

Docket File
50-454/455

SEP 30 1982

2.

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

FROM: Themis P. Speis, Assistant Director for Reactor Safety
Division of Systems Integration

SUBJECT: ICSB INPUT TO BYRON SSER #2

Plant Name: Byron Station, Units 1 & 2
Docket Nos.: STN 50-454/455
Licensing Status: OL
Responsible Branch: LB #1
Project Manager: S. Chesnut
Review Branch: ICSB
Review Status: Complete

DESIGNATED ORIGINAL

Certified By *Chris Thompson*

In response to your memorandum of July 30, 1982 requesting input to the next Byron SER Supplement (SSER #2), the following information is provided to update the status of the six ICSB confirmatory items listed therein and the two ICSB licensing conditions previously identified in the Byron SER, dated February 1982.

1. CONFIRMATORY ITEM 23: IEB 80-06 (Section 7.3.2.2)
Status is unchanged.
2. CONFIRMATORY ITEM 24: P-4 Interlock (Section 7.3.2.9)
Status changed to closed. (See attached ICSB Input To Byron SSER #2)
3. CONFIRMATORY ITEM 25: Remote Shutdown Capability (Section 7.4.2.2)
Status is unchanged.

Contact:
F. Burrows, ICSB
X29455

OFFICE					
SURNAME	8210220531	820930			
DATE	CF	ADOCK	05000454		
	CF				

- 4. CONFIRMATORY ITEM 26: Steam Generator Pressure Control (Section 7.4.2.3)
Status changed to closed (See attached ICSB Input To Byron SSER #2).
- 5. CONFIRMATORY ITEM 27: Switchover From Injection to Recirculation (Section 7.6.2.3)
Status is unchanged.
- 6. CONFIRMATORY ITEM 29: ICSB Site Visit (Section 7.1.3)
Status is unchanged.
- 7. LICENSE CONDITION 4: Response Time Testing (Section 7.2.2.5)
Status is unchanged.
- 8. LICENSE CONDITION 5: Post-Accident Monitoring (Section 7.5.2.2)
Status is changed to closed (See attached ICSB Input To Byron SSER #2).

Original Signed By *B. Speis*
Themis P. Speis

Themis P. Speis, Assistant Director
for Reactor Safety
Division of Systems Integration

cc: R. Mattson
T. Speis
T. Dunning
S. Chesnut
K. Kiper
F. Burrows

DISTRIBUTION:
Docket File
ICSB Reading File
F. Burrows (PF)
T. Speis
Byron Subject File

OFFICE ▶	ICSB/DSI	ICSB/DSI	ICSB/DSI	ADRS/DSI		
URNAME ▶	F. Burrows	T. Dunning	F. Rosa	T. Speis		
DATE ▶	9/29/82	9/29/82	9/29/82	9/30/82	-	

ICSB INPUT TO BYRON SSER #2

7.3.2.9 Test Jacks For P-4 Interlock Test

In the SER, the staff indicated that the applicant would provide test jacks at the reactor trip breakers to facilitate testing of the P-4 interlocks. The applicant's letter of May 12, 1982 commits to permanently install voltmeters for testing the P-4 interlocks. These additional components will eliminate the need for the test jacks and temporary connection of portable test equipments. Further, the applicant stated that a description of the voltmeter installation would be incorporated in the FSAR. We have reviewed the information provided on the installation and find it satisfactory. We consider this matter closed.

7.4.2.3 Steam Generator Pressure Control

In the SER, the staff indicated that the applicant was implementing design changes to provide hydraulic operators for the steam generator PORV's. The applicant's letter of April 23, 1982 confirms their commitment to provide these hydraulic operators. Further, the applicant has incorporated this information in Amendment 38 to the FSAR. We have reviewed the information provided on the installation and find it satisfactory. We consider this matter closed.

DESIGNATED ORIGINAL

Controlled By

Chris Thompson

7.5.2.2 Post Accident Monitoring

As stated in the Byron SER, it was indicated that the operating license would be conditioned to require the applicant to comply with Regulatory Guide 1.97, Revision 2 or provide justification for any alternative. Subsequently the staff has proposed, as Commission policy, that conformance to these requirements be addressed in the broader context of the requirements for Emergency Response Capability (ERC). This would include the evaluations of designs and implementation schedules for the Safety Parameter Display System, Control Room Design Review, upgraded Emergency Operating Procedures, Technical Support Center, Operational Support Center, Emergency Response Facility in addition to Regulatory Guide 1.97. Based on the review of the instrumentation provided for post-accident monitoring, the staff concludes that there is substantial conformance to Regulatory Guide 1.97 for plant operation. The staff has been instructed to use SECY 82-111B in implementation of Emergency Response Capability (including requirements for post-accident monitoring). Therefore this item will be addressed as part of the schedule for implementing the requirements for ERC and will not be included as a separate license condition.

It is the staff's position that the Byron plant can be operated without undue risk to the health and safety of the public until a Staff review and decision is made with respect to the applicant's overall compliance with Regulatory Guide 1.97, Rev. 2.

Docket
File
50-400/401

DEC 17 1982

4/.

MEMORANDUM FOR: Thomas Novak, Assistant Director for Licensing, Division of Licensing
FROM: Themis P. Speis, Assistant Director for Reactor Safety, Division of System Integration
SUBJECT: ICSB INPUT TO DRAFT SER - SHEARON HARRIS UNITS 1 AND 2

Plant Name: Shearon Harris Units 1 and 2
Docket Nos: 50-400/401
Licensing Status: OL
Responsible Branch: LB #3
Project Manager: N. Kadambi
Review Branch: ICSB
Review Status: Incomplete

DESIGNATED ORIGINAL

Certified By Cheryl Thompson

Enclosed is a draft Safety Evaluation Report (SER) prepared by the Instrumentation and Control Systems Branch (ICSB). This draft SER reflects the results of our review of the information presented in the Shearon Harris Units 1 and 2 Final Safety Analysis Report (FSAR) through Amendment No. 4. Also, the SER draft is based on a drawing review and our evaluation of the applicant's response during ICSB review meetings which were held on August 16-19, 1982 and September 14-16, 1982.

The open items in the Instrumentation and Control system areas for the Shearon Harris are identified in Section 7.1.4 of the enclosed SER draft.

Being a draft, this SER is subject to modification. Our continuing review may lead to new open issues in addition to those described in this draft.

Reviewed by
Themis P. Speis

Themis P. Speis, Assistant Director for Reactor Safety, DSI

Enclosure: As stated

cc: See next page

Contact: H. Li X-29452

ICSB/DSI
HLi:ct
12/15/82

^{F.P.}
ICSB/DSI
TDunnington
12/16/82

^{F.P.}
ICSB/DSI
FRosa
12/16/82

^{F.P.}
ADRS/DSI
TPSpeis
12/16/82

6212300386 821217
CP ADBCK 05600900
CP

Thomas Novak

2

cc: R. Mattson
F. Rosa
G. Knighton
N. Kadambi
E. Licitra
T. Dunning
R. Capra
H. Li

DISTRIBUTION:
Docket File
ICSB Reading File
H. Li (PF)
T. Speis
Shearon Harris Subject File

7. INSTRUMENTATION AND CONTROLS

7.1 Introduction

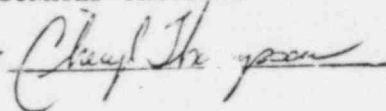
7.1.1 Acceptance Criteria

Section 7.1 of the Shearon Harris Final Safety Analysis Report (FSAR) 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 the Shearon Harris Units 1 and 2. The acceptance criteria used as the basis for this evaluation are those identified in the Standard Review Plan (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 General Design Criteria and IEEE Std. 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, Regulatory Guides, and Branch Technical Positions identified in Section 7.1 of the SRP. Conformance to the acceptance criteria provides the bases for concluding that the instrumentation and control systems meet the requirements of 10 CFR 50.

DESIGNATED ORIGINAL

7.1.2 Method of Review

Certified By



Shearon Harris employs a Westinghouse Nuclear Steam Supply system with balance-of-plant design provided by Ebasco Services Incorporated. Many safety related instrumentation and control systems are similar to those at North Ann, Beaver Valley and Virgil Summer, and have been previously reviewed and approved by the staff. We concentrated our review on those areas where the Shearon Harris design differs from previously reviewed designs and in those areas which have

remained of concern during reviews of other similar plants. Several meetings have held with the applicant including NSSS and BOP designers to clarify the design and to discuss concerns the staff has with the design. Detail drawings included P&I diagrams, logic diagrams, control wiring diagrams, electrical one line diagrams and electrical schematic diagrams were audited during the review.

7.1.3 Conformance to Criteria and Guidelines

The applicant has identified the instrumentation and control system 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 the systems as identified in FSAR Table 7.1.0-1.

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 nuclear steam supply system and the balance of plant 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 noted herein are applicable to the instrumentation and control systems important to safety with the exception of the open items listed below. The staff will review these items and report their resolution in a supplement to this report. The applicable sections of this report which address these items are indicated in parentheses following each open item.

- (1) Trip setpoint and margins (7.2.2.2)
- (2) Response time testing (7.2.2.3)
- (3) Independent verification of the operability of reactor trip breaker shunt and under-voltage coils (7.2.2.4)
- (4) Turbine trip following reactor trip (7.2.2.5)
- (5) Low feedwater flow trip (7.2.2.6)
- (6) System level ESF manual initiation capability (7.3.3.2)
- (7) Test of engineered safeguards P-4 interlock (7.3.3.3)
- (8) IE Bulletin 80-06 (7.3.3.4)
- (9) Level measurement errors due to environmental temperature effects on level instrument reference legs (7.3.3.5)
- (10) Steam generator level control and protection (7.3.3.6)
- (11) Containment spray system chemical addition control (7.3.3.7)
- (12) Non-Class IE input to Class IE control circuits (7.3.3.8)
- (13) Spare pump in component cooling water system (7.3.3.9)
- (14) Spare pump arrangement for charging pump (7.3.3.10)
- (15) BOP system isolation device testing (7.3.3.11)
- (16) SSLPS test circuits (7.3.3.12)
- (17) Failure modes and effects analyses (FMEA) of ESFAS (7.3.3.13)

- (18) Auxiliary feedwater control (7.4.2.1)
- (19) Capability to achieve cold shutdown (7.4.2.2)
- (20) Loss of non-class IE instrumentation and control power system bus during operation (IE Bulletin 79-27) (7.5.2)
- (21) Relief and safety valves need switch qualification (7.5.3)
- (22) RCS pressure control during low temperature operation (7.8.2.2)
- (23) Accumulator isolation valve interlock (7.6.2.3)
- (24) Control system failure caused by malfunctions of common power source or instrument line (7.7.2)
- (25) Control system failure caused by high energy line breaks (7.7.3)

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. Confirmatory items will not be addressed in a supplement to this report unless an unanticipated problem is found. The sections of this report which address these items are noted in parentheses.

- (1) Testing for remote shutdown operation (7.4.2.3)
- (2) Safety-related instrumentation freeze protection (7.7.1)

7.1.4.3 Site Visit

A site review will be performed for the purpose of confirming 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 prior to issuance of the license and any problems found will be addressed in a supplement to this report. --

7.1.4.4 Fire Protection Review

The review of the auxiliary shutdown panel discussed in Section 7.4 of this report covered the compliance of this panel with GDC 19, "Control Room." The aspects of the auxiliary shutdown panel related to Fire Protection 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-2 Action Plan Items

Guidance on implementation of the Action Plan was provided to applicants in NUREG-0737, "Clarification of TMI Action Plan Requirements." 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 (7.5.3)
- (2) II.E.1.2 - Auxiliary Feedwater System Automatic Initiation and Flow Indication (7.3.3.1)
- (3) II.F.3 - Instrumentation for Monitoring Accident Conditions (7.5.3)
- (4) II.K.3.9 - Proportional Integral Derivative Controller Modification (Later)
- (5) II.K.3.12 - Confirm Existence of Anticipatory Reactor Trip Upon Turbine Trip (Later)

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 inserting control rods. The RTS initiates a turbine trip when a reactor trip occurs. The RTS consists of sensors and analog and digital circuitry arranged in coincidence logic for monitoring plant parameters. Signals from 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 direct current undervoltage 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, means also are provided for manual trip by the operator. The manual trip consists of two switches. Actuation of either switch removes power from the undervoltage coils and energize 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 reactor trips listed below are provided in the Shearon Harris design. The numbers in parentheses after each trip function indicate the coincident logic as, 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 ΔT trip (2/3)
 - b. overpower ΔT 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)
 - b. reactor coolant pump undervoltage trip (2/3)
 - c. reactor coolant pump underfrequency trip (2/3)

- (5) Steam generator low-low level trip (2/3)

- (6) low feedwater flow (1/2 steam/feedwater flow mismatch in coincidence with 1/2 low steam generator level)

- (7) turbine trip (anticipatory)
 - a. low auto stop oil pressure (2/3)
 - b. turbine stop valve close (4/4)

(8) safety injection signal actuation trip (2/4, 2/3, or 1/2)

(9) manual trip (1/2)

(10) general warning alarm (2/2)

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 is active only during reactor startup and shutdown when the reactor is below 10% power.

The intermediate range trip provides protection during reactor startup and shutdown when the reactor is below 10% power.

The source range trip provides protection during reactor startup and shutdown when the neutron flux channel is below the P-6 interlock (6×10^{-11} amp).

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

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

The pressurizer high pressure trip is used to protect the reactor coolant system against system overpressure. The same transmitters used for the pressurizer low-pressure trip 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 blocked below approximately 10 percent 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 percent power) a reactor trip will occur if any two loops have low flow. Above the P-8 setpoint (approximately 38 percent power) a trip will occur if any one loop has low flow.

The reactor coolant pump undervoltage trip is provided to protect against the low flow that can result from loss of voltage to the reactor coolant pump motors. Three undervoltage sensing relays are provided for each pump motor. The relays provide an output signal when the voltage falls below approximate 70 percent of rate voltage. Signals from these relays are time-delayed to prevent spurious trips. The reactor coolant pump underfrequency trip is provided to protect against low flow resulting from underfrequency as a result of a major power grid disturbance. One sensing relay is provided for each reactor coolant pump motor (time delayed up to approximately 0.1 sec to prevent spurious trips caused by short term frequency perturbations). Two out of three signals trip the reactor if the power level is above 10 percent power (P-7 interlock).

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

A reactor trip on a turbine trip is actuated by two out of three trip fluid pressure signals or by all (four out of four) closed signals from the turbine steam stop valves. A turbine trip causes a direct reactor trip above 10 percent power (P-7 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 deenergizes the undervoltage coils in each logic train. At the same time the breaker shunt coils in these breakers are energized, which provides a diverse means to ensure that the trip and bypass breakers are tripped.

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

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

The digital portion of the RTS consists of the solid state logic protection system (SSLPS). The SSLPS takes binary inputs (voltage/no voltage) from the

PIS and NIS channels corresponding to normal/trip conditions for plant parameters. The SSLPS utilizes these signals in the required logic combinations and generates trip signals (no voltage) to the undervoltage coils of the reactor trip circuit breakers. The system also provides annunciator, status light, and computer input signals that indicate the condition of the bistable output signals, partial and full trip conditions, and the status of various blocking, permissive, and acutation functions. In addition, the SSLPS includes the logic circuits for testing.

Analog signals derived from protection channels used for nonprotective functions such as control, remote process indication, and computer monitoring are provided by the use of 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 (nonprotective side) will not affect the input signal. The signals obtained from the isolation amplifiers are not returned to the protective system cabinets.

7.2.2 Specific Findings

7.2.2.1 Cable Separation in NSSS Process Cabinets

Preservation of independence and redundancy is achieved in the protection system rack by using isolation amplifiers to separate individual channel inputs from both the control system outputs and the protection system outputs. Westinghouse performed tests to demonstrate that credible faults or electrical interference in cable associated with reactor trip system would not degrade the system performance requirements for the nuclear instrumentation system and the solid state protection system. These tests were made in support of the Diablo Canyon license application. Similar tests were made by Westinghouse on the 7300 series process control system were presented in Westinghouse topical report WCAP 8892A, "7300 Series Process Control System Noise Tests." The staff has reviewed and approved the procedures for and results of these reports. All cables external to the reactor trip system racks are installed to satisfy the requirements specified in the Westinghouse test reports.

7.2.2.2 Trip Setpoint and Margins

The setpoints for the various functions in the reactor trip system are determined based on the accident analysis requirements. As such, during any anticipated operation and occurrence, the reactor trip system limits the following parameters to:

- (1) Minimum departure from nucleate boiling ratio of 1.30
- (2) Maximum system pressure of 2750 pounds per square inch (absolute)
- (3) Fuel rod maximum linear power of 18.0 kilowatts per foot

The reactor trip system bistable setpoints are established considering the following:

- (1) Safety limit setpoint - value assumed in the accident analysis
- (2) Limiting setpoint - Technical Specification value
- (3) Normal setpoint - value set into the equipment and obtained by subtracting allowance for instrument drift, calibration uncertainty, transmitter error and base starting margin from the limiting setpoint

The detailed trip setpoint review will be performed as part of our review the plant Technical Specifications and will be completed prior to issuance of the operating license. The applicant was requested to provide an evaluation and/or an analysis of the effect of post-accident environmental conditions on the setpoint for the reactor trip system instrumentation (Technical Specification Table 2.2-1), and the engineered safety feature actuation system instrumentation (Technical Specification Table 2.2.2). The margins from the normal setpoint to the limiting setpoint should include the instrument drift, calibration uncertainty, transmitter error and base starting margin. This

item is being pursued with the applicant. Additional information and formal documentation is required.

7.2.2.3 Response-Time Testing

To ensure that the response time of each protective function of the reactor trip system and ESFAS is within the time limit assumed in the accident analyses, the Technical Specification requires response time testing at specified intervals. This aspect of the design will be reviewed when the plant test procedures are available for review. Consideration on lead, lag, and rate time constant for the setpoints should also be incorporated. Additional information and formal documentation is required.

7.2.2.4 Independent Verification of the Operability of Reactor Trip Breaker Shunt and Under-Voltage Coils

I&E Circular 81-12, "Inadequate Periodic Test Procedure for PWR Reactor Protection System dated July 22, 1981 was issued to all nuclear power reactor facilities holding an operating license or a construction permit. The Circular recommended that the procedures for surveillance testing of reactor trip circuit breakers provide independent testing of shunt and undervoltage coils. Further the circular noted that if trip circuit breakers do not have provisions for independent testing of each trip function then appropriate modifications should be made to include such features.

In the review of operating license applications, the Instrumentation and Control Systems Branch staff has discussed with applicants the concern for independently verifying the operability of shunt and undervoltage coils of reactor trip breakers. The staff conclusion is that the diverse features of reactor trip breakers (shunt and undervoltage coils) provide an additional degree of reliability for assuring the ability to trip the reactor. Further, surveillance procedures should independently verify the operability of these diverse features. The staff concludes that it would be unacceptable if the operability of one of these diverse features was not confirmed during the normal 40 year life of a plant. Thus the staff position is:

A function test of the undervoltage and shunt trips shall be conducted every 18 months and following adjustment or maintenance of the reactor trip breaker to independently verify the operability of the breaker to perform its safety function in response to a trip signal for each of these diverse trip features.

This requirement would be in addition to those surveillance requirements for reactor trip breakers covered in the plant technical specifications. The present Shearon Harris design does not allow the shunt trip to be independently tested. This item is being pursued with the applicant. Additional information and formal documentation is required.

7.2.2.5 Turbine Trip Following Reactor Trip

The interface design between NSSS and BOP scope of supplies is not clear. The applicant will reevaluate the turbine trip circuitry and logic. Additional information and formal documentation is required.

7.2.2.6 Low Feedwater Flow Trip

This trip is actuated by steam/feedwater flow mismatch in coincidence with low water level in any steam generator. However, the main feedwater flow elements are located in the turbine building. The instrument lines do not satisfy the safety grade requirements. It is the staff's position that all inputs to the Reactor Trip system must be seismically and environmentally qualified and conform to the requirements of IEEE standard 279-1971. Additional information is required to address this concern.

7.2.3 Evaluation Conclusion

LATER

7.3 Engineered Safety Features (ESF) System

7.3.1 System Description

The Engineered Safety Features Actuation System (ESFAS) is a portion of the plant protection system which monitors selected plant parameters and upon 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 which 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) Safety state and relay logic
- (3) Engineered safety features test circuits
- (4) Manual actuation circuits.

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 which receive inputs from the analog protection channels and perform the logic to actuate the ESF equipments. The ESFAS is composed of a nuclear steam supply system portion designed by Westinghouse and a balance-of-plant portion designed by Ebasco Services, Incorporated.

There are seven ESFAS actuation functions in the Sharon Harris design. The initiation signals for each of the ESFAS functions are as follows. The

numbers in parentheses after each initiation channel indicate the coincident logic, as for example, two-out-of-four (2/4).

(1) Emergency Core Cooling Actuation (Safety Injection "S" Signal)

- a. Low pressurizer pressure (2/3)
- b. Low steam line pressure (2/3 in any line)
- c. High containment pressure (HI-1) (2/3)
- d. Manual actuation (1/2)

(2) Containment Isolation Phase A Actuation ("T" Signal)

- a. Safety injection "S" signal
- b. Manual actuation (1/2)

(3) Containment Spray System Actuation and Containment Isolation Phase B Actuation ("P" Signal)

- a. High containment pressure (HI-3) (2/4)
- b. Manual actuation (2/4)

(4) Main Steam-Line Isolation Actuation

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

(5) Feedwater Line Isolation Actuation

- a. Safety Injection "S" signal
- b. Steam generator high level (2/3 in any generator)
- c. Low T_{avg} (2/3) coincident with reactor trip

(6) Auxiliary Feedwater System Actuation

- a. Safety injection "S" signal
- b. Steam generator low low level (2/3 on any generator)
- c. Blackout signal (complete loss of offsite electric power).
- d. Loss of both main feedwater pumps

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

- a. Low low level in two steam generators
- b. Blackout signal

(7) Containment Combustible Gas Control Manual Actuation (1/2)

The essential auxiliary support (EAS) systems are as follows:

- (1) On-Site Power Supply System
- (2) Emergency Service Water System
- (3) Component Cooling Water System
- (4) Essential Services Chilled Water System
- (5) 120V AC Plant Protection Power System
- (6) Safety Related 125V DC Power System
- (7) Control Room Air Conditioning System
- (8) RAB Equipment Cooling System
- (9) Diesel Generator Building Ventilation System

- (10) RAB Switchgear Room Ventilation System
- (11) Emergency Exhaust Systems
- (12) Spent Fuel Pool Pump Room Ventilation System
- (13) RAB Electrical Equipment Protection Room Ventilation System
- (14) Fuel Oil Transfer Pump House Ventilation System
- (15) Emergency Service Water Intake Structure Ventilation System

7.3.2 ESF and EAS System Operation

7.3.2.1 Emergency Core Cooling System Actuation

The Emergency Core Cooling System (ECCS) cools the reactor core and provides shutdown capability for pipe breaks in the Reactor Coolant System (RCS) which cause a loss of primary coolant greater than that which can be made up by the normal makeup system, for rod cluster control assembly ejection, for pipe breaks in the 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 centrifugal charging (safety injection) and residual heat removal pumps, accumulators, residual heat removal heat exchangers, refueling water storage tank (RWST), and boron injection tank with the associated piping, valves and instrumentation.

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

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

- (1) Starts centrifugal charging pumps (safety injection)
- (2) Opens RWST suction valves to charging pumps
- (3) Opens boron injection tank inlet and outlet discharge parallel isolation valves
- (4) Closes normal charging path valves
- (5) Closes charging pump miniflow valves
- (6) Closes boron injection tank recirculation valves
- (7) Stops boron injection tank recirculation pumps
- (8) Starts residual heat removal pumps
- (9) Closes volume control tank outlet isolation valves
- (10) Opens any closed accumulator isolation valves

Switchover from the injection mode to recirculation involves the following interlocks. The changeover from the injection mode to recirculation mode is initiated automatically and completed manually by operator action from the main control room. Protection logic is provided to automatically open the two containment sump isolation valves when refueling water storage tank level (two out of four) reaches a low-low level setpoint in conjunction with "S" signal. This automatic action will align the two residual heat removal pumps to take suction from the containment sump and deliver water directly to the RCS.

The charging pumps (safety injection) will continue to take suction from the refueling water storage tank following the above automatic action, until

manual operator action is taken to align these pumps in series with the residual heat removal pumps. A spare charging pump is provided to allow continued plant operation when one of the two charging pumps is out of service.

7.3.2.2 Containment Isolation System (CIS) Actuation

The function of the Containment Isolation System is to isolate nonessential lines which pass through the containment boundary. The Containment Isolation System is designed to limit the release of radioactivity emissions from the containment during abnormal events and accidents.

The Containment Isolation System is automatically actuated by signals developed by the Engineered Safety Features Actuation System in two phases: Phase A containment isolation and Phase B containment isolation. Phase A isolates all nonessential process lines penetrating the containment. Phase B isolates all other process lines not included in Phase A containment isolation, except the safety injection and containment spray lines.

Containment isolation valves, that are equipped with power operators and are automatically actuated, may also be controlled individually by positioning hand switches in the control room. Containment isolation valves with power operators are provided with an open/closed indication, which is displayed in the control room at the main Control Board and the Status Panel. All electric power supplies and equipment necessary for containment isolation are Class 1E.

7.3.2.3 Containment Spray System (CSS) Actuation

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

The CSS has two phases of operation, which are initiated sequentially following system actuation; they are the injection phase and the recirculation phase.

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

7.3.2.4 Main Steam Line Isolation Actuation

The main steam line isolation signal is generated on low steam line pressure or high high containment pressure. A manual block permissive is provided for the low steam line pressure signal for use during normal plant cooldowns and heatups. A high rate of steam line pressure decrease is used to initiate main steam isolation when the low steam line pressure signals are blocked during normal plant start up and shutdown. The block of the low steam line pressure signal is automatically removed and the high rate signal is automatically blocked when the pressurizer pressure is above a preset value. Stored energy for closing the main steam line isolation valves is supplied by pneumatic/hydraulic accumulators. Hydraulic fluid is pumped into the valve actuator to open the valve against a pressurized pneumatic system. The valve is closed by pneumatic pressure when the hydraulic fluid pressure is relieved. A dual hydraulic control system is provided to ensure redundancy. The main steam isolation valve is capable of being tested on-line by partial closure of the valve.

7.3.2.5 Feedwater Line Isolation Actuation

Feedwater line isolation is provided to terminate main feedwater following a pipe rupture or excessive feedwater event. The feedwater line isolation signal is generated on safety injection, high steam generator water level, or low reactor coolant temperature coincident with reactor trip. Upon receipt of this signal, the main feedwater isolation valves and other valves associated with the main feedwater lines are closed. Redundant actuation systems are provided for each valve operator and receive closure signals from the two redundant ESFAS trains.

7.3.2.6 Auxiliary Feedwater System

The function of the auxiliary feedwater system (AFS) is to provide an adequate supply of water to the steam generators in the event the main feedwater system is not available. The AFS consists of two motor driven pumps and one turbine driven pump with associated valves, controls, and instrumentation. The motor driven supply is independent of the turbine driven supply for each steam generator. The two supplies connect together in the containment at the auxiliary feedwater nozzle on the steam generator. The auxiliary feedwater actuation system will automatically start the pumps and position the valves to provide feedwater to the steam generators. The initiating conditions are listed in Section 7.3.1, item (6). The AFW pump suction is normally supplied from the seismic Category I condensate storage tank. It can be remote manually aligned to take suction from the Emergency Service Water system.

The AFS can be manually initiated and controlled from the main control board or the auxiliary shutdown panel. The AFS control is addressed in section 7.4 of this report.

The AFS has automatic isolation logic to terminate auxiliary feedwater to a faulted steam generator. The detailed design evaluation will be addressed in Section 7.4.1.3 of this report.

7.3.2.7 Combustible Gas Control System

The combustible gas control system controls the buildup of hydrogen gas inside the containment. The combustible gas control system consists of hydrogen monitoring, hydrogen recombiners, and hydrogen purge system. The hydrogen monitoring system has redundant and separate hydrogen analyzers located outside containment. Each analyzer is powered from an independent outside power source. Two hydrogen recombiners are manually controlled and are located inside containment. The design meets functional requirements in the postaccident containment environment including seismic Category I criteria. The two hydrogen recombiners are powered from separated safeguard buses. The containment hydrogen purge system is provided as a backup means of controlling hydrogen inside the containment

building. It consists of a purge makeup penetration line, an exhaust penetration line and a filtered exhaust system which discharges to the vent stack. The hydrogen purge system would be used only if the recombiners were ineffective.

7.3.2.8 Onsite Power Supply System

The onsite AC power system consists of two 6.9 KV diesel generators, two 6.9 KV ESF buses, various ESF and non-ESF 480 V buses, motor control centers, and 208/120V power panels. The DC power system consists of two safety 125V batteries, one non-safety 125V battery and one non-safety 250V battery, each with its own battery chargers, and DC load center. There are four 120V AC safety related power distribution panels for safety related vital instrumentation and control loads. Each power panel has separate rectifier/inverter.

7.3.2.9 Emergency Service Water System

The normal service water pumps take suction from the cooling tower basin. If both cooling towers are inoperative, service water will be provided by the emergency service water pumps. Only equipment essential to accident mitigation or safe plant shutdown will be supplied by the emergency service water system. The emergency service water pumps take suction from either main reservoir or auxiliary reservoir. The emergency service water system is designed to seismic Category I requirements. The non-safety related parts of the service water system will be automatically isolated during emergency operation by a safety injection actuation signal.

7.3.2.10 Component Coolant Water System

The component cooling water (CCW) system provides an intermediate closed cooling loop for removing heat from reactor plant auxiliary systems and transferring it to the service water system. Two 100 percent redundant CCW loops are provided. One installed spare pump can be manually connected to either CCW loop and supplied emergency power from the source associated within that loop.

7.3.2.11 Essential Service Chilled Water System

The essential service chilled water system provides chilled water to various safety related air conditioning systems in the auxiliary building. It consists of two 100 percent systems which are powered from redundant emergency buses. The non-essential portions of the chilled water system are automatically isolated from the essential portions upon receipt of an safety injection actuation signal.

7.3.2.12 Control Room Area Ventilation System

The control room area ventilation system is designed to maintain suitable control room temperature and humidity for continuous plant operation, to detect the radioactive material, chlorine, or smoke in the control room, and to automatically isolate the control room on detection of the above hazardous conditions. The control room area ventilation system serves both Unit 1 and 2 control rooms. The system consists of four 50 percent capacity air handling units, four 50 percent exhaust fans, four 50 percent capacity purge fans, and two 100 percent capacity filtration systems.

7.3.2.13 Engineered Safety Feature Ventilation System

The ESF ventilation systems consist of auxiliary building ESF equipment cooling, switchgear room ventilation, fuel oil transfer pump house ventilation, diesel generator building ventilation, emergency service water intake structure ventilation, and spent fuel pool pump room ventilation. The ESF ventilation system is designed to serve all areas containing equipments essential for accident mitigation and safe shutdown.

7.3.2.14 Containment Vacuum Relief System

There are two redundant vacuum relief trains. Each of the redundant trains has a butterfly valve that can be remotely operated by a control switch in the Control room. Each train is automatically controlled based on negative containment building pressure between 0.25 and 2.5 inches water gage. The butterfly valve

and damper will close and be prevented from opening when a containment isolation signal is present.

7.3.3 Specific Findings

7.3.3.1 Auxiliary Feedwater Automatic Initiation and Flow Indication (TMI-2 Action Plan Item II.E.1.2)

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 IE power sources. The initiation signals and circuits are testable during power operation and the test requirements are included in the plant Technical Specification. Manual initiation and control can be performed from the main control board or the auxiliary 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 of this system is addressed in section 3.11 of this report.

One auxiliary feedwater flow indicator and one wide range level indicator are provided for each steam generator. The level and flow indication for two steam generators are powered from the class IE Channel A power source, and the other from the Channel B power source. The staff concludes that Shearon Harris design satisfies the requirements of TMI-2 Action Plan Item II.E.1.2.

7.3.3.2 System Level ESF Manual Initiation Capability

IEEE Standard 279-1971 requires that the protection system shall include means for manual initiation of each protective action at the system level. Manual initiation should depend upon the operation of a minimum of equipment. In Shearon Harris design, some of the protection systems do not have system level ESF manual initiation capability. These protection systems include the feedwater line isolation, containment ventilation isolation, control room isolation, FHB ventilation isolation, RAB ventilation isolation, and

auxiliary feedwater isolation. This concern is being pursued with the applicant and its resolution will be addressed in a supplement to this report.

7.3.3.3 Test of Engineered Safeguards P-4 Interlock

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

In order to minimize the possibility of accidental shorting or grounding of safety system circuits during testing, suitable test jacks should be provided to facilitate testing of the P-4 interlocks. The applicant has been requested to provide a discussion on how the above issue will be resolved. This concern is being pursued with the applicant and its resolution will be addressed in a supplement to this report.

7.3.3.4 IE Bulletin 80-06

As was done for operating reactors through IE Bulletin 80-06, the staff requested that the applicant review all safety systems to determine if any safety equipment would change state after reset. Since the applicant has not responded to this concern, its resolution will be addressed in a supplement to this report.

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

The staff requested the applicant to evaluate the effects of high temperatures in reference legs of water level measurement after high energy line breaks. This issue was addressed for operating reactor through IE Bulletin 79-21. Since the applicant has not responded to this concern, its resolution will be addressed in a supplement to this report.

7.3.3.6 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 and one of the three level channels is used for control. This design for actuation of feedwater isolation does not meet 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. Since the applicant has not responded to this concern, its resolution will be addressed in a supplement to this report.

7.3.3.7 Containment Spray System Chemical Additional Control

The containment spray system cools the containment atmosphere and removes the fission products after a LOCA event. The staff has identified the concerns on the adequacy of the instrumentation for terminating sodium hydroxide addition in the containment spray system and the capability to test the spray additive tank isolation valves. Since the applicant has not responded to this concern, its resolution will be addressed in a supplement to this report.

7.3.3.8 Non-Class IE Inputs to Class IE Control Circuits

In response to a staff request, the applicant provided a list of non-class IE control signals that are used as inputs to class IE control circuits. The applicant stated that all of non-class IE signals are through an isolation device before signals are input to class IE control circuits. Schematic drawings related to these circuits to verify the adequacy of the isolation scheme have been requested. This matter is subject to further staff review.

7.3.3.9 Spare Pump in Component Cooling Water System

A spare CCW pump is provided to allow continued plant operation when one of the two CCW pumps is out of service. The spare pump can replace either pump in the redundant CCW loops and still maintain the required redundancy in electrical

power supply and control. The spare pump has a dual breaker arrangement so that it can be powered and started from the same electrical sources as the pump it replaced. It is interlocked so that it cannot be connected to both redundant power sources at the same time. Interlocks are provided to assure that both pumps (normal and spare) are not started automatically which could lead to overloading the emergency power bus. The staff has reviewed the design and finds it to be acceptable. However, the interlocks and the circuit breakers should be tested periodically under Technical Specification surveillance requirement. This matter will be addressed during the staff review of the proposed Technical Specifications. The staff has requested that the applicant provide a control scheme of the service water to the component cooling water heat exchanger to ensure that the power supply and control of service water are from the same power source as the CCW pump it replaced. This matter is subject to further staff review.

7.3.3.10 Spare Charging Pump

The applicant has stated that there are three centrifugal charging pumps in Shearon Harris design. The spare pump is considered as swing pump which can replace either of the pumps used for safety injection. However, no description has been provided in the FSAR to address how redundancy in electrical power supply and control is obtained when the spare pump is used. The applicant has been requested to provide information which demonstrates that this design satisfies applicable regulatory requirements. This matter is subject to further staff review.

7.3.3.11 BOP System Isolation Devices Testing

The staff has reviewed the results of analysis and tests performed to demonstrate proper isolation between separation groups and between safety and non-safety systems. The staff has requested additional information to justify the adequacy of the test program for isolation devices. This matter is subject to further staff review.

7.3.3.12 SSLPS Test Circuits

On August 6, 1982, the Westinghouse informed NRC under 10 CFR 50.55(e) that a potential significant deficiency was identified in the Solid State Logic Protection System (SSLPS) test circuits.

During testing of the master relays, the voltage applied to the slave relay is reduced from 120 vac to 15 vdc to preclude their operation during this phase of the testing. Also during this test a light is placed in series with the master relay contact which is normally used to pick up the slave relays. Upon completion of these tests the light used to confirm the continuity of master relay contacts and slave relay coil is removed from the circuit. The problem revealed is that these tests do confirm that the continuity light is removed from the circuit. If the light remained in series with the slave relay coil the operability of the protective action would not be assumed. The staff review of this matter is pending the applicant's proposal to resolve this concern.

7.3.3.13 Failure Modes and Effects Analyses (FMEA) of ESFAS

The description of the Engineered Safety Feature Actuation System (ESFAS) analysis, which is provided in the FSAR Section 7.3.2.1, is incomplete. It does not provide all of the information required by R.G. 1.70 Section 7.3.2 of the standard format, which demonstrates how the requirements of the general design criteria and IEEE standard 279-1971 are satisfied and the extent to which the recommendations of the applicable Regulatory Guides are satisfied. The applicant has referred to the Failure Modes and Effects Analysis referenced in FSAR Section 7.2.2 and Table 7.3.1-1. The staff has requested the applicant to confirm that this FMEA:

- (1) is applicable to all engineered safety features equipment within the BOP and NSSS scope of supply,
- (2) is applicable to design changes subsequent to the design analyzed in the referenced WCAP, and

(3) interface requirements have been met.

The staff review of this matter is pending the applicant's response to the concern identified.

7.3.4 Evaluation Conclusion

LATER

7.4 System 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 located outside the main control room that enable safe shutdown of the plant in the event the main control room is evacuated.

7.4.1.1 Safe Shutdown System

The systems required for safe shutdown are those required to control the reactor coolant system temperature and pressure, to borate the reactor coolant, and to provide adequate residual heat removal. Equipment used for the identified mode of shutdown includes:

(1) Hot Standby

- a. Auxiliary feedwater pumps and associated valves
- b. Boric acid transfer pumps and associated valves
- c. Steam generator safety valves
- d. Reactor coolant charging pumps and letdown orifice valves
- e. Pressurizer heaters
- f. Pressurizer sprays
- g. Steam generator PORVs

Items (e), (f) or (g) are desirable, but not required to maintain hot standby conditions.

(2) Hot Shutdown

- a. Auxiliary feedwater pumps and associated valves
- b. Boric acid transfer pumps and associated valves
- c. Steam generator PORVs
- d. Reactor coolant charging pumps and letdown orifice valves

- e. Residual heat removal pumps and associated valves
- f. Pressurizer heaters and sprays

Item (f) is desirable, but not required to maintain hot shutdown conditions.

(3) Cold Shutdown

- a. Residual heat removal pumps and associated valves
- b. Boric acid transfer pumps and associated valves
- c. Reactor coolant charging pumps and letdown orifice valves
- d. Reactor coolant pumps

Item (d) is desirable, but not required to reach cold shutdown conditions.

(4) The Supporting Systems and Associated Equipment Required for All Modes of Shutdown:

- a. Component cooling water system
- b. Service water system
- c. Onsite power supply system
- d. Diesel generator fuel oil storage and transfer system
- e. Safety related HVAC systems
- f. Control room panels or auxiliary control panels
- g. Emergency lighting

To achieve and maintain safe shutdown, the reactor and the turbine are tripped. Automatic protection and control system functions are discussed in Sections 7.2 and 7.3. The controls and the indicators for all of the equipment listed above are provided in the main control room. In addition, an auxiliary control panel is provided that allows the plant to be maintained in a hot shutdown condition or taken to cold shutdown should the main control room become uninhabitable.

7.4.1.2 Remote Shutdown Capability

If temporary evacuation of the control room becomes necessary, an auxiliary shutdown panel located outside the control room is provided to bring the plant to a hot standby condition. The plant can also be taken to cold shutdown from outside the control room by using instrumentation and controls on the auxiliary shutdown panel in conjunction with local control stations and local manual actions. Two transfer panels are provided for the two safety trains. The transfer of control, by the transfer panels, will arm the controls of the respective electrical trains on the auxiliary shutdown panel. Control will take place only when the switch at auxiliary shutdown panel is activated. The transfer panels are designed as enclosed cabinets and all controls are mounted inside. Opening of the cabinet activates an alarm on the main control board. The auxiliary shutdown panel and the two transfer panels are designed in accordance with class IE requirements and are located in three separate fire zones.

The instrumentation on the auxiliary shutdown panel has sufficient backup controls and indications to satisfy the single-failure criterion.

7.4.1.3 Auxiliary Feedwater Control

The staff's review on the auxiliary feedwater system include the following consideration:

- (1) Automatic initiation (discussed in section 7.3)
- (2) Capability of controlling flows to establish and maintain steam generator level
- (3) Capability of controlling the steam generator pressure
- (4) Capability of isolating a faulted steam generator resulting from feedwater or steam line breaks
- (5) Capability for post trip control from auxiliary shutdown panel

Steam generator level is manually controlled by positioning the auxiliary feedwater regulating valves. The two motor driven pumps and their associated controls are redundant and powered from safety train A and B, respectively. The auxiliary feedwater pump turbine is driven by steam supplied from the main steam piping of two steam generators. The pump speed is automatically controlled by the differential pressure between pump discharge pressure and the turbine steam inlet pressure. Manual speed control can be performed at main control board or auxiliary control panel.

During plant colddown, the main steam Power Operated Relief Valves (PORV) are automatically controlled by steamline pressure with remote manual adjustment of the pressure setpoint from the control room or the auxiliary shutdown panel. Manual adjustment of the auxiliary feedwater flowrate and steam generator pressure setpoint is used to control cooldown rate.

The Shearon Harris design has a system to terminate AFW to a faulted steam generator. The detailed design has not been completed at the present time. Staff review of this system will be addressed in a supplement to this report.

7.4.2 Specific Findings

7.4.2.1 Auxiliary Feedwater System

The design of the auxiliary feedwater system has not been completed at present time. Additional information and formal documentation is required in following areas:

- (1) The capability to isolate a faulted steam generator
- (2) Design change on steam inlet valves to the auxiliary feedwater pump steam turbine
- (3) Design change on auxiliary feedwater flow control valves

- (4) Reliability analysis on auxiliary feedwater system (TMI Action Item 2.E.1.1)

7.4.2.2 Capability to Achieve Cold Shutdown

The Shearon Harris design uses the steam generator PORVs in conjunction with the auxiliary feedwater system to allow the plant to be cooled from the pressure setpoint of the lowest safety valve setting down to the point where the Residual Heat Removal (RHR) system can be placed in service. However, the PORVs are located in the steam tunnel and the PORV actuator is only qualified to 165°F (the steam tunnel normal temperature is around 105°F). The staff has a concern that the PORV may not function under a postulated steam line break accident in the steam tunnel, therefore, the plant may not be able to achieve cold shutdown. This item is being pursued with the applicant. Additional information is required.

7.4.2.3 Testing for Remote Shutdown Operation

During the review process, a concern was raised by the staff regarding the remote shutdown capability and the need for a test to verify design adequacy. The applicant stated that emergency procedures will be prepared to include remote shutdown and a test will be conducted during startup testing to confirm the capability for remote shutdown. This item is confirmatory, subject to confirmation that this test has been successfully completed.

7.4.3 Evaluation Conclusion

LATER

7.5 Information System Important to Safety

7.5.1 Description

The safety-related display instrumentation systems provide the information necessary for the operator to perform the required manual safety functions

following a reactor trip. Information that the operator needs to maintain the plant in a hot standby condition or to proceed to cold shutdown within the limits of the Technical Specifications is also displayed. The operator uses these information systems to monitor conditions in the reactor, the reactor coolant system, the containment and the process systems during normal operation of the plant, including anticipated operational occurrences, and for postaccident monitoring. The display system also include bypassed and inoperable status information.

The following information systems are provided.

- (1) Plant process display instrumentation
- (2) Reactor trip system monitoring
- (3) Engineered safety features system monitoring
- (4) ESF support systems monitoring
- (5) Auxiliary control panel instrumentation
- (6) Control rod position indication system
- (7) Safe shutdown monitoring system
- (8) Post accident monitoring instrumentation
- (9) Bypassed and inoperable status indication
- (10) Control board annunciation and light boxes

The bypass and inoperative status indication for the Shearon Harris design is in conformance with Regulatory Guide 1.47. The bypass indication on the bypass panel is arranged for the ESF and the essential auxiliary support system

on a train basis. The system bypass indication will be indicated automatically whenever an ESF system is bypassed or becomes inoperable due to loss of control power or valve not in a proper position. Bypassed or inoperable condition can be actuated/reset manually by the operator by depressing the system window push-button. The subsystem level bypassed and inoperable status will be monitored by the plant computer system.

The postaccident monitoring system is designed to monitor plant variables during and following an accident. Instrumentation provided for the monitoring of post-accident parameters is qualified for operation in post accident environmental and seismic conditions. The instruments are powered from the 120V AC instrument buses which are normally energized from the onsite emergency busses. Each channel is powered from a separated power supply.

The following systems parameters are included in the postaccident monitoring system.

- (1) Reactor coolant COLD LEG and HOT LEG temperature (loops 1 and 2 only)
- (2) Pressurizer water level
- (3) Reactor coolant pressure (wide range)
- (4) Containment pressure
- (5) Steam line pressure
- (6) Steam generator water level (wide range)
- (7) Steam generator water level (narrow range)
- (8) Component cooling water heat exchanger discharge pressure
- (9) Component cooling water surge tank level

- (10) Component cooling water heat exchanger discharge temperature
- (11) Refueling water storage tank level
- (12) Containment spray pump A and B discharge header pressure
- (13) Auxiliary feed water flow to steam generator
- (14) Auxiliary feed water pumps A and B discharge pressure
- (15) Turbine auxiliary feedwater pumps discharge pressure
- (16) Emergency service water pumps A and B discharge pressure
- (17) Service water pumps A and B header flow
- (18) Service water booster pumps A and B pressure
- (19) Service water booster pumps A and B flow
- (20) Diesel generators A and B voltage
- (21) Diesel generators A and B field voltage
- (22) Diesel generators A and B current
- (23) Batteries A and B voltage
- (24) Containment sump level

7.5.2 Loss of Non-Class IE Instrumentation and Control Power System Bus During Operation (IE Bulletin 79-27)

The staff requested that the applicant review the adequacy of emergency operating procedures, to be used by control room operators to attain safe

shutdown on loss of any class IE or non-class IE buses supplying power to safety or nonsafety related instrument and control systems. This issue was addressed for operating reactor through IE Bulletin 79-27.

The applicant has not responded to this request. Additional information is required.

7.5.3 TMI Action Plan Items

II.D.3 Direct Indication of Relief and Safety Valve Positions

Each of the three pressurizer safety relief valves is equipped with a reed type switch which provides a position indication (open or closed) in the control room. An alarm is provided in conjunction with this indication. The valve position indication is powered from a vital instrument bus. The code safety valve position is derived from reed type switches mounted on the valve top. The safety valves positions are displayed on the Safety Parameter Display System (SPDS) CRT located on the main control board. The resistance temperature detectors (RTD) are provided as the backup device to detect if there is valve seat leakage. The RTD will actuate on annunciator on the main control board.

The valve position indicating switch will be seismically qualified. However, the FSAR has not addressed the environmental qualification status. The staff has requested that the applicant confirm that the reed switch will be qualified for its appropriate environment. Additional information is required.

II.F.3 Instrumentation for Monitoring Accident Conditions (Regulatory Guide 1.97, Rev. 2)

The Commission has instructed the staff to use SECY-82-111 (Supplement 1 of NUREG-0737) in implementation of Emergency Response Capability (including requirements for postaccident monitoring). Therefore, conformance to the guidelines of Regulatory Guide 1.97, Revision 2 will be included in the evaluation of designs for the emergency support facilities. The implementation schedule will be established in conformance with Supplement 1 of NUREG-0737. The com-

pletion of the review of this item will be performed during the post implementation review discussed under TMI Action Plan Item III.A.1.2, Upgrading Emergency Support Facilities.

7.5.4 Evaluation Conclusions

LATER

7.6 Interlock Systems Important to Safety

7.6.1 Interlock Description

This section addresses the safety related interlocks which:

- (1) Prevent the overpressurization of low-pressure systems
- (2) Prevent the overpressurization of the primary coolant system during low temperature operation
- (3) Assure the availability of ECCS accumulators
- (4) Automatically open sump isolation valves for recirculation mode of operation

The objectives of the review has to confirm that design considerations such as redundancy, independence, single failures, qualification, bypasses, status indication, and testing are consistent with the design bases of these safety related systems.

7.6.2 Specific Findings

7.6.2.1 Residual Heat Removal (RHR) System Isolation Valves Interlock

The RHR isolation valve interlocks are provided to prevent overpressurization of the RHR system. There are two motor operated valves in series in each of

the two residual heat removal pump suction lines from the reactor coolant system hot legs. Separate and diverse pressure transmitters powered from separate safety power trains are used for the isolation valve interlocks. Each valve is interlocked to prevent opening if RCS pressure is greater than 425 psig and to automatically close if RCS pressure exceeds 750 psig. Valve position indication is provided in the control room.

The redundant valve interlock design include independence, separation, and diversity satisfies the Branch Technical position ICSB 3, "Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System."

7.6.2.2 RCS Pressure Control During Low Temperature Operation

The limiting pressure conditions for the reactor vessel is a function of temperature. The pressurizer power operated relief valves setpoint is reduced during low temperature operation. There are two trains of instrumentation in the RCS pressure control logic. Train A instruments monitor the RCS hot leg temperatures to generate a reference pressure setpoint. If the Train A monitored RCS pressure is greater than the setpoint, the logic will open the A train PORV and give a permissive for the B train PORV to open. The B train instruments monitor the RCS cold leg temperatures to generate its reference pressure setpoint. If the Train B monitored RCS pressure is greater than the setpoint, the logic will open the Train B PORV and give a permissive for the Train A PORV to open. The intent of this control logic is to prevent an inadvertent opening of either PORV. The staff has concern that a single failure in the auctioneering device used to determine the lowest loop temperature could prevent both "PORV A" and "PORV B" to open when required. This item is being pursued with the applicant. Additional information is required to demonstrate that the design satisfies the single failure criterion.

7.6.2.3 Accumulator Isolation Valves Interlock

A motor operated isolation valve is provided at each accumulator outlet. These valves are normally open during the plant operation. To prevent an inadvertent closing of these valves power is removed from the valve motor circuit breakers.

Administrative control is required to ensure that power is restored to the valve circuit breakers during plant shutdown. These valves are interlocked such that:

- (1) They open automatically on receipt of a safety injection signal.
- (2) They open automatically whenever the RCS pressure is above SI unblock (P-11) setpoint.
- (3) They cannot be closed as long as the safety injection signal is present.

Administrative controls require the performance of a periodic check valve leakage test. The interlock will assure that the safety function is maintained during the test.

There are two sets of valve position indicating lights on the main control board. One set of lights is operated by valve motor limit switch and the other set is actuated by valve stem limit switch. An alarm will also sound when either of the limit switch senses that the valve is not fully open. The staff is concerned that when the valve power is locked out during normal operation, the control power is removed from one set of position indication. Therefore, the valve position and alarm would not satisfy the single failure criterion. This item is being pursued with the applicant. Additional information is required.

7.6.2.4 RHR Recirculation System Sump Isolation Valves Interlock

This interlock is provided to automatically open the four safety injection system recirculation sump isolation valves (two series valves per train) when two out of four refueling water storage tank (RWST) level reaches the low low level setpoint after safety injection actuation. The valve cannot be closed as long as an SI signal is present. The interlock from SI signal can be removed by a reset switch which is separate from the system level safety injection reset switch. The interlock reset switch only resets the slave relay in the solid state protection system output cabinet. The purpose of this reset capability is to permit the operator to remove the actuation signal in the event the corresponding sump isolation

valve must be closed and maintained in a closed position following a LOCA. The staff finds the design acceptable.

7.6.3 Evaluation Conclusion

LATER

7.7 Control Systems

7.7.1 Description

The plant control systems that are not relied on to perform safety functions but which control plant processes having an impact on plant safety are described in this section and include the following:

- (1) Rod control system
- (2) Plant control interlocks
- (3) Pressurizer pressure and level control
- (4) Steam generator water level control
- (5) Steam dump control
- (6) Safety instrumentation freeze protection

The rod control system provides for reactor power modulation by manual or automatic control of control rod banks in a preselected sequence. It displays control rod positions, alerts the operator in the event of control rod deviation exceeding a preset limit and alerts the operator on inadequate shutdown margins due to excessive control rod insertion. The automatic rod control system is designed to maintain a programmed average temperature in the reactor coolant by regulating the reactivity within the core. The system is capable of restoring reactor coolant average temperature to within $\pm 3.5^{\circ}\text{F}$ of the programmed temperature. The automatic rod control is performed between 15 and 100 percent of rated power.

The plant control interlocks prevent further withdrawal of the control rod banks either by a control system malfunction or an operator error. The interlocks are derived from nuclear instrument channels or RC overtemperature, overpower channels. The interlocks also limit automatic turbine load increases

during a rapid return to power transient (through the negative moderator coefficient). The interlock can be cleared by an increase in coolant temperature which is accomplished by reducing the boron concentration in the coolant.

The RC pressure is controlled by using either the heaters or the spray of the pressurizer plus PORV steam relief for large transients. The water inventory in the RCS is maintained by the CVCS. During normal plant operation, the charging flow varies to match the flow demanded of the pressurizer water level controller. The pressurizer water level is programmed as a function of coolant average temperature. During startup and shutdown operations, the charging flow is manually regulated to maintain pressurizer water level.

The steam generator level is programmed by a three-element feedwater controller, which regulates the feedwater valves by continuously comparing the feedwater flow signal, the water level signal, the programmed level set point and the steam flow signal. An override signal closes all feedwater valves when the RC T_{avg} is below setpoint and the reactor has tripped. During startup or low power operation, a feed-forward control scheme which uses steam generator level and nuclear power signals to position a bypass control valve which is in parallel with the main feedwater regulating valve.

The steam dump system is designed to accept a 100 percent load rejection without tripping the reactor. The system functions automatically by bypassing steam directly to the condenser and/or atmosphere to maintain an artificial load on the primary system. The rod control system can then reduce the reactor coolant 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 RC reference average temperature (based on turbine impulse chamber pressure) and the measured RC average temperature exceeds a preset value. To prevent actuation of steam dump on small load perturbation, 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. The applicant stated that no credit for steam dump other than code safety relief valves is taken in any safety analysis.

The staff has requested the applicant to submit a description in FSAR Section 7.7 to describe the features of the Shearon Harris environmental control system which insures that instrumentation sensing and sampling lines for systems important to safety are protected from freezing during extremely cold weather. Additional information is required.

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

To provide assurance that the Chapter 15 analysis 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 applicant has not provided a response to this item. Additional information is required.

7.7.3 Control System Failure Caused by High Energy Line Breaks

Operating reactor licensees were informed by IE Information Notice 79-22, issued September 19, 1979, that certain nonsafety grade control equipment, if subjected to the adverse environment of a high energy line break, could impact the safety analyses and the adequacy of the protection functions performed by the safety grade equipment. The staff has requested a review by the applicant to determine whether the harsh environment associated with high energy line breaks might cause control system malfunction and result in consequence more severe than those of Chapter 15 analyses or beyond the capability of operators or safety systems.

The applicant has not provided a response to this item. Additional information is required.

7.7.4 Evaluation Conclusion

LATER