NUREG-0800
(Formerly NUREG-75/087)

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

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.