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 IEEE Std 603, "Criteria for Safety Systems for Nuclear Power Generating Stations," has since superseded ANSI/IEEE Std 279.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

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 execute 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.