



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

SEP 10 1981

3.

MEMORANDUM FOR: Robert L. Tedesco, Assistant Director for Licensing
Division of Licensing

FROM: Paul S. Check, Assistant Director for Plant Systems
Division of Systems Integration

SUBJECT: CALLAWAY PLANT, UNITS 1 AND 2 AND WOLF CREEK, UNIT 1
SAFETY EVALUATION REPORT, FSAR CHAPTER 7, INSTRUMENTATION
AND CONTROL SYSTEMS

Plant Names: SNUPPS, Callaway Plant, Units 1 & 2; Wolf Creek
Docket Nos.: 50-483/486 and 50-482
Licensing Stage: OL
Responsible Branch: LB #1
Project Manager: G. E. Edison
ICSB Reviewer: C. E. Rossi
Consultants: EG&G
Requested Completion Date: September 11, 1981



Enclosed is the Safety Evaluation Report (SER) input for the SNUPPS plants, Callaway Plant, Units 1 & 2, and Wolf Creek, Unit 1 prepared by the Instrumentation and Control Systems Branch (ICSB) with assistance from our Consultants, EG&G. The SER reflects information received up through Amendment 6 to the SNUPPS FSAR and the information in SNUPPS letter SLNRC 81-82 dated September 1, 1981. The SER was written with the presumption that the Amendment 7 items contained in SLNRC 81-82 will be in the formal submission of Amendment 7 to the FSAR.

The enclosed SER input applies to Section 7 of the Standard Review Plan and includes all SER input for which ICSB has responsibility. There are two open items for which ICSB has primary review responsibility and one for which ICSB has secondary review responsibility. These open items are listed in Section 7.1.3.1 of the SER.

The enclosed SER is applicable to both Callaway and Wolf Creek except that the information discussed in Section 7.2.2.1 on sensor time response testing is required on only the first unit to begin operation.

Please note that Section 7.1.3 of the SER lists not only the Open Items, but also the Confirmatory Items, Technical Specification Items, and Licensing Conditions discussed in the SER. SSER input will not be provided for Confirmatory Items unless a problem is found when final documentation is submitted by the

MEMO 4

Contact:
C. E. Rossi
X29431

8109280753 810910
CF ADOCK 05000482 XA
CF

applicants. We have included as Licensing Conditions those design commitments made by the applicants during the review process and upon which we based our Evaluation Findings.

Original Signed by
Paul S. Check

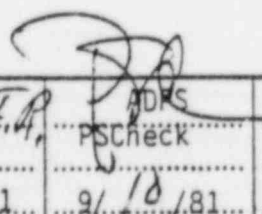
Paul S. Check, Assistant Director
for Plant Systems
Division of Systems Integration

Enclosure:
As stated

- cc: R. Mattson
- B. J. Youngblood
- F. Rosa
- T. Speis
- O. Parr
- M. Srinivasan
- T. Dunning
- G. Edison
- M. Nishimura (EG&G)
- C. Rossi

DISTRIBUTION:

- Docket Files (2) ✓
- ICSB Reading File
- CRossi (PF)
- Wolf Creek Subject File
- Callaway Subject File



OFFICE	ICSB <i>CR</i>	ICSB <i>FR</i>	ADRS <i>PS</i>			
SURNAME	CRossi:cc	FRosa	PScheck			
DATE	9/10/81	9/10/81	9/10/81			

applicants. We have included as Licensing Conditions those design commitments made by the applicants during the review process and upon which we based our Evaluation Findings.

Paul S. Check, Assistant Director
for Plant Systems
Division of Systems Integration

Enclosure:
As stated

cc: R. Mattson
B. J. Youngblood
F. Rosa
T. Speis
O. Parr
M. Srinivasan
T. Dunning
G. Edison
M. Nishimura (EG&G)
C. Rossi

7. INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

7.1.1 Acceptance Criteria

The instrumentation and control systems for the SNUPPS plants, Callaway Plant, Units 1 and 2 and Wolf Creek, Unit 1, have been reviewed. The bases for evaluation of the applicant's design, design criteria, and design bases are set forth in the Standard Review Plan (SRP), NUREG-0800 in Table 7-1, "Acceptance Criteria for Instrumentation and Control Systems." These acceptance criteria include the applicable General Design Criteria (Appendix A to 10 CFR Part 50), and IEEE Standard 279, "Criteria for Protection Systems for Nuclear Power Generating Stations (10 CFR Part 50.55 a(h))." Guidelines for implementation of the requirements of the acceptance criteria are provided in the IEEE Standards, Regulatory Guides (RG), and Branch Technical Positions (BTPs) of the Instrumentation and Control Systems Branch (ICSB) identified in Section 7.1 of the SRP. Conformance to the acceptance criteria provides the bases for concluding that the instrumentation and control systems meet the requirements of 10 CFR Part 50.

7.1.2 General Findings

The applicant has identified the instrumentation and control systems important to safety. The acceptance criteria, consisting of the General Design Criteria (GDC) and IEEE Standard 279, are included in the Commission's regulations, and are applicable to the systems as identified in the SRP. In addition, the applicant has identified the guidelines, consisting of the regulatory guides and the industry codes and standards which are applicable to the systems. The acceptance criteria and guidelines identified by the applicant are provided in Table 7.1-2 of their Final Safety Analysis Report (FSAR).

Based on the review of Section 7.1 of the applicant's FSAR, we conclude that the implementation of the identified acceptance criteria and guidelines satisfies the requirements of General Design Criterion (GDC) 1, "Quality Standards and Records," with respect to the design, fabrication, erection, and testing to quality standards commensurate with the importance of the safety functions to be performed. We find that the instrumentation and control systems important to safety, addressed in Section 7.1 of the applicant's Final Safety Analysis Report (FSAR), satisfy the requirements of GDC 1 and, therefore, are acceptable.

7.1.3 Specific Findings

7.1.3.1 Open Items

The staff's conclusions noted herein are applicable to the instrumentation and control systems important to safety with the exception of the open items listed below. The staff has not completed its review of these items. The sections of this report which address these items are noted in parentheses.

- (1) Level Measurement Errors Due to Environmental Temperature Effects on Level Instrument Reference Legs (7.3.2.3)
- (2) Reactor Coolant Temperature Indicators on the Auxiliary Shutdown Panel (7.5.2.1)

It should be noted that primary review of TMI Action Plan Item II.F.2, "Instrumentation for Detection of Inadequate Core Cooling" (See Section 7.1.4), is covered in Section 4.4 of this SER where it is an open item. The resolution of the open items will be addressed in a supplement to this report.

7.1.3.2 Confirmatory Items

In a number of areas the applicants have committed to make design changes or to provide additional documentation to address concerns raised by the staff during its review. Based upon information provided during meetings and discussions with the applicants, the staff has concluded that the technical issues have been resolved in an acceptable manner. However, the applicants must formally provide final documentation of these items. The staff will confirm that final documentation is provided prior to issuance of the operating license. These Confirmatory Items are addressed in the following sections of this report:

- (1) Steam Generator Level Control and Protection (7.3.2.8)
- (2) Capability for Safe Shutdown Following Loss of a Bus Supplying Power to Instruments and Controls (7.4.3.1)
- (3) Operator Actions Required to Maintain Safe Shutdown from Outside the Control Room (7.4.3.2)
- (4) Volume Control Tank Level Control and Protection Interaction (7.6.7.2)
- (5) Boron Dilution Control (7.6.7.3)
- (6) Environmental Qualification of Control Systems (7.7.11.3)

The Confirmatory Items will not be addressed in supplements to this report unless an unanticipated problem is found at the time the documentation to be provided by the applicants is reviewed.

7.1.3.3 Technical Specification Items

Items to be included in the plant technical specifications and information to be audited as part of the effort to issue technical specifications are discussed in the following sections of this report:

- (1) Protection System Temperature Detector Flow Bypass Loops (7.2.2.2)
- (2) Testing of Diverse Reactor Trip Feature (7.2.2.5)
- (3) Lead, Lag, and Rate Time Constant Setpoints Used in Safety System Channels (7.2.2.6)
- (4) Safety System Set Point Methodology (7.3.2.5)
- (5) Indicator, Alarm, and Test Features Provided for Instrumentation Used for Safety Functions (7.3.2.9)

7.1.3.4 Licensing Conditions

Items to be included as licensing conditions are discussed in the following sections of this report:

- (1) Sensor Time Response Testing (7.2.2.1)
- (2) Test of Engineered Safeguards P-4 Interlock (7.3.2.2)
- (3) Automatic Indication of Block of Signals Initiating Auxiliary Feedwater Following Trip of the Main Feedwater Pumps (7.3.2.7)
- (4) Steam Generator Level Control and Protection (7.3.2.8)
- (5) Indicator, Alarm, and Test Features Provided for Instrumentation Used for Safety Functions (7.3.2.9)
- (6) Actuation of Valve Component Level Windows on the Bypassed and Inoperable Status Panel (7.5.2.2)
- (7) Post Accident Monitoring (7.5.2.3)
- (8) Interlocks for Reactor Coolant System (RCS) Pressure Control During Low Temperature Operation (7.6.7.1)
- (9) Volume Control Tank Level Control and Protection Interaction (7.6.7.2)
- (10) Boron Dilution Control (7.6.7.3)

Items (2), (3), (4), (5), (6), (8), (9), and (10) above, involve specific designs and/or design changes which, during the course of the staff's review, the applicants committed to include in the plant. These designs or design changes should be installed prior to fuel loading. The schedules for items (1) and (7) are included in the sections of the SER which discuss these items.

7.1.3.5 Site Visit

A site review will be performed for the purpose of confirming that the physical arrangements and installation of electrical equipment are in accordance with the design criteria and descriptive information reviewed by the staff. The site review will be completed prior to issuance of the license and any problems found will be addressed in a supplement to this report.

7.1.3.6 Fire Protection Review

The review of the Auxiliary Shutdown Panel discussed in Section 7.4 of this report covered the compliance of this panel with GDC 19, "Control Room." The aspects of the Auxiliary Shutdown Panel related to Fire Protection (10 CFR Part 50, Appendix R) are discussed in Section 9.5.1 of this report.

7.1.4 TMI-2 ACTION PLAN ITEMS

The TMI Action Plan was developed to provide a comprehensive and integrated plan for actions now judged necessary to correct or improve the regulation and operation of nuclear facilities based on the experience from the accident at TMI-2. Guidance on implementation of the Action Plan was provided to applicants in NUREG-0737, "Clarification of TMI Action Plan Requirements." This section addresses the applicant's response to items related to instrumentation and control systems. Those items are:

II.D.3 Direct Indication of Relief and Safety Valve Position
Safety-grade position indication is provided for each pressurizer safety valve and power-operated relief valve (PORV) to indicate when the valve is not in its fully closed position. The position indication is seismically and environmentally qualified. The position indication for each valve is displayed in the control room, and an alarm is provided if any of the relief or safety valves is not fully closed. In addition, nonsafety-grade instrumentation is available on the valve discharge piping and the pressurizer relief tank to provide an alternate means of assessing the positions of the relief and safety valves.

The staff finds the design of this system to conform with the Action Plan guidelines.

II.E.1.2 Auxiliary Feedwater System Automatic Initiation and Flow Indication

Part 1: Auxiliary Feedwater System Automatic Initiation

The auxiliary feedwater system automatic initiation is part of the engineered safety features actuation system and conforms to the requirements for protection systems in accordance with IEEE 279. Therefore, we find that the design of this system conforms to the Action Plan guidelines.

Part 2: Auxiliary Feedwater System Flowrate Indication

A single auxiliary feedwater flow indicator is provided for each steam generator. Each of the flow indicators is assigned to a different safety system separation group and the flow indicators meet all of the recommendations of Item II.E.1.2 contained in NUREG-0737. Wide range steam generator level indication is also provided for each steam generator. Therefore, the staff finds that the design conforms to the Action Plan Guidelines.

II.F.2 Instrumentation for Detection of Inadequate Core Cooling, Attachment 1, Design and Qualification Criteria for Pressurized Water Reactor Incore Thermocouples

Redundant, safety grade core subcooling monitors utilizing hot and cold leg resistance temperature detectors, core outlet thermocouples and reactor coolant system pressure are provided. 25 core outlet thermocouples are provided for each subcooling monitor. Redundant, safety grade microprocessors are employed to calculate margin to core saturation. Information display includes digital readout of the core outlet temperatures and indication of margin to saturation with a range extending up to the physical limitations of the incore thermocouples (approximately 2300°F). All core exit thermocouples are also recorded by Class 1E digital recorders. The resistance temperature detectors, core thermocouples, and reactor coolant system pressure sensors providing input to the subcooling monitors are seismically and environmentally qualified.

Open Item The applicant has not provided the documentation required by Item II.F.2. This documentation will be reviewed subsequent to its receipt by the staff and reported on in a supplement to this report.

II.K.3.1 Installation and Testing of Automatic Power-Operated Relief Valve Isolation System

The applicants design includes instrumentation and circuitry to automatically close the block valves in the pressurizer power operated relief valve discharge lines on low reactor coolant system

pressure. We find that the design satisfies the Action Plan guidelines and therefore is acceptable.

II.K.3.9 Proportional Integral Derivative (PID) Controller Modification.

Westinghouse recommended that the derivative time constant in the pressurizer power operated relief valve PID controller be set to off. This action removes the derivative action from the controller such that the actuation signal is no longer sensitive to the rate of change of pressure. The applicants have implemented this recommendation. We therefore find that the applicants have complied with the Action Plan guidelines for this item.

II.K.3.10 Proposed Anticipatory Trip Modification and

II.K.3.12 Confirm Existence of Anticipatory Reactor Trip Upon Turbine Trip.

The SNUPPS design includes an anticipatory reactor trip upon turbine trip. Provisions are included to permit the reactor trip upon turbine trip to be blocked at power levels below 50% where the condenser steam dump is capable of mitigating the reactor coolant system temperature and pressure transient to minimize the possibility of actuating pressurizer power operated relief valves. A decision to trip the reactor following turbine trip at all power levels above 10% would involve only bistable setpoint changes and not instrument hardware changes. The staff finds that the design satisfies the Action Plan guidelines and therefore is acceptable. The specific power level setpoint below which a reactor trip following turbine trip is blocked will be specified in the plant technical specifications.

7.2 REACTOR TRIP SYSTEM (RTS)

7.2.1 Description

The Reactor Trip System (RTS) is designed to automatically limit reactor operation within the limits established in the safety analysis. This function is accomplished by tripping the reactor when predetermined safety limits are approached or reached. The RTS monitors variables that are directly related to system limitations or calculated from process variables. When a variable exceeds a setpoint, the reactor is tripped by inserting control rods. The RTS initiates a turbine trip when a reactor trip occurs. The RTS consists of sensors and analog and digital circuitry arranged in coincidence logic for monitoring plant parameters. Signals from the analog channels are used in redundant logic trains. Each of the two trains opens a separate and independent reactor trip breaker. During normal power operation, a direct current undervoltage coil on each reactor trip breaker holds the breaker closed. For a reactor trip, the removal of power to the undervoltage coils opens the breakers. Opening either of two series-connected breakers interrupts the power from the rod drive motor generator sets and the control rods fall, by gravity, into the core. The rods cannot be withdrawn until the trip breakers are manually reset. The trip breakers cannot be manually reset until the abnormal condition that initiated the trip is corrected. Bypass breakers are provided to permit the testing of the primary breakers.

The following reactor trips are provided in the SNUPPS (Callaway Plant, Units 1 and 2, and Wolf Creek Plant, Unit 1) design. The numbers in parentheses after each trip function indicate the coincident logic as, for example, (2/4) indicates two-out-of-four.

(1) Nuclear Power Trips

- (a) Power range high neutron flux trip (2/4)
- (b) Intermediate range high neutron flux trip (1/2)
- (c) Source range high neutron flux trip (1/2)
- (d) Power range high positive neutron flux rate trip (2/4)
- (e) Power range high negative neutron flux rate trip (2/4)

(2) Core Thermal Power Trips

- (a) Overtemperature ΔT trip (2/4)
- (b) Overpower ΔT trip (2/4)

- (3) Reactor Coolant System Pressurizer Pressure and Water Level Trips
 - (a) Pressurizer low pressure trip (2/4)
 - (b) Pressurizer high pressure trip (2/4)
 - (c) Pressurizer high-water-level trip (2/3)
- (4) Reactor Coolant System Low Flow Trips
 - (a) Low reactor coolant flow (2/3 in any loop)
 - (b) Reactor coolant pump undervoltage trip (1/2 pumps per bus)
 - (c) Reactor coolant pump underfrequency trip (1/2 pumps per bus)
- (5) Steam Generator Low Water Level Trip (2/4 in any loop)
- (6) Turbine Trip (anticipatory) (2/3 low trip fluid pressure or 4/4 turbine stop valves closed)
- (7) Safety Injection Actuation
- (8) General Warning Alarm (in both Solid State Protection System Trains)
- (9) Manual Trip (1/2)

The power range high neutron flux trip has two bistables in each channel for two separate trip settings. The high trip setting is active during all modes of operation. The lower trip setting is active only during reactor startup and shutdown when the reactor is below approximately 10 percent power (P-10 interlock).*

An intermediate range trip provides diverse protection to the lower power range trip during reactor startup and shutdown when the reactor is below approximately 10 percent power (P-10 interlock).

A source range trip provides protection during reactor startup and shutdown when the neutron flux is below a preset value in the intermediate range (P-6 interlock).

*Unless otherwise indicated, setpoint values discussed in this Safety Evaluation Report are not final values. Final setpoints will be determined at the time the plant Technical Specifications are issued.

A power range high positive neutron flux rate trip occurs when a sudden abnormal increase in nuclear power is detected. This trip provides departure from nucleate boiling (DNB) protection against certain rod ejection accidents and is active during all modes of operation.

A power range high negative neutron flux rate trip occurs when a sudden abnormal decrease in nuclear power is detected. This trip provides protection against two or more dropped rods and is active during all modes of operation.

The overtemperature ΔT trip protects the core against DNB. The setpoint for this trip is continuously calculated by analog circuits to compensate for the effects of temperature, pressure, and axial neutron flux difference on DNB limits.

The overpower ΔT trip protects against excessive power (fuel rod rating protection). The setpoint for this trip is continuously calculated by analog circuits to compensate for the effects of temperature and axial neutron flux difference.

The pressurizer low pressure trip is used to protect against low pressure that could lead to DNB. The reactor is tripped when the pressurizer pressure (compensated for rate of change) falls below a preset limit. This trip is blocked below approximately 10 percent power (P-7 interlock) to allow startup and controlled shutdown.

The pressurizer high pressure trip is used to protect the reactor coolant system against system overpressure. The same sensors used for the pressurizer low pressure trip are used for the high pressure trip.

The pressurizer high-water-level trip is provided as a diverse trip to the high pressurizer pressure trip and serves to prevent water relief through the pressurizer safety valves. This trip is blocked below approximately 10 percent power (P-7 interlock) to allow startup and controlled shutdown.

Low reactor coolant flow is sensed by transmitters connected to elbow taps in each coolant loop. The reactor is tripped on low flow in one loop above the power setting of interlock P-8 or in two loops between the power settings of interlocks P-7 and P-8. The low flow trip is blocked below the power setting of interlock P-7 (approximately 10% power). This trip protects the core from low DNB for a loss of primary coolant flow.

The reactor coolant pump undervoltage trip is provided to protect against low flow that can result from loss of voltage to the reactor coolant pump motors. One undervoltage sensing relay is provided for each pump at the motor side of each reactor coolant pump breaker. The relay provides an output signal when the pump voltage goes below approximately 70 percent of rated voltage. Signals from these relays are time delayed to prevent spurious trips. The trip is bypassed if the power level is below approximately 10 percent power (P-7 interlock).

The reactor coolant pump underfrequency trip protects against low flow resulting from underfrequency. One underfrequency sensing relay is provided for each reactor coolant pump motor. Signals from these relays are time delayed to prevent spurious trips. The trip is bypassed if the power level is below approximately 10 percent power (P-7 interlock).

The steam generator low water level trip protects the reactor from loss of heat sink.

A reactor trip on a turbine trip is actuated from emergency trip fluid pressure signals or by all closed signals from the turbine steam stop valves. A turbine trip causes a reactor trip above approximately 50% power (P-9 interlock).

A safety injection signal initiates a reactor trip. This trip protects the core for a loss of reactor coolant or a steam line rupture.

A General Warning Alarm in both solid state protection system trains initiates a reactor trip. The General Warning Alarm is activated for each train of the solid state protection system when the train is in test or otherwise inoperable. The General Warning Alarm trip provides protection for conditions under which both trains of the protection system may be rendered inoperable.

The manual trip consists of two switches. Operation of either switch de-energizes the reactor trip breaker undervoltage coils in each logic train. At the same time, the shunt coils in these breakers are energized which provides a diverse means to insure that the breakers are tripped.

The analog portion of the RTS consists of a portion of the Process Instrumentation System (PIS) and the Nuclear Instrumentation System (NIS). The PIS includes those devices that measure temperature, pressure, fluid flow, and level. The PIS also includes the power supplies, signal conditioning, and bistables that provide initiation of protective functions. The NIS includes the neutron flux monitoring instruments, including power supplies, signal conditioning, and bistables that provide initiation of protective functions.

The digital portion of the RTS consists of the Solid State Logic Protection System (SSLPS). The SSLPS takes binary inputs (voltage/no voltage) from the PIS and NIS channels corresponding to normal/trip conditions for plant parameters. The SSLPS utilizes these signals in the required logic combinations and generates trip signals (no voltage) to the undervoltage coils of the reactor trip circuit breakers. The system also provides annunciator, status light, and computer input signals that indicate the condition of the bistable input signals, partial and full trip functions, and the status of various blocking, permissive, and actuation functions. In addition, the SSLPS includes the logic circuits for testing.

Analog signals derived from protection channels are used for nonprotective functions such as control, remote indication, and computer monitoring and are provided by the use of isolation amplifiers located in the protective system cabinets. The isolation amplifiers are designed such that a short circuit, open circuit, or the application of credible fault voltages on the isolated output portions of the circuit (nonprotective side) will not affect the protection system circuits. The signals obtained from the isolation amplifiers are not returned to the protective system cabinets.

The Reactor Trip System is the standard Westinghouse system used on previous plants reviewed and approved by the staff such as the W. B. McGuire Station (Docket No. 50-369).

7.2.2 RESOLUTION OF ISSUES

7.2.2.1 Sensor Time Response Testing

The applicants intend to use a computer based system using process noise with the plant at power for sensor time response testing. Although staff review during meetings with the applicants indicates that the method is satisfactory, there is only limited experience to date with the method on operating plants.

The applicants will be required to submit a summary of the results from and experience with this method of time response testing within three months following the testing done at the time of initial plant startup. A similar summary will be required within three months following the testing done at each of the first three plant refuelings. Each summary will contain conclusions on the adequacy of the test method and the adequacy of the sensor time response values measured. This will allow a confirmatory review of the adequacy of the time response testing method to be obtained and applies to the first of the SNUPPS units going into operation.

The license will be conditioned to require the submittal of the above information on response time testing and evaluation.

7.2.2.2 Protection System Temperature Detector Flow Bypass Loops

The reactor coolant system hot and cold leg resistance temperature detectors used for reactor protection are located in reactor coolant bypass loops. A bypass loop from upstream of the steam generator to downstream of the steam generator is used for the hot leg resistance temperature detector and a bypass loop from downstream of the reactor coolant pump to upstream of the pump is used for the cold leg resistance temperature detector. The flow rate affects the overall time response of the temperature signals provided for reactor protection and, thus, should be monitored at appropriate intervals. The staff will require that the magnitude of the RTD bypass loop flow rate be verified to be within required limits at each refueling period. This requirement will be incorporated in the plant technical specifications.

7.2.2.3 Design Criteria of Circuits and Equipment Used to Trip the Turbine Following a Reactor Trip

It was not clear from the drawings provided and the description of the turbine trip circuits in the FSAR that the circuits used to trip the turbine following a reactor trip meet the criteria applicable to equipment performing a safety function. The applicants were asked to verify that the circuits used to trip the turbine following

a reactor trip meet the criteria applicable to a safety function with the exception of the fact that the circuits are routed through non-seismic qualified structures and the turbine itself is not seismically qualified.

The applicants responded that the equipment employed to trip the turbine is the turbine protection system, which is part of the turbine Electro-Hydraulic Control system. Each of the redundant circuits used to trip the turbine following a reactor trip is independently routed to and processed within the turbine protection system to provide two independent means of tripping the turbine. The circuits which traverse non-seismic qualified structures are isolated from the circuits of the Solid State Protection System. The circuits are fully testable during full power operation. The staff finds this design to be consistent with the function's importance to safety and, therefore, acceptable.

7.2.2.4 Trip of Reactor Coolant Pump Breakers on Underfrequency

The staff asked the applicants to provide justification that tripping the reactor coolant pump breakers on underfrequency is not a safety function and, thus, the reactor coolant pump breakers do not have to be designed and qualified to meet the criteria applicable to equipment performing a safety function. The applicants have stated that analyses have been performed to demonstrate that pump breaker trip is not required to maintain acceptable core design limits for frequency decay rates less than 5 Hz/sec. Grid stability studies have shown credible frequency decay rates to be less than 5 Hz/sec. The staff finds the applicant's justification for the design basis of the reactor coolant pump breakers to be acceptable.

7.2.2.5 Testing of Diverse Reactor Trip Feature

Operation of either of two manual reactor trip switches deenergizes the reactor trip breaker undervoltage coils and, at the same time, energizes the breaker shunt coils for the breakers associated with both protection logic trains. The use of both the undervoltage and shunt trips provides diversity for insuring that the reactor trip breakers open.

The staff will include in the plant technical specifications a requirement to periodically, independently verify the operability of the undervoltage and shunt trip functions.

7.2.2.6 Lead, Lag, and Rate Time Constant Setpoints Used in Safety System Channels

Several safety system channels make use of lead, lag, or rate signal compensation to provide signal time responses consistent with assumptions in the Chapter 15 analyses. The time constants for these signal compensations are adjustable setpoints within the analog portion of the safety system. The time constant setpoints will be incorporated into the plant technical specifications.

7.2.3 Evaluation Findings

We have conducted an audit review of the Reactor Trip System (RTS) for conformance to guidelines of the applicable regulatory guides and industry codes and standards. In Section 7.1 of this SER, we concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon our audit review of the design for conformance to the guidelines, we find that there is reasonable assurance that

the systems will conform to the guidelines applicable to them.

Our review has included the identification of those systems and components for the RTS which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based upon our review, we conclude that the applicant has identified the systems and components consistent with the design bases for the RTS. Sections 3.10 and 3.11 of this SER address the qualification programs to demonstrate the capability of these systems and components to survive applicable events. Therefore, we find that the identification of the systems and components satisfies this aspect of the GDC-2, "Design Bases for Protection Against Natural Phenomena," and GDC-4, "Environmental and Missile Design Bases."

Based on our review, we conclude that the RTS conforms to the design bases requirements of IEEE-279. The RTS includes the provision to sense accident conditions and anticipated operational occurrences and initiate reactor shutdown consistent with the analysis presented in Chapter 15 of the SAR. Therefore, we find that the RTS satisfies the requirements of GDC-20, "Protection System Functions."

The RTS adequately conforms to the guidance for periodic testing in Regulatory Guide (RG) 1.22 and IEEE-338 as supplemented by RG 1.118. The bypassed and inoperable status indication adequately conforms to the guidance of RG 1.47. The RTS adequately conforms to the guidance on the application of the single failure criterion in IEEE-379, as supplemented by RG 1.53. Based on our review, we conclude that the RTS satisfies the requirement of IEEE-279 with regards to system reliability and testability. Therefore, we find that the RTS satisfies the requirement of GDC-21, "Protection System Reliability and Testability."

The RTS adequately conforms to the guidance in IEEE-384 as supplemented by RG 1.75 for the protection system independence. Based on our review, we conclude that the RTS satisfies the requirement of IEEE-279 with regards to the independence of systems. Therefore, we find that the RTS satisfies the requirement of GDC-22, "Protection System Independence."

Based on our review of failure modes and effects for the RTS, we conclude that the system is designed to fail into a safe mode if conditions such as disconnection of the system, loss of energy, or a postulated adverse environment are experienced. Therefore, we find that the RTS satisfies the requirements of GDC-23, "Protection System Failure Modes."

Based on our review of the interfaces between the RTS and plant operating control systems, we conclude that the system satisfies the requirements of IEEE-279 with regards to control and protection system interaction. Therefore, we find that the RTS satisfies the requirements of GDC-24 "Separation of Protection and Control Systems."

Based on our review of the Reactor Trip System, we conclude 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 addresses the capability of the system to assure that fuel design limits are not exceeded for such events. Therefore, we find that the RTS satisfies the requirements of GDC-25, "Protection System Requirements for Reactivity Malfunction."

Our conclusions, noted above, are based upon the requirements of IEEE-279 with respect to the design of the RTS. Therefore, we find that the RTS satisfies the requirement of 50.55a(h) with regards to IEEE-279.

Our review of the RTS has examined the dependence of this system on the availability of essential auxiliary support (EAS) systems. Based on our review, we conclude that the design of the RTS is compatible with the functional performance requirements of EAS systems. Therefore, we find the interfaces between the RTS design and the design of the EAS systems to be acceptable.

In summary, the staff concludes that the design of the Reactor Trip System (RTS) and the design of the essential auxiliary support (EAS) systems are acceptable and meet the relevant requirements of General Design Criteria 2, 4, 20, 21, 22, 23, 24, and 25, and 10 CFR Part 50, 50.55a(h).

7.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

7.3.1 Description

This section describes the review of the portion of the protection system used to initiate the operation of the engineered safety features systems and essential auxiliary supporting systems. The engineered safety features actuation system (ESFAS) includes both automatic and manual initiation of these systems. This section also includes the review of control systems which regulate the operation of the engineered safety feature systems following their initiation by the protection system.

The ESFAS consists of:

1. Process instrumentation
2. Solid state and relay logic
3. Engineered safety features test circuits
4. Manual actuation circuits

The ESFAS includes two discrete types of circuitry: 1) an analog portion consisting of two to four redundant channels per parameter or variable to monitor various plant parameters such as the reactor coolant system and steam system pressures, temperatures and flows, and containment pressures; and 2) a digital portion consisting of redundant logic trains which receive inputs from the analog protection channels and perform the logic to actuate the engineered safety features. The ESFAS is composed of a Nuclear Steam Supply System portion designed by Westinghouse and a Balance of Plant portion designed by Bechtel. The Nuclear Steam Supply System portion is the standard Westinghouse system used on previous plants reviewed and approved by the staff such as the W. B. McGuire Station (Docket No. 50-369).

There are ten ESFAS functions in the SNUPPS design. The following actuation functions have been provided and the numbers in parentheses after each function indicate the coincident logic as for example, (2/3) indicates two out of three.

- *1. Safety Injection Actuation (Emergency Core Cooling)
 - a. Low pressurizer pressure (2/4)
 - b. Low steamline pressure (2/3 in any line)
 - c. High containment pressure (HI-1) (2/3)
 - d. Manual actuation (1/2)

- *2. Containment Isolation Phase A Actuation
 - a. Safety injection
 - b. Manual actuation (1/2)

- *3. Containment Spray System Actuation and Containment Isolation Phase B Actuation
 - a. High containment pressure (HI-3) (2/4)
 - b. Manual actuation (2/4)

- *4. Main Steamline Isolation Actuation
 - a. Low steamline pressure (2/3 in any line)
 - b. High containment pressure (HI-2) (2/3)
 - c. High steam pressure rate (2/3 in any line)
 - d. Manual actuation (1/2 for all lines or 1/1 for each valve)

- *5. Feedwater Line Isolation Actuation
 - a. Safety injection
 - b. Steam generator high level (2/4 on any generator)
 - c. Low T_{avg} (2/4) coincident with reactor trip

- **6. Containment Combustible Gas Control Actuation
 - a. Manual (1/2)

- **7. Containment Purge Isolation Actuation
 - a. Containment Isolation Phase A
 - b. High Containment Atmosphere Radiation (1/2)
 - c. High Containment Purge Exhaust Radiation (1/2)
 - d. Manual Actuation (1/2)

- **8. Fuel Building Ventilation Isolation Actuation
 - a. High Fuel Building Radiation (1/2)
 - b. Manual Actuation (From Fuel Building) (1/2)
 - c. Manual Actuation (From Main Control Room) (1/2)

**9. Control Room Ventilation Isolation Actuation

- a. Containment Isolation Phase A
- b. Fuel Building Ventilation Isolation
- c. Control Room Ventilation Isolation (other unit)
- d. High Containment Atmosphere Radiation (1/2)
- e. High Containment Purge Exhaust Radiation (1/2)
- f. High Control Room Air Intake Gaseous Radiation (1/2)
- g. High Chlorine Concentration (1/2)
- h. Manual Actuation (1/2)

***10. Auxiliary Feedwater System Actuation

- a. Safeguards Sequencer (safety injection or loss of offsite power)
- b. Steam Generator low level (2/4 on any generator)
- c. Both main feedwater pumps tripped (2/2)
- d. Manual Actuation (1/3)

*Westinghouse designed portion of ESFAS performs function.

**Bechtel designed portion of ESFAS performs function.

***Both Bechtel and Westinghouse portions of ESFAS used in performing function.

7.3.1.1 Safety Injection (Emergency Core Cooling) Actuation

The Safety Injection (Emergency Core Cooling) System (ECCS) cools the reactor core and provides shutdown capability for pipe breaks in the Reactor Coolant System (RCS) which cause a loss of primary coolant greater than that which can be made up by the normal makeup system, for rod cluster control assembly ejection, for pipe breaks in the steam system, and for a steam generator tube failure. The primary function of the ECCS is to remove the stored and fission product decay heat from the reactor core during accident conditions. The ECCS consists of the centrifugal charging, safety injection and residual heat removal pumps; accumulators; residual heat removal heat exchangers; refueling water storage tank (RWST); boron injection tank; boron injection surge tank; and boron injection recirculation pumps with the associated piping, valves and instrumentation.

The ECCS provides shutdown capability for the accidents described above by injecting borated water into the reactor coolant system. The system safety function can be performed with a single active failure (short term) or passive failure (long term). The emergency diesel generators supply power in the event that a loss of

offsite power occurs.

A safety injection signal initiates a reactor trip and turbine trip, isolates the essential service water system from the non-seismically qualified service water system, starts essential service water pumps, starts a component cooling water pump in a second train, aligns the containment cooling system, and starts emergency diesel generators. Safety injection initiates the following Emergency Core Cooling System (ECCS) actions:

1. Start centrifugal charging pumps
2. Open RWST suction valves to charging pumps
3. Open boron injection tank suction and discharge parallel isolation valves
4. Close normal charging path valves
5. Close charging pump miniflow valves
6. Close boron injection tank recirculation valves
7. Load-shed boron injection tank recirculation pumps from the Class 1E busses
8. Start safety injection pumps
9. Start residual heat removal pumps
10. Close volume control tank outlet isolation valves
11. Close RWST discharge isolation valves to the spent fuel pool cooling and cleanup system

Switchover from the injection mode to recirculation involves the following interlocks: The suction valves in the line from the sump to the RHR pumps open when two out of four level transmitters indicate a low level in the RWST in conjunction with an SIS. The valves from the RWST to the RHR suction will close automatically after the sump suction valves are open. The safety injection pump and charging pump recirculation suction isolation valves can be opened, provided that the safety injection pump miniflow lines have been isolated.

7.3.1.2 Containment Isolation System (CIS) Actuation

The function of the containment isolation system is to isolate nonessential lines which pass through the containment boundary to limit the escape of fission products from postulated accidents. The containment isolation system is designed to limit radioactive emission from the containment during abnormal events and accidents.

The containment isolation system is automatically actuated by signals developed by the engineered safety features actuation system in two phases: Phase A containment isolation and Phase B containment isolation. Phase A containment isolation isolates all nonessential process lines penetrating the containment. Phase B containment isolation isolates all process lines not included in Phase A containment isolation, except safety injection lines and containment spray lines.

Containment isolation valves that are equipped with power operators and are automatically actuated may also be controlled individually by positioning hand switches in the control room. Containment isolation valves with power operators are provided with an open/closed indication, which is displayed in the control room. The valve mechanism also provides a local, mechanical indication of valve position. All power supplies and equipment necessary for containment isolation are Class 1E.

7.3.1.3 Containment Spray System (CSS) Actuation

The two redundant trains of containment spray provide a spray of cold borated water, containing NaOH, from the upper regions of the containment to reduce the containment pressure and temperature and to remove fission products following a LOCA, a main steam line break accident, or a feedwater line break accident.

The CSS has two phases of operation, which are initiated sequentially following system actuation; they are the injection phase and the recirculation phase. Once the CSS actuation signal is initiated, isolation valves open to begin the injection phase and the valves associated with the spray additive tank open to allow NaOH to mix with the spray. For the recirculation phase, spray pump suction is manually switched from the refueling water storage tank (RWST) to the containment recirculation sump when a low level in the RWST is reached. The system includes features for periodic testing to confirm proper functioning.

7.3.1.4 Main Steamline Isolation Actuation

The main steam line isolation signal is generated on low steam line pressure or on high containment pressure. A manual block permissive is provided for the low steam line pressure signal for use during normal plant cooldowns and heatups. A high rate of steam line pressure decrease is used in lieu of low steam line pressure for main steam line isolation actuation during normal plant cooldowns and heatups. The block of the low steam line pressure signal is automatically removed and the high rate signal is automatically blocked when the pressurizer

pressure is above a preset value. Stored energy for closing the main steam line isolation valves is supplied by pneumatic/hydraulic accumulators. For emergency closure, solenoids are energized which causes high pressure hydraulic fluid to be admitted to the top of the valve driving piston and also causes the fluid stored below the piston to be dumped to a fluid reservoir. Two separate pneumatic/hydraulic trains are provided for each valve. Electrical solenoids for the separate pneumatic/hydraulic power trains are energized from separate Class 1E power sources. The valves are designed to close in between 1.5 and 5 seconds against the flows associated with line breaks on either side of the valve, assuming the most limiting normal operating conditions prior to occurrence of the break. The redundant actuator trains of the main steamline isolation valves are tested periodically by exercising the valve to approximately 90 percent of full open. The closure time of the valves is checked at each refueling.

7.3.1.5 Feedwater Line Isolation Actuation

Feedwater line isolation is provided to terminate main feedwater following a pipe rupture or excessive feedwater event. The feedwater line isolation signal is generated on safety injection, high steam generator water level, or low reactor coolant temperature coincident with reactor trip. Upon receipt of this signal, the main feedwater isolation valves and other valves associated with the main feedwater lines are closed. Two complete actuation systems are provided for each valve operator corresponding to the two redundant ESFAS trains. The valves are designed and constructed with provisions for periodic inservice testing by partial valve stroke tests.

7.3.1.6 Containment Combustible Gas Control Actuation

Hydrogen gas may be generated inside the containment following an accident. To ensure that the hydrogen concentration is maintained below the minimum capable of combustion, redundant hydrogen recombiners, a redundant hydrogen mixing system, a redundant hydrogen monitoring system, and a backup hydrogen purge subsystem are provided. Operation of the recombiners is performed manually from either local controls, located on a motor control center in an accessible area outside the containment, or from the main control room panels. Controls are provided on a one-to-one basis with the mechanical equipment so that the controls preserve the redundancy of the mechanical equipment.

7.3.1.7 Containment Purge Isolation Actuation

The containment purge isolation system detects an abnormal level of radioactivity in the containment atmosphere or in the containment purge effluent and automatically closes the containment purge isolation valves to ensure that the release of radioactivity to the environs is limited. The containment purge isolation system is also actuated by Containment Isolation Actuation.

7.3.1.8 Fuel Building Ventilation Isolation Actuation

The fuel building ventilation isolation system detects an abnormal level of radioactivity in the fuel building exhaust effluent, automatically isolates normal ventilation, and initiates the emergency exhaust system which filters the exhaust air before it is discharged to the atmosphere.

7.3.1.9 Control Room Ventilation Isolation Actuation

The control room ventilation isolation system detects an abnormal level of radioactivity or chlorine in the air provided to the main control room, automatically terminates the normal supply of outside air to the control room, recycles and filters the air in the control room, and provides a small supply of fresh makeup air.

7.3.1.10 Auxiliary Feedwater System Actuation

The auxiliary feedwater supply system provides feedwater to maintain sufficient steam generator level to ensure heat removal from the reactor coolant system in order to achieve a safe shutdown following a main feedwater line break, a main steamline break, or other abnormal plant situation requiring shutdown when main feedwater may not be available. The motor-driven auxiliary feedwater pumps start automatically on low water level in any steam generator, a trip of both main feedwater pumps, or a safeguards sequencer signal (safety injection or loss of offsite power). The turbine-driven pump is automatically initiated on either low water level in any two steam generators or on loss of offsite power. Upon receipt of two out of three auxiliary feed pump suction low pressure signals, the water supply to the auxiliary feedwater pumps automatically transfers from the condensate storage tank to the essential service water system.

7.3.2 RESOLUTION OF ISSUES

7.3.2.1 Loss of Safety Function After Reset

As was done for operating reactors through IE Bulletin 80-06, the staff requested that the applicants review all safety equipment to determine which, if any, safety functions might be unavailable after reset and what changes would be implemented to correct any problems. The applicants provided a response stating that a review has been conducted to determine whether or not all safety related equipment will remain in its emergency mode following reset of an ESF actuation signal. The review revealed that certain equipment would change state upon ESF reset. The control circuits for this equipment were revised to provide seal-in features so that an ESF reset would not change the safeguards state of the equipment. Preoperational tests will verify that the installed controls are consistent with schematic diagrams reviewed and that all equipment remains in its emergency mode upon ESF reset. The staff finds this acceptable.

7.3.2.2 Test of Engineered Safeguards P-4 Interlock

On November 7, 1979, Westinghouse notified the Commission of a potential undetectable failure which could exist in the engineered safeguards P-4 interlocks. Test procedures were developed to detect failures which might occur. The procedures require the use of voltage measurements at the terminal blocks of the reactor trip breaker cabinets. In order to minimize the possibility of accidental shorting or grounding of safety system circuits during testing, the staff position was that suitable test jacks be provided to facilitate testing of the P-4 interlocks. The applicants have committed to provide the test jacks. The staff concludes that the applicants commitment is an acceptable resolution of this item and will make provision of the test jacks a condition of the license.

7.3.2.3 Level Measurement Errors Due to Environmental Temperature Effects on Level Instrument Reference Legs

The staff asked the applicants to evaluate the effects of high temperatures in reference legs of water level measuring instruments on the measurement errors following high energy linebreaks. This issue was addressed for operating reactors through IE Bulletin 79-21.

Open Item: Although the applicants submitted a response on this item, the response was not received in time to be reviewed prior to issuance of this SER. The resolution of this item will be addressed in a supplement to this report.

7.3.2.4 Failure Modes and Effects Analysis (FMEA) Interface Requirements

The applicants have referred to the Westinghouse Topical Report WCAP-8584, "Failure Mode and Effects Analysis (FMEA) of the Engineered Safety Features Actuation System," as the supporting document of FMEA for ESFAS equipment within the Westinghouse scope of supply. The staff has reviewed WCAP-8584 and finds the methodology and the general conclusions to be acceptable. However, in Appendices B and C of the report, Westinghouse specifies interface requirements for electrical circuit and instrument impulse line separation involving systems included in the balance of plant. The conformance to these requirements was not addressed in the FSAR. The staff requested that the applicants identify any difference between the SNUPPS design and the Westinghouse specified interface requirements as described in WCAP-8584. In response, the applicants have stated that the interface criteria have been met. The staff finds the applicant's response acceptable.

7.3.2.5 Safety System Set Point Methodology

The staff has requested that the applicant document the following information concerning safety system setpoint methodology and setpoint error allowances:

- 1) The setpoint methodology or reference to the methodology to be used for the SNUPPS plants.
- 2) The method of including the effect of test equipment accuracy on setpoint errors.
- 3) The sensor environmental error allowance used for each reactor trip and engineered safeguards setpoint.
- 4) The list of protection channels where the Technical Specification setpoint with adjustment for all assumed errors falls within 5% span of an instrument range limit or within 5% span of a level tap. In these cases, the remaining margin to the range limit or tap is to be provided.

The applicant has not compiled all of this information at this point in time. Since the primary function of this information is to confirm the adequacy of setpoints specified in the plant technical specifications, the staff will audit this information at the time the technical specifications are available for review.

7.3.2.6 Isolation Devices in the Balance of Plant Engineered Safeguards Features Actuation System

The Balance of Plant Engineered Safeguards Features Actuation System (BOP ESFAS) is used to provide actuation signals for:

- 1) Auxiliary Feedwater
- 2) Containment Purge Isolation

- 3) Control Room Ventilation Isolation
- 4) Fuel Building Ventilation Isolation

The hardware consists of solid-state bistables and logic elements, with electromechanical relays as the final output devices. The system is divided into three input-logic output separation groups with the separation groups designed to meet the independence and separation criteria applicable to systems performing safety functions. Interconnection of differing separation groups within the BOP ESFAS is by means of digital signal isolation modules. Analog signal isolation modules are included to provide isolated analog signals to the Balance of Plant Computer.

The staff asked the applicants to document the design criteria for the isolation modules and the testing performed to verify that the design criteria are met. In response, the applicants stated that the digital signal isolation modules utilize optical isolators and that there are no connections between the input and output circuits except for the optical coupling. The analog isolation modules utilize transformers as the isolation devices and there are no connections between the input and output circuits except for the magnetic coupling in the transformers. Both the analog and the digital isolation modules are tested to ensure a minimum isolation potential of 1500 VAC RMS between the input terminals and the output terminals and between the terminals and ground.

The staff finds the applicant's design and test criteria for the isolation modules to be satisfactory.

7.3.2.7 Automatic Indication of Block of Signals Initiating Auxiliary Feedwater Following Trip of the Main Feedwater Pumps

The signal which initiates auxiliary feedwater when the main feedwater pumps are tripped is manually blocked on normal shutdown of the main feedwater pumps. The design is such that the block is not automatically removed when the plant is returned to an operating mode where auxiliary feedwater initiation on loss of main feedwater is needed. Even though the signal to initiate auxiliary feedwater when the main feedwater pumps are tripped is considered to be an "anticipatory signal" for which no credit is taken in the analyses of FSAR Chapter 15, the staff position was that the design should include appropriate features to insure that the block is removed when the plant is returned to an operating mode where auxiliary feedwater initiation on loss of main feedwater is needed. The applicants have committed to provide automatic indication of the block of the signals which initiate auxiliary feedwater on loss of both main feedwater pumps on the bypassed and inoperable status panel. Operating procedures will limit the operating modes where the block

can be in effect. Blocking will be permitted just prior to shutdown of the last operating main feedwater pump and removed just after the first main feedwater pump is put into service. The staff concludes that the applicants design and operating procedures will provide adequate assurance that the auxiliary feedwater start signal on loss of both main feedwater pumps will not be blocked during operating modes where the diversity of this signal is desirable. The applicants design is, therefore, acceptable. The license will be conditioned to require the bypassed and inoperable status panel indication described above.

7.3.2.8 Steam Generator Level Control and Protection

In its review, the staff noted that three steam generator level channels were used in two out of three logic for isolation of feedwater on high steam generator level and that one of the three level channels was also used for control. This design for actuation of feedwater isolation does not meet Paragraph 4.7 of IEEE Standard 279 on "Control and Protection System Interaction." The staff asked the applicants to submit analyses justifying that isolation of feedwater on high steam generator level is not a safety function. In lieu of submitting analyses, the applicants have committed to using four level channels in two out of four logic to actuate feedwater isolation. This design satisfies Paragraph 4.7 of IEEE Standard 279. The staff finds that the applicants modified design negates the need for additional analyses and is acceptable. The license will be conditioned to require the modified design.

Confirmatory Item: The applicants will modify the FSAR to indicate that four channels with two out of four logic will be used to actuate feedwater isolation on high steam generator level.

7.3.2.9 Indicator, Alarm, and Test Features Provided for Instrumentation Used for Safety Functions

Instrumentation for process measurements used for safety functions such as reactor trip or emergency core cooling typically are provided with the following:

- a) An indicator in the control room to provide the operator information on the process variable being monitored.
- b) An alarm to indicate to the operator that a specific safety function has been actuated.
- c) Indicator lights or other means to inform the operator which specific instrument channel has actuated the safety function.
- d) Rod positions, pump flows, or valve positions to verify that the actuated safety equipment has taken the action required for the safety function.

- e) Design features to allow test of the instrument channel without interfering with normal plant operations, and without lifting instrument leads or using jury rigs.

During review of the applicant's design, it was found that one or more of the features above was not provided for certain instrumentation used to initiate safety functions. Examples included instrumentation used to isolate essential service water to the air compressors and instrumentation used to isolate the non-safety-related portion of the component cooling water system. The applicants were requested to provide the staff with a list of all instrument channels which perform a safety function where one or more of the features listed in a through e above were not provided. The staff position was that the applicant should, at a minimum, provide features b through e above or provide a justification applicable to the specific safety function involved where any of the features would not be provided. The applicants provided the requested list of instrument channels and an evaluation of the alarms, indicators, and capability of testing for each. For all of these safety functions, the applicants have verified that the instrument channels can be tested without interfering with normal plant operations and without lifting instrument leads or using jury rigs. The applicants have further committed to provide additional indicators and alarms on the plant computer for specific functions as a result of the evaluations. The staff has reviewed the indications and alarms to be provided and found them acceptable. The additional indications and alarms to be provided by the applicants will be a condition of the license. The staff will provide requirements in the plant technical specifications for testing these safety functions.

7.3.3 Evaluation Findings

The review of the instrumentation and control aspects of the engineered safety feature (ESF) systems included the engineered safety features actuation system (ESFAS) and the ESF control systems. The ESFAS detects a plant condition requiring the operation of an ESF system and/or essential auxiliary support (EAS) system and initiates operation of these systems. The ESF control system regulates the operation of the ESF system following automatic initiation by the protection system or manual initiation by the plant operator.

We have conducted an audit review of these systems for conformance to guidelines of the applicable regulatory guides and industry codes and standards. In Section 7.1 of this SER we concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon our audit review of the system design for conformance to the guidelines, we find that upon satisfactory resolution of the open item identified in Section 7.3.2 of this report, there is reasonable assurance that the systems conform to the applicable guidelines.

Our review has included the identification of those systems and components for the ESFAS and ESF control systems which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based upon our review, we conclude that the applicant has identified those systems and components consistent with the design bases for the systems. Sections 3.10 and 3.11 of this SER address the qualification programs to demonstrate the capability of these systems and components to survive applicable events. Therefore, we find that the identification of the systems and components satisfies this aspect of the GDC-2, "Design Bases for Protection Against Natural Phenomena" and GDC-4, "Environmental and Missile Design Bases."

Based on our review, we conclude that the ESFAS conforms to the design bases requirements of IEEE-279. The system includes the provisions to sense accident conditions and anticipated operational occurrences to initiate the operation of ESF and EAS systems consistent with the analyses presented in Chapter 15 of the SAR. Therefore, we find that the ESFAS satisfies the requirements of GDC-20, "Protection System Functions."

The ESFAS adequately conforms to the guidance for periodic testing in Regulatory Guide (RG) 1.22 and IEEE-338 as supplemented by RG 1.118. The bypassed and inoperable status indication adequately conforms to the guidance of RG 1.47. The

ESFAS adequately conforms to the guidance on the application of the single failure criterion in IEEE-379 as supplemented by RG 1.53. Based on our review we conclude that the ESFAS satisfies the requirement of IEEE-279 with regards to the system reliability and testability. Therefore, we find that the ESFAS satisfies the requirement of GDC-21, "Protection System Reliability and Testability."

The ESFAS adequately conforms to the guidance in IEEE-384 as supplemented by RG 1.75 for the protection system independence. Based on our review, we conclude that the ESFAS satisfies the requirement of IEEE-279 with regards to the systems independence. Therefore, we find that the ESFAS satisfies the requirement of GDC-22, "Protection System Independence."

Based on our review of the ESFAS, we conclude that the system is designed with due consideration of safe failure modes if conditions such as disconnection of the system, loss of energy, or a postulated adverse environment are experienced. Therefore, we find that the ESFAS satisfies the requirements of GDC-23, "Protection System Failure Modes."

Based on our review of the interfaces between the ESFAS and plant operating control systems, we conclude that the system satisfies the requirements of IEEE-279 with regards to control and protection system interactions. Therefore, we find that the ESFAS satisfies the requirement of GDC-24, "Separation of Protection and Control Systems."

Our conclusions noted above are based upon the requirements of IEEE-279 with respect to the design of the ESFAS. Therefore, we find that the ESFAS satisfies the requirement of 50.55a(h) with regards to IEEE-279.

Our review of the ESFAS and ESF control systems has examined the dependence of these systems on the availability of essential auxiliary supporting (EAS) systems. Based on our review and coordination with those having primary review responsibility of the EAS systems, we conclude that the design of the ESFAS and ESF control systems are compatible with the functional performance requirements of EAS systems. Therefore, we find the interfaces between the ESFAS and ESF control systems and the EAS systems to be acceptable.

Our review of the ESF control systems included conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures consistent with the General Design Criteria applicable to these ESF systems. We conclude that the ESF control systems are testable and are operable on either onsite or offsite power (assuming only one source is available) and that the controls associated with redundant ESF systems are independent and satisfy the requirement of the single failure criterion. Therefore, we find the ESF control systems meet the relevant requirements of GDC-34, Residual Heat removal, GDC-35, Emergency Core Cooling, GDC-38, Containment Heat Removal, and GDC-41, Containment Atmosphere Cleanup.

In summary, the staff concludes that the ESFAS and the ESF control systems will be acceptable and meet the relevant requirements of General Design Criteria 2, 4, 20 thru 24, 34, 35, 38, and 41 and 10 CFR Part 50 50.55a(h) with satisfactory resolution of the open item identified in Section 7.3.2.3 of this report.

7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN

7.4.1 Description

The systems required for safe shutdown are those required to control the reactor coolant system temperature and pressure, to borate the reactor coolant, and to provide adequate residual heat removal. The plant design is such that the plant can be placed in a safe shutdown condition using only safety grade systems. The systems used for safe shutdown are:

- (1) Reactor Coolant System (RCS)
- (2) Main Steam System
- (3) Auxiliary Feedwater System
- (4) Chemical and Volume Control System
- (5) Borated Refueling Water System
- (6) Residual Heat Removal System (RHR)
- (7) Component Cooling Water System
- (8) Essential Service Water System
- (9) Supportive HVAC Systems
- (10) Emergency Diesel Generators
- (11) Spent Fuel Pool Cooling System
- (12) Supportive Portions of Instrument Air Systems

The Reactor Coolant System (RCS) transfers core residual heat to the steam generators. The reactor core is at a lower elevation than the steam generators ensuring that heat can be transported from the reactor core to the steam generators via natural circulation.

The main steam system consists of main steam piping, power operated atmospheric steam relief valves, safety valves, and main steam isolation valves. The system is used for maintaining a hot standby condition and for plant cooldown to the temperature and pressure at which the Residual Heat Removal System (RHR) can be placed in operation. Core residual heat and reactor coolant system sensible heat can be removed by use of the power operated atmospheric steam relief valves if the main condenser is not in service. The power operated atmospheric steam relief valves are safety grade air-operated valves with independent controls for each steam generator.

- 1 -

The auxiliary feedwater system is used to maintain water inventory in the steam generators when the main feedwater system is not available. The auxiliary feedwater system is used following a reactor shutdown in conjunction with the condenser dump valves (if available) or atmospheric steam relief valves, to cool the reactor coolant system to the temperature and pressure at which the RHR system can be brought into operation.

The Chemical and Volume Control System (CVCS) is used for reactor coolant boration and inventory control. In the event normal charging and letdown paths are not available, boration and inventory control functions can be accomplished by utilizing redundant safety grade paths. The Refueling Water Storage Tank will be used as the source of borated makeup to the RCS in the event that the boric acid transfer pumps are not available.

The Residual Heat Removal System transfers heat from the RCS to the Component Cooling Water System (CCWS) to reduce the temperature of the reactor coolant to the cold shutdown temperature at a controlled rate during the second part of a plant cooldown, and maintains this temperature until the plant is started up. Parts of the RHR system also serve as parts of the Emergency Core Cooling System (ECCS) during the injection and recirculation phases of a LOCA.

The Component Cooling Water System (CCWS) provides cooling water to selected auxiliary components during normal plant operation and during shutdown. It also provides cooling water to several engineered safety feature systems following an accident. The system is a closed loop system which serves as an intermediate barrier between the Service Water System or Essential Service Water System and potentially radioactive systems in order to eliminate the possibility of an uncontrolled release of radioactivity.

The Essential Service Water System (ESWS) removes heat from plant components which require cooling for safe shutdown of the reactor or following an accident. The ESWS also provides emergency makeup to the spent fuel pool and the CCWS, and is the backup water supply to the auxiliary feedwater system. The ESWS consists of two redundant cooling water trains.

Portions of the plant HVAC systems are required to function following an accident and to maintain the plant in a safe shutdown condition. These portions of the HVAC systems are safety grade.

The onsite power system is provided with preferred power from the offsite system through two independent and redundant sources of power. The Class 1E ac system loads required to maintain the plant at safe shutdown or to mitigate the consequences of an accident are separated into two load groups which are powered from separate Engineered Safety Features transformers when offsite power is available or from two independent diesel generators (one per load group) when offsite power is not available.

The fuel pool cooling system consists of two 100-percent-capacity cooling trains for the removal of decay heat generated by irradiated fuel stored in the spent fuel pool. The fuel pool cooling heat exchangers are serviced by the component cooling water system on the shell side with remote manual-operated isolation valves provided.

The Compressed Air System (CAS) provides a safety grade backup compressed gas supply for the auxiliary feedwater control valves and main steam atmospheric relief valves.

To effect a unit shutdown, the unit will be brought to, and maintained at, a safe shutdown condition under control from the main control room or the auxiliary shutdown control panel. Controls for the systems discussed above are required to maintain a safe shutdown under non-accident conditions. The applicant has identified the following monitoring indicators as essential to maintaining safe shutdown:

1. Water level for each steam generator
2. Pressure for each steam generator
3. Pressurizer water level
4. Reactor coolant system pressure
5. Suction pressure for each auxiliary feedwater pump
6. Boric acid tank level
7. Emergency letdown flow
8. Reactor coolant pump seal water flow
9. Boron injection flow
10. Refueling water storage tank level
11. Component cooling water system flow to components inside containment.

In addition, the applicant has committed to provide safety grade reactor coolant temperature indication and safety grade auxiliary feedwater flow indication.

7.4.2 Remote Shutdown Capability

If temporary evacuation of the control room is required because of some abnormal station condition, the operators can establish and maintain the station in a hot standby condition from outside the control room through the use of controls and indicators located at the auxiliary shutdown control panel, switchgear, and motor control centers, and by control of individual equipment at the device location. The auxiliary shutdown panel is located in a locked room to restrict access. The auxiliary shutdown panel is designed to seismic Category I requirements and essential short term controls and indicators (those required to maintain hot standby for the first 24 hours following shutdown) are designed to comply with applicable portions of IEEE Standard 279-1971. Although the prime intent of the auxiliary shutdown control panel is the maintaining of hot standby from outside the control room, this panel can also be used for certain functions when implementing cold shutdown from outside the control room. The plant design includes the capability of attaining cold shutdown from outside the control room. For this, instrumentation and controls may require some jury-rigging.

- 7.4.3 RESOLUTION OF ISSUES

7.4.3.1 Capability for Safe Shutdown Following Loss of a Bus Supplying Power to Instruments and Controls

The staff requested that the applicants review the adequacy of emergency operating procedures to be used to obtain safe shutdown upon loss of any Class 1E or non-Class 1E bus supplying power to safety or non-safety-related instruments and controls. This issue was addressed for operating reactors through IE Bulletin 79-27.

The applicants have conducted a review using the guidelines of Bulletin 79-27 and concluded that no design modifications are required. However, since the preparation of plant procedures has not been completed, all actions requested in the Bulletin have not been completed.

Confirmatory Item: The applicants have been asked to provide the staff with the following confirmatory information subsequent to completion of plant procedures:

- a) Confirm that all a.c. and d.c. instrument buses that could affect the ability to achieve a cold shutdown condition were reviewed. Identify these buses.
- b) Confirm that all instrumentation and controls required by emergency shutdown procedures were considered in the review. Identify these instruments and controls at the system level of detail.
- c) Confirm that clear, simple, unambiguous annunciation of loss of power is provided in the control room for each bus addressed in Item a above. Identify any exceptions.
- d) Confirm that the effect of loss of power to each load on each bus identified in Item a above, including ability to reach cold shutdown, was considered in the review.
- e) Confirm that the re-review of IE Circular No. 79-02 which is required by Action Item 3 of Bulletin 79-27 was extended to include both Class 1E and non-Class 1E inverter supplied instrument or control buses. Identify these buses or confirm that they are included in the listing required by Item a above.

7.4.3.2 Operator Actions Required to Maintain Safe Shutdown From Outside the Control Room

In Amendment 5 to the FSAR the applicants included descriptive information on controls used to maintain safe shutdown from outside the control room which indicated that jury-rigging of controls may be required after the first 24 hours. In discussions with the staff the applicants have stated that the description in Amendment 5 was in error. Only local control of specific valves and pumps is required. The staff finds this acceptable.

Confirmatory Item: The applicants have committed to correct the FSAR and to provide a description of the specific local actions required after 24 hours. The information to be incorporated in the FSAR will include the location of the equipment involved and the available redundancy.

7.4.4 Evaluation Findings

The review of systems required for safe shutdown included the sensors, circuitry, redundancy features, and actuated devices that provide the instrumentation and control functions that prevent the reactor from returning to criticality and provide means for adequate residual heat removal.

We have conducted an audit review of these systems for conformance to guidelines of the applicable regulatory guides and industry codes and standards. In Section 7.1 of this SER we concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon our audit review of the systems designs for conformance to the guidelines we find that there is reasonable assurance that

the systems conform fully to the applicable guidelines.

Our review has included the identification of those systems and components required for safe shutdown which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based upon our review, we conclude that the applicant has identified those systems and components consistent with the design bases for the systems. Sections 3.10 and 3.11 of this SER address the qualification programs to demonstrate the capability of these systems and components to survive applicable events. Therefore, we find that the identification of these systems and components satisfies this aspect of the GDC-2, "Design Bases for Protection Against Natural Phenomena" and GDC-4, "Environmental and Missile Design Bases."

Based on our review, we conclude that instrumentation and controls have been provided to maintain variables and systems which can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems within prescribed operating ranges during plant shutdown. Therefore, we find that the systems required for safe shutdown satisfy the requirements of GDC-13, "Instrumentation and Control."

Instrumentation and Controls have been provided within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown including a shutdown following an accident. Equipment at appropriate locations outside the control room have been provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and

controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures. Therefore, we conclude that the systems required for safe shutdown satisfy the requirements of GDC-19, "Control Room."

Our review of the instrumentation and controls required for safe shutdown has examined the dependence of these systems on the availability of essential auxiliary support (EAS) systems. Based on our review and coordination with those having primary review responsibility for the EAS systems, we conclude that the design of EAS systems are compatible with the functional performance requirements of the systems reviewed in this section. Therefore, we find the interfaces between the design of safe shutdown systems and the design of EAS systems to be acceptable.

Our review of the instrumentation and control systems required for safe shutdown included conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures consistent with the General Design Criteria applicable to safe shutdown systems. We conclude that these systems are testable, and are operable on either onsite or offsite electrical power, and that the controls associated with redundant safe shutdown systems are independent and satisfy the requirements of the single failure criterion. Therefore, we find that these systems meet the relevant requirements of GDC-34, Residual Heat Removal, GDC-35, Emergency Core Cooling, and GDC-38 Containment Heat Removal.

In summary, the staff concludes that the systems required for safe shutdown are acceptable and meet the relevant requirements of General Design Criteria 2, 4, 13, 19, 34, 35, and 38.

7.5 INFORMATION SYSTEMS IMPORTANT TO SAFETY

7.5.1 Description

The information systems important to safety are composed of display instruments which provide information to enable the operator to assess reactor status, the onset and severity of accident conditions, and engineered safety feature systems (ESFS) status and performance, and to enable the operator to intelligently perform vital manual actions such as safe shutdown and initiation of manual ESFSs. The systems consist of both safety grade and non-safety grade instruments and cover the following functions:

- 1) Reactor Trip
- 2) Engineered Safety Features
- 3) Safe Shutdown

The protective system provides the operator with information pertinent to system status and safety. All transmitted signals (flow, pressure, temperature, etc.) which can cause a reactor trip are either indicated or recorded for each channel, including all neutron flux power range signals (top detector, bottom detector, algebraic difference, and average of bottom and top detector signals). Parameters associated with automatic actuation as well as those required to enable the operator to manually initiate Engineered Safety Feature Systems are displayed. The indicators provided for the actuating parameters display the same analog signals monitored by the Engineered Safety Features Actuation System. Any reactor trip will actuate an alarm and an annunciator. Such protective actions are indicated and identified down to the channel level.

Alarms and annunciators are also used to alert the operator of deviations from normal operating conditions so that the operator may take appropriate corrective action to avoid a reactor trip. Actuation of any rod stop or trip of any reactor trip channel will actuate an alarm.

ESF Status Panel displays are provided to meet the requirements of Regulatory Guide 1.47, on a separation group basis. Inputs are isolated from annunciation and logic circuitry via IEEE-323 qualified isolators. Under normal plant conditions, component level windows are either dark or lit white in a prescribed manner. If a component is normally in its safeguards state its window is lit white. If a component is not normally in its safeguards state its window is dark. System level windows are dark under full power conditions with no components bypassed. Upon an ESF actuation, all component level windows within the associated actuation system will be lit white provided all components have correctly responded to the actuation signal. In this case, the system level window also goes into a white mode. However, if one or more components do not respond correctly to the actuation signal, the system level window would remain dark.

When a bypass or inoperable condition exists on any component (breaker racked out, loss of control voltage, handswitch in a pull to lock mode), its component level window is lit amber. Simultaneously the associated system level window is also lit amber, actuating an audible alarm and alerting the operator of a bypassed or inoperable condition. On certain critical valves (for example, the auxiliary feedwater discharge valves) an amber light and/or audio annunciation provides bypassed/inoperable status upon valve misalignment. Automatic system level indication of bypass and inoperable status applies to automatically initiated components including those components which directly support the automatically initiated components but which themselves may not be automatically initiated because they are normally in the operating mode.

The shutdown control display instruments are required for manual operations to safety maintain the plant in a shutdown condition. These instruments are provided on the main control board in the main control room and on the auxiliary shutdown control panel outside of the main control room. Two or more separate and redundant channels of display information are provided for each required process variable.

The following safety grade readouts are provided in the control room to maintain the plant in a safe shutdown condition, or to take the correct action during the course of an event or during post accident recovery.

Nuclear Steam Supply System (NSSS) Indicators:

- (1) Wide Range T_{hot} and T_{cold}
- (2) Pressurizer Water Level
- (3) Steam Generator Pressures
- (4) Steam Generator Water Levels (narrow range and wide range)
- (5) Containment Pressure (narrow range and wide range)
- (6) Reactor Coolant System Wide Range Pressure
- (7) Boric Acid Water Level
- (8) Refueling Water Storage Tank Water Level
- (9) Safety Injection Flow
- (10) Reactor Coolant System Excess Letdown Heat Exchanger Temperature

Balance of Plant (BOP) Indicators:

- (1) Auxiliary Feedwater Flow
- (2) Condensate Storage Tank Pressure
- (3) Auxiliary Feedwater Pump Suction Pressure
- (4) Control Room Air Intake Chlorine
- (5) Control Room Air Intake Gaseous Radioactivity
- (6) Containment Gaseous Radioactivity
- (7) Containment Hydrogen
- (8) Containment Sump/Containment Level
- (9) Containment Purge Gaseous Radioactivity
- (10) Containment Spray Additive Tank Level
- (11) Fuel Building Gaseous Radioactivity
- (12) Containment Air Temperature
- (13) Containment Post Accident Radiation
- (14) Control Building Sump Level
- (15) Diesel Generator Building Sump Level
- (16) RHR Pump Room Sump Level
- (17) Auxiliary Building Sump Level

The parameters indicated on the auxiliary shutdown panel are as follows (those which are safety grade are designated with an "s"):

- (1) Pressurizer Pressure
- (2) Pressurizer Water Level (s)
- (3) RCS Pressure (s)
- (4) Steam Generator Pressures (s)
- (5) Steam Generator Water Levels (s)
- (6) Auxiliary Feedwater Flow (s)
- (7) Auxiliary Feedwater Pump Suction Pressures (s)
- (8) Auxiliary Feedwater Pump Discharge Pressures
- (9) Condensate Storage Tank Level
- (10) RCS Cold Leg Temperature
- (11) Source Range Nuclear Instruments
- (12) Intermediate Range Nuclear Instruments

In addition to the indicators for the above systems, position indication lights are provided for the associated remote control valves.

7.5.2 RESOLUTION OF ISSUES

7.5.2.1 Reactor Coolant Temperature Indicators on the Auxiliary Shutdown Panel

During the staff review, the applicants were asked to clarify the design criteria for wide range reactor coolant temperature indication at the auxiliary shutdown panel. The applicants stated that reactor coolant wide range temperature indication is not essential for maintaining safe hot shutdown. However, the applicants did commit to providing one reactor coolant cold leg indicator per loop with the indicators for Loops 1 and 2 powered from a different power supply and routed in a different non-safety-grade separation group from the indicators for Loops 3 and 4.

Open Item: The staff has expressed concern that hot leg temperature indicators may also be required in order to insure that subcooled conditions are maintained in the reactor coolant system during shutdown. The resolution of this issue will be addressed in a supplement to this report.

7.5.2.2 Actuation of Valve Component Level Windows on the Bypassed and Inoperable Status Panel

The original design for actuation of the accumulator valve component level windows on the bypassed and inoperable status panel was such that the bypass indication was not actuated until the valve reached the fully closed position rather than when the valve left the fully open position. The staff position was that bypass indication should be actuated when a valve leaves the position required for it to accomplish its safety function. The applicants have changed the design for the accumulator valve position switches such that the bypass is indicated when a valve is not fully open. The applicants have also stated that for other valves where valve misalignment is indicated on the bypassed and inoperable status panel, the bypass indication occurs when the valve leaves the position required for it to accomplish its safety function. The staff finds the applicants response to be adequate. The license will be conditioned to require the accumulator valve position switches to be changed as discussed above.

7.5.2.3 Post-Accident Monitoring

Revision 2 to Regulatory Guide 1.97, "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," was issued in December 1980. The Operating License will be conditioned to require that the applicants comply by June 1983 with Regulatory Guide 1.97, Revision 2 or provide justification for any alternatives.

7.5.3 Evaluation Findings

The information systems important to safety provide the operator with information on the status of the plant to allow manual safety actions to be performed when necessary. The scope of review included tables of system variables and component states to be indicated, functional diagrams, electrical and physical layout drawings, and descriptive information. The review has included the applicable acceptance criteria and guidelines and design bases, including those for indication of bypassed or inoperable safety systems. The review has also included the applicant's analyses of the manner in which the design of information systems conforms to the acceptance criteria and guidelines which are applicable to these systems as noted in the staff's Standard Review Plan.

We have conducted an audit review of these systems for conformance to guidelines of the applicable regulatory guides and industry codes and standards. In Section 7.1 of this SER, we concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon our audit review of the systems designs for conformance to the guidelines, we find that upon satisfactory resolution of the open item identified in Section 7.5.2 there is reasonable assurance that the systems conform to the guidelines applicable to them.

Our review has included the identification of those systems and components of the information systems which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based upon our review, we conclude that the applicant has identified those systems and components consistent with the design bases for the systems. Sections 3.10 and 3.11 of this SER address the qualification programs to demonstrate the capability of these systems and components to survive applicable events. Therefore, we find that the identification of these systems and components satisfies this aspect of GDC-2, "Design Bases for Protection Against Natural Phenomena" and GDC-4, "Environmental and Missile Design Bases."

The redundant safety grade information systems adequately conform to the guidance for the physical independence of electrical systems provided in RG 1.75.

We conclude that the information systems important to safety include appropriate variables and that their range and accuracy are consistent with the plant safety analysis. Therefore, we find that the information systems satisfy the requirements of GDC-13, "Instrumentation and Control" for monitoring variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions. Further, we find that conformance to GDC-13 and the applicable guidelines satisfies the requirements of GDC-19, "Control Room" with respect to information systems provided in the control room from which actions can be taken to operate the unit safely under normal conditions and to maintain it in a safe condition under accident conditions.

In summary, the staff concludes that the information systems important to safety will be acceptable and meet the requirements of General Design Criteria 2, 4, 13, and 19 with satisfactory resolution of the open item identified in Section 7.5.2.1.

7.6 INTERLOCK SYSTEMS IMPORTANT TO SAFETY

The group of instrumentation systems included in this section are those required for safety but not previously discussed in Sections 7.2 through 7.5.

7.6.1 Residual Heat Removal System Isolation Valves

The residual heat removal system (RHRS) isolation valves are normally closed and are opened only for residual heat removal system operation after system pressure is reduced to approximately 425 psig and system temperature has been reduced to approximately 350°F.

There are two motor-operated valves in series in each of the two residual heat removal pump suction lines from the reactor coolant system (RCS) hot legs. The two valves nearest the RCS are designated as the inner isolation valves, while the two valves nearest the residual heat removal pumps are designated as the outer isolation valves. The interlock features provided for the outer isolation valves are identical to those provided for the inner isolation valves, except that equipment diversity is employed by virtue of the fact that a different manufacturer is used for the pressure transmitters for the two sets of valves.

Each valve is interlocked so that it cannot be opened unless the RCS pressure is below a preset pressure. This interlock prevents the valve from being opened when the RCS pressure and the residual heat removal pump head are above the RHRS design pressure. A second pressure interlock is provided to close the valve automatically if the RCS pressure subsequently increases to a preset value.

In addition, the valves cannot be opened unless the isolation valves in the following lines are closed:

- (1) Recirculation line from the residual heat exchanger outlet to the suction of the high head safety injection pumps.
- (2) RHR pump suction line from the refueling water storage tank.
- (3) RHR pump suction line from the containment sump.

7.6.2 Accumulator Motor-Operated Valves

The safety injection system (SIS) accumulator discharge isolation valves are motor-operated, normally open valves which are controlled from the main control board. These valves are interlocked so that:

- (1) They open automatically on receipt of an SIS with the main control board switch in either the "AUTO" or "CLOSE" position.
- (2) They open automatically whenever the RCS pressure is above the safety injection unblock pressure (P-11 interlock) when the main control board switch is in the "AUTO" position.
- (3) They cannot be closed as long as a safety injection signal is present.

During plant shutdown, the accumulator valves are closed. To prevent an inadvertent opening of these valves during that period, the accumulator valve motor circuit breakers will be opened or withdrawn. Administrative control is required to ensure that these valve circuit breakers are closed during the pre-startup procedures.

An alarm will sound for any accumulator isolation valve, under the following conditions, when the RCS pressure is above the safety injection unblocking pressure (P-11 interlock):

- (1) Valve motor-operated limit switch indicates valve not open.
- (2) Valve stem-operated limit switch indicates valve not open.
-The alarm on this switch will repeat itself at given intervals.

7.6.3 Interlocks for RCS Pressure Control During Low Temperature Operation

The RCS pressure control includes automatic actuation logic for two pressurizer power-operated relief valves (PORVs). The function of this actuation logic is to continuously monitor RCS temperature and pressure conditions, with the actuation logic unblocked only when plant operation is below a preset temperature and manual action has been taken to unblock the logic. The monitored system temperature signals are processed to generate the reference pressure limit program which is compared to the actual monitored RCS pressure. This comparison provides automatic actuation signals to open the PORVs to prevent pressure conditions from exceeding allowable limits. The generating station variables required for the RCS pressure control interlock are channelized with a different protection train used for each pressurizer power operated relief valve.

7.6.4 Switchover from Injection to Recirculation

The suction valves in the line from the containment sump to the residual heat removal (RHR) pumps open when two-out-of-four level transmitters indicate a low level in the refueling water storage tank (RWST) in conjunction with a safety injection signal. The valves from the RWST to the RHR suction will close automatically after the sump suction valves are open. The safety injection pumps and charging pumps are manually realigned for the recirculation mode.

The low RWST level signal is alarmed to inform the operator to initiate the manual action required to realign the pumps for the recirculation mode.

7.6.5 Isolation of Essential Service Water (ESW) to the Air Compressors

For each train of ESW, a differential pressure transmitter and bistable is provided to sense flow to the non-safety-related air compressors. On high flow (indicative of gross leakage in the non-seismic portion of the system), an isolation valve in that ESW train is automatically closed. The isolation valve will remain in the closed position until the valve is manually reset by the operator in the control room. A means of remote manual isolation and indication of valve positions are provided in the control room. The isolation valves are air-operated, and are designed to fail closed on the loss of air or electrical power.

7.6.6 Isolation of the Non-Safety-Related Portion of the Component Cooling Water (CCW) System

The non-seismic portion of the CCW system is isolated by two isolation valves in series provided in both the supply and return lines. These valves are air-operated, designed to fail closed on loss of air or electrical power, and automatically close upon low CCW surge tank level, SIS, or high flow. The non-seismic portion of the CCW system can also be isolated by remote manual means.

Two independent flow transmitters in the supply line sense flow through the isolation valves. On high flow (indicative of gross leakage in the non-seismic portion of the system), the isolation valves are automatically closed and will remain in the closed position until the valves are manually reset by the operator in the control room. Each flow transmitter and its associated bistable provides isolation signals to one valve in the supply line and one valve in the return line.

Two independent level transmitters (one per surge tank) are provided. On low surge tank level, the isolation valves are automatically closed and will remain in the closed position until the valves are manually reset by the operator in the control room. Each level transmitter and its associated bistable provides isolation signals to one valve in the supply line and one valve in the return line.

7.6.7 RESOLUTION OF ISSUES

7.6.7.1 Interlocks for Reactor Coolant System (RCS) Pressure Control During Low Temperature Operation

To minimize the potential of RCS overpressurization during low temperature operation, an automatic system, which is manually enabled during low temperature operation, is provided to maintain pressure within allowable limits. The original design described by the applicants in the FSAR included two reactor coolant system temperature actuators. The design was such that the failure of either actuator could defeat the overpressure protection at low temperatures. During the course of the staff review, the applicants redesigned this system. In the modified design, the generating station variables required for reactor coolant system pressure protection during low temperature operation are channelized with a different protection train used for each of the two pressurizer power operated relief valves. The modified design eliminates the potential for a single failure to defeat overpressure protection at low temperatures. The staff has reviewed the modified design and finds it acceptable. The license will be conditioned to require this modified design.

7.6.7.2 Volume Control Tank Level Control and Protection Interaction

On May 21, 1981, Westinghouse notified the Commission of a potentially adverse control and protection system interaction whereby a single random failure in the Volume Control Tank level control system could lead to a loss of redundancy in the high head safety injection system for certain Westinghouse designed plants. The applicants were asked to determine whether the generic problem identified by Westinghouse exists on the SNUPPS plants.

The applicants have stated that the level control function will be separated from the charging pump protection function on the SNUPPS plants such that the problem identified by Westinghouse cannot occur. The staff finds the applicants response acceptable and will condition the license to require the design described above.

Confirmatory Item: A formal revision to the FSAR is required to describe the above design.

7.6.7.3 Boron Dilution Control

In response to questions from the staff on design features provided for mitigating the consequences of an inadvertent boron dilution, the applicants have committed to incorporate the same design for terminating boron dilution as provided for Comanche Peak (Docket No. 50-445). The source range and intermediate range nuclear instrumentation will be seismically and environmentally qualified. The staff finds this

commitment to be acceptable and will condition the license to require these design features.

Confirmatory Item: The applicants will include the description of the boron dilution control instrumentation in the FSAR.

7.6.8 Evaluation Findings

The staff concludes that

the designs of the interlock systems important to safety are acceptable and meet the relevant requirements of General Design Criteria 2, "Design Bases for Protection Against Natural Phenomena" and 4 "Environmental and Missile Design Bases." This conclusion is based on the following:

The review of the interlock systems important to safety included the interlocks to prevent overpressurization of low pressure systems when connected to the primary coolant system. The staff position with regards to this interlock system is set forth in Branch Technical Position ICSB-3, "Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System." Based on our review, we conclude that the design of this system adequately complies with the staff's guidance.

Our review included the interlock provided to prevent overpressurization of the primary coolant system during low temperature operation. The staff's position with regards to this interlock system is set forth in Branch Technical Position RSB5-2, "Overpressurization Protection of Pressurized Water Reactors While Operating At Low Temperatures." Based on our review, we conclude that the design of this system adequately complies with the staff's guidance.

Our review included the interlocks for the ECCS accumulator valves. The staff's position with regards to this interlock system is set forth in Branch Technical Position ICSB-4, "Requirements of Motor Operated Valves in the ECCS Accumulator Lines." Based on our review we conclude that these interlocks adequately comply with the staff's guidance.

Based on our review of the interlock systems important to safety, we conclude that their design bases are consistent with the plant safety analysis and the systems importance to safety. Further, we conclude that the aspects of the

design of these systems with respect to single failures, redundancy, independence, qualification, and testability are adequate to assure that the functional performance requirements will be met.

Our review has included the identification of those systems and components of interlock systems important to safety which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based upon our review, we conclude that the applicant has identified the systems and components consistent with the design bases for the interlock systems. Sections 3.10 and 3.11 of this SER address the qualification programs to demonstrate the capability of these systems and components to survive applicable events. Therefore, we find that the identification of the systems and components satisfies this aspect of the GDC-2, "Design Bases for Protection Against Natural Phenomena," and GDC-4, "Environmental and Missile Design Bases."

IMAGE EVALUATION
TEST TARGET (MT-3)

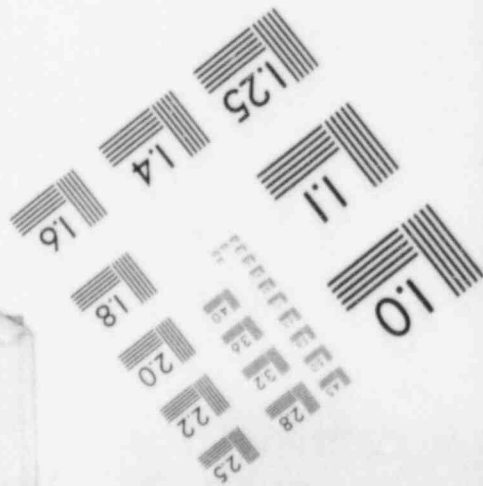
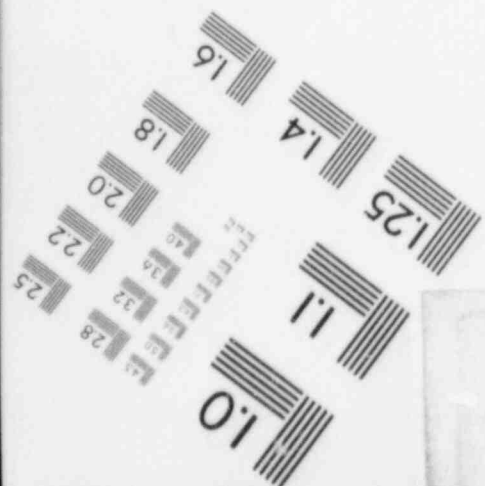
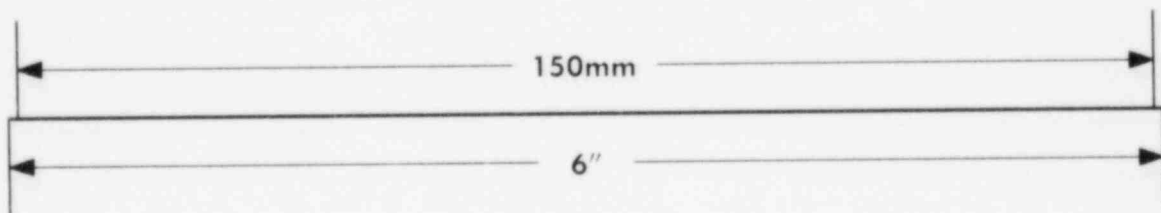
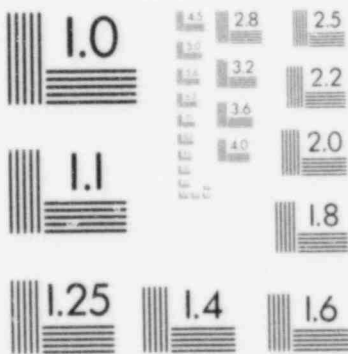
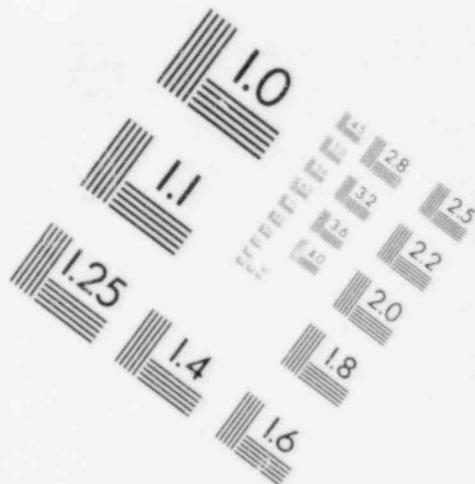
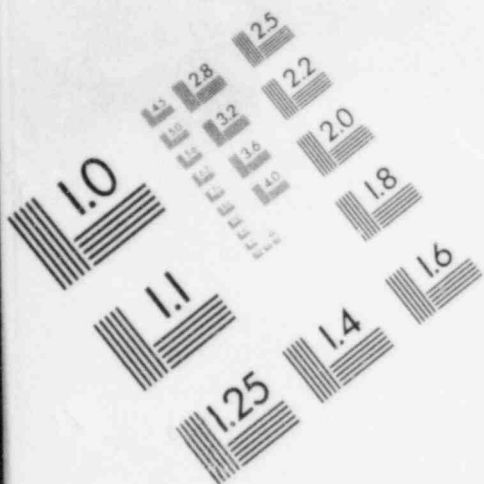
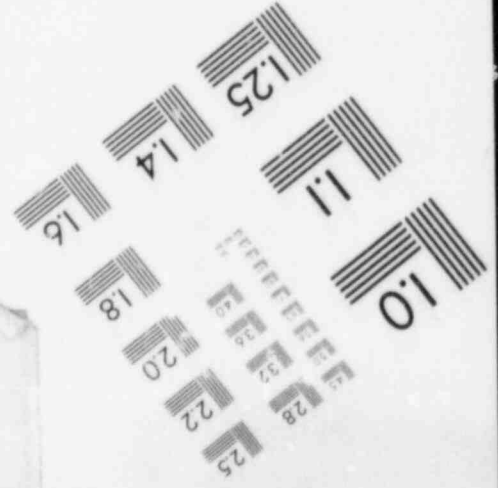
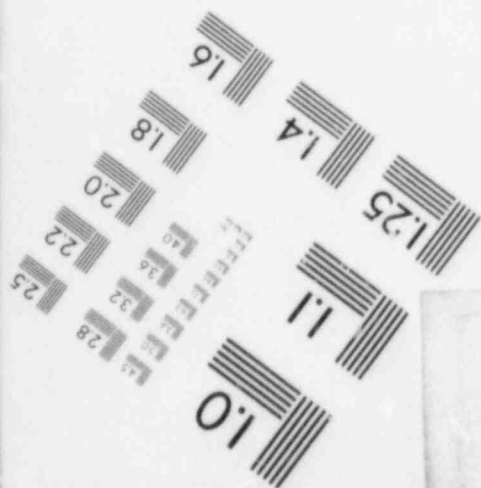
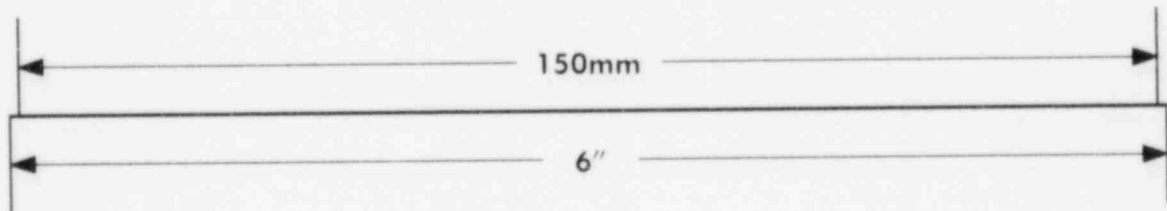
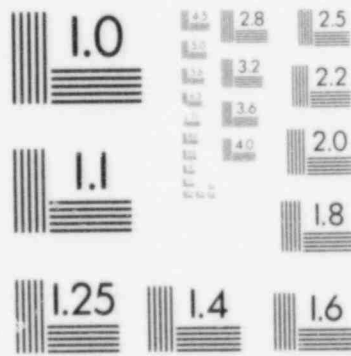
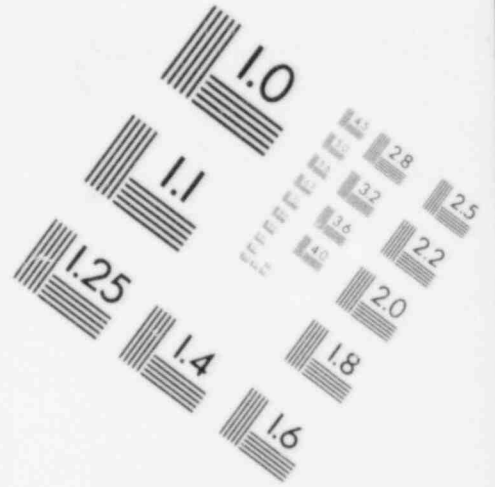
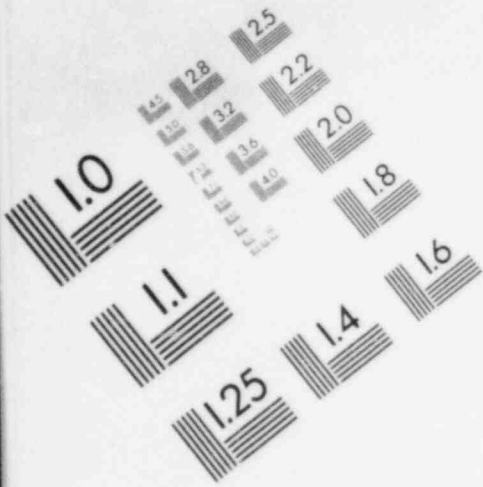


IMAGE EVALUATION
TEST TARGET (MT-3)



7.7 CONTROL SYSTEMS

The plant control systems described in this section include the following:

- (1) Reactor Control
- (2) Rod Control
- (3) Pressurizer Pressure Control
- (4) Pressurizer Water Level Control
- (5) Steam Generator Water Level Control
- (6) Steam Dump Control
- (7) Plant Control System Interlocks
- (8) Incore Instrumentation
- (9) Boron Concentration Monitoring System
- (10) Plant Control Signals for Monitoring and Indicating

7.7.1 Reactor Control

The reactor control system enables the nuclear plant to follow load changes automatically, including the acceptance of step load increases or decreases of 10 percent and ramp increases or decreases of 5 percent per minute within the load range of 15 percent to 100 percent, without reactor trip, steam dump, or pressure relief (subject to possible transient xenon limitations). The system is also capable of restoring coolant average temperature to within the programmed temperature deadband following a change in load. Manual control rod operation may be performed at any time within the range of defined control rod insertion limits.

7.7.2 Rod Control

The rod control system receives rod speed and direction signals from the Reactor Control System. The rod speed demand signal varies over the range of 3.75 inches to 45 inches per minute (6 to 72 steps/minute), depending on the magnitude of the input signal. Manual control is provided

to move a control bank in or out at a prescribed fixed speed. A permissive interlock (C-5) derived from measurements of turbine impulse chamber pressure prevents automatic control when the turbine load is below 15 percent.

The five shutdown banks are always in the fully withdrawn position during normal operation and are moved to this position at a constant speed by manual control prior to criticality. The control banks are the only rods that can be manipulated under automatic control. Each control bank is divided into two groups to obtain smaller incremental reactivity changes per step. All rod cluster control assemblies (RCCAs) in a group are electrically paralleled to move simultaneously. There is individual position indication for each RCCA. A reactor trip signal causes all the rods to fall by gravity into the core and, thus, totally overrides the control system.

7.7.3 Pressurizer Pressure Control

The reactor coolant system pressure is controlled by using either the heaters (in the water region) or the spray (in the steam region) of the pressurizer plus steam relief for large transients.

The electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater group is proportionally controlled to correct for small pressure variations. These variations are caused by heat losses, including heat losses due to a small continuous spray. The remaining (back-up) heaters are turned on when the pressurizer pressure control signal demands approximately 100 percent proportional heater power.

The spray nozzle is located on the top of the pressurizer. Spray is initiated when the pressure controller spray demand signal is above a given setpoint. The spray rate increases proportionally with increasing spray demand signal until it reaches a maximum value. Steam condensed by the spray reduces the pressurizer pressure. A small continuous spray is normally maintained to reduce thermal stresses and thermal shock and to help maintain uniform water chemistry and temperature in the pressurizer.

Power relief valves limit system pressure for large positive pressure transients and reduce the possibility of actuating the pressurizer safety valves.

7.7.4 Pressurizer Water Level Control

The pressurizer operates by maintaining a steam cushion over the reactor coolant. As the density of the reactor coolant varies with temperature, the steam water interface is adjusted to compensate for the density variations with relatively small pressure disturbances. The water inventory in the reactor coolant system is maintained by the chemical and volume control system. During normal plant operation, the charging flow is varied to automatically produce the flow demanded by the pressurizer water level controller. The pressurizer water level is programmed as a function of coolant average temperature, with the highest measured average temperature (auctioneered) being used. The pressurizer water level decreases as the load is reduced from full load. This is a result of coolant contraction following programmed coolant temperature reduction from full power to low power. The programmed level is designed to match as nearly as possible the level changes resulting from the coolant temperature changes.

7.7.5 Steam Generator Water Level Control

Each steam generator is equipped with a three-element feedwater flow controller which maintains a programmed water level which is a function of turbine load. The three-element feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the water level signal, the programmed level, and the pressure compensated steam flow signal. The feedwater pump speed is varied to maintain a programmed pressure differential between the steam header and the feedwater pump discharge header. The speed controller continuously compares the measured ΔP with a programmed ΔP_{ref} which is a linear function of steam flow. Manual override of the feedwater control system is available at all times.

7.7.6 Steam Dump Control

The steam dump system, together with control rod movement, is designed to accept a 50 percent loss of net load without tripping the reactor. The automatic steam dump system is able to accommodate this abnormal load rejection and to reduce the effects of the transient imposed upon the reactor coolant system. By bypassing main steam directly to the condenser, an artificial load is thereby maintained on the primary system. The rod control system can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions. The steam dump steam flow capacity is 40 percent of full load steam flow at full load steam pressure.

7.7.6.1 Load Rejection Steam Dump Controller

This mode of control prevents a large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is the difference between the lead-lag compensated auctioneered reactor coolant T_{avg} and the reference T_{avg} based on turbine impulse chamber pressure.

7.7.6.2 Plant Trip Steam Dump Controller

The plant trip controller modulates the steam dump valves to regulate the rate of removal of decay heat and thus gradually establish the equilibrium hot standby condition after a reactor turbine trip.

7.7.6.3 Steam Header Pressure Controller

Residual heat removal during shutdown is accomplished by the steam pressure controller which controls the amount of steam flow to the condensers based on measured steam pressure. This controller operates a portion of the same steam dump valves to the condensers which are used during the transient following load rejection or plant trip.

7.7.7 Plant Control System Interlocks

7.7.7.1 Rod Stops

Rod stops are provided to prevent abnormal plant conditions which could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures.

7.7.7.2 Automatic Turbine Load Runback

Automatic turbine load runback is initiated by an approach to an overpower or overtemperature condition. The runback prevents high power operation that might lead to an undesirable condition which, if reached, would be protected by reactor trip. Turbine load reference reduction is initiated by either an overtemperature or overpower ΔT signal.

7.7.7.3 Turbine Loading Stop

An interlock (C-16) is provided to limit turbine loading during a rapid return to power transient when a reduction in reactor coolant temperature is used to increase reactor power through the negative moderator coefficient. This interlock limits the reduction in coolant temperature so that it does not reach cooldown accident limits and preserves satisfactory steam generator operating conditions. Subsequent automatic turbine loading can begin after the interlock setpoint has been cleared by an increase in coolant temperature, which is accomplished by reducing the boron concentration in the coolant.

7.7.8 Incore Instrumentation

The incore instrumentation system consists of chromel-alumel thermocouples at fixed core outlet positions and movable miniature neutron detectors which can be positioned at the center of selected fuel assemblies, anywhere along the length of the fuel assembly vertical axis. The thermocouple readings are monitored by the computer. A control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors while plotting neutron flux versus detector position. The equipment for control, position indication, and flux recording for each detector is located in the control room. (See discussion of II.F.2 under Section 7.1.4 for a discussion of the use of the incore thermocouples in the core subcooling monitors).

7.7.9 Boron Concentration Monitoring System

The boron concentration monitoring system utilizes a sampler assembly unit which contains a neutron source and neutron detector located in a shield tank. Piping within the shield tank is arranged to provide coolant sample flow between the neutron source and the neutron detector. Neutrons originating at the source are thermalized in the sample and surrounding moderator and pass through the sample and impinge upon the detector. The boron concentration is calculated by monitoring the neutron count rate. The neutron cross-section of the boron in the sample is a function of the sample temperature. Therefore, the sample temperature is also monitored and the neutron count rate to boron concentration modified to compensate for the variance of temperature. The boron concentration monitoring system is designed for use as an advisory system. It is not used for fundamental operating decisions but, rather, provides information as to when additional check analyses are warranted.

7.7.10 Plant Control Signals for Monitoring and Indicating

Plant control system signals are used to provide indications for monitoring plant conditions to insure that variables are maintained within operating limits. The following will discuss those systems used to monitor the operating status of the reactor.

The power range nuclear instrumentation channels are used to monitor core power level, axial flux imbalance, and radial flux imbalance. These channels are capable of recording overpower excursions up to 200 percent of full power. The following alarms are provided:

- 1) Deviation of indicated nuclear power from the four channels
- 2) Upper core power radial tilt from the upper sections of the detectors for the four channels
- 3) Lower core power radial tilt from the lower sections of the detectors for the four channels
- 4) Axial flux difference imbalance (this alarm is derived from the plant computer)

Two separate systems are provided to sense and display control rod position. The digital position indication system measures the actual position of each rod. The control board display unit contains a column of light-emitting-diodes (LEDs) for each rod. At any given time, the one LED illuminated in each column shows the position for that particular rod. The demand position system counts pulses generated in the rod drive control system to provide a digital display of the demanded (not actual) bank position. Operating procedures require the reactor operator to compare the demanded position to the position indicated by the digital rod position indication system to verify correct operation of the rod control system.

An alarm is generated by the digital rod position indication system if a preset limit is exceeded as a result of a comparison of any rod in a control bank with the other rods in the bank. The deviation alarm for a shutdown rod is actuated when a preset insertion limit is exceeded. The demanded and measured rod position signals are also monitored by the plant computer which provides a visual printout and an audible alarm whenever an individual rod position signal deviates from the other rods in the bank by a preset limit. The alarm can be set with appropriate allowance for instrument error and within sufficient narrow limits to preclude exceeding core design hot channel factors. A rod bottom signal from the digital rod position system is used to generate a "Rod Bottom Rod Drop" alarm.

When the reactor is critical, the normal indication of the status of reactivity in the core is the position of the control rod bank in relation to reactor power (as indicated by the RCS loop ΔT) and the coolant average temperature. These parameters are used to calculate insertion limits for the control banks. Two alarms are provided for each control bank. The "low" alarm alerts the operator to an approach to the rod insertion limits which will require boron addition by following normal procedures with the chemical and volume control system. The "low-low" alarm alerts the operator to take immediate action to add boron to the RCS by any one of several alternate methods.

7.7.11 RESOLUTION OF ISSUES

7.7.11.1 Effects of Control System Failures

The staff requested that the applicant identify any power sources, sensors, or sensor impulse lines which provide power or signals to two or more control systems and demonstrate that failures of these power sources, sensors, or sensor impulse lines will not result in consequences outside the bounds of the Chapter 15 analyses or beyond the capability of operators or safety systems.

The applicants have submitted a response describing the results of a study to determine the effect on the plant of the following:

- 1) Loss of power to all control systems powered by a single power supply
- 2) Failure of each instrument sensor which provides a signal to two or more control systems
- 3) Break of any sensor impulse line which is used for sensors providing signals to two or more control systems

The applicant has provided a summary of the events resulting from each postulated failure and identified the specific Chapter 15 analysis which delineates the bounding consequences of the failure.

The staff has reviewed the bases for the applicants study and concludes that, with reasonable assurance, the consequences of single failures within the control systems are bounded by analyses in Chapter 15 of the FSAR. Unresolved Safety Issue A-47, "Safety Implications of Control Systems" will address control system designs and the need for any control system design modifications. The applicant will be required to address staff guidance which may result from the resolution of the unresolved safety issue.

7.7.11.2 Design Features Limiting the Consequences of Single Failures in the Rod Control System

The staff requested that the applicants provide information describing design features used in the rod control system to 1) limit reactivity insertion rates resulting from single failures within the system and 2) limit incorrect sequencing or positioning of control rods.

The applicant submitted information discussing design features which limit rod speeds and rod malpositionings. The applicant stated that even in the unlikely event of simultaneous multiple failures in the rod control system the rod speed is limited to 100 steps per minute by mechanical limitations of the drive mechanism

and that this speed has been verified by tests. The consequences of positive reactivity insertion rates which include the rod speed of 100 steps per minute are bounded by analyses contained in Chapter 15. The applicant has further stated that no single failure within the rod control system can cause either reactivity insertions or mal-positioning of the control rods resulting in core thermal conditions not bounded by analyses contained in Chapter 15. The staff finds the applicants response satisfactory.

7.7.11.3 Environmental Qualification of Control Systems

Operating reactor licensees were informed by IE Information Notice 79-22, issued September 19, 1979, that certain non-safety grade or control equipment, if subjected to the adverse environment of a high energy line break, could impact the adequacy of the protection functions performed to mitigate the consequences of the high energy linebreak. The applicants were requested to review their designs to determine whether the harsh environments associated with high-energy line breaks might cause control system malfunctions resulting in consequences more severe than those analyzed in Chapter 15 or beyond the capability of operators or safety systems. The applicants performed the requested review and submitted the results to the staff. Staff review of the applicants response resulted in the staff asking the applicants for additional information concerning the effects of a high energy line break on rod control system equipment outside the containment. The applicants have stated that a typical bounding analysis of the steamline rupture accident of concern has been performed assuming consequential failure of the rod control system and the results found acceptable. The applicants have committed to submit a plant-specific analysis of the transient prior to January 1, 1982. The staff finds the applicants response acceptable.

Confirmatory Item: The applicants will submit the analysis of the steamline rupture with consequential failure of the rod control system by January 1, 1982.

7.7.12 Evaluation Findings

The control systems used for normal operation that are not relied upon to perform safety functions, but which control plant processes having a significant impact on plant safety, have been reviewed. These control systems include the reactivity control systems and the control systems for the primary and secondary coolant systems. The staff concludes that

the control systems are acceptable and meet the relevant requirements of General Design Criteria 13 "Instrumentation and Control" and 19 "Control Room." This conclusion is based on the following:

Based on our review of the applicant's design bases, functional diagrams, and discussion of the control systems presented in the FSAR, we conclude that the control systems are capable of maintaining system variables within prescribed operating limits. Therefore, we find that the control systems satisfy this aspect of GDC-13, "Instrumentation and Control."

Our review of control systems included the features of these systems for both manual and automatic control of the process systems. We find that the control systems permit actions which can be taken to operate the plant safely during normal operation, including anticipated operational occurrences; therefore, the control systems satisfy GDC-19, "Control Room" with regards to normal plant operations. The conclusions of the analysis of anticipated operational occurrences and accidents as presented in Chapter 15 of the FSAR have been used to confirm that plant safety is not dependent upon the response of the control systems. We conclude that failure of the systems of themselves or as a consequence of supporting systems failures, such as power sources, do not result in plant conditions more severe than those bounded by the analysis of anticipated operational occurrences.

Finally, we have concluded that the consequential effects of anticipated operational occurrences and accidents do not result in control system failures

that would cause plant conditions more severe than those bounded by the analysis of these events. We find that the control systems are not relied upon to assure plant safety and are, therefore, acceptable.