.1-6, 7.1-12, 7.1-13, 7.1-A-21, 7.1-A-24, 7.1-A-26, 7.1-A-28, 7.1-C-10, 7.1-C-16, 7.2-8, 7.8-5, BTP-14-2, BTP-14-7, BTP-14-8, BTP-14-10, BTP-14-14, BTP-14-17, BTP-14-22, BTP-14-23, BTP-14-26, BTP-14-27, BTP-14-38, BTP-14-39, BTP-16-3, BTP-18-2, BTP-19-4, T7.1-5

Verifiability, 7-C-8, 7-C-9, 7.1-B-3, 7.1-C-7, BTP-14-5, BTP-14-9, BTP-14-28-36

Verification and validation (see also V&V), 7-C-3, 7-C-9, 7.0-4, 7.0-6, 7.0-A-5, 7.0-A-7, 7.0-A-12, 7.1-6, 7.1-12, 7.1-A-24, 7.1-A-26, 7.1-C-10, BTP-14-7, BTP-14-10, BTP-14-17, BTP-14-22, BTP-14-26, BTP-14-38, BTP-18-2

Verification, 7-C-3, 7-C-9, 7.0-4, 7.0-6, 7.0-A-5, 7.0-A-7, 7.0-A-9, 7.0-A-12, 7.0-A-14, 7.0-A-15, 7.1-4, 7.1-6, 7.1-12, 7.1-13, 7.1-A-24, 7.1-A-26, 7.1-A-28, 7.1-B-3, 7.1-C-7, 7.1-C-10, 7.2-8, 7.9-5, BTP-13-2-4, BTP-14-5, BTP-14-7, BTP-14-10, BTP-14-11, BTP-14-17, BTP-14-22, BTP-14-23, BTP-14-26, BTP-14-38, BTP-14-39, BTP-17-4, BTP-18-2, BTP-19-4, BTP-21-4-6, T7.1-5

Walkthrough(s), 7-C-9, 7.1-A-24

Watchdog timer(s), 7-C-9, BTP-17-2, BTP-17-3