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

SECTION 7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

REVIEW RESPONSIBILITIES

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

Secondary - Auxiliary and Power Conversion Systems Branch (APCSB)
Reactor Systems Branch (RSB)
Quality Assurance Branch (QAB)

I. AREAS OF REVIEW

The areas reviewed in this section of the applicant's safety analysis report (SAR) include such control systems as the primary system pressure, temperature and water level controls, feedwater controls, and main turbine controls. The intent of the review is to assure that failures of these would not impair the protection system capability in any significant manner. Since the control systems of interest may vary from plant to plant depending on individual designs, the applicant should identify all such systems and provide analyses to support their classification as non-safety-related control systems.

The EICSB will review the following aspects of the non-safety-related control systems: the circuit-to-circuit failure modes of a single non-safety control system and their effect on the protection system, and gross failure modes of non-safety control systems and their functional effect on the protection system.

The APCSB and RSB provide assistance in verifying that all control systems have been identified and that the input signal parameters for the control systems are correct. The RSB determines that the control systems identified in this section are not required for safety and that no credit is taken in the plant accident analyses for the control systems identified as non-safety in this section.

The QAB verifies that the quality assurance program implemented for control system components, where necessary, is adequate.

II. ACCEPTANCE CRITERIA

The control systems not required for safety are acceptable if failures of control system components or total systems would not significantly affect the ability of plant safety systems to function as required, or cause plant conditions more severe than those for which the plant safety systems are designed.

Table 7-1 of this plan lists ghose deneral cesign Criteria (GDC) of Appendix A to 10 CFR Part 50, and standards of the Institute of Electrical and Electronic Engineers (IEEE) that are used as references in arriving at this conclusion. GDC 13 and 24 and IEEE Std 279, Section 4.7, are of special importance among these references.

1. Conformance with GDC 13 for Instrumentation and Control Requirements. Instrumentation should be provided to monitor variables and systems over their anticipated ranges for normal operation and for anticipated operational occurrences as appropriate to minimize challenges to safety systems. Appropriate controls should be provided to maintain these variables and systems within prescribed operating ranges.

2. Conformance with GDC 24 for Separation of Control Systems from Protection Systems. The protection system shall be separated from control systems to the extent that failure of any single control system component or channel which is common to control and protection systems shall not violate the reliability, redundancy, and independence requirements of the protection system. The interconnections between the protection and control system shall be limited so as to assure that safety is not significantly impaired.

3. Conformance to IEEE Std 279, Section 4.7 for Control and Protection System Interaction. The direct circuit-to-circuit and functional interactions between control and protection systems for single random or multiple failures in the control system shall not prevent the protection system channel from meeting the minimum performance requirements specified in the design bases.

III. REVIEW PROCEDURES

1. The objectives in the review are:
   a. To establish that control systems identified as being non-safety-related, which may include, depending on plant design, the primary system pressure, temperature, and feedwater controls, steam generator water level controls, and main turbine controls are, in fact, not required for plant safety.
   b. To verify that no credit is taken for the operability of these control systems in the plant accident analyses in Chapter 15 of the SAR.
   c. To assure that failures of these control systems would not impair the capability of the protection system in any significant manner or cause plant conditions more severe than those for which the plant safety systems are designed.
   d. To establish that control system designs meet applicable requirements of the general design criteria and industry standards with regard to independence between control and protection functions.

2. In the construction permit (CP) review the descriptive information including the design bases and preliminary analyses, are reviewed to determine that there is reasonable assurance that the final design will meet these objectives. The RSB and APCSB identify the systems whose control system designs are to be reviewed and verify that no credit is taken for their operability in the plant accident analyses. EICSB reviews the descriptive information provided for those systems

at the CP stage to assure that control and protective functions are adequately separated and to assess the effects of control system failures, or to verify that commitments are made that such failures will be included in the plant safety design bases.

3. At the operating license (OL) stage, the objectives in (1) above are verified during the review of control system schematics. At the OL stage, EICSB reviews electrical schematic drawings for these control systems as necessary to assure that adequate attention has been given to the separation of control and protective functions and to possible effects of failures of these systems. The review includes interactions between control systems and effects on plant operation and safety systems due to control system malfunctions or failures.

4. A typical review procedure for pressurized water reactor (PWR) primary and secondary control system functions follows:

   a. The primary system pressure is maintained within specified limits by the use of pressurizer heaters and spray valves. The primary pressure control system description and schematics are reviewed:
      (1) To confirm that the system will maintain the primary coolant pressures within prescribed limits for normal and transient operating conditions.
      (2) To determine the effects of loss of power to the pressurizer heaters and spray valves.
      (3) To determine the effects of loss of air to any pneumatically-operated valves in the spray system.

      Assistance as needed is obtained from the RSB in evaluating these items.

   b. To meet the requirements of GDC 24 and Section 4.7 of IEEE Std 279 on control system interactions with the protection system, loss of primary pressure control function is analyzed. Assistance is obtained from RSB in establishing the sequence of events that would follow. The evaluation should show that failure of the primary pressure control system would not significantly degrade the capability of the protection system. Also, the reviewer determines that where a random failure in the pressure control system results in a plant condition requiring protective action and can also prevent proper action of a protection channel designed to protect against the condition, the remaining redundant channels will provide the protective action even when degraded by another random failure.

   c. The system description and control schematics of the feedwater regulating system are reviewed for failure modes of the system components. Assistance is obtained from the RSB and APCSB in identifying the control function parameters. The system actions are established for loss of air to the feedwater control valves and malfunction in the feedwater heater bypass valves. The reviewer should verify that manual override of the automatic control is designed into the system.

   d. The reviewer evaluates the effects of multiple failures in control systems resulting from single events. Failures in the secondary system water level

(i.e., feedwater flow and steam generator water level) controls are analyzed along with failure in the primary coolant pressure control, where a single event can cause these multiple failures. With the assistance from the RSB and APCSB the reviewer determines that control function failures of both primary pressure and secondary water level controls would not prevent the minimum required number of reactor protection system channels from tripping the reactor.

5. The following aspects of main turbine control systems are reviewed:
   a. The reviewer verifies that the turbine overspeed protection system is designed with redundant speed sensing instrumentation and logic circuitry, so as to ensure that no single failure would prevent the overspeed trip system from operating. The overspeed trip system should have the capability to permit online testing of its instrumentation and logic circuitry when the turbine is in operation.
   b. The controls that provide for automatic turbine runback on receipt of appropriate signals from the reactor systems are reviewed for the following points:
      (1) The signals should be redundant, with independent power supplies.
      (2) Physical independence should be maintained between redundant initiating circuits.
      (3) Although redundancy is not practical in the final device, the signals should actuate different control devices.
      (4) The final actuating device should be of high reliability.

In certain instances, it will be the reviewer's judgement that for a specific case under review, emphasis should be placed on specific aspects of the design, while other aspects of the design need not receive the same emphasis and in-depth review. Typical reasons for such a non-uniform placement of emphasis are the introduction of new design features or the utilization in the design of design features previously reviewed and found acceptable.

IV. EVALUATION FINDINGS

At the CP stage, it should be established that the information and commitments documented in the preliminary safety analysis report (PSAR) provide reasonable assurance that the final designs of non-safety-related control systems will conform with the intent of this plan.

At the OL stage, sufficient design detail of these control systems is reviewed to determine adequate conformance. Exceptions to the acceptance basis given in Section II are identified, with a statement as to how these exceptions provide a conservative basis for engineering design of the affected control systems.

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

"The staff has reviewed the controls for systems not required for safety, to determine the affects of failures or malfunctions of these controls on the reactor protection system and other plant safety-related systems. We conclude that failures

or malfunctions of these controls would not be expected to degrade the capabilities of plant safety systems in any significant degree, or to lead to plant conditions more severe than those for which the safety systems are designed."

V. REFERENCES

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

SRP Appendix 7-A