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

OCT 22 1984

MEMORANDUM FOR: ~~Thomas M. Novak, Assistant Director for~~ Licensing
~~Division of Licensing~~

FROM: R. Wayne Houston, Assistant Director for Reactor Safety
Division of Systems Integration

SUBJECT: ICSB INPUT TO SER - BEAVER VALLEY UNIT 2

Plant Name: Beaver Valley 2
Docket No.: 50-412
Licensing Stage: OL
Responsible Branch: LB #3
Project Manager: L. Lazo
Review Branch: ICSB
Review Status: Incomplete

Enclosed, as Enclosure 1, is the Safety Evaluation Report (SER) input for the Beaver Valley Power Station, Unit 2, prepared by the Instrumentation and Control Systems Branch (ICSB). This SER reflects the results of our review of the information presented in the Beaver Valley Unit 2 Final Safety Analysis Report (FSAR) through Amendment 6 and the applicant's responses to ICSB open items contained in the Beaver Valley Unit 2 draft SER.

The enclosed SER input applies to Section 7 of the Standard Review Plan and contains all SER input for which ICSB has responsibility. There are eight open items, eleven confirmatory items, six technical specification items and one licensing condition listed in Section 7.1.4 of the SER.

In accordance with Office Letter No. 44, we have attached, as Enclosure 2, our input into the Beaver Valley Unit 2 SALP as related to the development of this SER input.

R. Wayne Houston, Assistant Director
for Reactor Safety
Division of Systems Integration

Enclosures:
As stated

cc: R. Bernero
D. Eisenhut
G. Knighton
L. Lazo

8411030379 XA

Contact:
F. Burrows, ICSB
X29455

C/35

SAFETY EVALUATION REPORT
BEAVER VALLEY UNIT NO. 2

# 7 INSTRUMENTATION AND CONTROL

## 7.1 Introduction

### 7.1.1 Acceptance Criteria

FSAR Section 7.1 contains information pertaining to safety-related instrumentation and control systems, their design bases, and applicable acceptance criteria. The staff has reviewed the applicant's design, design criteria, and design bases for the instrumentation and control systems for Beaver Valley Unit 2. The acceptance criteria used as the basis for this evaluation are those identified in the SRP (NUREG-0800) in Table 7-1, "Acceptance Criteria for Instrumentation and Control Systems Important to Safety," and Table 7-2, "TMI Action Plan Requirements for Instrumentation and Control System Important to Safety." These acceptance criteria include the applicable GDC and the Institute of Electrical and Electronics Engineers (IEEE) Standard 279 "Criteria for Protection System for Nuclear Power Generating Stations" (10 CFR 50.55a(h)). Guidelines for implementation of the requirements of the acceptance criteria are provided in the IEEE standards, RGs, and BTPs identified in SRP Section 7.1. Conformance to the acceptance criteria provides the bases for concluding that the instrumentation and control systems meet the requirements of 10 CFR 50.

### 7.1.2 Method of Review

Beaver Valley Unit 2 uses a Westinghouse NSSS with balance of-plant (BOP) design provided by Stone and Webster Engineering Corporation. Many safety-related instrumentation and control systems in the NSSS scope of supply are similar to those at Comanche Peak and McGuire and have been previously reviewed and approved by the staff. The staff concentrated its review on those areas where the Beaver Valley Unit 2 design differs from previously reviewed designs

and on those areas that have been of concern during reviews of other similar plants. A meeting was held with the applicant and the NSSS and BOP designers to clarify the design and to discuss concerns the staff has with the design. Detail drawings--including piping and instrumentation diagrams, logic diagrams, control wiring diagrams, electrical one-line diagrams, and electrical schematic diagrams--were audited during the review.

7.1.3 General Conclusion

The applicant has identified the instrumentation and control systems important to safety and the acceptance criteria that are applicable to those systems as identified in the SRP. The applicant has also identified the guidelines--including the regulatory guides and the industry codes and standards--that are applicable to tne systems as identified in FSAR Table 7.1-1.

Based on the review of FSAR Section 7.1, the staff concludes that the implementation of the identified acceptance criteria and guidelines satisfies the requirements of 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. The staff finds that the NSSS and the BOP instrumentation and control systems important to safety, addressed in FSAR Section 7.1, satisfy the requirements of GDC 1 and, therefore, are acceptable.

7.1.4 Specific Findings

7.1.4.1 Open Items

The staff's conclusions apply to the instrumentation and control systems important to safety with the exception of the open items listed below. The staff will reveiw these items and report their resolution in a subsequent version of this report. The applicable sections of this report that address these items are indicated in parentheses following each open item.

1. Design Modification for Automatic Reactor Trip Using Shunt Coil Trip Attachment (7.2.2.3)

2. Service Water System Isolation on Low Header Pressure (7.3.3.4)

3. Control Room Isolation (7.3.3.8)

4. Steam Generator Level Control and Protection (7.3.3.12)

5. Remote Shutdown Capability (7.4.2.1)

6. Bypass and Inoperable Status Panel (7.5.2.4)

7. Primary Component Cooling Water Isolation from Reactor Coolant Pump Thermal Barriers (7.6.2.3)

8. Control System Failure Caused by Malfunctions of Common Power Source or Instrument Line (7.7.2.3)

7.1.4.2 Confirmatory Items

In a number of cases, the applicant has committed to provide additional documentation to address concerns raised by the staff during its review. Based on information provided during meetings and discussions with the applicant, the technical issue has been resolved in an acceptable manner. However, the applicant must formally document his commitments for resolution of these items. The sections of this report that address these items are indicated in parentheses.

1. Design Modification for Automatic Reactor Trip Using Shunt Coil Trip Attachment (7.2.2.3)

2. Service Water System Isolation on Low Header Pressure (7.3.3.4)

3. Main Feedwater Isolation (7.3.3.7)

4. Control Room Isolation on High Radiation Signal (7.3.3.9)

5. Automatic Opening of Service Water System Valves MOV 113C and 113D (7.3.3.10)

6. IE Bulletin 80-06 Concerns (7.3.3.13)

7. Remote Shutdown Capabilty (7.4 2.1)

8. NUREG-0737 Item II.F.1 Accident Monitoring Instrumentation Positions (4), (5), and (6) (7.5.2.2)

9. Bypass and Inoperable Status Panel (7.5.2.4)

10. Cold Leg Accumulator Motor-Operated Valve Position Indication (7.6.2.4)

11. NUREG-0737 Item II.K.3.9, Proportional Integral Derivative (PID) Controller Modification (7.7.2.1)

7.1.4.3 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:

1. Lead, Lag, and Rate Time Constant Setpoints Used in Safety System Channels (7.2.2.1)

2. Turbine Trip Following A Reactor Trip (7.2.2.2)

3. Trip Setpoint and Margins (7.2.2.4)

4. NUREG-0737 Item II.K.3.10, Proposed Anticipatory Trip Modification (7.2.2.5)

5. Undetectable Failure in Online Testing Circuitry for Engineered Safeguards Relays (7.3.3.3)

6. Reactor Coolant System Loop Isolation Valve Interlocks (7.6.2.2)

7.1.4.4 Licensing Condition

The following item is to be included as a license condition:

1. Emergency Response Capability - R.G. 1.97 Rev. 2 Requirements (7.5.2.1)

7.1.4.5 Site Visit

A site review will be performed to confirm that the physical arrangement 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 before a license is issued; any problems found will be addressed in a supplement to this report.

7.1.4.6 Fire Protection Review

The review of the emergency 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 emergency shutdown panel related to fire protection and the review for conformance to 10 CFR 50, Appendix R (safe shutdown analysis) are included in Section 9.5 of this report.

7.1.5 TMI Action Plan Items

Guidance on implementation of the TMI Action Plan was provided to applicants in NUREG-0737. The items related to instrumentation and control systems are listed below. The specific section of the report addressing each item is indicated in parentheses.

(1) II.D.3 - Direct Indication of PORV and Safety Valve Position (7.5.2.3)

(2) II.E.1.2 - Auxiliary Feedwater System Automatic Initiation and Flow Indication (7.3.3.1)

(3) II.F.1 - Accident Monitoring Instrumentation Positions (4), (5), and (6) (7.5.2.2)

(4) II.K.3.1 - Installation and Testing of Automatic Power - Operated Relief Valve Isolation System (7.6.2.1)

(5) II.K.3.9 - Proportional Integral Derivative Controller Modification (7.7.2.1)

(6) II.K.3.10 - Proposed Anticipatory Trip Modification (7.2.2.5)

(7) II.K.3.12 - Anticipatory Reactor Trip Upon Turbine Trip (7.2.2.6)

## 7.2 Reactor Trip System

### 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 whenever predetermined safety limits are approached or reached. The RTS monitors variables that are directly related to system limitations or calculated from process variables. Whenever a variable exceeds a setpoint, the reactor is tripped by the insertion of 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 these 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 dc under-voltage coil in 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, and 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.

In addition to the automatic trip of the reactor described above, there is also provision for manual trip by the operator. The manual trip consists of two switches. Actuation of either switch removes power from the undervoltage coils and energizes the shunt trip coils of both reactor trip breakers. The shunt trip coils are a diverse means for tripping the reactor trip breakers. The reactor will also be tripped by actuating either of the two manual switches for safety injection.

The generic implications of the Salem anticipated transient without scram (ATWS) events are discussed in Section 7.2.2.3 of this report.

The reactor trips listed below are provided in the Beaver Valley Unit 2 design. The numbers in parentheses after each trip function indicate the coincident logic; for example, two-out-of-three (2/3).

(1) Nuclear Overpower 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 Overpower Trips

(a) Overtemperature $\Delta T$ Trip (2/3)

(b) Overpower $\Delta T$ Trip (2/3)

(3) Reactor Coolant System Pressurizer Pressure and Water Level Trips

(a) Pressurizer Low Pressure Trip (2/3)

(b) Pressurizer High Pressure Trip (2/3)

(c) Pressurizer High Water Level Trip (2/3)

(4) Reactor Coolant System Low Flow Trips

(a) Low Reactor Coolant Flow (2/3 per loop) (2/3) between P-7 and P-8 (1/3) above P-8

(b) Reactor Coolant Pump Breaker Trip (2/3)

(c) Reactor Coolant Pump Bus Undervoltage (2/3)

(d) Reactor Coolant Pump Bus Underfrequency (2/3)

(5) Low Feedwater Flow Trip (1/2 steam/feedwater flow mismatch in coincidence with 1/2 low steam generator water level)

(6) Steam Generator Low-Low Level Trip (2/3 per loop)

(7) Turbine Trip (anticipatory)

(a) Low Auto Stop Oil Pressure (2/3)

(b) Turbine Stop Valves Closed (4/4)

(8) Safety Injection Signal Actuation Trip (See Section 7.3) Coincident with Actuation of Safety Injection (1/2)

(9) Manual Trip (1/2)

The power range high neutron flux trip has two bistables for a high and a low trip setting. The high setting trip is active during all modes of operation.

The low setting trip provides protection during reactor startup and shutdown when the reactor is below 10% power. The low setting trip can be manually blocked above 10% power (P-10) and is automatically reinstated below the P-10 interlock.

The intermediate range trip provides protection during reactor startup and shutdown. This trip can be manually blocked above 10% power (P-10) and is automatically reinstated below the P-10 interlock.

The source range trip provides protection during reactor startup and shutdown when the neutron flux channel is below the P-6 interlock ($6 \times 10^{-11}$ amp). This trip can be manually blocked above P-6 interlock and is automatically reinstated below the P-6 interlock. It is also automatically blocked above the P-10 interlock.

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 low-worth rod ejection accidents from midpower 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 $\Delta T$ trip protects the core against a low departure from nucleate boiling ratio (DNBR). 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 DNBR limits.

The overpower $\Delta T$ 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) fails below a preset limit. This trip is automatically blocked below approximately 10% 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 transmitters are used as for the pressurizer low pressure trip except that separate bistables are used for the high-pressure trip. The reactor is tripped when pressurizer pressure exceeds a preset limit.

The pressurizer high water level trip is provided as a backup to the pressurizer high pressure trip and serves to prevent water relief through the pressurizer safety valves. This trip is automatically blocked below approximately 10% of full power (P-7 interlock) to allow startup.

The low reactor coolant flow trip protects the core against DNB resulting from a loss of primary coolant flow. Above the P-7 setpoint (approximately 10% power), a reactor trip will occur if any two loops have low flow. Above the P-8 setpoint (approximately 48% power), a trip will occur if any one loop has low flow.

The reactor coolant pump breaker, bus undervoltage and bus underfrequency trips protect the reactor core from DNB. These trips are all automatically blocked below the P-7 setpoint to allow startup.

The low feedwater flow trip (steam/feedwater flow mismatch coincident with low steam generator level) protects the reactor from a sudden loss of a heat sink. This trip is active during all modes of operation.

The steam generator low-low water level trip protects the reactor from loss of heat sink in the event of sustained steam/feedwater flow mismatch.

A reactor trip on a turbine trip is actuated by trip fluid pressure switches (two-out-of-three) or by closed signals from the turbine steam stop valve position switches (four-out-of-four). A turbine trip causes a direct reactor trip above 70% power (P-9 interlock).

A safety injection signal initiates a reactor trip. This trip protects the core against a loss of reactor coolant or overcooling.

The manual trip consists of two switches. Operation of either switch de-energizes the undervoltage coils in each logic train. The breaker shunt coils in these breakers are energized at the same time, which provides a diverse means to ensure that the trip and bypass 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 uses 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 output signals, partial and full trip conditions, 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 used for non-protective functions such as control, remote process indication, and computer monitoring are provided by isolation amplifiers located in the protective system cabinets. The isolation amplifiers are designed so that a short circuit, open circuit, or the application of credible fault voltages from within the cabinets on the isolated output portions of the circuit (non-protective side) will not affect the input signal. The signals obtained from the isolation amplifiers are not returned to the protective systems cabinets.

7.2.2 Specific Findings

7.2.2.1 Lead, Lag, and Rate Times 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.

7.2.2.2 Turbine Trip Following A Reactor Trip

Credit is taken in the accident analysis for turbine trip on a reactor trip. The protection system trips the turbine following a reactor trip using the turbine emergency trip system. Redundant circuits used to trip the turbine are independently routed to and processed within the emergency trip system to provide two independent means of tripping the turbine. The circuits which traverse non-seismic qualified structures are isolated from 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.

The staff will include in the plant technical specifications a requirement to periodically test these circuits.

7.2.2.3 Design Modification for Automatic Reactor Trip Using Shunt Coil Trip Attachment

The Westinghouse Owners Group (WOG) has submitted a generic design modification to provide automatic reactor trip system (RTS) actuation of the breaker shunt trip attachments in response to Salem ATWS events. The staff has reviewed and accepted the generic design modification and has identified additional information required on a plant specific basis. The applicant's letter dated March 30, 1984 provided a response to Generic Letter 83-28 which established the requirements for this modification. In that response the applicant stated

that automatic shunt trip actuation would not provide substantial, additional protection if incorporated into the plant design. The staff found this response unacceptable. In a September 7, 1984 response, the applicant committed to provide the Westinghouse Owners Group generic design modification. The staff finds this acceptable, but considers the issue an open item until the modification installation is completed.

In addition, the staff has identified additional information required on a plant specific basis as part of the acceptance of the generic modification. The staff considers the submittal of the required information and an FSAR revision covering the modification to be a confirmatory item.

7.2.2.4 Trip Setpoint and Margins

The setpoints for the various functions in the reactor trip system are determined on the basis of the accident analysis requirements. As such, during any anticipated operational occurrence or accident, the reactor trip maintains system parameters with the following limits:

(1) minimum departure from nucleate boiling ratio of 1.30.

(2) maximum system pressure of 2750 psi (absolute).

(3) fuel rod maximum linear power of 18.0 kW per foot.

The staff requested detailed information on the methodology used to establish the technical specification trip setpoints and allowable values for the Reactor Protection System (including Reactor Trip and Engineered Safety Feature channels) assumed to operate in the FSAR accident and transient analyses. This includes the following information:

(1) The trip setpoint and allowable value for the Technical Specifications.

(2) The safety limits necessary to protect the integrity of the physical barriers which guard against uncontrolled release of radioactivity.

(3) The values assigned to each component of the combined channel error allowance (e.g., modeling uncertainties, analytical uncertainties, transient overshoot, response time, trip unit setting accuracy, test equipment accuracy, primary element accuracy, sensor drift, nominal and harsh environmental allowances, trip unit drift), the basis for these values, and the method used to sum the individual errors. Where zero is assumed for an error, a justification that the error is negligible should be provided.

(4) The margin (i.e., the difference between the safety limit and the setpoint less the combined channel error allowance).

The detailed trip setpoint review will be performed as part of the staff's review of the plant Technical Specifications and will be completed before the operating license is issued.

7.2.2.5 NUREG-0737 Item II.K.3.10, Proposed Anticipatory Trip Modification

The design includes an anticipatory reactor trip upon turbine trip. Provisions are included to automatically block the reactor trip upon turbine trip at power levels below approximately 70% (P-9 interlock) where the condenser steam dump is capable of mitigating the reactor coolant system temperature and pressure transient without actuating pressurizer power operated relief valves. A decision to trip the reactor following turbine trip at the 50% power level, noted in the TMI Action Plan requirements, would involve only bistable setpoint changes and not instrument hardware changes. The staff finds that the design is, therefore, acceptable. The specific power level setpoint below which a reactor trip following a turbine trip is blocked will be reviewed and specified in the plant technical specifications.

7.2.2.6 NUREG-0737 Item II.K.3.12, Anticipatory Reactor Trip on Turbine Trip

As stated above, the design includes an anticipatory reactor trip on turbine trip. The staff reviewed the design for conformance to BTP ICSB-26 and identified the following concerns:

(1) The 4/4 logic, although redundant in each RPS train, has four input channels developed from position switch contacts on the four turbine stop valves. The installation of the stop valve position contacts and their cable routing to the RPS input cabinets do not preclude a single failure from preventing either train from performing its safety function.

(2) The sensors and stop valve contacts are not qualified to operate in a seismic event.

In response to the staff's first concern, the applicant stated, in a February 21, 1984 letter, that the reactor trip on turbine low auto stop oil pressure provides a diverse backup for the trip on stop valve closure. The applicant also reiterated that this trip is anticipatory, is included for the protection of the turbine equipment, and no credit is taken for this trip in any FSAR Chapter 15 accident analysis. The staff finds the applicant's response acceptable and considers this concern resolved.

In response to the staff's second concern, the applicant stated in an August 9, 1984 letter, that the pressure sensors and stop valve contacts fail in a safe direction (provide the trip) if they fail due to a seismic event. The staff finds the applicant's response acceptable and considers this issue closed.

7.2.3 Conclusions

We have conducted an audit review of the Reactor Trip (RTS) for conformance to guidelines of the applicable regulatory guides and industry codes and standards as outlined in the Standard Review Plan, Section 7.2, Part II and III. 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 upon satisfactory resolution of the open item identified in Section 7.2.2.3 there is reasonable assurance that the systems will conform to the applicable guidelines.

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) subject to resolution of the open item identified in Section 7.2.2.3 of this report.

## 7.3 Engineered Safety Features Systems

### 7.3.1 Engineered Safety Features Actuation System (ESFAS)

The ESFAS is a portion of the plant protection system that monitors selected plant parameters and, on detection of out-of-limit conditions of these parameters,

will initiate actuation of appropriate engineered safety features (ESF) systems and essential auxiliary support systems equipment. The ESFAS includes both automatic and manual initiation of these systems. Also included with the ESF systems are the control systems that regulate operation of ESF systems following their initiation by the protection system.

The ESFAS is a functionally defined system and consists of:

(1) process instrumentation and control

(2) solid-state and relay logic

(3) ESF test circuits

(4) manual actuation circuits

(5) emergency generator load sequence control logic

The ESFAS includes two distinct portions of circuitry: (1) an analog portion consisting of three to four redundant channels per parameter or variable to monitor various plant parameters such as reactor coolant and steam system pressures, temperatures, and flows and containment pressure and (2) a digital portion consisting of redundant logic trains that receive inputs from the analog protection channels and perform the logic to actuate the ESF equipments. The ESFAS is composed of NSSS circuits designed by Westinghouse and BOP circuits designed by Stone and Webster Engineering Corporation.

The actuation signals for each of the ESFAS functions are listed below. The numbers in parentheses after each actuation channel indicate the coincident logic; for example, two-out-of-four (2/4).

(1) Safety Injection

(a) Manual (1/2)

(b) High-1 Containment Pressure (2/3)

(c) Low Compensated Steam Line Pressure (2/3 in any line)

(d) Low Pressurizer Pressure (2/3)

(2) Containment Depressurization

(a) Manual (2/4)

(b) High-3 Containment Pressure (2/4)

(3) Containment Isolation

(a) Automatic Safety Injection (Phase A isolation)

High-1 Containment Pressure (2/3)

Low Compensated Steam Line Pressure (2/3 in any line)

Low Pressurizer Pressure (2/3)

(b) High-3 Containment Pressure (2/4) (Phase B isolation)

(c) Manual

Phase A Isolation (1/2)

Phase B Isolation (2/4)

(4) Steam Line Isolation

(a) Low Compensated Steam Line Pressure (2/3 in any line)

(b) High-2 Containment Pressure (2/3)

(c) High Steam Line Pressure Rate (2/3 in any line)

(d) Manual (1/2 for all lines of 1/1 for each valve)

(5) Feedwater Line Isolation

(a) Safety Injection (same as item 1 above)

(b) High Steam Generator Level (2/3 in any generator)

(c) Low Tavg (2/3) Coincident with Reactor Trip

(6) Auxiliary Feedwater System Actuation

The motor driven auxiliary feedwater pumps will be started on any of the following signals:

(a) Safety Injection (same as Item 1 above)

(b) Low-Low Steam Generator Level (2/3 in any generator) (2/3)

(c) Loss of Main Feedwater Pumps (2/2)

(d) Loss of Turbine Driver Auxiliary Feedwater Pump Discharge Pressure (1/1) Coincident with Turbine Driven Pump Steam Admission Valves Open

(e) Manual Actuation (local or remote) (1/1)

The turbine-driven auxiliary feedwater pump will be started on any of the following signals:

(a) Low-Low Steam Generator Level (2/3 in any steam generator)

(b) Loss of Power (2/3 undervoltage at 4.16 KV bus)

(c) Manual Actuation (local or remote) (2/2)

(7) Control Room Isolation

(a) High-3 Containment Pressure (2/4)

(b) High Chlorine Content (2/3)

(c) Manual Containment Spray (1/2)

(8) Service Water System Pump Start and Isolation

(a) Safety Injection (same as Item 1 above)

(9) Emergency Diesel Generator Start-up

(a) Safety Injection (same as Item 1 above)

7.3.2 ESF and EAS System Operation

The following Engineered Safety Features (ESF) and Essential Auxiliary Support (EAS) systems are identified in the FSAR:

A. Engineered Safety Features Systems

1. Emergency Core Cooling System (ECCS)

2. Containment Depressurization System

a. Quench Spray System

b. Recirculation Spray System

3. Containment Isolation System (including main steam and feedwater isolation)

4. Combustible Gas Control System

5. Auxiliary Feedwater System

6. Habitability System for the Control Room Envelope

7. Supplementary Leak Collection and Release System

B. Essential Auxiliary Support Systems

1. Service Water System

2. Safety-related Ventilation Systems

3. Emergency Onsite Power Supply System

4. Emergency Diesel Generator Associated Systems

7.3.2.1 Emergency Core Cooling Systems

The emergency core cooling system (ECCS) cools the reactor core and provides shutdown capability for pipe breaks in the reactor coolant system (RCS) that 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 secondary coolant system and for 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 high head safety injection (HHSI)/charging pumps, low head safety injection (LHSI) pumps, safety injection accumulators, containment recirculation spray pumps, refueling water storage tank (RWST), the associated piping, valves, and instrumentation.

The ECCS provides shutdown capability for the accidents described above by injecting borated water into the RCS. The system's safety function can be performed with a single active failure (short term) or passive failure (long term). The emergency diesel generators supply power if offsite power is unavailable.

The safety injection signal will start the diesel generators and automatically initiate the following actions in the ECCS:

(1) starts HHSI/charging pumps

(2) opens RWST suction valves to charging pumps

(3) opens charging pumps to RCS cold leg injection headers isolation valves

(4) closes normal charging path valves

(5) closes charging pump miniflow valves

(6) starts LHSI pumps

(7) opens any closed accumulator isolation valves

(8) closes volume control tank outlet isolation valves

The changeover from the injection mode to recirculation mode is initiated automatically on RWST low-low level coincident with an SI signal and involves the following procedures:

(1) Automatically

(a) valves 8811A/B associated with the LHSI pumps and two containment recirculation spray pumps are aligned for cold leg recirculation

(b) the HHSI/charging pumps are aligned to the recirculation spray pump discharge

(c) the LHSI pumps stop on open signals from valves 8811A/B

(d) the RWST is isolated

(2) Following these automatic actions, the operator manually aligns valves to provide two separate HHSI/charging pump subsystems with each consisting of a charging pump and a recirculation spray pump.

(3) After approximately 24 hours, the operator manually aligns valves to esablish hot leg injection with two recirculation spray pumps and two charging pumps providing the flow.

7.3.2.2 Containment Depressurization System

The containment depressurization system consists of the quench spray system and the recirculation spray system. Subsequent to a design basis accident (DBA), the quench spray pumps and one of two chemcial injection pumps are started automatically on receipt of a containment isolation phase B (CIB) signal. The isolation valves to the quench spray discharge headers and from the RWST receive a confirmatory open signal. Each redundant quench spray subsystem draws water independently from the RWST. Sodium hydroxide solution is added to the quench spray from the chemical addition tank via the chemical injection pumps. On receipt of an RWST low-low signal, the quench spray pumps stop and chemical addition flow is diverted to the containment sump.

The four recirculation spray pumps start automatically in approximately 210 seconds following receipt of a CIB signal and take suction from the containment sump. Two of the recirculation spray pumps perform the containment spray function to replace the quench spray pumps after receipt of the RWST low-low signal and the remaining two pumps are aligned for cold leg injection.

7.3.2.3 Containment Isolation System Including Main Steam And Feedwater Isolation

The safety function of the containment isolation system (CIS) is to automatically isolate the process lines penetrating the containment structure. The CIS is

designed to limit the release of radioactive materials from the containment following an accident.

The CIS is automatically actuated by signals developed by the ESFAS in two phases: phase A containment isolation and phase B containment isolation. Phase A isolates all non-essential process lines penetrating the containment. Phase B isolates all other process lines not included in phase A containment isolation, except for the reactor coolant pump seal injection, safety injection, auxiliary feedwater and containment depressurization lines.

Containment isolation valves, which are equipped with power operators and are automatically actuated, may also be controlled individually by manual 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. All electric power supplies and equipment necessary for containment isolation are Class 1E.

The main steam line isolation signal is generated on low steam line pressure, high-2 containment pressure or high steam pressure rate. 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 decreasing steam line pressure is used to initiate main steam line isolation when the low steam line pressure signals are blocked. The main steam isolation valves, ball-type valves, are designed to prevent steam flow in both the forward and reverse directions. These valves are opened hydraulically and are held open by a mechanical latch. Upon receipt of a closure signal, de-energization of two solenoids or energization of a third solenoid releases the latch and the valve closes by spring force. Each main steam isolation valve is capable of being tested on-line by partial closure of the valve.

Feedwater line isolation is provided to terminate main feedwater following a pipe rupture or excessive feedwater event. Upon receipt of an SI or steam generator high-high level signal all main feedwater pumps trip and all feedwater isolation and feedwater control bypass valves close. Upon receipt of either of the above two signals or low reactor coolant average temperature coincident with reactor trip, all main feedwater control valves close.

7.3.2.4 Combustible Gas Control System

The combustible gas control system controls the concentration of hydrogen gas inside the containment following a DBA. The system consists of two redundant sets of hydrogen analyzers and combiners powered from separate emergency buses. Each set has a separate control panel located in the safeguards area outside the containment and is manually operated following a DBA.

7.3.2.5 Auxiliary Feedwater System

The function of the auxiliary feedwater system (AFWS) is to provide an adequate supply of water to the steam generators if the main feedwater system is not available. The AFWS consists of two motor-driven pumps and one turbine-driven pump with associated valves, controls, and instrumentation. Each motor-driven pump supplies water to a separate header while the turbine-driven pump can be manually aligned to either header. Water can be supplied to each steam generator from either header. Flow is controlled by a separate flow control valve for each header. The auxiliary feedwater pumps are started automatically by the initiating conditions listed in Section 7.3.1, item (6). Each pump takes suction directly through a separate supply line from the seismic Category I primary plant demineralized water storage tank (PPDWST) with makeup capability from the demineralized water storage tank (DWST). A secondary seismic Category I water supply is available from piping cross-connections to the service water system.

The motor-driven pumps can be automatically or manually operated from either the main control board or the emergency shutdown panel (ESP). The turbine-driven pump can be operated automatically or manually from the main control board but only manually from the ESP. One motor-driven pump can be operated manually at the alternate shutdown panel (ASP).

The amount of flow to any steam generator is limited by cavitating venturis located in the auxiliary feedwater line to each steam generator. The cavitating venturis will prevent runout flow to a depressurized steam generator.

7.3.2.6 Habitability System for the Control Room Envelope

The control room envelope consists of the Beaver Valley Unit 2 (BV-2) control room, computer room and air-conditioning equipment room; and the Beaver Valley Unit 1 (BV-1) control room, computer room, kitchen, medical, and sanitary facilities, heating, ventilating, and air conditioning equipment room, communication equipment and relay panel room, and process instrument and rod position room. The environmental habitability system for the control room envelope includes radiation shielding, redundant air supply and filtration systems, and redundant air-conditioning systems.

The control room envelope air-conditioning system is safety-related and maintains the ambient control room temperature, under normal conditions, at 75°F. The system consists of two 100% capacity air-conditioning units (ACU), each containing one fan, one service water cooling coil, a direct-expansion cooling coil, a bag-type filter, and a roll-type filter. One of the ACU's supplies a mixture of outside and return air during normal operation. Redundant chlorine gas detectors are located at the control room air intake. Detection of chlorine by 2-out-of-3 detectors or a containment isolation phase B (CIB) signal will automatically close the outside air intake dampers. During this condition the control room is maintained above atmospheric pressure by bottled compressed air to preclude infiltration of outside air. Sixty minutes after the receipt of a CIB signal, redundant parallel, motorized dampers will open and one of the two redundant emergency control room supply fans will automatically start and maintain the pressure in the area after the bottled air supply is exhausted. Air is drawn through one of two redundant filtration units. The control room air intake is also provided with smoke detectors with local alarms and annunciation in the control room. Intake dampers can be manually closed and smoke can be purged from the control room.

The main control room area for both units are open to each other. Their control room air-conditioning systems are independent and physically separated. The bottled compressed air system is common to both units and is sized based on the combined area. Detection of chlorine or a CIB signal in either unit will isolate the control room from the outside air.

7.3.2.7 Supplementary Leak Collection and Release System

The primary function of the supplementary leak collection and release system (SLCRS) is to ensure that radioactive leakage from the containment following a DBA or radioactive release due to a fuel handling accident is collected and filtered for iodine removal prior to discharge to the atmosphere. The system consists of two normal exhaust fans, two filter exhaust fans powered from emergency buses, four filter banks, two demister assemblies, and two emergency charging pump cubicle exhaust fans. During normal operation, one normal exaust fan is operated with the other fan as standby. Also during normal operation both filter exhaust fans are manually started and isolation dampers for one demister assembly and filter bank are opened.

On a containment isolation (phase A) signal, the normal exhaust fans are isolated and air is diverted through one of the two parallel demister assemblies and the aligned filter banks before flowing to the filter exhaust fans. High differential pressure across each filter bank is annunciated in the control room.

Each exhaust fan can be manually started or stopped from the control room and can supply emergency ventilation for the charging pump cubicles and component cooling water pumps.

7.3.2.8 Service Water System

The service water system (SWS) performs both safety and non-safety functions by providing cooling water for heat removal components during all modes of operation. The service water system consists of two trains, each of which contains one half-capacity pump, one strainer, and associated piping and valves. A third half-capacity pump is provided for backup redundancy. During normal plant operation both trains are required but only one train is required for safe shutdown.

The service water system is designed to meet the single failure criterion. Power is supplied to the two normally operating pumps from separate emergency buses and the third pump can be manually connected to either emergency bus.

On receipt of a containment isolation (phase B) signal, water is diverted from the primary component cooling water heat exchangers, secondary component cooling water heat exchangers, and chillers to the four containment recirculation spray coolers. On receipt of an SI or loss-of-offsite power signal, the SWS pumps receive an automatic start signal and water is supplied to the emergency diesel generator cooling system heat exchangers. The secondary component cooling water heat exchangers are not required after loss-of-offsite power and will be automatically isolated on low header pressure to maintain required flow to other equipment.

On receipt of a containment isolation (phase A) signal, double motor-operated isolation valves isolate the non-safety-related portion of the system from the safety-related portions. In the event of a failure in the non-safety-related portion of the system, the valves close automatically on low system header pressure.

7.3.2.9 Safety-Related Ventilation Systems

The applicant has identified that the following systems are safety-related:

(1) Control building ventilation system
(2) Emergency diesel generator building ventilation system
(3) Primary intake structure ventilation system
(4) Main steam and feedwater valve area ventilation system
(5) Battery room ventilation system
(6) Emergency switchgear room ventilation system
(7) Safeguards area ventilation system
(8) Cable vault and rod control area ventilation system

The evaluation of these systems are addressed in Section 9.4 of this report.

7.3.2.10 Emergency Onsite Power Supply System

The emergency onsite power supply system consists of two 4.16 KV diesel generators, two 4.16 KV ESF buses, various ESF and non-ESF 480V buses, motor

control centers, and 208/120V power panels. There are four 120 VAC safety-related vital bus power supplies for safety-related vital instrumentation and control loads. The evaluation of the emergency onsite power supply system is addressed in Section 8.3 of this report.

7.3.2.11 Emergency Diesel Generator Associated Systems

The applicant has identified that the emergency diesel generator cooling water, combustion air intake and exhaust, fuel oil storage and transfer, air-starting, and lubrication systems are safety-related systems. The evaluation of these systems are addressed in Section 9.5 of this report.

7.3.3 Specific Findings

7.3.3.1 NUREG-0737 Item II.E.1.2, AFWS Automatic Initiation and Flow Indication

The automatic system used to initiate the operation of the auxiliary feedwater system is part of ESFAS. The redundant actuation channels that provide signals to the pumps and valves are physically separated and electrically independent. Redundant trains are powered from independent Class 1E power sources. The initiation signals and circuits are testable during power operation, and the test requirements will be included in the plant Technical Specifications. Manual initiation and control can be performed from the main control board or the emergency shutdown panel. No single failure within the manual or automatic initiation system for the auxiliary feedwater system will prevent initiation of the system by manual or automatic means. The environmental qualification is addressed in Section 3.11 of this report.

Redundant auxiliary feedwater flow instrument channels are provided for each steam generator. Each channel is powered from a separate Class 1E power source. Auxiliary feedwater flow indicators are located at the main control board and the emergency shutdown panel. The staff concludes that the design satisfies the requirements of NUREG-0737, item II.E.1.2.

7.3.3.2 Test of Engineered Safeguards P-4 Interlock

On November 7, 1979, Westinghouse notified the Commission of an undetectable failure that could exist in the engineered safeguards P-4 interlocks. Test procedures were developed to detect failures that might occur. The procedures require the use of voltage measurements at the terminal blocks of the reactor trip breaker cabinets.

The staff raised a concern on the possibility of accidental shorting or grounding of safety system circuits during testing of the P-4 interlocks. The applicant's response, dated April 10, 1984, stated that accidental shorting or grounding has not been a problem during approximately four years of testing this interlock on BV-1.

In light of the applicant's response, the staff will further investigate this issue during the site visit and address any unacceptable findings in a supplement to this report.

7.3.3.3 Undetectable Failure in Online Testing Circuitry for Engineered Safeguards Relays

On August 6, 1982, Westinghouse notified the staff of a potential undetectable failure in online test circuitry for the master relays in the engineered safeguards systems. The undetectable failure involves the output (slave) relay continuity proving lamps and their associated shunts provided by test pushbuttons. If after testing, a shunt is not provided for any proving lamp because of a switch contact failure, any subsequent safeguards actuation could cause the lamp to burn open before its associated slave relay is energized. This would then prevent actuation of any associated safeguards devices on that slave relay. Westinghouse has provided test procedures that ensure that the slave relay circuits operate normally when testing of the master relays is completed.

Until an acceptable circuit modification is installed, the staff will require plant Technical Specifications to include monthly (in lieu of quarterly)

testing of slave relays. These tests should be performed immediately following the monthly testing of associated master relays.

7.3.3.4 Service Water System Isolation on Low Header Pressure

During the staff's review of the service water system, it was noted that on low service water system header pressure the service water system is isolated from the secondary component cooling water heat exchangers and the standby service water pump is automatically started. There was little information in FSAR Section 7 on this circuitry for our review and the FSAR did not provide a design basis for this system. Therefore the staff requested sufficient information be provided for review and, if this isolation was safety significant, that information be provided in the appropriate section of the FSAR.

In a September 11, 1984 letter the applicant provided additional information and stated that this isolation was a safety function isolating the safety-related portion of the system from the non-safety-related portion. During the staff's subsequent review, conflicts were found between the information provided and piping and instrumentation diagrams. The staff considers this an open item until appropriate and accurate information is provided for our review. Additionally, the staff considers the applicant's pending FSAR revision covering this isolation to be a confirmatory item.

7.3.3.5 Normal Letdown Line Relief Valve

The staff raised a concern that the relief valve located on the letdown line would relieve primary coolant to the pressurizer relief tank in the event the isolation valves inside containment did not close on a containment isolation signal (while the isolation valve outside containment did close) or if the outside containment isolation valve failed closed. By a letter dated June 20, 1984, the applicant addressed the staff's concern by presenting various failure mode analyses. The analyses show that the containment isolation is accomplished, there is sufficient instrumentation to detect the flow into the pressurizer relief tank, and the core integrity is maintained and 10 CFR 50, Appendix K limits are not exceeded. The staff finds the analyses acceptable and considers this matter closed.

7.3.3.6 Switchover from Injection to Recirculation

The applicant had indicated that the design is incomplete for several areas related to this item. Based on a review of preliminary information, the staff expressed concerns in the following areas:

(1) Charging pump mini-flow valve control design was not finished. Valve positions were not provided as inputs into bypass or inoperable status indication. Deadheading of the charging pumps may be a problem.

(2) The interlocks used for the switchover are complex and make testing complicated.

The staff requested detailed schematic drawings and piping diagrams be provided when the design was finalized. By a letter dated May 14, 1984, the applicant provided final design drawings in response to our concerns. During a June 29, 1984 meeting with the applicant, our concerns and the system design was discussed. The staff finds the design for switchover from injection to recirculation (including charging pump mini-flow protection) acceptable and considers this issue closed.

7.3.3.7 Main Feedwater Isolation

During the staff's review of the main feedwater isolation circuitry, discussions with the applicant indicated that for S.I. or steam generator high level only one train of automatic closure is provided for the main feedwater isolation valves. An additional train of protection is provided by automatic closure of the main feedwater control and bypass valves with tripping of the main feedwater pumps and subsequent closure of their discharge valves. Also on a low Tavg coincidence with reactor trip only a single train of automatic closure is provided for the main feedwater control valves with no closure provided for the main feedwater isolation and bypass valves.

The staff has expressed concern that the lack of redundancy for protection action initiated by low Tavg coincident with reactor trip may be a safety significant issue. In a June 20, 1984 letter, the applicant stated that main

feedwater isolation provided by this signal is not assumed in Chapter 15 of the FSAR and is not necessary for safety and is therefore not required to be redundant. The staff has reviewed the applicant's response and finds that since there is no current basis to apply additional regulatory requirements, the design is acceptable and considers this issue closed.

Additionally, FSAR Figures 7.2-1 (Sheet 13) and 7.3-18 do not agree with the information (discussed above) provided by the applicant. The staff considers the revision of these FSAR figures to agree with the final design to be a confirmatory item.

7.3.3.8 Control Room Isolation

The applicant had indicated that the design of the control room and pressurization system was incomplete during a December 1983 meeting. Based on our review of preliminary information, the staff expressed a concern that the design, which is integrated into the current control room isolation and pressurization system, may not meet the requirements of GDC-5, "Sharing of Structures, Systems, and Components."

The staff requested detailed schematic drawings be provided for this system when the design was finalized. In a September 7, 1984 letter, the applicant provided information on the design and the interrelationship between Unit 1 and Unit 2. The staff has reviewed this information and requires additional information covering testability of the system. This is an open item.

7.3.3.9 Control Room Isolation on High Radiation Signal

During the staff's review of the control room isolation system, a conflict was found between the plant schematics and the information provided by FSAR Figures 7.2-1 (Sheet 8) and 7.3-13. These figures show that the control room is isolated by a high radiation signal which is, according to the applicant, in error. This item is confirmatory subject to revision of the FSAR to eliminate this error.

7.3.3.10 Automatic Opening of Service Water System Valves MOV113C and 113D

During the staff's review of the service water system, an error was found in FSAR Figure 9.2-4 which shows that valves MOV113C and D receive automatic open signals. Since the applicant indicated that this is not the case, this item is confirmatory subject to revision of the FSAR to eliminate this error.

7.3.3.11 Level Measurement Errors Resulting From Environmental Temperature Effects on Level Instrument Reference Legs

The staff requested that the applicant evaluate the effects of high temperature in reference legs of water level measurement systems due to high energy-line breaks. This issue was addressed for operating reactor through IE Bulletin 79-21. In FSAR Amendment No. 4, the applicant committed to insulate the steam generator reference legs in response to the heat up concern addressed in IE Bulletin 79-21. The staff finds this acceptable.

7.3.3.12 Steam Generator Level Control and Protection

Three steam generator level channels are used in a two-out-of-three logic for isolation of feedwater on high steam generator level. One of the three level channels is used for control. This design for actuation of feedwater isolation does not meet the requirements of Paragraph 4.7 of IEEE 279 on "Control and Protection System Interaction" in that the failure of the level channel used for control could require protective action and the remainder of the protection system channels would not satisfy the single-failure criterion.

The applicant has responded to this concern in letters dated March 28, May 30, and June 8, 1984. The staff has not completed its review of the applicant's responses and considers this issue still as an open item.

7.3.3.13 IE Bulletin 80-06 Concerns

IE Bulletin 80-06 requests a review of all systems serving safety-related functions to ensure that no device will change position solely because of the

reset of a ESF actuation signal. The applicant was requested to respond to IE Bulletin 80-06.

The staff reviewed the applicant's response, contained in Amendment 4 of the FSAR, and found that the applicant only indicated a review of the specific potential problems listed in IE Bulletin 80-06. The intent of IE Bulletin 80-06 and NRC Question 420.3 was to require all safety-related systems to be reviewed. In a July 30, 1984 letter, the applicant stated that his review included all safety-related systems and that the only modifications required were discussed in the Amendment 4 response. The staff considers this issue resolved subject to confirmation of successful completion of the verification test required by IE Bulletin 80-06.

7.3.3.14 Independence Between Manual and Automatic Actions

In the applicant's response to IE Bulletin 80-06, the statement is made that "all circuitry for components actuated by an ESF actuation signal have been designed such that the ESF signal cannot be overridden manually or automatically with an ESF actuation signal present. A component may be reset by first resetting the ESF actuation signal and then manually resetting the component." Also the staff's review of the transfer from the control room to the ESP revealed that safety injection pumps cannot be stopped manually if SI is initiated after the transfer.

The staff was concerned that under accident conditions, as well as inadvertent initiation of safety actions, the inability of the operator to exercise control could lead to consequential damage of safety-related equipment or prevent initiation of protection systems. The staff favors independence between manual and automatic safety-related actions and believes that a safety significant issue may be introduced if the operator is prevented from exercising manual control.

During a June 29, 1984 meeting with the applicant, the staff's concerns were discussed. As a result of that meeting and a subsequent audit of schematics for control circuitry of safety-related components, the staff has reached the following conclusions:

(1) Our initial concern centered on our interpretation of the applicant's statement, "a component may be reset by first resetting the ESF actuation...," to include not only manual termination but also manual initiation of protection systems and components. Based on further review and discussion, we now conclude that statement (and the design) only applies to manual termination and that the operator is not prevented from manually initiating safety-related actions.

(2) Also based on further review and discussion, we conclude that since an SI reset button (identical to those in the control room) is provided on the ESP, safety injection can be stopped from the ESP by following the same procedure as used in the control room; that is, to first reset the SI actuation signal and then manually stop the pump.

The staff finds the plant's degree of independence between manual and automatic actions acceptable and considers this issue closed.

7.3.3.15 Power Lockout for Motor-Operated Valves

Certain motor-operated valves, such as those for cold leg accumulator isolation, require power lockout (removal) to meet the single-failure criterion. The power lockout scheme used by the applicant uses an additional, manually controlled (via removable banana plugs) contractor. The staff concluded that a short or relay failure in this circuitry could constitute a nondetectable failure and thus violate the single-failure criterion.

The staff has expressed this concern to the applicant. The resolution of this issue is addressed in Section 8.3 of this report.

7.3.4 Conclusion

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

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 as outlined in the Standard Review Plan, Section 7.3, Parts II and III. 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 items identified in Sections 7.3.3.4, 7.3.3.8, and 7.3.3.12 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 addressed 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 Phenomena," and GDC-4, "Environmental and Missile Design Bases."

Based on our review, we conclude that that 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 Regulatory Guide 1.118. The bypassed and inoperable status indication adequately conforms

to the guidance of Regulatory Guide 1.47 subject to satisfactory resolution of the open item in Section 7.5.2.4. The ESFAS adequately conforms to the guidance on the application of the single failure criterion in IEEE-379 as supplemented by Regulatory Guide 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 Regulatory Guide 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 subject to satisfactory resolution of the open item identified in Section 7.3.3.12 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 satisifies the requirement of 10 CFR Part 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 requirements of the single failure criterion. Therefore, we find the ESF control systems meet the relevant requirements of GDC-34, "Residual Heat Removal," and 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 50.55a(h) subject to resolution of the open items identified in Sections 7.3.3.4, 7.3.3.8, and 7.3.3.12 of this report.

## 7.4 Systems Required for Safe Shutdown

### 7.4.1 System Description

This section describes the equipment and associated controls and instrumentation of systems required for safe shutdown. It also describes controls and instrumentation outside the main control room that enable safe shutdown of the plant in case the main control room needs to be evacuated.

#### 7.4.1.1 Safe Shutdown Systems

Securing and maintaining the plant in safe shutdown condition can be achieved by appropriate alignment of selected systems that normally serve a variety of operational functions. The functions which the systems required for safe shutdown must provide are:

(1) Prevent the reactor from achieving criticality, and

(2) Provide an adequate heat sink such that the design and safety limits of the reactor coolant system temperature and pressure are not exceeded.

To perform the above functions, the systems required for safe shutdown must have the following capabilities.

(1) Boration
(2) Adequate supply of auxiliary feedwater, and
(3) Residual heat removal

In addition to the operation of systems required to provide the above functions to achieve and maintain safe shutdown, the following conditions are applicable:

(1) The turbine is tripped (in addition to automatic trip this can be accomplished manually at the turbine as well as from the control room);

(2) The reactor is tripped (in addition to automatic trip this can also be accomplished manually at the reactor trip switchgear as well as from the control room);

(3) All automatic protection and control systems are functioning (discussed in Section 7.2 and 7.3).

The monitoring indicators for maintaining hot standby are as follows:

(1) Water level for each steam generator
(2) Pressure for each steam generator
(3) Pressurizer water level
(4) Pressurizer pressure
(5) Primary coolant hot and cold leg temperatures
(6) Auxiliary feedwater flow for each steam generator
(7) Primary plant demineralized water storage tank level
(8) Source range flux monitor

The above indicators are provided in the main control room and also on the emergency shutdown panels except for the PPDWST level which is not provided on the emergency shutdown panels.

The systems used for safe shutdown include the following:

(1) Reactor Coolant System (RCS)
(2) Main Steam System
(3) Auxiliary Feedwater System
(4) Chemical and Volume Control System (CVCS)
(5) Primary Plant Component Cooling Water System
(6) Service Water System (SWS)
(7) Residual Heat Removal System (RHR)
(8) Supportive HVAC Systems

7.4.1.1.1 Reactor Coolant System

The reactor coolant system 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.

7.4.1.1.2 Main Steam System

The main steam system consists of main steam piping, power-operated atmospheric steam relief valves (PORVs), 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 RHR can be placed in operation. Core residual heat and RCS sensible heat can be removed by use of the safety grade PORV's if the main condenser is not in service.

7.4.1.1.3 Auxiliary Feedwater System

See Section 7.3 for a discussion of the auxiliary feedwater system.

7.4.1.1.4 Chemical and Volume Control System

The CVCS is designed to:

1. Maintain a predetermined water level in the pressurizer.

2. Maintain seal water injection flow to the reactor coolant pumps.

3. Control reactor coolant water chemistry conditions, radioactivity level, and soluble chemical neutron absorber concentration.

4. Provide emergency core cooling.

5. Provide means for filling and draining the reactor coolant system.

The safety-related part of the CVCS consists of the HHSI/charging pumps and their associated valves and piping used for emergency core cooling. For safe shutdown the CVCS provides a safety grade means to borate the RCS via the boric acid pumps and tanks and the charging pumps and their valves and piping. Additionally, the CVCS provides a safety grade means for RCS inventory control with the aforementioned equipment and the reactor head letdown system.

7.4.1.1.5 Primary Plant Component Cooling Water System

The primary plant component cooling water system serves as an intermediate system and a secondary boundary between the RCS and the SWS. The SWS provides an assured source of cooling water to the primary plant component cooling water heat exchangers. The primary plant component cooling water system is not required to mitigate the consequences of accidents, but is required to supply water to the RHR heat exchangers in the long term for the cold shutdown condition. During normal operation, cross-ties between redundant flow paths are open. Valves are provided to allow isolation of redundant flow paths to ensure that at least one primary plant component cooling water pump and heat exchanger can supply cooling to one RHR heat exchanger in the long term. A third primary plant component cooling water pump is provided as a back-up.

7.4.1.1.6 Service Water System

See Section 7.3 for a discussion of the service water system.

7.4.1.1.7 Residual Heat Removal System

The residual heat removal system (RHRS) transfers heat from the RCS to the primary plant component cooling water system during plant cooldown from hot standby to cold shutdown and controls the temperature of the primary coolant during cold shutdown. The RHRS consists of two redundant, separate, and independent trains each of which is powered from a different Class 1E bus and is capable of maintaining its design cooling function even with a major single failure such as a failure of a pump, valve, or heat exchanger.

.4.1.1.8 Supportive HVAC Systems

S section 9.4 for an evaluation of these systems.

7.4.1.2 Remote Shutdown Capability

In the event the control room must be evacuated, the operators can establish and maintain the plant in a hot shutdown condition from outside the control room through the use of controls and indicators located at the emergency shutdow panel (ESP). Two redundant trains of controls are provided for the ESP which is located in a locked room with access controlled by key or keycard. Transfer switches on the ESP allow the operator to transfer control of individual components required for safe shutdown from the control room to the ESP. Any tranfer action is annunciated in the control room and any automatic action, such as SI, initiated from the control room continues functioning upon transfer.

7.4.2 Specific Findings

7.4.2.1 Remote Shutdown Capability

GDC-19 requires that equipment at appropriate locations outside the control room be provided to achieve a safe shutdown of the reactor. The Standard

Review Plan (SRP) Section 7.4 interprets the GDC-19 requirements. The design should provide redundant safety grade capability to achieve and maintain safe shutdown from a location or locations remcte from the control room, assuming no fire damage to any required systems and equipment and assuming no accident has occurred. The remote shutdown equipment should be capable of maintaining functional operability under all service conditions postulated to occur including the seismic event. The remote shutdown station and the equipment used to maintain safe shutdown should be designed to accommodate a single failure.

In the FSAR Section 7.4.1.3, the applicant states that the design basis for control room evacuation does not consider a single failure. The staff found the applicant's design basis for remote shutdown capability unacceptable and required that the applicant clarify the design criteria for remote shutdown and address the isolation, separation, qualifiction and transfer/override provisions of the remote shutdown equipment in Section 7.4 of the FSAR.

In a June 13, 1984 response, the applicant stated that the next FSAR amendment will indicate that the design criteria for the control room evacuaton includes the single failure criterion and coincident loss of offsite power. Additionally the applicant stated separation of redundant train-related and non-1E circuits is maintained by barriers or appropriate air space, all Class 1E control equipment (other than indicators) meet the requirements of IEEE-STD-344-1975 and IEEE-STD-323-1974, and that transfer to the ESF is accomplished by push-buttons and switches on the shutdown panel.

The staff has reviewed the applicant's response and finds it acceptable with the exception of the seismic qualification of indicators of the ESP. The staff has requested additional information on this issue and considers this an open issue pending our review of the applicant's response.

Additionally, the staff considers the applicant's pending FSAR amendment to include the information provided in the June 13, 1984 response to be a confirmatory item.

7.4.3 Conclusions

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 adequte 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 as outlined in the Standard Review Plan, Section 7.4, Parts II and III. In Section 7.1 of this SER we concluded that the applicant had adequately identified the guidlines applicable to these systems. Based upon our audit review of the system 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 indentification 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, "Environmenal 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 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 has 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 suitabe 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 subject to satisfactory resolution of open item identified in Section 7.4.2.1 of this report.

## 7.5 Information Systems Important to Safety

### 7.5.1 System Description

Indicators, annunciators, recorders, and lights are used to provide information to the operator during post-accident monitoring and normal operating conditions. The information is dispalyed on the operator's console, the various control boards in the control room, and the remote shutdown panels. The systems for which this information is provided include the following functions:

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

#### 7.5.1.1 Safety-Related Display Instrumentation

The applicant has conducted an analysis to identify the appropriate variables for the operator to monitor conditions in the reactor coolant system, the secondary heat removal system, the containment, the engineered safety features systems and the safe shutdown systems. The safety-related display instrumentation provides the information necessary for the operator to perform the required manual safety functions following a reactor trip. It provides information for all operating conditions, including anticipated operational occurrences, accidents and post accident conditions.

Table 7.5-1 in the applicant's FSAR identifies the safety-related display instrumentation and includes the following information for each variable:

1. Instrument range
2. Environmental qualification
3. Seismic qualification
4. Display methodology
5. Type and category (per the definition in R.G. 1.97 Rev. 2)

The evaluation of environmental qualification is addressed in Sections 3.10 and 3.11 of this report.

7.5.1.2 Bypass and Inoperable Status Indication

Automatic bypass or inoperable status indication is provided in the control room for each redundant portion of a safety-related system. The indication of bypassed or inoperable status was designed following the guidance provided by R.G. 1.47 Revision 0.

The function bypass alarms receive their inputs from valve position limit switches, circuit breaker auxiliary contacts, switch contacts, relays, etc. indicative of function inoperability. Means for manual actuation of each bypass alarm are also provided in the control room.

Bypass indication alarms are tested by a test contact that simulates operation of the remote contacts to verify proper operation of the alarm circuits.

The design and installation of the bypass and inoperable status indication is such that a failure in an alarm circuit will have no adverse affect on the function monitored or on any of the other functions monitored by the bypass alarm panel.

Bypass indication is provided in the control rooom for each train of the following systems:

Residual heat removal
Auxiliary feedwater
High head safety injection
Safety injection accumulators (Train A only)
Low head safety injection
Quench spray
Recirculation spray
Containment penetration
Service water
Primary plant component cooling water
Fuel pool cooling
Solid state protection

Vital instrumentation electrical
Main control room ventilation isolation
Control building ventilation
Safeguards area ventilation
Cable vault and rod control area ventilation
Supplementary leak collection
Auxiliary building ventilation
Emergency switchgear area ventilation
Battery room ventilation
Emergency diesel generator
Emergency diesel generator support
4,160 V emergency electrical
480 V emergency electrical
125 V dc emergency electrical
Intake structure ventilation
Bypassed inoperable status indication inhibited (indicating light only)

7.5.2 Specific Findings

7.5.2.1 Emergency Response Capability - R.G. 1.97 Rev. 2 Requirements

Generic Letter No. 82-33 included additional clarification regarding Regulatory Guide 1.97, Revision 2, relating to the requirements for emergency response capability. The applicant's letter dated September 12, 1983, provided the response to the part of Generic Letter No. 82-33 pertaining to R.G. 1.97, Rev. 2. The staff will perform an audit of the applicant's method of implementing R.G. 1.97, Rev. 2, and the applicant's supporting technical justification for any proposed alternatives. Until the staff completes its review for compliance to R.G. 1.97, Rev. 2 recommendations, a license condition will be imposed requiring the satisfactory resolution of all review findings.

7.5.2.2 NUREG-0737 Item II.F.1 Accident Monitoring Instrumentation Positions (4), (5), and (6)

Positions (4), (5), and (6) of this action plan item require installation of the extended range containment pressure monitors, containment water level

monitors, and containment hydrogen concentration monitors. Table 7.5-1 of the FSAR provides information for positions (4) and (5), but indicates that information for position (6) will be provided later. Since the applicant and our review thus far indicates conformance with the requirements for positions (4), (5), and (6), this is confirmatory subject to revision of FSAR Table 7.5-1 for position (6).

7.5.2.3 NUREG-0737 Item II.D.3 - Direct Indication of Relief and Safety Valve Positions

The three pressurizer power operated relief valves (PORV) are operated automatically or by remote manual control. Each valve is provided with positive open/closed indication lights in the control room. The three safety valves are also provided with positive open/closed indication lights. The temperature in each of the safety valve and PORV discharge lines is measured and indicated in the control room. An increase in a discharge line temperature is an indication of leakage or relief through the associated valve. High temperature is alarmed in the control room. The valves position indicating limit switches are seismically and environmentally qualified.

The above information was provided by Amendment 5 to the FSAR and during a June 29, 1984 meeting with the applicant. The staff finds that the design is in conformance with the action plan guidelines, and is, therefore, acceptable.

7.5.2.4 Bypass and Inoperable Status Panel

The FSAR Section 1.8 states that the design follows the guidance of R.G. 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems. During our review, the staff audit reviewed some of the design drawings which contain information of the bypass and inoperable status panel. However, there is little information in the FSAR to describe the system. The staff requested that the applicant provide the descriptive information in Section 7.5 of the FSAR to demonstrate the conformance with R.G. 1.47.

In a June 13, 1984 letter, the applicant provided descriptive information on conformance to R.G. 1.47 and committed to include similar information in the

next FSAR amendment. The staff considers the applicant's pending FSAR amendment covering this information to be a confirmatory item.

The staff has reviewed the applicant's response and finds it acceptable with one exception. The staff, during a June 29, 1984 meeting with the applicant, expressed a concern that the bypassing of a supporting system may not lead to a bypass indication for a protection system whose operation depends on the supporting system. The staff considers this an open item.

7.5.2.5 IE Bulletin 79-27, Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation

The staff requested that the applicant review the adequacy of emergency operating procedures to be used by control room operators to attain cold shutdown on loss of any Class 1E or non-Class 1E buses supplying power to safety or nonsafety-related instrument and control systems. This issue was addressed for operating reactors through IE Bulletin 79-27.

The staff reviewed the applicant's response, contained in Amendment 4 of the FSAR, and found it to be inadequate. The intent of Bulletin 79-27 and NRC Question 420.2 was for the applicant to do an in-depth review of all non-Class 1E and Class 1E buses which could affect the plant's ability to achieve a cold (not just hot) shutdown. If problems were uncovered by the in-depth review, design modifications were to be made or emergency procedures were to be developed to ensure that cold shutdown could be achieved.

The following statements, which caused staff concern, were contained in the applicant's response:

(1) "At present no such control room alarm or indication has been provided for the normal 120V ac/125V dc distribution system."

(2) "...loss of a vital or normal bus could affect the unit's ability to attain cold shutdown."

Accordingly, to provide assurance that the concerns of Bulletin 79-27 have been adequately addressed, the following information was requested from the applicant:

(1) An affirmative or clearly implied statement of conformance to all the bulletin requirements.

(2) A list of instrumentation and control power buses reviewed, or a positive statement that all required buses were reviewed.

(3) An affirmative or clearly implied statement that loss of bus alarms and indications in the control room have been reviewed.

(4) An implemented or proposed design change for all deficiencies identified.

(5) A schedule for completion of proposed design changes, if applicable.

In a July 30, 1984 letter, the applicant provided responses covering the requested information. The staff has reviewed the applicant's responses and finds them acceptable. This issue is considered resolved.

7.5.3 Conclusions

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 acceptable 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 as outlined in the Standard Review Plan, Section 7.3, Parts II and III. 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 items identified in Sections 7.5.2.1 and 7.5.2.4 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 demontrate 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 Regulatory Guide 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 are acceptable and meet the requirements of General Design Criteria 2, 4, 13 and 19 subject to satisfactory resolution of open items identified in Sections 7.5.2.1 and 7.5.2.4.

## 7.6 Interlock Systems Important to Safety

### 7.6.1 System Description

The systems described in this section operate to reduce the probability of occurrence of specific events or to maintain safety systems in a state to assure their availability when required.

#### 7.6.1.1 Residual Heat Removal Isolation Valve Interlocks

The Residual Heat Removal System (RHRS) consists of two residual heat exchangers, two pumps, and the associated piping, valves, and instrumentation necessary for operational control. The inlet lines to the RHRS are connected via a single suction header to a hot leg of a reactor coolant loop, and the return lines are connected to the cold legs of two reactor coolant loops.

The RHRS is a low-pressure system and is isolated during normal operation from the high-pressure reactor coolant system. The isolation is provided by two motor-operated valves in series in each of the two residual heat removal pump suction lines and a motor-operated valve and a series check valve in each discharge line. Interlocks prevent opening of the motor-driven valves until the reactor coolant system pressure is below a predetermined value (approximately 425 psig). Once opened, the valves will close automatically if the pressure increases above a preset value (approximately 750 psig). The positions of the valves are indicated on the main control board by lights actuated by valve limit switches. Two pressure transmitters, powered from separate emergency power sources and supplied from separate vendors, are used to derive the isolation valve interlocks.

7.6.1.2 Cold Leg Accumulator Motor-Operated Valve Interlocks

The accumulators are pressure vessels partially filled with borated water and pressurized with nitrogen gas. During normal operation each accumulator is isolated from the reactor coolant system (RCS) by two check valves in series. Should the RCS pressure fall below the accumulator pressure, the check valves open and borated water is forced into RCS. To prevent injection of borated water at low pressure operation during shutdown and startup, each of the accumulators is provided with a motor-operated isolation valve in series with the check valves. The valve is closed by the operator shortly after the RCS is depressurized below the safety injection unblock setpoint.

The motor-operated isolation valves are controlled by switches on the main control board and are interlocked as follows:

(1) They open automatically on receipt of a safety injection signal ("S")

(2) They open automatically whenever the RCS pressure is above the safety injection unblock pressure (P-11 interlock)

(3) They cannot be closed as long as an "S" signal is present.

After the RCS pressure is decreased during shutdown and the motor-operated isolation valves are closed, power to the valves is disconnected to prevent accidental operation. The power to the valves is also disconnected after the valves are opened during normal power operation to prevent accidental closing. Lights, actuated by the valve limit switches, provide valve position indication in the control room. Alarms, operated by both the valve motor-operator limit switch and valve stem limit switch, are activated when a valve is not fully open with the system above the safety injection unblock pressure.

7.6.1.3 RCS Overpressure Protection During Low Temperature Operation

The reactor coolant system overpressure protection during low temperature operation is dependent upon semiautomatic opening of two pressurizer power

operated relief valves (PORVs). The actuation logic for the PORVs continuously monitor RCS temperature and pressure conditions.

When the RCS is at normal operating pressure and temperature conditions, an ARM/BLOCK switch on the main control board is in the block position. The monitored RCS temperature signals are processed to generate a reference pressure limit and to generate an alarm to alert the operator to manually arm the system at a low temperature setpoint. An actuation signal to open the PORV's is generated when the system pressure exceeds the reference pressure and the system is manually armed.

Wide range temperature signals are used to generate the reference pressure limit which is compared to the actually RCS pressure monitored by wide range pressure channels. The difference signal will first actuate a main control board alarm whenever the measured pressure approaches, within a predetermined amount, the reference pressure. A further increase in measured pressure will then generate an annunciated actuation signal. Upon sufficient RCS inventory letdown, the RCS pressure decrease will clear the actuation signal and cause the PORV's to close. Separate temperature and pressure transmitters are provided for each train of PORV actuation.

7.6.1.4 Reactor Coolant System Loop Isolation Valve Interlocks

The purpose of these interlocks is to ensure that an accidental reactor coolant pump start-up in an unborated and/or cold, isolated reactor coolant loop results in a relatively slow reactivity insertion rate. This is accomplished by ensuring that the intial flow from an isolated loop to the remainder of the RCS is through the relief line bypass around the closed cold leg isolation valve. This small flow, which allows the boron concentration/temperature to be brought into equilibrium relatively slowly, must exist for approximately one hour before the cold leg isolation valve can be opened.

The reactor coolant system loop isolation interlocks are as follows:

(1) Hot leg isolation valve cannot be opened unless cold leg isolation valve is closed.

(2) Reactor coolant pump cannot be started unless:

a. Cold leg isolation valve is closed and relief line bypass valve is open or

b. Cold leg and hot leg isolation valves are both open.

(3) Cold leg isolation valves cannot be opened unless:

a. Hot leg isolation and relief line bypass valves have been open and relief line flow has existed all for a specified time and

b. Cold leg temperature/hot leg temperature are within 20°F of the highest cold leg temperature/hot leg temperature in other loops.

Redundant and independent valve limit switches and differential pressure switches are used to develop the above interlocks.

7.6.2 Specific Findings

7.6.2.1 NUREG-0737 Item II.K.3.1, Installation and Testing of Automatic Power-Operated Relief Valve Isolation System

This Action Plan item requires all PWR licensees to provide a system that uses a PORV block valve to protect against a small break loss-of-coolant accident. The system would automatically close the block valve when the reactor coolant system pressure decays after the PORV opens. The staff requirements provide, however, that such a system is not required if studies provided in response to item II.K.3.2 show that the probability for the PORV sticking open is sufficiently small.

Although the staff's review indicates that an automatic closure is provided for the PORV block valves, the applicant has stated that he agrees with the Westinghouse determination that the addition of a safety grade block valve closure system is not required because of the low probability of a stuck open

PORV. If the staff does not accept the Westinghouse conclusions (under II.K.3.2 review), we will address this item in a supplement to this report.

7.6.2.2 Reactor Coolant System Loop Isolation Valve Interlocks

The FSAR 7.6.6 describes the reactor coolant system loop isolation valve interlocks. The description was incomplete and additional information was required to clarify that the design is in conformance with IEEE STD-279 requirements. Additionally, the staff was concerned that, during operation with N-1 loops, the criteria for testing and single failure may not be met due to reduced protection logic.

In a July 12, 1984 letter, the applicant responded to this issue. The staff has reviewed the applicant's response and will pursue this issue as part of plant Technical Specifications review.

7.6.2.3 Primary Component Cooling Water Isolation from Reactor Coolant Pump Thermal Barriers

The FSAR Section 9.2.2 describes the isolation of the reactor coolant pump thermal barriers from the primary component cooling water system. A check valve is installed in each inlet cooling water line to the thermal barrier cooling coil and an air-operated isolation valve is installed in each outline line. Each isolation valve closes on signals developed from a corresponding line's pressure or flow sensor. Because the FSAR does not provide the design basis for this isolation, the staff is concerned about its safety significance. Therefore, the staff requests the applicant provide information about the design basis for this system and a discussion on the consequences of either the check valve or the air-operated isolation valve failing to close under conditions related to the design basis. This is an open item.

7.6.2.4 Cold Leg Accumulator Motor-Operated Valve Position Indication

During the staff's review of the power lockout circuitry, a conflict was found between plant schematics and the information provided by FSAR Section 6.3.5.5. The FSAR states that the valve position indicating lights are powered by the

valve control power which is removed during power lockout. The schematics indicate that redundant valve position indication is provided and is not effected by power removal. This item is confirmatory subject to revision of the FSAR to update the description to eliminate this conflict.

7.6.3 Conclusions

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 GDC-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 guidelines.

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 RSB 5-2, "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 guidelines.

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 the 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."

In summary, the staff concludes that the interlock systems important to safety are acceptable subject to satisfactory resolution of open items identified in Section 7.6.2.3 of this report.

## 7.7 Control Systems

The general design objectives of the Plant Control System are:

(1) To establish and maintain power equilibrium of the primary and secondary system during steady state unit operation;

(2) To constrain operational transients so as to preclude unit trip and re-establish steady-state unit operation; and

(3) To provide the reactor operator with monitoring instrumentation that indicates all required input and output control parameters of the systems and provides the capability of assuming manual control of the system.

7.7.1 System Descriptions

(1) Reactor Control System

The reactor control system enables the plant to accept a step load increase or decrease of 10% and a ramp increase or decrease of 5% per minute within the load range of 15% to 100% without reactor trip, steam dump, or pressurizer relief actuation (subject to possible xenon limitations). The system also maintains the reactor coolant average temperature within established limits by generating the demand signals for moving the control rods.

(2) Rod Control System

The rod control system modulates the reactor power by automatic or manual control of full length control rod banks. The system receives rod speed and direction signals from the reactor control system. Manual control is provided to move control banks in or out at a predetermined fixed speed. An interlock derived from measurements of turbine impulse chamber pressure prevents automatic control when the turbine load is below 15%.

The two shutdown banks are moved to the fully withdrawn position by manual control prior to criticality. These rods remain in that position during normal operation. The control banks are the only rods that are manipulated under automatic control. Each control bank is divided into two groups to obtain smaller incremental reactivity changes per step. All rod control cluster assemblies (RCCAs) in a group move simultaneously. There is individual position indication for each rod cluster control assembly.

(3) Plant Control Signals for Monitoring and Indication

(a) Nuclear Instrumentation Power Range System - Four channels are provided. Each of the channels uses a dual-section ionization

chamber as a neutron flux detector. The currents from the ionization chambers are used to measure the power level, axial flux imbalance, and radial flux imbalance.

(b) Rod Position Monitoring System - Two separate systems are provided, digital rod position indication and the demand position system. The digital rod position indication system measures the actual position of each rod. The demand position system counts pulses generated in the rod drive control system to provide a readout of the demanded bank position.

(c) Control Bank Rod Insertion Monitoring - Provides warning to the operator of excessive rod insertion. The "low" alarm alerts the operator of an approach to the rod insertion limits requiring boron addition by following normal procedures with the chemical and volume control system. The "low-low" alarm alerts to a need for immediate action to add boron by any one of several alternate methods.

(d) Rod Deviation Alarm - The rod deviation alarm is generated by the digital rod position indication system whenever any individual control rod position deviates from the bank demand position by a preset limit.

(e) Rod Bottom Alarm - A "Rod Bottom Rod Drop" alarm is generated for each of the rods by the digital rod position indication system.

(4) Plant Control System Interlocks

(a) Rod Stops - Prevent abnormal power conditions which could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures. The interlocks are generated by signals from the neutron flux, overtemperature $\Delta T$, overpower $\Delta T$, and turbine impulse chamber pressure measurement channels.

(b) Automatic Turbine Load Runback - Prevents high power operation which, if reached, would initiate reactor trip. Signals from overtemperature $\Delta T$ and overpower $\Delta T$ measurement channels are used to initiate automatic turbine load runback when an overpower or overtemperature condition is approached.

(5) 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 small pressure variations. These variations are due to heat losses, including heat losses due to a small continuous spray. The remaining (backup) heaters are turned on when the pressurizer pressure control signal demands approximately 100 percent proportional heater power.

The spray nozzles are located on the top of the pressurizer. 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. Spray is initiated when the pressure controller spray demand signal exceeds a setpoint and the spray rate increases proportionally with increasing spray demand signal until it reaches a maximum value.

(6) Pressurizer Water Level Control

The pressurizer operates by maintaining a steam cushion over the reactor coolant. As the density of the reactor coolant adjusts to the various temperatures, the steam-water interface moves to absorb the variations with relatively small pressure disturbances.

A programmed pressurizer water level is maintained by the chemical and volume control system. During normal plant operation, the charging flow varies to 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 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.

To control pressurizer water level during startup and shutdown operations, the charging flow is manually regulated from the main control room.

(7) 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.

Continued delivery of feedwater to the steam generators is required as a sink for the heat stored and generated in the reactor following a reactor trip and turbine trip. An override signal closes all feedwater valves when the average coolant temperature is below a set value and the reactor has tripped. Manual override of the feedwater control system is available at all times.

When the plant is at very low power, a secondary automatic control system is utilized. This system uses the steam generator water level programmed setpoint in conjunction with the power range neutron flux signal to control the position of the bypass valves which parallel the main feed water control valves. Switchover to this secondary system is initiated by the operator at approximately 15% power.

(8) Steam Dump Control System

The steam dump system, together with the rod control system, is designed to accept a 100% loss of net load without tripping the reactor. The system functions automatically by bypassing 90% of the main steam directly to the condenser and atmosphere to maintain an artificial load 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.

A demand signal for the load-rejection steam dump controller is generated if the difference between the reference average temperature based on turbine impulse chamber pressure and the lead/lag compensated auctioneered average temperature exceeds a preset value. To prevent actuation of steam dump on small load perturbations, an independent load rejection sensing circuit is provided. This circuit senses the rate of decrease in the turbine load as detected by the turbine impulse chamber pressure and blocks the steam dump unless the rate exceeds a preset value.

Following a reactor trip, the load-rejection steam dump controller is deactivated and the plant-trip steam dump controller becomes active. The demand signal for this controller is generated if the difference between the lead/lag compensated auctioneered average temperature and the no-load reference average temperature exceeds a preset value. As the error signal reduces in magnitude following tripping of the dump valves, the dump valves are modulated by the plant-trip controller to regulate the rate of heat removal and thus gradually establish the equilibrium hot shutdown condition.

Removal of the residual heat during a shutdown is accomplished by the steam-pressure controller which controls the steam flow to the condensors based on measured steam pressure. This controller operates a portion of the same steam dump valves to the condenser which are used following load rejection or plant trip.

(9) Incore Instrumentation

The incore instrumentation system consists of chromelalumel thermocouples at fixed core outlet positions and movable miniature neutron detectors at selected fuel assemblies. The thermocouple readings are monitored by the plant computer with backup readout provided by an indicator in the main control room. The movable detectors can perform flux mapping at various core quadrant to obtain a flux map for any region of the core. The data collection, calculation and recording are performed by the plant computer.

7.7.2 Specific Findings

7.7.2.1 NUREG-0737 Item II.K.3.9, Proportional Integral Derivative (PID) Controller Modification

In FSAR Section 1.10, the applicant stated that this item was not applicable to BV-2 because the hardware is not installed. FSAR Figure 7.7-4 shows the PID controller is part of the plant's pressurizer pressure control system. To resolve this conflict, the applicant stated, in a June 20, 1984 letter, that the PID controller is installed in the plant and that FSAR Section 1.10 will be revised. Additionally, the applicant stated that the derivative time constant will be set to zero to satisfy this NUREG requirement.

The staff finds this acceptable and considers this item resolved subject to confirmation of FSAR revision.

7.7.2.2 High Energy Line Breaks and Consequential Control System Failures

A concern was raised in IE Information Notice 79-22, issued September 19, 1979, that certain nonsafety-grade or control equipment, if subjected to the adverse environment of a high energy line break, could malfunction and cause the plant conditions to be more severe than those analyzed in the Safety Analyses of Chapter 15. The applicant was requested to perform a review to determine what, if any, design changes or operator actions would be necessary to assure that high energy line breaks will not cause control system failures to complicate the event beyond the Chapter 15 Safety Analyses.

The staff reviewed the applicant's initial response, contained in FSAR Amendment 4, and found it needed further clarification in the following areas:

(1) PT 444 and 445, used for the pressurizer PORV control are not qualified. Applicant's response indicated all equipment associated with this control system were Category I.

(2) The intent of NRC Question 420.4 was to require the applicant to review all possible control system malfunctions due to high energy line break inside or outside of containment. It appeared that the applicant only reviewed the four scenarios described in IE Information Notice 79-22 and further limited that to inside containment.

The applicant, in an April 30, 1984 letter, has now provided additional information as a revised response to FSAR Question 420.4. In addition to the analysis conducted for the four nonsafety-grade systems identified by the IE Information Notice 79-22: (1) steam generator PORV control system, (2) pressurizer PORV control system, (3) main feedwater control system, and (4) automatic rod control system; the applicant stated that his review has not identified any other nonsafety-grade equipment whose performance, when subjected to an adverse environment, would impact the protective functions performed by safety grade equipment.

The results of the analysis conducted for the four systems indicate that the steam generator PORV control system does not contain nonsafety-grade control equipment which can be exposed to environments resulting from a high-energy-line break. The other three systems do contain nonsafety-grade components that can be exposed to high-energy-line break environments; but, for those components, the analysis concluded that the present design employs sufficient design features and emergency procedures to provide adequate assurance that high-energy-line breaks will not cause control system failures to complicate the event beyond the BV-2 Chapter 15 analysis. Based on the results of the applicant's review, the staff considers this issue resolved.

7.7.2.3 Control System Failure Caused by Malfunctions of Common Power Source or Instrument Line

To provide assurance that the FSAR Chapter 15 analyses adequately bounds events initiated by a single credible failure or malfunction, the staff has asked the applicant to identify any power source or sensors that provide power or signals to two or more control functions, and demonstrate that failures or malfunctions of these power sources or sensors will not result in consequences more severe than those of Chapter 15 analyses or beyond the capability of operator or safety systems.

The staff has reviewed the applicant's response, contained in Amendment 4 to the FSAR, and finds it needs further clarification in the following areas:

(1) The applicant's response is based on the satisfactory review of this issue on other Westinghouse plants. A statement is needed to address the similarity of BV-2 to the other referenced plants as pertaining to this issue.

(2) Where similarity does not exist, further analysis should be provided to properly address this issue.

This is an open item.

7.7.3 Conclusions

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 GDC-19, "Control Room." This conclusion is based on the following:

Based on our review of the plant transient response to normal load changes and anticipated operational occurrences, such as reactor trip, turbine trip, upsets in the feedwater and steam bypass systems, 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 conclude that the features for manual and automatic control facilitate the capability to maintain plant variables within prescribed operating limits. 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, subject to resolution of the open item identified in Section 7.7.2.3 of this report, 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 confirmed 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.

In summary the staff concludes that the control systems are acceptable subject to satisfactory resolution of the open item identified in Section 7.7.2.3 of this report.

ICSB SALP INPUT

PLANT: Beaver Valley 2
SUBJECT: Safety Evaluation Report

| EVALUATION CRITERIA | PERFORMANCE CATEGORY | BASIS |
|---|---|---|
| 1. Management Involvement | N/A | No basis for assessment. |
| 2. Approach to Resolution of Technical Issues | 3 | An understanding of the issues was frequently lacking. Resolutions are/were delayed due to the lack of understanding of the technical issues involved. |
| 3. Responsiveness | 3 | Draft SER contained 23 open items. SER contains 8 open items. Considerable NRC effort and repeated submittals were needed and are still needed to obtain acceptable resolutions. |
| 4. Enforcement History | N/A | No basis for assessment. |
| 5. Reportable Events | N/A | No basis for assessment. |
| 6. Staffing | N/A | No basis for assessment. |
| 7. Training | N/A | No basis for assessment. |