U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

SECTION 7.2 REACTOR TRIP SYSTEM

REVIEW RESPONSIBILITIES

Primary - Electrical, Instrumentation and Control Systems Branch (EICSB)

Secondary - Auxiliary and Power Conversion Systems Branch (APCSB)
Core Performance Branch (CPB)
Mechanical Engineering Branch (MEB)
Quality Assurance Branch (QAB)
Reactor Systems Branch (RSB)

I. AREAS OF REVIEW

EICSB reviews Section 7.2 of the applicant's safety analysis report (SAR), which describes the reactor trip system (RTS). The reactor trip system, which is part of the reactor protection system, includes those power sources, sensors, initiation circuits, logic matrices, bypasses, interlocks, racks, panels and control boards, and actuation and actuated devices, that are required to initiate reactor shutdown. The RTS is designed to initiate automatically the reactivity control system (control rods), to assure that specified acceptable fuel design limits are not exceeded. It also includes those safety-related portions of control systems, the actions of which inhibit or limit the response of the reactivity control system to ensure that fuel design limits and safety limits are not exceeded.

Although the design configurations of RTS's for nuclear reactors vary significantly, it is possible by use of the diagram in Figure 7.2-1 to define the RTS of each nuclear steam supply system (NSSS) to the extent necessary for the purpose of identifying the EICSB primary review responsibility.

As shown in Figure 7.2-1, the RTS includes several sensors (usually 4) to measure each parameter such as neutron flux, primary system pressure, reactor outlet temperature, etc. These parameters are detected by sensors of various principles and types that provide electrical signals, mostly at low current or voltage levels. The sensors are located at many locations throughout the plant. It is necessary to determine that each location is suitable for the type of sensor used and that its transmission circuitry (channel) is properly routed to the RTS cabinets in which the electronic signal conditioning equipment is located. Most often, sensors are mounted on local racks and panels. Their arrangement should be considered in the review. For example, consideration should be given to the routing of sensing lines

from the process system taps to the sensors, the sensor mountings on racks, and the arrangement of local racks and panels within the plant. The paths of transmission circuitry include routing through containment electrical penetrations and into the cable spreading room. These regions deserve special review attention with regard to ascertaining RTS compliance with the acceptance criteria of Section II of this review plan.

The reactor trip system cabinets that include signal conditioning equipment, logic arrangements, test circuitry, indicators, alarms, and other features are the focal point of the RTS. The cabinets are usually located in the control room area. In addition to reviewing the cabinets and their contents against the acceptance criteria, the reviewer must show that the cabinets are not vulnerable to significant degradation from external influences. Other significant RTS cabinets include those that contain the system trip actuation devices themselves. The actuation devices and the power circuitry to the actuated devices (control rod drives) are also within the scope of the EICSB review; however, the control rod poison sections and the control drives are reviewed by others.

The power supply for the RTS is included in the EICSB review to the extent that the review must show that loss of power would not result in RTS failure to function. The review need not address the capability of the power supplies, usually motor-generator sets, to supply power. However, uniqueness of voltage and frequency requirements for certain RTS motor-generator sets and power supplies must be considered.

Testability of the RTS must be reviewed to ensure that the entire system is fully testable. The EICSB reviewer must ascertain that the test circuitry and test methods used do not compromise the independence of redundant circuits and equipment and do, in fact, enhance RTS reliability. This concern is particularly significant for newer solid state designs incorporating automatic test features.

Another review area of significance includes the interlock circuits that are provided to inhibit control rod motion. These are actuated from safety-related control system sensors such as those that monitor control rod position, turbine trip, etc. Also, protective interlocks actuated from loop isolation valve switches that are used to reset RTS parameter trip levels to more conservative values must be reviewed, along with manual selector switches that are also used to reset protection system trip levels as required for other modes of operation than the normal full power operating mode. These are shown schematically in Figure 7.2-1.

A review of measures involving reactor shutdown that are required to satisfy the design requirements for "anticipated transient without scram" (ATWS) events is included in this section. These measures, for the most part, have not been defined by nuclear steam system suppliers. The EICSB review of the proposed measures will be conducted to assure compliance with the staff technical report WASH-1270, Section V (Ref. 5). The criteria for measures required to make ATWS acceptable are currently under development and will be promulgated as branch technical positions and subsequently as regulatory guides.

The descriptive information, including electrical single line diagrams, electrical schematics (for the operating license stage only), logic diagrams, and physical arrangement drawings are reviewed. The objectives are to determine, on the basis of the most recent diagrams available, that the RTS satisfies the acceptance criteria and to determine that the RTS will perform its intended function during accident conditions and other transient conditions identified in the safety analysis report (SAR) accident analyses. This capability must be maintained during all plant operating modes including start-up power operation, shutdown, and refueling, as defined by the technical specifications.

The depth of review for a plant at the construction permit (CP) stage is limited. For a construction permit, design criteria and preliminary designs are reviewed in order to establish a basis for acceptance. The level of detail need only be sufficient to provide reasonable assurance that the final design will conform to the design bases and that the design bases themselves provide an adequate margin for plant safety. For an operating license (OL), the final design diagrams and results of analyses are reviewed to determine that the required safety functions can be accomplished.

The review is also to include evaluation of the proposed technical specifications to assure their adequacy. Refer to Standard Review Plan (SRP) 7.1 for the considerations involved.

In summary, the primary review area within the scope of the EICSB for SAR Section 7.2 includes:

1. The descriptive information, design bases, and analyses for the reactor trip system.

2. The descriptive information and design bases for supporting systems interfacing with and essential to the operation of the reactor trip system.

In cases where the design is similar to that of plants previously reviewed, the reviewer may determine that it is not necessary to review every facet of the design but may instead select and place emphasis on the most critical areas. Conversely, when concepts that have not previously been reviewed by the staff are received for review, evaluation considerations beyond those outlined in this section may be applied as necessary to assure that the proposed designs will function properly and meet all applicable requirements.

To assure that the auxiliary supporting systems that are essential to RTS operation will adequately maintain the required environmental conditions in areas of the plant where RTS equipment is located, APCSB support is required in the evaluation of cooling systems, heating and air conditioning systems, etc. The APCSB provides assistance in determining that the RTS will be capable of performing its function with auxiliary supporting systems degraded to their limiting conditions for operation. The auxiliary systems are described in SAR Chapters 9 and 10, for which APCSB has primary review responsibility.

Assistance is required from the CPB in reviewing the reactivity control aspects of the RTS, including negative reactivity available in control rods, allowable reactivity insertion or withdrawal rates, and reactivity distributions throughout plant life. The CPB reviews the

placement of neutron sensors with regard to measurement of the flux spatial dependence, the flux magnitude, and calibration effects for all operating modes throughout core life. CPB assistance is also required to establish technical specifications for core protection instrumentation with regard to limiting conditions for operation and limiting safety system settings. The plant nuclear design is discussed in SAR Section 4.3, for which CPB has primary review responsibility.

EICSB requires support from the MEB to review seismic qualification tests and supporting analysis for RTS equipment. The MEB review responsibilities in this regard are discussed in SRP 3.10.

The RTS design and construction must be carried out in accordance with the quality assurance requirements of 10 CFR Part 50, General Design Criterion 1 and Appendix B. QAB assistance is required to make this determination. QAB also determines that the quality assurance program documentation required of applicants and the proposed QA/QC organizations are acceptable. The QAB review responsibilities are discussed in SRP 17.1 and 17.2.

To assure that the location, number, and ranges of sensors provided to monitor the performance of the reactor heat transfer systems and related equipment are adequate, the EICSB requires RSB support. RSB assistance is also required to establish technical specification requirements for heat transfer system instrumentation with regard to limiting conditions for operation and limiting safety system settings. The RSB primary review responsibilities are discussed in SRP 4.4, 6.3, and 15.

II. ACCEPTANCE CRITERIA

In general, the reactor trip system is acceptable if it includes adequate redundancy; meets the single failure criterion; has the capacity and capability to safely and reliably shut down the reactor; is fully testable; is capable of functioning during and after design basis events and accidents; and satisfies applicable requirements of the regulations and the recommendations of Institute of Electrical and Electronic Engineers (IEEE) standards, regulatory guides, and branch technical positions. Section V of this plan lists those regulations, standards, guides, and positions used by the reviewer as aids in ascertaining that the above criteria have been met. Section III of this plan discusses the application of these evaluation guides to the review.

The general design criteria and IEEE Std 279-1971 set forth requirements that must be met by all RTS designs. Supporting auxiliary systems must also satisfy these requirements. Appendix A to this plan provides the reviewer with a summary of the use of IEEE Std 279 in the review.

The regulatory guides and branch technical positions set forth acceptable methods of implementing criteria and are not requirements. They serve to resolve problems by proposing particular solutions. Industry standards and topical reports referenced in a SAR may be used as a basis for approval of a design. However, acceptability of the standards and topical reports referenced, but not previously reviewed, must be determined in order to complete the review of the SAR.

Acceptance criteria for specific areas of RTS design are as follows (a complete listing of these criteria is included in Table 7-1, attached to the Chapter 7 standard review plans):

1. System Redundancy Requirements

   General Design Criteria 20 through 29 set forth requirements with regard to functional redundancy considerations. General Design Criteria 2, 3, and 4 set forth the external considerations that must be reviewed to assure that redundancy is not compromised. IEEE Std 279 and IEEE Std 379 are also useful to the reviewer in determining redundancy requirements for the RTS.

2. System Conformance with the Single Failure Criterion

   The General Design Criteria applicable to the preceding discussion on system redundancy requirements (II.1, above) apply equally to system conformance to the single failure criterion. In addition to the general requirements of these regulations, Regulatory Guide 1.53 (as it relates to IEEE Std 379) and IEEE Std 279, paragraphs 4.2, 4.7.3, 4.7.4, 4.7.4.1, 4.7.4.2, and 4.11 explicitly address the single failure criterion and form the basis for judging system conformance to the single failure criterion. Also, see Appendix A to this plan for additional guidance.

3. System Capability and Reliability

   The general requirements for RTS capability are included in General Design Criteria 20 through 29. With the exception of RTS response time, the analyses performed by the CPB and described in SRP 4.3 serve as the basic acceptance criteria for capability. The basis for system response time acceptance is established in the SAR, usually in Chapters 7 and 15. RTS reliability considerations and their conformance to General Design Criterion 21 are based on analyses, as documented in NSSS topical reports, and on testing and operating experience with given hardware.

4. System Testability

   The criteria used to judge system testability and conformance with General Design Criterion 21 are basically those contained in IEEE Std 279, IEEE Std 338, and Regulatory Guide 1.22. In addition, initial qualification of the system must be found acceptable on the basis of IEEE Std 336, IEEE Std 344 (as modified by Branch Technical Position EICSB 10), and Regulatory Guide 1.68 with regard to surveillance. Also, an acceptable design must satisfy Regulatory Guide 1.47 as augmented by Branch Technical Position EICSB 21.

5. System Capability During and Following Design Basis Events

   The method used to assure that the RTS will be capable of performing its protective function during and following design basis accidents is that of equipment qualification for the conditions postulated to accompany the events.

   General Design Criteria 2, 3, and 4 identify events of concern and state acceptance objectives. IEEE Std 344 (as modified by Regulatory Guide 1.29 and Branch Technical Position EICSB 10) for seismic qualification, IEEE Std 317, IEEE Std 323, and

IEEE Std 336 for environmental qualification provide the acceptance criteria. IEEE Std 336 is augmented by Regulatory Guide 1.30, IEEE Std 317 is augmented by Regulatory Guide 1.63, and IEEE Std 323 is augmented by Regulatory Guide 1.89.

6. Identification of Control Panels, Racks, Equipment, Cables, and Cable Trays
The method used for identifying RTS cables and cable trays as safety-related equipment in the plant, and the identification scheme used to distinguish between redundant equipment, racks, panels, cables, and cable trays are acceptable if found to be in accordance with Section 5.1.2 of Regulatory Guide 1.75. IEEE Std 279, paragraph 4.22 also addresses identification criteria.

7. Separation of Equipment, Cables, and Cable Trays
Regulatory Guide 1.75 provides a basis for review and acceptance of the separation criteria presented in the SAR.

8. Vital Supporting Systems
The auxiliary systems that are required to assure RTS functional capability should satisfy the same acceptance criteria as the RTS.

9. Technical Specifications
The acceptance criteria for technical specifications are identified in 10 CFR §50.34 and 50.36. Usually the most recently licensed plant of the type being reviewed serves as a model for the technical specifications. Standard technical specifications are also in preparation at this time. Refer to SRP 7.1 for technical specification considerations.

For those areas of review identified in Section I of this plan as being the responsibility of other branches, the acceptance criteria and their application are included in the appropriate sections of the applicable standard review plans. There are criteria that are used by both primary and secondary review branches as the basis for accepting a design. As they relate to the RTS, some of these criteria and their application are presented below.

In assuring the adequacy of the seismic design of Category I instrumentation and electrical equipment, both the MEB and EICSB perform reviews to ascertain that the proposed design satisfies IEEE Std 344 as supplemented by Branch Technical Position EICSB 10.

To assure that the requirements of General Design Criterion 1 and Appendix B of 10 CFR Part 50 are met in the reactor trip system, the quality assurance program for the RTS Class IE instrumentation and electrical equipment must satisfy the requirements of IEEE Std 336, as augmented by Regulatory Guide 1.30.

III. REVIEW PROCEDURES

The main objectives in the review of the reactor trip system are to determine that this system includes the required redundancy, satisfies electrical and physical independence requirements and the single failure criterion, has the capability and reliability required, is testable, is capable of performing its function during and following design basis events,

and can safely shut down the reactor in conformance with all the general design criteria requirements for RTS and the requirements documented in the accident analysis chapter of the safety analysis report.

In the construction permit (CP) review, the descriptive information, including system safety design bases and their relationship to the acceptance criteria, preliminary analyses, electrical single line diagrams, preliminary physical arrangement drawings, functional logic diagrams, and functional piping and instrument diagrams (P&IDs) are examined to determine that there is reasonable assurance that the final design will meet the above objectives. Included in this review, the design criteria for establishing trip setpoints must be evaluated to show conformance to the following guidelines:

(1) The range selection for instrumentation shall be such as to exceed the expected range of the process variable being monitored.
(2) The accuracy of all the safety trip points will not be numerically larger than the accuracy that was assumed in the accident analysis.
(3) The trip setpoints should be located in that portion of the instrument's range which is most accurate and must be located in a region with the required accuracy.
(4) All safety trip points will be chosen to allow for the normal expected instrument system setpoint drift such that the technical specification limit will not be exceeded.
(5) Verification of the above criteria shall be demonstrated as a part of the qualification test program required by IEEE Std 323-1974.

At the operating license (OL) stage of review, these objectives are verified in the review of final electrical schematics and physical arrangement drawings. In addition, a site visit is conducted to assure that the design objectives have, in fact, been implemented in accordance with the design bases and criteria. Appendix 7-B to the Chapter 7 standard review plans contains a typical site visit agenda.

This section describes the method and reasoning to be employed by the reviewer in making a determination as to RTS acceptability. For the purpose of illustration, the RTS system as presented in Figure 7.2-1 is shown as being comprised as two identical, redundant subsystems.

Prior to reviewing Section 7.2 of the SAR, the following background information should be briefly reviewed, in addition to the balance of Chapter 7:

Chapter 1 of the SAR, to become familiar with the general operation of the plant, from both the safety and the operational standpoints.

Chapter 4, the reactor design, in particular the nuclear design, Section 4.3, and the thermal and hydraulic design, Section 4.4.

Chapter 5, on the design of the reactor coolant system, Sections 5.1, 5.2.1, and 5.2.2.

Chapter 6, to note the engineered safety feature provisions.

Chapter 15, to become familiar with the representative types of events for which analyses have been documented. In particular, the effects of failures of the protective functions, and the assumptions and initial conditions that form the bases of the accident analyses are noted.

Chapter 16, to become familiar with limiting conditions for operation, limiting safety system settings (i.e., trip setpoints), and surveillance requirements that pertain to the RTS.

Chapter 17, to note the quality assurance considerations addressed.

The single most relevant document used in the review of the RTS is IEEE Std 279. Conformance of the RTS to the design requirements stated in Sections 3 and 4 of this standard, together with conformance to the requirements of the general design criteria and the functional requirements derived from the accident analyses, will result in an acceptable design. Guidance on the use of IEEE Std 279 is provided in Appendix A of this plan. The general methodology by which the reviewer conducts his review is outlined below by addressing "key concerns" such as redundancy, independence, single failures, capability, and testing.

1. System Redundancy Requirements

With the assistance of the CPB and the RSB, as needed, EICSB determines that the system redundancy requirements are satisfied. Generally, a minimum degree of redundancy of one satisfies RTS requirements. Most RTS parameters are monitored by four sensor channels and only two of four channels are required to initiate the RTS logic channel protective action.

Where it is determined that the spatial dependence of a parameter requires several sensor channels to assure core protection, the redundancy requirements are determined for the individual case. Once design adequacy is established, the reviewer must relate the design requirement to the limiting conditions for operation in the technical specifications. In certain designs, for example, adequate monitoring of core power requires a minimum number of sensors arranged in a given configuration to permit unrestricted power operation. When, because of system degradation, the minimum number of sensors are not available, operation must be restricted. This aspect of redundancy must be dealt with in coordination with the CPB to establish conditions of restricted operation.

Another area where the redundancy requirement of the RTS may have to be defined on an individual core basis is the allowable power operation for reactor coolant systems that have loop isolation valves. Here, the redundancy of the instrumentation provided on the reactor coolant system piping, and on steam generators in the case of pressurized water reactors (PWR's), must be reviewed with the RSB to determine whether the reactor system instrumentation redundancy (not channel redundancy) requirement has been degraded below that on which the accident analyses are based if isolation valves are closed.

With regard to redundancy requirements considered strictly from an electrical point of view, it is only necessary to assure that at least two redundant logic trains (minimum degree of redundancy of one) are provided to initiate reactor trip. From this standpoint the review may be reduced to a simple analysis in which redundant paths from sensors to logic and to actuation devices are identified to assure that the RTS functional requirements are met. It is pointed out that redundancy may be accomplished by equipment that is diverse in principle so long as the same level of protection is provided.

In this discussion on RTS redundancy, it is appropriate to reference Figure 7.2-1. Notice that for required protective functions, the RTS sensors, initiation devices, logic matrices, and actuation and actuated devices all must be redundant. Also note that modules of one channel must not affect those of another channel.

Another area that must be reviewed with regard to redundancy has to do with the measures to be included in nuclear power plants to deal with ATWS events. These measures must be reviewed to assure that they are unaffected by failures that could disable the RTS.

2. System Conformance with the Single Failure Criterion

In evaluating the adequacy of the RTS system in meeting the single failure criterion, both electrical and physical independence must be considered.

a. Electrical Independence

To assure electrical independence, the design bases governing the electrical independence of redundant sensors, logic elements, and actuation channels are required to satisfy not only paragraph 4.6 of IEEE Std 279, which states that, "channels that provide signals for the same protection function shall be independent, and the likelihood of interaction between channels is considered," but also, the requirement of paragraph 4.7.2. This paragraph requires that, "the transmission of signals from protection system channels that are used for other purposes, (non-protective) such as control or readout and indication, are properly isolated to ensure that no credible failure at the output of an isolation device shall prevent the associated protective channel from meeting performance requirements." Examples of credible failures at the output of isolation devices are provided in paragraph 4.7.2.

b. Physical Independence

To assure physical independence, the design bases governing the physical separation of redundant equipment including sensors, cables, cable trays, racks, panels, and control boards are required to be in accordance with Regulatory Guide 1.75, "Physical Independence of Electric Systems." This regulatory guide sets forth acceptance criteria for the physical separation of circuits and electrical equipment that is included in the RTS.

Another review objective is to determine whether the RTS is located in seismic Category I structures. In certain designs, RTS sensors may be located in

non-seismic Category I structures such as the turbine building. For these special cases, the reviewer must assure that the most reasonable installation of sensors and circuits is provided in regard to physical protection against damage from a seismic event. Further guidance is provided by Branch Technical Position EICSB 15.

c. Single Failure Criterion

To assess the RTS acceptability with regard to the single failure criterion, IEEE Std 379 and Regulatory Guide 1.53 are used. Again, as was the case for redundancy requirements, review for compliance with the single failure criterion may be reduced to an analysis in which it is determined that the system can perform all protective functions concurrent with failure of any sensor, logic circuitry and components that meet the single failure cirterion. IEEE Std 279, paragraph 4.2, provides an additional example of single faiulre criterion application.

With regard to power requirements, the RTS must be reviewed to assure that no failure of a power supply will result in maintaining power to the system such that the protective function (trip) of the RTS is negated (fail-safe design). For example, loss of power to a sensor channel should cause a channel trip. Similarly, a loss of power to a logic element or actuator channel should result in a trip. Exception to this latter rule may be taken so long as the single failure criterion is satisfied and the power sources required are designed as Class IE power systems.

The RTS logic matrices should be reviewed to determine whether redundant circuitry includes the contacts of relays or switches in mutually redundant logic ciruits. This task can be accomplished during the OL detailed drawing review. When violations of the single failure criterion are found, they are to be identified to the applicant and corrected. The staff safety evaluation report should discuss the final disposition of designs that are revised to satisfy the acceptance criterion.

The RTS equipment arrangement must be reviewed to assure that no single credible event will result in a loss of redundant circuits or equipment. This matter is discussed further in III.5.b, below.

3. Identification of Control Boards, Equipment, Cables, and Cable Trays

To determine that the identification scheme used for Class IE equipment, cables, and raceways in the plant and Class IE internal wiring in the control boards is consistent with Regulatory Guide 1.75, the criteria proposed for identifying Class IE wiring cables, and cable trays are reviewed. This includes such criteria as those for distinguishing between safety-related cable trays of different channels, non-Class IE cable which is run through Class IE cable trays, and non-Class IE cable which is not physically associated with any Class IE division. IEEE Std 279, paragraph 4.22, also discusses identification. Color coding is a preferred method of identification. In

multi-unit paths that share source spaces, it is particularly important to retain unit identifications along with channel identification.

4. System Testing and Inoperability Surveillance

The proposed preoperational and initial startup test programs for the RTS and its supporting systems are reviewed to verify that the proposed programs are consistent with the requirements set forth in IEEE Std 279, IEEE Std 308 (as augmented by Regulatory Guide 1.32), and Regulatory Guides 1.22 and 1.68.

The descriptive information as supplemented by functional logic diagrams (CP and OL) and electrical schematics (OL) are reviewed to verify that the design has the necessary provisions to permit testing of the RTS on a periodic basis when the reactor is in operation. The reviewer is guided by the recommendations set forth in Regulatory Guide 1.22 and IEEE Std 279, paragraph 4.10, in arriving at an acceptable method of periodic testing of actuation devices (e.g., solenoids, breakers) and actuated equipment (control rods). The same guidance is used to review testability of all modules, relays, permissives, bypasses, and safety-related control devices.

The descriptive information (CP and OL) and the design implementation as depicted on electrical drawings (OL) of the means proposed for automatically indicating, at the system level, bypassed or deliberately inoperable RTS protection channels are reviewed to ascertain that the design is consistent with Regulatory Guide 1.47 as supplemented by Branch Technical Position EICSB 21 and with IEEE Std 279, paragraph 4.13.

5. Other Matters

a. The Technical Specification considerations for the RTS are outlined in SRP 7.1

b. The APCSB reviews supporting systems such as heating and ventilating component cooling water, service water, etc. to assure that failure of these supporting systems will not result in loss of RTS function as result of a degraded environment. It is necessary to assure that those systems required to maintain environmental conditions within the envelope for which the RTS equipment and circuits were designed and qualified be monitored for performance. Examples of such systems include control room and switchgear room heating and ventilating systems.

THE APCSB should also assist in determining hazardous conditions that might follow failure of non-safety equipment in regions where RTS components and circuits are located. Specific failures must include, as a minimum, the following: fire, missiles, flooding, jet impingment from pipe breaks, and damage that may be caused by failure of non-seismic Category I structures and components. The EICSB relates these conditions to the ability of the RTS to retain functional capability.

c. To assure that the RTS provides adequate core protection, the CPB should confirm that the accident analyses of SAR Chapter 15 have addressed the requirements of IEEE Std 279, Section 3, "Design Basis." To accomplish this task, it is necessary to confirm that the accident analyses have taken into consideration such matters

as spatial dependences, operational limits and margins, transient ranges, system response times, and signal and instrument accuracies.

d. The MEB has primary responsibility for assuring that the seismic design of Category I instrumentation and electrical equipment satisfies appropriate requirements. These include IEEE Std 344 and Branch Technical Position EICSB 10. EICSB supplements the MEB by reviewing the description of the seismic qualification test program (CP) and the results of such tests and analyses (OL) that demonstrate the capability of Class IE instrumentation, control devices, and associated circuits to withstand the effects of seismic event. An integrated review is required.

IV. EVALUATION FINDINGS

The reviewer verifies that sufficient information has been provided and that the review supports conclusions of the following type, to be included in the staff's safety evaluation report:

"The reactor trip system includes the initiating circuits, logic, bypasses, interlocks, redundancy, diversity, and actuated devices utilized to implement reactor shutdown. The scope of the review included the descriptive information (CP and OL), functional logic diagrams (CP and OL), functional instrumentation and electrical diagrams (CP and OL), and preliminary (CP) and final (OL) physical arrangement drawings and schematics. The review has included the applicant's design bases and their relation to the proposed design for the reactor trip system. The review has also included the proposed means for identification of cables and equipment, periodic testing capability, and the qualification test program (CP) and the results (OL) for demonstrating the suitability of the reactor trip system.

"The basis for acceptance in our review has been conformance of the applicant's designs, design criteria, and design bases for the reactor trip system and vital supporting systems to the Commission's regulations as set forth in the general design criteria and to applicable regulatory guides, branch technical positions, and industry standards. These are listed in Table 7-1.

"On the basis of our review we have concluded that the reactor trip system conforms to applicable regulations, guides, technical positions, and industry standards, and is acceptable."

V. REFERENCES

1. Standard Review Plan Table 7-1, "Acceptance Criteria for Controls."

2. Standard Review Plan Appendix 7-A, "Branch Technical Positions (EICSB)."

3. Standard Review Plan Appendix 7-B, "General Agenda, Station Site Visits."

4. Regulatory Staff, "Technical Report on Anticipated Transients Without Scram," WASH-1270, U.S. Atomic Energy Commission, September 1973.

APPENDIX A

STANDARD REVIEW PLAN 7.2

USE OF IEEE STD 279 IN THE REVIEW OF THE RTS

This appendix discusses the requirements of IEEE Std 279-1971, Section 4, as they are used in the review of the RTS.

1. Section 4.1 - This section requires that the RTS perform automatically and with precision and reliability. These requirements must be met over the full range of transient and steady-state conditions. The system must meet these requirements in any environmental condition expected during plant operation in which the applicant's accident analyses take credit for the function performed by the RTS. Other criteria which set forth similar requirements are GDC 2, 4, 10, 13, 20, 21, and 29.

   a. Automatic initiation is required for all protective functions. Manual initiation is also provided and is a requirement. (See Section 4.17 and Regulatory Guide 1.62.)

   b. The precision required in the RTS is that assumed in the accident analyses. (Precision requirements are identified in Section 3.9 of IEEE Std 279.)

   c. Quantitative reliability information for RTS often presented in NSSS topical reports. The reliability requirements for RTS are primarily satisfied by related reactor operating experience. The staff is actively pursuing the question of RTS reliability and the potential for RTS loss of function. (See Reference 5, Section V of SRP 7.2.)

   d. The requirements for precise and reliable operation suggest that the RTS design should avoid unnecessary complexity. "Unnecessary complexity" is a difficult judgement: the reviewer should discuss his concerns with the system designer in detail, and should consult with the section leader and branch chief on this matter.

2. Section 4.2 - This section requires that the reviewer examine several different aspects of each single failure to determine its effect.

   a. The first step in a single failure analysis is to identify components that are not seismic Category I, those that are not qualified for accident environments, and those that serve both safety and non-safety systems. Each of the non-qualified and non-safety grade components and systems are assumed to fail to function if failure adversely affects RTS performance and are assumed to function if functioning adversely affects RTS performance.

b. The consequences of events for which the RTS is designed to provide a protective function are examined. All failures in the RTS that can be predicted to occur as a result of the events are assumed to occur if such events adversely affect RTS performance. In general, the lack of equipment qualification may serve as a basis to assume failures.

c. After assuming the failures of non-safety grade, non-qualified equipment and those failures in the RTS caused by an event, any other single failure is arbitrarily assumed and the resultant performance of the RTS is analyzed to assure that the minimum protective function will be performed.

d. The single failure criterion applies to all electric equipment. No distinction is made between active and passive components.

e. IEEE Std 379 and Regulatory Guide 1.53 are used for additional insight to single failure criterion analysis.

3. Section 4.3 - There are no specific criteria to judge the quality of the equipment used in the RTS. However, Appendix B to 10 CFR Part 50 provides some guidance from which a judgment may be made of the quality of equipment required for the RTS.

4. Section 4.4 - It is verified that each component and module has been qualified for normal, upset (i.e., operational transient), and accident environments at its installed location. This applies to all normal and upset conditions, but only to those accident conditions where the components and modules provide a protective function. The components must provide the accuracy, range, and response times required by the accident analyses. SRP 3.10 and 3.11 discuss equipment qualification.

5. Section 4.5 - No credit should be given for "safe" failure modes in meeting this requirement. The comments of Section 4.4 apply. For example, if the most probable effect of a given accident is a loss of energy supply to the RTS, it does not matter, in meeting this requirement, whether or not the loss of energy causes the RTS to perform its protective function. Even though GDC 23 requires that the RTS be designed to "fail safe," acceptance of the RTS design shall not be based on an accident causing a failure, even if that accident-induced failure accomplishes the protective function.

6. Section 4.6 - The requirement for channel independence applies to all portions of the RTS that are designated as redundant channels. Independence is maintained in a number of ways. Physical independence is attained by physical separation and physical barriers. Electrical independence is achieved by isolation devices and utilization of separate power sources and other circuit devices. Verification of compliance with physical separation requirements may be made by comparing the design to Regulatory Guide 1.75 recommendations.

7. Section 4.7 - Control and protection system interaction involves more than examining their electrical isolation and interconnection. The functional performance of control systems must be reviewed to the extent that it is determined that a control system cannot prevent

proper action of a protection system. This section of IEEE Std 279, with regard to isolation devices and multiple failures resulting from a credible single event, is explained by example in the document.

8. Section 4.8 - This requirement is self-explanatory. A protection system that requires loss of flow protection would normally derive its signal from flow sensors. A designer might elect to use an indirect parameter such as a pressure signal or pump speed. The reviewer should review the system to determine whether the indirect parameter would be valid at all times.

   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.

9. Section 4.9 - The most common method used to verify the availability of the RTS input sensors is by cross checking between redundant channels that have readout available. When only two channels of readout are provided, evaluate the applicant's analysis of the effect of the operator choosing the incorrect readout as a basis for operator actions.

   When non-indicating sensors are used, check the test procedure to see whether a bypass indication is provided when the sensor is disabled. Of course, this latter approach should also be applied to indicating sensors when the design necessitates.

10. Section 4.10 - The extent of test and calibration capability that is provided bears heavily on whether the design meets the single failure criterion.

    a. Any failure that is not detectable must be considered concurrently with any postulated, detectable, single failure.

    b. Periodic testing should duplicate, as closely as practical, the overall performance required of the RTS. The test should confirm operability of both the automatic and manual circuitry. This capability must be provided to permit testing during power operation. When this capability can only be achieved by overlapping tests, the test scheme must be reviewed in detail to confirm that the tests do, in fact, overlap from one test segment to another.

    c. Test frequencies are acceptable if identical to frequencies recently approved on other identical plants. Any changes made in the design or test procedures are not an adequate basis for reducing test frequencies until after experience is gained and the results submitted for review.

    d. 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. Check that periodic tests conducted during power operation use only permanently installed test equipment. Also see Regulatory Guide 1.22 and Branch Technical Positions EICSB 22, 24, and 25.

11. Section 4.11 - It is verified that tests can be conducted without initiating a protective action at the system level, and that tests can be conducted without preventing the initiation of a protective action at the system level. In general, it is an operational rather than a safety problem if testing causes the initiation of a protective action. For those parts of the RTS with a degree of redundance greater than one, testing should not require bypass of the channel level protective action. For one-out-of-two systems, the channel protective action may be bypassed only if initiation of the protective action would disrupt plant operation. The bypassed channel must remain operable and operating. In these cases, verify that an interlock is provided that prevents, even with a single failure in the interlock circuits, bypassing both channels and that the single bypass is indicated. See Regulatory Guide 1.22 and Branch Technical Position EICSB 24.

12. Section 4.12 - The requirement for automatic removal of operational bypasses means that the reactor operator shall have no role in such removal. The operator may be required to take action to prevent the unnecessary initiation of a protective action and this is acceptable. In no circumstance should a design be approved where action or inaction of the reactor operator is required to make available the protective actions needed in any operational or shutdown mode of the plant.

13. Section 4.13 - See Regulatory Guide 1.47 and Branch Technical Position EICSB 21 for an explanation of this requirement as it pertains to the RTS.

14. Section 4.14 - In practice, administrative control is used as the basis for assuring 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.

15. Section 4.15 - This requirement is similar to Section 4.12. The phrase "positive means" can be interpreted as either automatic or manual. In the case of manual means, the design must be such that no action or inaction on the part of the reactor operator will prevent the more restrictive set point from being available. It is acceptable for the design to be such that incorrect action or inaction by the operator will cause an unnecessary protective action or prevent placing the plant in an operating mode for which there is inadequate protection.

16. Section 4.16 - "Completion of a protective action" must be defined by the applicant for the RTS. This information should be supplied as a part of the design basis information required by Section 3.0 of IEEE Std 279.

    Generally, completion consists of causing negative reactivity to be inserted. Verify that once initiated, the protective action will continue to completion. Termination by deliberate actions of the operator should never inhibit the protective action.

17. Section 4.17 - Regulatory Guide 1.62 describes an acceptable method of implementing the requirement for manual initiation of protective actions. For those designs that take no credit (in the accident analyses) for manual initiation of protective actions, conformance

with Regulatory Guide 1.62 is an adequate basis for acceptance. In practice, the requirements of IEEE Std 279 are applied to all equipment used by the operator to detect the need for the protective action, to accomplish the protection action, and to confirm completion of the protective action. However, it first should be established that automatic initiation need not or cannot be provided. Cost is not sufficient justification for the lack of automatic initiation.

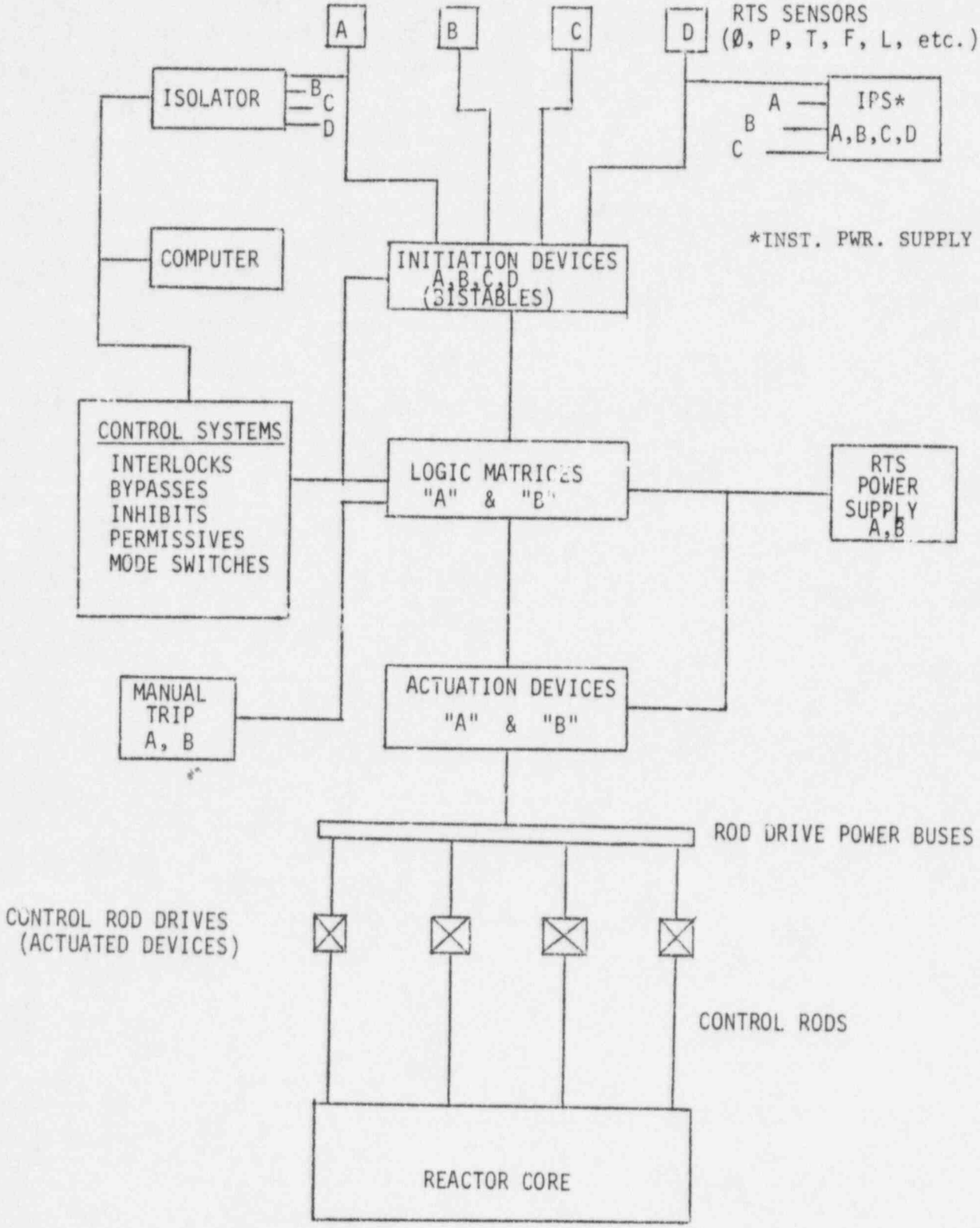
18. Section 4.18 - See procedure above for Section 4.14.

19. Section 4.19 - The method of identification of status at the channel level may be accomplished by lights, indicators, and annunciators.

20. Section 4.20 - The method used to establish adequacy of information readout would include a review of the RTS system inputs to annunciators and event recorders. Engineering judgement serves as the basis for acceptance.

21. Section 4.22 - This requirement is self-explanatory. The preferred identification method is color coding of components, cables, and cabinets. See also Regulatory Guide 1.75.

FIGURE 7.2-1
REACTOR TRIP SYSTEM
(Typical)



SRP 7.3