NUREG-0800
(Formerly NUREG-75/087)

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.

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.