11

Docket File

JAN 14 198

1/10/83

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

FROM: Walter Butler, Acting Assistant Director for Reactor Safety
Division of Systems Integration

SUBJECT: CATAWBA NUCLEAR STATION, UNITS 1 AND 2 -
SAFETY EVALUATION REPORT, FSAR SECTION 7.0,
INSTRUMENTATION AND CONTROL SYSTEMS

Plant Name: Catawba Nuclear Station, Units 1 & 2
Docket Nos.: 50-413/414
Licensing Status: OL
Responsible Branch: LB #4
Project Manager: K. Jabbour
Review Branch: ICSB
Review Status: Incomplete

DESIGNATED ORIGINAL

Certified By

Enclosed, as enclosure (1), is the Safety Evaluation Report (SER) input for the Catawba Nuclear Station, Units 1 and 2, prepared by the Instrumentation and Control Systems Branch (ICSB). The enclosed SER input applies to Section 7.0 of the Standard Review Plan (SRP) and includes evaluation information for which the ICSB has responsibility. This SER reflects the results of our review of the information presented in the Catawba Final Safety Analysis Report (FSAR) through Amendment No. 28. Also, the SER is based on a drawing review, a site visit, and our evaluation of the applicant's responses to ICSB's requests for additional information.

It should be noted that, in response to your memorandum dated November 18, 1982, the enclosed SER is a marked-up copy of the CRESS version to expedite processing. As such, the sections categorizing our issues into open, confirmatory, technical specification, TMI Action Plan, or licensing condition items were removed from our draft SER. To aid in identifying and categorizing these issues in the updated SER, enclosure (2) has been provided. It should also be noted that Supplemental Safety Evaluation Report (SSER) inputs will not be provided for the Confirmatory Items unless a problem is found when final documentation is received from the applicant.

If there are any questions please contact ICSB.

-cc SER Jacket

8301200025 830110
CF ADOCK 05000413
CF

Walter Butler, Acting Assistant Director
for Reactor Safety
Division of Systems Integration

Enclosures: ★ See previous concurrence
As stated

cc: See attached list

Contact:
F. Burrows, ICSB
x29455

OFFICE ►		ICSB/DSI ★	ICSB/DSI ★	ICSB/DSI	AADRS/DSI
SURNAME ►		FBurrows:vp	TDunning	FRosa	WButler
DATE ►		1/ /83	1/ /83	1/11 /83	1/11 /83

OFFICIAL RECORD COPY

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

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

SUBJECT: CATAWBA NUCLEAR STATION, UNITS 1 AND 2 -
SAFETY EVALUATION REPORT, FSAR SECTION 7.0,
INSTRUMENTATION AND CONTROL SYSTEMS

Plant Name: Catawba Nuclear Station, Units 1 & 2
Docket Nos.: 50-413/414
Licensing Status: OL
Responsible Branch: LB #4
Project Manager: K. Jabbour
Review Branch: ICSB
Review Status: Incomplete

Enclosed, as enclosure (1), is the Safety Evaluation Report (SER) input for the Catawba Nuclear Station, Units 1 and 2, prepared by the Instrumentation and Control Systems Branch (ICSB). The enclosed SER input applies to Section 7.0 of the Standard Review Plan (SRP) and includes evaluation information for which the ICSB has responsibility. This SER reflects the results of our review of the information presented in the Catawba Final Safety Analysis Report (FSAR) through Amendment No. 28. Also, the SER is based on a drawing review, a site visit, and our evaluation of the applicant's responses to ICSB's requests for additional information.

It should be noted that, in response to your memorandum dated November 18, 1982, the enclosed SER is a marked-up copy of the CRESS version to expedite processing. As such, the sections categorizing our issues into open, confirmatory, technical specification, TMI Action Plan, or licensing condition items were removed from our draft SER. To aid in identifying and categorizing these issues in the updated SER, enclosure (2) has been provided. It should also be noted that Supplemental Safety Evaluation Report (SSER) inputs will not be provided for the Confirmatory Items unless a problem is found when final documentation is received from the applicant.

If there are any questions please contact ICSB.

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

Enclosures:
As stated

cc:See attached list

Contact:
F. Burrows, ICSB

OFFICE	ICSB/DSI	ICSB/DSI	ICSB/DSI	ADRS/DSI
NAME	FBurrows:vp	TDunning	FRosa	TPSpeis
DATE	1/10/83	1/10/83	1/ /83	1/ /83

NRC FORM 318 (10-80) NRCM 0240

OFFICIAL RECORD COPY

cc: R. Mattson
F. Rosa
K. Jabbour
T. Dunning
C. Rossi
R. Capra
E. Adensam
J. Elsbergas (ANL)

DISTRIBUTION:
Docket File
ICSB R/F
Catawba Units 1 & 2 S/F
F. Burrows (PF)
W. R. Butler

OFFICE							
URNAME							
DATE							

Enclosure 1

7 INSTRUMENTATION AND CONTROLS

7.1 Introduction

Section 7.1 of the FSAR contains information pertaining to safety-related instrumentation and control systems, their design bases, and applicable acceptance criteria.

DESIGNATED ORIGINAL

Certified By

7.1.1 Acceptance Criteria

The staff has reviewed the applicant's design, design criteria, and design bases for the instrumentation and control systems for the Catawba Nuclear Station Units 1 and ~~Units~~ 2. The acceptance criteria used as the basis for the staff's evaluation are set forth in SRP (NUREG-0800) 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 Systems Important to Safety." These acceptance criteria include the applicable GDC and IEEE Standard 279, "Criteria for Protection Systems 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 of the Instrumentation and Control Systems Branch (ICSB) identified in Section 7.1 of the SRP. Conformance to the acceptance criteria provides the bases for concluding that the instrumentation and control systems meet the requirements of 10 CFR 50.

7.1.2 General Findings

The applicant has identified the instrumentation and control systems important to safety and the acceptance criteria which are applicable to those systems identified in the SRP. The applicant also has identified the guidelines, including the RGs and the industry codes and standards, which are applicable to

the systems. The acceptance criteria and guidelines identified by the applicant are provided in Section 7.1.2 of the FSAR.

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 (NSSS) and the balance-of-plant (BOP) instrumentation and control systems important to safety, addressed in FSAR Section 7.1, satisfy the requirements of GDC 1 and, therefore, are acceptable.

7.2 Reactor Trip System

7.2.1 System Description

The reactor trip system (RTS) automatically shuts down the reactor to prevent the established limits of safe operation from being exceeded. To accomplish its function, the RTS includes instrumentation channels to monitor various plant variables, process and nuclear, pertinent to the reactor safety. Whenever a monitored variable reaches a set limit, the associated instrumentation channel trips a bistable. This turns off power to the relays that provide inputs (voltage/no voltage) corresponding to the condition (normal/abnormal) of the measured parameter to the solid-state logic protection system consisting of two redundant trains. Each of the trains controls power to the undervoltage coil of a separate and independent, series-connected, reactor trip breaker. Whenever an established combination of input signals is received by the solid-state logic protection system, power to the undervoltage coils is interrupted and the breakers open. Opening either of two breakers interrupts power to the control rods, and the rods fall by gravity into the core, shutting down the reactor.

Concurrent with the reactor trip, the RTS also initiates a turbine trip to prevent reactivity insertion that would otherwise result from excessive reactor system cooldown.

In addition to the automatic trip of the reactor described above, means also are provided for manual trip by the operator. The manual reactor trip consists of two switches, one on train A and one on Train B. Each of the switches controls power to the undervoltage and shunt trip coils of the reactor trip breaker for the corresponding train. Actuation of a switch removes power from the undervoltage coil and also energizes the shunt trip coil, either of which trips the breaker. In the same manner the reactor will be tripped by actuating either of two manual switches for safety injection (see Section 7.3).

The trips included in the RTS are listed below. The first number in parentheses after each trip parameter is the number of coincident trips required, and the second number is the number of redundant channels provided.

(1) power range high neutron flux	
(a) low setting	(2/4)
(b) high setting	(2/4)
(2) intermediate range high neutron flux	(1/2)
(3) source range high neutron flux	(1/2)
(4) power range high positive neutron flux rate	(2/4)
(5) power range high negative neutron flux rate	(2/4)
(6) overtemperature ΔT trip	(2/4)
(7) overpower ΔT trip	(2/4)
(8) pressurizer low pressure	(2/4)
(9) pressurizer high pressure	(2/4)
(10) pressurizer high water level	(2/3)
(11) low reactor coolant flow	(2/3 in any loop)
(12) reactor coolant pump bus undervoltage	(2/4)
(13) reactor coolant pump bus underfrequency	(2/4)
(14) low-low steam generator water level	(2/4 in any loop)
(15) safety injection (see Section 7.3)	Coincident with actuation of safety injection
(16) turbine trip	
(a) Low control valve oil pressure, or	(2/4)
(b) turbine stop valve close	(4/4)
(17) general warning alarm	(2/2)
(18) manual	(1/2)

Most of the trip parameters shown in the list above are monitored directly and their functions are self-explanatory. Exceptions are the overtemperature ΔT, the overpower ΔT, and the general warning alarm. The overtemperature ΔT protects against a low departure-from-nucleate-boiling-ratio (DNBR). The set point for this trip is continuously calculated by analog circuitry for each loop and depends on temperatures in the loop, neutron flux distribution in the

reactor, and primary system (pressurizer) pressure. The overpower ΔT protects against excessive local linear power density. As for the overtemperature ΔT, the trip set point for the overpower ΔT is continuously calculated by analog circuitry for each loop and depends on the temperatures in the loop and the neutron flux distribution in the reactor. The general warning alarm system monitors various conditions, such as power supply output and test switch position, in the solid-state logic protection system. If any of the monitored conditions in a train are abnormal, the alarm relay for that train is deenergized. This actuates the train trouble annunciator in the control room. If an abnormal condition occurs simultaneously in both trains, the reactor is automatically tripped.

Some of the trips shown in the list are not effective below or above certain power levels. The source range high neutron flux trip can be manually bypassed when one of the two intermediate range channels reads above approximately 10^{-10} amperes (P-6 interlock, one decade into intermediate range). The intermediate range high neutron flux trip and the power range high neutron flux low-setting trip can be manually bypassed, and the source range high neutron flux trip is automatically bypassed above approximately 10% power (P-10 interlock). All the above bypasses are automatically removed (source range high neutron flux trip is manually removed when below P-10) when the power level decreases below the set value.

The pressurizer low-pressure and high-water-level trips, low reactor coolant flow trip, and the reactor coolant pump bus undervoltage and underfrequency trips are automatically blocked below approximately 10% power (P-7 interlock). The reactor trip on turbine trip is blocked below approximately 52% power (P-9 interlock). In addition, at power levels below approximately 50% (P-8 interlock) the trip logic for the low reactor coolant flow is changed from 2/3 in any loop to 2/3 in any two loops. All the above blocks are automatically removed when the power increases above the set value.

The RTS includes provisions for testing system operation. Where only parts of the system are tested at any one time, the testing is carried out in steps, in a sequence that provides the necessary overlap to ensure complete system operability. All of the system functions can be tested at power, except for the

manual reactor trip and manual safety injection initiation trip. Actuation of these manual switches would trip the reactor. Also, the nuclear channel trips that are not effective above certain power levels are tested at reduced power levels or at shutdown. Bypassing of the trip functions during testing is only required for the source and intermediate range nuclear channels since they are arranged in one-out-of-two trip logic.

The analog process channel testing is performed by introducing dummy input signals into the instrumentation channels and observing the tripping of the appropriate output bistables. The power range nuclear channels are tested by superimposing a test signal on the actual detector signal. To test the logic matrices of the solid-state logic protection system, pulse test signals are used in all possible trip and nontrip logic combinations. The test pulses are of short duration and the trip logic is not maintained sufficiently long to permit opening of the reactor trip breakers. During logic testing of one train, the other train can initiate any required protective action. To test the reactor trip breakers, bypass breakers are provided. After a bypass breaker is closed, the associated reactor trip breaker can be tripped with a signal from the corresponding logic train. Actuation of a manual reactor trip switch opens the corresponding reactor trip breaker and its bypass breaker.

In addition to providing inputs to the solid-state logic protection system, analog signals of the protection channels are used for nonprotective functions, such as control, remote indication, and computer monitoring. To protect from faults in the nonsafety circuits affecting the protection system, isolation amplifiers are used. The isolation amplifiers are classified as part of the protection system.

7.2.2 Specific Findings

7.2.2.1 Testing the Reactor Trip Breakers and Manual Trip Switches

The reactor trip breakers are provided with undervoltage and shunt trip coils. Interrupting power to the undervoltage coil or energizing the shunt coil will trip the breaker. The undervoltage coils receive trip signals from both the

solid-state logic protection system and the manual trip switches (including the manual reactor trip switches and the safety injection switches). The shunt trip coils receive trip signals from the manual trip switches only. This provides diversity and enhances the separation between the automatic and manual reactor trip systems.

Testing of the undervoltage coil operation is carried out with a trip signal from the solid-state logic protection system. Testing of the manual reactor trip channel does not allow independent verification of the operability of the shunt coil and the undervoltage coil because the operation of a manual trip switch results in a simultaneous trip action by both coils. ~~A requirement will be added to Technical Specifications to test the manual trip/shunt trip coils operation independently at least once each refueling outage.~~

see insert 1

7.2.2.2 Protection System Sensors and Cabling in Nonseismic Structures

Protection system trip circuit inputs that are located in the nonseismic turbine building are (1) turbine stop valve closure limit switches, (2) turbine control valve oil pressure switches, and (3) turbine impulse pressure transducers.

Items 1 and 2 provide inputs to the reactor trip on turbine trip circuit; Item 3 provides inputs to the P-7 interlock. The reactor trip on turbine trip is classified as an anticipatory trip for which no credit is taken in the safety analyses. The staff position regarding anticipatory trips, as stated in BTP ICSB 26, requires that all reactor trips, including the anticipatory trips, should meet the requirements of IEEE Standard 279. Also, it requires that no credible fault, such as grounding or shorting in the portion of the trip circuitry in the nonseismic structures, should cause any adverse consequences in the protection system operation.

Although the turbine control valve pressure switches, the turbine stop valve closure limit switches, and the turbine impulse pressure transducers are not seismically and environmentally qualified for use in the turbine building, they are fully qualified for use in other safety-grade applications. Because no credit is taken in the safety analysis for these inputs to the reactor

Insert 1

The applicant has indicated that plant surveillance procedures will not include provisions to verify the operability of the shunt trip coils. The staff does not find this to be acceptable since the shunt trip feature provides a diverse means to assure reactor trip consistent with the intent of GDC-22, "Protection System Independence," and that the failure to conduct periodic surveillance testing to insure the operability of this diverse feature is contrary to the intent of GDC-21, "Protection System Reliability and Testability." The resolution of this matter will be addressed in a supplement to this report.

protection system (RPS), the staff finds their use acceptable for this application.

The interlocked armor cables for the two turbine stop inputs and the turbine impulse pressure input are routed in cable trays through the turbine building. Although the cables and trays are located in a nonseismic area, they have been treated, insofar as possible, as safety related; mutually redundant cables are adequately separated. ~~Isolators are~~ Relay coil-contact isolation is used to isolate these trip inputs to the RPS.

~~All of~~ The circuitry in the turbine building complies with the requirements of IEEE Standard 279 in that no credible fault in these portions of the trip circuitry in the turbine building would degrade the performance of the RPS. This is in compliance with the requirements of BTP ICSB 26 and is therefore acceptable.

7.2.2.3 Water Level Measurement Errors

The steam generator and pressurizer water level measurement channels utilize differential pressure transmitters. The measurement accuracy of such a system is affected by several factors. Of primary importance is the increase in the indicated water level caused by a decrease of the water density in the reference leg resulting from an increase in the ambient temperature ~~resulting from a~~ due to high-energy line breaks. For such an accident, the steam generator water level provides the primary trip function and the trip set points need to be selected to ensure that the action required by the safety analyses will be initiated throughout the range of temperatures that can be expected. This issue was addressed for operating reactors in IE Bulletin 79-21. The staff has requested the applicant to evaluate the effect of high temperature in the reference legs of water level measurement systems following a high-energy line break to ensure that measurement errors are factored into the basis for establishing trip set points. The applicant ~~intends to~~ will use insulation on the reference legs to minimize measurement errors ~~in the trip set points~~. The staff finds this approach acceptable and will ensure that any environmental errors are taken into account during its review of set point methodology and Technical Specifications.

7.2.2.4 Lead, Lag, and Rate Time Constant Set Points 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 FSAR ~~Chapter 15~~ safety analyses. The time constants for these signal compensations are adjustable set points within the analog portion of the safety system. The time constant set points will be incorporated into the station Technical Specifications.

7.2.2.5 Response Time Testing

To ensure that the response time of each protective function of the reactor trip system and engineered safety features actuation system is within the time limit assumed in the accident analyses, Technical Specifications require testing the time response at specified intervals. The applicant intends to use an approach that differs from the procedures proposed for other current Westinghouse plants undergoing operating license reviews. The applicant's test procedures will be evaluated by the staff during Technical Specification review.

7.2.2.5 Trip of Reactor Coolant Pump Breakers on Underfrequency

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

7.2.2.6 Verification of the Resistance Temperature Detectors Bypass Loop Flow

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

7.2.2.7 TMI-2 Action Plan Item II.K.3.10, Proposed Anticipatory Trip Modification

The Catawba design includes an anticipatory reactor trip upon turbine trip. Provisions are included to permit the reactor trip upon turbine trip to be blocked at power levels below approximately 50% (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, based on a Westinghouse analysis for the Catawba station. A decision to trip the reactor following turbine trip at different power levels would involve only bistable set point changes and not instrument hardware changes. The staff finds that the design, therefore, is acceptable. The specific power level set point below which a reactor trip following a turbine trip is blocked will be reviewed and specified in the station Technical Specifications.

7.2.2.8 TMI-2 Action Plan Item II.K.3.12, Confirm Existence of Anticipatory Reactor Trip Upon Turbine Trip

The Catawba station has an anticipatory reactor trip on turbine trip, which satisfies this item.

7.2.2.9 Turbine Trip Following A Reactor Trip

Credit is taken in the Catawba accident analysis for turbine trip on a reactor trip. The applicant 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 that traverse nonseismic 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 station Technical Specifications a requirement to periodically test these circuits.

7.2.3 Evaluation Findings

Based on its review, the staff concludes that the RTS conforms with the design-bases requirements of IEEE Standard 279. The RTS includes the provision to sense accident conditions and anticipated operational occurrences and initiate reactor shutdown consistent with the safety analysis presented in Chapter 15 of the FSAR. Therefore, the staff finds that the RTS satisfies the requirements of GDC 20, "Protection System Functions."

The RTS adequately conforms with the guidance for periodic testing in RG 1.22 and IEEE Standard 338 as supplemented by RG 1.118. The bypassed and inoperable status indication adequately conforms with the guidance of RG 1.47. The RTS adequately conforms with the guidance on the application of the single-failure criterion in IEEE Standard 379, as supplemented by RG 1.53. Based on its review, the staff concludes that the RTS satisfies the requirement of IEEE Standard 279 with regard to system reliability and testability. Therefore, the staff finds that the RTS satisfies the requirement of GDC 21, "Protection System Reliability and Testability."

The RTS adequately conforms with the guidance in IEEE Standard 384 as supplemented by RG 1.75 for the protection system independence. Based on its review, the staff concludes that the RTS satisfies the requirement of IEEE

Standard 279 with regard to the independence of systems. Therefore, the staff finds that the RTS satisfies the requirement of GDC 22, "Protection System Independence."

Based on its review of failure modes and effects for the RTS, the staff concludes 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, the staff finds that the RTS satisfies the requirements of GDC 23, "Protection System Failure Modes."

Based on its review of the interfaces between the RTS and plant operating control systems, the staff concludes that the system satisfies the requirements of IEEE Standard 279 with regard to control and protection system interaction. Therefore, the staff finds that the RTS satisfies the requirements of GDC 24, "Separation of Protection and Control Systems."

Based on its review of the RTS, the staff concludes that the system satisfies the protection system requirements for malfunctions of the reactivity control system, such as accidental withdrawal of control rods. FSAR Chapter 15 addresses the capability of the system to ensure that fuel design limits are not exceeded for such events. Therefore, the staff finds that the RTS satisfies the requirements of GDC 25, "Protection System Requirements for Reactivity Malfunction."

The staff's conclusions, noted above, are based on the requirements of IEEE Standard 279 with respect to the design of the RTS. Therefore, the staff finds that the RTS satisfies the requirement of 50.55a(h) with regard to IEEE Standard 279.

The staff's review of the RTS has examined the dependence of this system on the availability of essential auxiliary support (EAS) systems. Based on its review, the staff concludes that the design of the RTS is compatible with the functional performance requirements of EAS systems. Therefore, the staff finds 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 RTS and the design of the EAS systems are acceptable and meet the relevant requirements of GDCs 2, 4, 20, 21, 22, 23, 24, and 25 and 10 CFR 50, 50.55a(h), subject to the resolution of the concern identified in Section 7.2.2.1 of this report.

~~7.2.3 Evaluation Findings~~

The staff has conducted an audit review of the RTS for conformance to guidelines of the applicable RGs and industry codes and standards as outlined in SRP Section 7.2, Part II and III. In Section 7.1 of this SER, the staff concluded that the applicant had adequately identified the guidelines applicable to these systems. Based on its audit review of the design for conformance to the guidelines, the staff finds that upon satisfactory resolution of the concern identified in Section 7.2.2, there is reasonable assurance that the systems will conform to the applicable guidelines. The staff's 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 on its review, the staff concludes 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, the staff finds 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."

move 1st paragraph under 7.2.3

7.3 Engineered Safety Features Actuation Systems

7.3.1 System Description

This section describes the engineered safety features actuation system (ESFAS) that initiates the operation of both the engineered safety features (ESF) and essential auxiliary support systems. Also described are the control systems that regulate the operation of those systems following their initiation.

7.3.1.1 Engineered Safety Features Actuation System

The ESFAS monitors selected plant parameters and, whenever predetermined safety limits are reached, the system sends actuation signals to the appropriate ESF and the auxiliary support systems equipment. Typical accidents that require actuation of the ESF systems are a loss of primary coolant and steamline

breaks. The plant variables that are monitored by the analog circuitry of the ESFAS include pressurizer pressure, steamline pressures, containment pressure, and reactor coolant average temperature. Whenever a monitored variable reaches a set limit, the associated instrumentation channel trips a bistable. This turns off power to the relays that provide inputs (voltage/no voltage) corresponding to the condition (normal/abnormal) of the measured parameter to the solid-state logic protection system consisting of two redundant trains each capable of actuating the ESF equipment required. Whenever a required logic combination of inputs is received by the solid-state logic protection system, each train operates an appropriate master relay. Contacts of these relays are used to operate slave relays that in turn provide contacts to actuate various ESF system equipment.

The ESFAS signals and the plant conditions that generate these signals are as follows: (The first number in parentheses after each parameter indicates the

number of coincident trips required, and the second number is the number of redundant channels provided.)

(1) Safety Injection

(a)	high containment pressure	(2/3)
(b)	low compensated steamline pressure	(2/3 in any steamline)
(c)	pressurizer low pressure	(2/4)
(d)	manual	(1/2)

(2) Containment Spray and Containment Isolation, Phase B

(a)	containment pressure high-high	(2/4)
(b)	manual	(1/2)

(3) Containment Isolation, Phase A

(a)	safety injection	See Items a through d for Function 1 above
(b)	high containment radioactivity (nonredundant and not part of ESFAS)	(1/1)
(c)	manual	(1/2)

(4) Steamline Isolation

(a)	low steamline pressure	(2/3 in any steamline)
(b)	containment pressure high-high	(2/4)
(c)	high steam negative pressure rate	(2/3 in any steamline)
(d)	manual	(1/1 for any loop) (1/2 for all loops)

(5) Feedwater Line Isolation

(a)	safety injection	See Items a through d for Function 1 above

(b)	steam generator level high-high	(2/3 for any steam ~~high-high~~ generator)
(c)	low T_{avg} (interlocked with P-4)	(2/4)
(d)	doghouse high level (only lines entering doghouse isolated)	(1/2)

(6) Auxiliary Feedwater Pump Actuation

Motor-Driven Pump

(a)	steam generator level low-low	(2/4 for any steam generator)
(b)	loss of main feedwater pumps	(2/2)
(c)	safety injection	See Items a through d for Function 1 above
(d)	blackout signal (undervoltage on 4160-V bus)	(2/3)
(e)	manual (local or remote)	(1/1)

Turbine-Driven Pump

(a)	steam generator level low-low	(2/4 in any 2 steam generators)
(b)	blackout signal	(2/3)
(c)	manual (local or remote)	(1/1)

(7) Containment Air Return and Hydrogen Skimmer System

(a)	containment pressure high-high	(2/4)
(b)	manual	(1/2)

(8) Annulus Ventilation System

(a)	safety injection	See Items a through d for Function 1 above

(b) manual	(1/2)
(9) Combustible Gas Control System	
(a) manual	(1/2)
(10) Nuclear Service Water System	
(a) safety injection	See Items a through d for Function 1 above
(b) containment spray and containment isolation, phase B	See Items a through b for Function 2 above
(c) manual	(1/2)
(11) Emergency Diesel Generator	
(a) safety injection	See Items a through d for Function 1 above
(b) blackout signal	(2/3)
(c) manual	(1/1)
(12) Control Room Area Heating, Ventilation and Air Conditioning System	
(a) safety injection	See Items a through d for Function 1 above
(b) blackout signal	(2/3)
(c) manual	(1/2)
(13) Auxiliary Building Ventilation System	
(a) safety injection	See Item a through d for Function 1 above
(b) blackout signal	(2/3)
(c) manual	(1/2)

(14) Diesel Building Ventilaton System

(a) safety injection	See Item a through d for Function 1 above
(b) blackout signal	(2/3)
(c) manual	(1/2)

The testing of the ESFAS analog instrumentation channels and the solid-state logic protection system is carried out in the same manner as described for the RTS in Section 7.2. The solid-state logic testing checks the signal path, from and including input relay contacts, through the master relay coils and performs continuity tests on the coils of the output slave relays. During logic testing of one train, the other train can initiate the required actuation function. Final actuator testing operates the output slave relays and verifies operability of those devices that require safeguards actuation and that can be tested without causing plant upset. A continuity check is performed on the actuators of the untestable devices. To enable continuity check, these devices have been assigned to slave relays for which additional test circuitry has been provided to individually block actuation to a final device. Interlocking prevents blocking the output from more than one output relay in a protection train at a time. Interlocking between trains also is provided to prevent continuity testing in both trains simultaneously.

7.3.1.2 ESF and Essential Auxiliary Support Systems Operation

7.3.1.2.1 Auxiliary Feedwater System

The function of the auxiliary feedwater system (AFS) is to provide adequate cooling water to the steam generators in the event the main feedwater supply is not available. The AFS has two full-capacity motor-driven pumps that start automatically on low-low water level in any steam generator, a trip of both main feedwater pumps, a safety injection signal, or a blackout signal. These pumps are powered from two separate trains of emergency onsite electrical power. Additionally, a turbine-driven pump is provided that starts automatically on low water level in any two steam generators or a blackout

signal. Upon receipt of two-out-of-three indications of low differential pressure in the auxiliary feedwater pump suction piping, the water supply to the pumps automatically transfers from the condensate supply to the nuclear service water system during a condition that automatically starts the auxiliary feedwater pumps.

A manual control switch is provided for each pump on the main control board and at the remote shutdown panels. Also, the auxiliary feedwater flow can be adjusted from manual control stations at the main control board or at the remote shutdown panels. To activate the pump and flow controls at the remote shutdown panels, transfer switches located at the remote shutdown panels must be used.

7.3.1.2.2 Containment Isolation

The function of the containment isolation is to provide a barrier against uncontrolled release of radioactivity to the environment following an accident that releases radioactive material inside the containment. The containment isolation system is actuated automatically by signals from the ESFAS (see Section 7.3.1.1). The phase A signal isolates all nonessential process lines penetrating the containment; phase B isolates the rest of the lines, except the safety injection and containment spray lines.

All remote operated (automatic or manual) containment isolation valves are provided with control switches and position indicating lights on the main control board.

7.3.1.2.3 Safety Injection (Emergency Core Cooling)

The primary function of the emergency core cooling system (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 (RHR) pumps; low pressure cold-leg injection and high pressure upper head injection accumulators; a boron injection tank; RHR heat

exchangers; the refueling water storage tank; and associated piping, valves, and instrumentation.

The ECCS is a two-train, fully redundant standby ESF. The system safety function can be performed with a single credible active failure during injection or an active or passive failure during recirculation. The instrumentation and controls of one train are electrically independent and physically separated from the instrumentation and controls of the other train. Redundant, as well as functionally independent variables, are used to initiate the safety injection signals. Power sources for the ECCS are divided into two independent trains supplied from offsite power. Emergency diesel generators supply power on loss of offsite power.

The safety injection signal initiates the following actions in the ECCS:

(1) starts centrifugal charging pumps

(2) isolates the valves in the centrifugal charging pumps suction header to the volume control tank and aligns them to the refueling water storage tank

(3) opens the boron injection tank (BIT) suction and discharge parallel isolation valves

(4) closes normal charging path valves

(5) isolates the BIT recirculation loop and stops the recirculation pumps

(6) starts safety injection pumps

(7) starts residual heat removal pumps

(8) terminates the refueling water storage tank recirculation and isolates the makeup line to the spent fuel pool

No manual actions are required of the operator for proper operation of the ECCS during the injection mode of operation. Only limited manual actions are required to realign the system for recirculation mode of operation (see Section 7.3.1.2.15).

7.3.1.2.4 Containment Spray System

Two redundant trains of containment spray provide a spray of cold borated water from the upper regions of the containment to reduce containment pressure and temperature following a loss-of-coolant accident (LOCA), or a main steamline or a feedwater line break accident. Each train has an independent electrical power source backed up by a separate emergency diesel generator during the loss of offsite electrical power.

The containment spray system (CSS) operates in three sequential modes

(1) spraying a portion of the contents of the refueling water storage tank (RWST) into the containment atmosphere, using the containment spray pumps

(2) recirculating water from the containment sump through the containment spray pumps and heat exchangers back to the containment atmosphere after the RWST has been drained,

(3) diverting a portion of the recirculation flow from the RHR system through the residual spray headers

The CSS is provided with instrumentation and controls to permit the monitoring and actuation of the system from outside the containment. The containment spray pumps and valves are activated automatically by the containment high-high pressure signal. Manual control switches are provided on the main control board. The status of pumps and valve positions are indicated in the control room. Abnormal conditions in the pump and valve operation and the spray water supply are alarmed on the main control board.

The containment pressure control system (CPCS) is provided to prevent excessive depressurization of the containment through inadvertent or excessive operation of the CSS. The CPCS prevents manual or automatic operation of the CSS below 0.25 psig. Four independent pressure sensors and logic channels are provided for each train of the CSS. Electrical power to each train of the CPCS is supplied by a separate 120-V ac vital instrumentation and control inverter. Indication of the CPCS interlock status is provided in the control room and alarms are provided on a loss of power to the system.

7.3.1.2.5 Containment Air Return and Hydrogen Skimmer System

The containment air return and hydrogen skimmer system is designed to (1) ensure rapid return air to the lower containment compartment after initial loss-of-coolant blowdown and (2) prevent accumulation of hydrogen in restricted areas within the lower compartment resulting from a LOCA. This system has two independent, 100%-capacity hydrogen skimmer fans, with associated piping and valves and two independent, 100%-capacity air return fans with associated dampers. Each redundant air return fan and hydrogen skimmer fan is powered from a separate train of emergency, Class 1E standby power.

The instrumentation and controls for each redundant train are powered from the same bus that powers the equipment in the train. Variables important to system operation are indicated in the control room and alarms are provided to warn the operator of abnormal conditions. Manual control switches are provided in the control room. The air return fans, the hydrogen skimmer fans, and the associated dampers and valves are activated automatically by the containment high-high pressure signal.

The containment pressure control system, as described in Section 7.3.1.2.4, also prevents manual and automatic operation of the containment air return and hydrogen skimmer system below 0.25 psig.

7.3.1.2.6 Annulus Ventilation System

The annulus ventilation system is designed to (1) produce and maintain a negative pressure in the annulus following a LOCA, (2) minimize the release of radioactivity following a LOCA by filtering and recirculating a large volume of annulus air, and (3) provide long-term fission product removal capacity by decay and filtration. This system has two independent, 100%-capacity ventilation filter subsystems consisting of fans, filters, dampers, ductwork, and controls. Electrical and control component separation is maintained between each subsystem. Each subsystem is powered by a separate train of emergency Class 1E standby power. The instrumentation and controls of each redundant train are powered from the same train that powers the equipment in that train. Information readouts are provided in the control room to monitor the safety functions of the annulus ventilation system. Manual controls for the system are provided in the control room. Switchover from the operating train to the standby train is accomplished manually by the operator.

7.3.1.2.7 Combustible Gas Control System

Hydrogen gas may be generated inside the containment following an accident. To ensure that the hydrogen concentration is maintained below the minimum capable of combustion, redundant hydrogen recombiners are provided. A hydrogen sample and purge system is provided to determine if the hydrogen recombiners are working and to control the hydrogen concentration, if necessary. Each hydrogen recombiner is powered from a separate safeguards bus with a separate control panel located outside of the containment. The recombiners are started manually after a LOCA. The hydrogen sample and purge system is operated manually.

7.3.1.2.8 Nuclear Service Water System

The nuclear service water (NSW) system supplies cooling water to safety and nonsafety loads. Two trains of service water are supplied for each unit. The NSW system is controlled manually from the control room during normal operation with one train per unit in operation; the pump suction and discharges are shared between units to provide cooling water from Lake Wylie. Manual control

is provided also at the auxiliary shutdown complex. On receipt of a safety injection signal, both ~~trains of the affected unit are automatically aligned to supply cooling water from the NSW pond and the NSW pumps are started.~~ NSW pumps are automatically started and isolation valves for safety-related heat exchangers receive a confirmatory open signal for the affected unit. On receipt of a phase B isolation signal, ~~heat exchanger valves between NSW trains and~~ the isolation valves for nonessential heat exchangers are closed, ~~and isolation valves for safety-related heat exchangers are automatically opened.~~ and the crossover valves between NSW trains close for the affected unit. Additionally, NSW suction for both units transfers from Lake Wylie to the SNSWP on phase B containment isolation or low pit level. ~~Or~~ A low pit level signal also starts the NSW pumps.

TP NSW system safety-related instrumentation and controls are powered from the same train of essential auxiliary power as their associated train of NSW equipment. The safety-related instrumentation and controls for each train are physically separated and electrically isolated. Information readouts for monitoring the operation of the safety-related functions of the NSW system are provided in the control room.

7.3.1.2.9 Feedwater Line Isolation

Feedwater isolation is provided to isolate the steam generators from feedwater flow to

(1) rapidly terminate feedwater flow and steam blowdown inside the containment following a main steam or feedwater line break

(2) prevent loss of steam generator inventory resulting from pipe rupture

(3) prevent overfilling the steam generators if normal means of controlling level fails

(4) prevent excessive cooldown of the reactor vessel

Upon receipt of the feedwater isolation signal, the main feedwater isolation valves and other valves associated with the main feedwater lines are closed. Two complete actuation systems are provided for each valve operator corresponding to two redundant ESFAS trains. The feedwater valves are tested routinely during refueling outages and are not tested at power since induced transients would cause reactor trip.

7.3.1.2.10 Steamline Isolation

An automatically operated main steam isolation valve is installed in each main steamline to stop uncontrolled steam flow from the steam generators in the event of a break in the main steam piping. ~~A manual block and permissive is provided for safety injection actuation and steamline isolation on low-compensated steamline pressure. This allows steamline isolation on high negative pressure rate during normal plant heatup and cooldown. The block of the low steamline pressure is automatically removed and the high rate is automatically blocked when the pressurizer pressure is above the P-11 set point.~~

The isolation valves are held open against four springs by control air applied to the bottom of a piston. Loss of control air allows the valves to close in less than 5 sec. Control air is supplied to the main steam isolation valves through two series (one train A and one train B) of electrically operated solenoid valves. In addition, air from the bottom of the piston is dumped through either of two electrically operated solenoid valves (one train A and one train B) in series with variable restrictors used to adjust closure speed. The solenoid valves are powered from Class 1E ~~nonsafety 120-V ac and loss of offsite power will close the main steam isolation valves.~~ 125 V dc. The isolation valves are ~~periodically~~ tested to 10% of full stroke.

See Insert 2

7.3.1.2.11 Emergency Diesel Generators

Each train of the 4160-V ac essential auxiliary power system is supplied with emergency standby power from an independent diesel generator. Each diesel generator can be manually started for test and maintenance purposes from the control room or the local diesel control panel.

When the diesel generators receive an emergency start signal, all manual modes of operation are overridden. If a diesel is in the maintenance mode, a starting signal is inhibited. A local annunciator, an annunciator window in the control room, and an alarm on the bypassed and inoperable status panel in the control room are provided to alert the operator whenever a diesel is in the maintenance mode. Protective trips also are provided for the diesels that are

Insert 2

H A manual block switch is provided for the safety injection actuation and steamline isolation. The use of this switch bypasses safety injection actuation and steamline isolation initiated on low steamline pressure and enables steamline isolation initiated by high steam pressure rate. This bypass and enable usage is only permitted when the pressurizer pressure is below the P-11 setpoint and is automatically removed when the pressurizer pressure goes above the P-11 setpoint.

not bypassed by starting signals. These trips are annunciated locally and in the control room.

7.3.1.2.1.12 Control Room Area Heating, Ventilation and Air Conditioning System

The function of the control room heating, ventilation, and air conditioning (HVAC) system is to maintain the environment in the control room, control room area, and switchgear rooms within acceptable limits for equipment operation and habitability under normal and postaccident conditions. The system is divided into two 100% capacity, redundant trains that are interlocked so that only one train is operating at a time. During normal operation one train of the system is manually controlled with the other train in standby. A safety injection or blackout signal automatically ensures one train is operating and, if necessary, loads the system onto the essential auxiliary power. Controls in the control room allow the operator to switch the operating and standby trains. Remote controls are provided in the HVAC equipment room.

Smoke detectors, chlorine detectors, and radiation monitors take necessary isolating action to ensure control room habitability. The instrumentation and controls are powered by the same train of essential auxiliary power as their associated train of the HVAC system. The safety-related instrumentation and controls for the redundant trains are physically separated and electrically isolated.

7.3.1.2.13 Auxiliary Building Ventilation System

This system provides adequate capacity to ensure that proper temperatures are maintained in the auxiliary building (except for the control room area and fuel handling area) during normal operating and shutdown conditions. This system also provides filtering for potentially contaminated areas of the auxiliary building and cooling air for the auxiliary shutdown panel rooms. The auxiliary building ventilation system consists of six subsystems. Two of those subsystems, the auxiliary building filtered exhaust system and the auxiliary shutdown panel room air conditioning system, are ESFs. Upon receipt of a

safety injection (via sequencer) signal, all nonessential auxiliary building ventilation system components shut down and the auxiliary building filtered exhaust system cycles on with emergency Class 1E standby power. All areas of the auxiliary building except the ECCS pump rooms are automatically isolated from the filtered exhaust system.

All air exhausted from the auxiliary building is directed to the unit vent where radiation is monitored. Upon indication of a high radiation level, the system is automatically shut down. A safety injection signal or blackout signal bypasses these permissives in the filtered exhaust system to maintain their safety function.

The auxiliary building filtered exhaust system and the auxiliary shutdown panel room air conditioning system have two separate and redundant trains. Electrical power and control separation between trains is maintained.

7.3.1.2.14 Diesel Building Ventilation System

The diesel building ventilation system automatically maintains a suitable environment for operation of equipment and personnel in the diesel building. The system consists of two subsystems for each enclosure: (1) the normal ventilation system and (2) the emergency ventilation system. The normal ventilation system operates only during normal plant operations and its fan is cycled off and its shutoff damper is closed when its associated diesel is started. When the diesel starts, the emergency ventilation system fans automatically start and the automatic return air and outdoor air dampers are activated. When the diesel is shut down, the emergency ventilation system dampers and fans are shut down. The diesel building ventilation system is automatically shut down on receipt of a fire protection signal.

A train of safety-related instrumentation and controls serve each of the emergency ventilation systems. These trains are physically separated and electrically isolated so that no single failure can affect the ventilation of more than one diesel room. The emergency ventilation system can be manually

initiated in the diesel room. Temperature alarms and indication are provided in the control room.

7.3.1.2.15 Switchover From Injection to Recirculation

The switchover from the injection mode to the recirculation mode is initiated automatically and completed manually by the operator from the main control room. During the injection mode, the RHR pumps deliver water to the reactor coolant system from the RWST. The water is taken from the containment sump during the recirculation mode. The transfer of the RHR pump suction to the containment sump is accomplished automatically when the RWST level decreases below the low level set point coincident with a safety injection signal. Four level measurement channels are provided and arranged in a two-out-of-four coincidence logic to open the two sump isolation valves and to close the RHR/RWST isolation valves. The RHR pumps continue to run during the switchover.

The two charging pumps and two safety injection pumps continue to take suction from the RWST following the automatic switchover described above. As part of the manual switchover procedure, the two charging pumps and the two safety injection pumps are realigned in series with the RHR pumps.

The four RWST level channels provide level indication in the control room and also generate high, makeup, low, and low-low level alarms. The low level alarm coincident with the safety injection signal alerts the operator to complete the switchover as described above.

7.3.2 Specific Findings

7.3.2.1 Steam Generator Level Control and Protection

As listed in Section 7.3.1.1, three steam generator level channels are used in two-out-of-three logic to isolate the feedwater on high-high water level. In addition, one of these channels is used to provide a level signal to the three-element feedwater controller. A downscale failure of the level channel used

for control would result in a continuous request for feedwater and at the same time make this channel ineffective in providing protection for high water level. This would reduce the high level trip logic from two-out-of-three to two-out-of-two. This would be in violation of the requirements of IEEE Standard 279, Paragraph 4.7, "Control and Protection System Interaction," because the remaining protection system would not meet the single-failure criterion. The staff expressed its concern on this apparent conflict with regulatory requirements. The applicant intends to make design changes to rectify this issue. The staff considers this issue resolved subject to confirmation of installation of acceptable design modifications.

7.3.2.2 Compliance With IE Bulletin 80-06

IE Bulletin 80-06 requests a review of the ESF systems with the objective of ensuring that no device will change position solely because of the reset of the actuation signal. In response to the staff's question on how the Catawba design meets the requirements of IE Bulletin 80-06, the applicant has performed the requested review and did not identify any component that would not remain in a safety state following reset. A test to verify that the actual installed instrumentation and controls are in compliance with the requirements of IE Bulletin 80-06, will be conducted as part of the preoperational tests. Based on this commitment by the applicant, the staff considers this issue resolved subject to confirmation of the test completion.

7.3.2.3 Failure Modes and Effects Analysis (FMEA) Interface Requirements

The applicant has referred to Westinghouse Topical Report WCAP-8584, "Failure Mode and Effects Analysis (FMEA) of the Engineered Safety Features Actuation System," as the supporting document of FMEA for ESFAS equipment within the Westinghouse scope of supply. The staff requested the applicant to confirm that the interface requirements specified in WCAP-8584 have been met. In response, the applicant stated that the interface criteria have been met and a statement of confirmation was added to the FSAR. Based on the applicant's response, the staff considers this matter resolved.

7.3.2.4 Safety System Trip Set Point Methodology

The methodology followed in setting the safety system trip set points has not been described in the FSAR. In response to the staff's request for information concerning this item, the applicant stated that the set point study has not yet been completed for Catawba station. Because the primary function of this information is to confirm the adequacy of set points specified in the plant Technical Specifications, the staff will audit this information at the time the Technical Specifications are available for review.

7.3.2.5 Auxiliary Feedwater System

During its review of the AFS for Catawba, the staff has been concerned with several instrumentation and control features provided. These concerns are centered on the use of nonsafety-grade equipment and systems, the design may not meet the single-failure criterion, and manually operated valves may block automatic initiation. The staff has expressed these concerns to the applicant and will evaluate the applicant's response in a supplement to this report.

7.3.2.6 TMI-2 Action Plan Item II.E.1.2, Auxiliary Feedwater System Automatic Initiation and Flow Indication

Action Plan Item II.E.1.2 requires the following features: (1) a reliable automatic indication of the AFS and (2) a reliable indication in the control room of the auxiliary feedwater flow.

The staff's review of the Catawba design shows that

(1) Automatic initiation of the AFS is part of the ESFAS. The staff has expressed its concerns (see Section 7.3.2.5) on this area of the auxiliary feedwater design and will address the applicant's response in a supplement to this report.

(2) A single auxiliary feedwater flow indicator is provided in the control room for each steam generator. From the information provided by the

Insert 3

7.3.2.5 Auxiliary Feedwater System (AFS)

The review of the design of an auxiliary feedwater system ~~typically~~ included a number of considerations to assure its capability as an effective post trip decay heat removal system. These considerations include

(1) Automatic initiation
(2) The capability to control flow to establish and maintain steam generator level
(3) The capability to control steam generator pressure
(4) The capability to isolate faulted steam generators due to feedwater / steamline breaks or tube ruptures
(5) The capability for post trip control from remote shutdown panel

The functional requirements for ~~the~~ an auxiliary feedwater system are provided in Branch Technical Position RSB 5-1, "Design Requirements of the Residual Heat Removal System." These requirements include the following:

(1) The design shall be such that shutdown conditions can be achieved using only safety-grade systems satisfying GDCs 1 through 5

(2) The systems shall have suitable redundancy in components and features to assure that the system function can be accomplished assuming a single failure.

(3) The systems shall be capable of being operated from the control room.

(4) The systems shall be capable of operation with only onsite or offsite power available.

During the staff's review of the AFS for Catawba, several concerns were identified and are summarized as follows:

(1) The control of steam generator level following automatic initiation of the AFS is performed by the plant operator positioning the control valve in the AFS line to each steam generator. Two control valves are provided for each steam generator. One valve regulates the flow supplied from a motor-driven AFS pump and the other regulates the flow supplied by the turbine-driven pump. The electrical power requirement for the two control valves for each steam generator are supplied from independent power sources. The plant instrument air system provides the motive power to position all of the control valves. An isolation valve in series with each flow control valve provides the means to control steam generator level (valve open or closed) in the event that instrument air is not available from the single, non-safety grade instrument air system. Since that the operability of the AFS isolation valves is not dependent on non-safety components or support systems and that two valves associated with each steam generator are powered from redundant class 1E power sources, we find the design acceptable.

(2) Two isolation valves are provided for each steam generator. One isolation valve isolates flow from a motor-driven

pump and the other isolates flow from the turbine-driven pump. These are the only safety grade components, other than tripping the AFS pumps, which can terminate auxiliary feedwater flow to a faulted steam generator. The applicant has stated that termination of flow to a faulted steam generator is not required prior to thirty minutes. Flow can be terminated by manual closure of the safety grade isolation valves or by use of the non-safety grade flow control valves. Further, local handwheels permit closure of the air-operated control valves on loss of instrument air. We find this acceptable.

(3) The only safety grade components provided to control steam generator pressure following post-trip conditions are the steam generator code safety valves. In that the code safety valves only limit pressure to their set value, they do not provide a means for control room control of plant cool down to permit operation of the RHR system nor provide the means to mitigate the consequences of steam generator tube ruptures. These concerns are being pursued with the applicant as noted in Section 5.4.3 of this SER. The resolution of this matter will be addressed in a supplement to this report.

(4) As noted in item (3) above, the staff has questioned the ~~design~~ adequacy of the design in that control of steam generator pressure has not included the steam generator PORV's as safety grade components. These concerns are further compounded by interlocks used with the PORV's which preclude their use following a main steam isolation signal of the failure of either train of redundant logic associated with these interlocks. The resolution

of these concerns will be ~~addressed~~ pursued with those noted in item (3) above.

7.3.2.6 TMI-2 Action Plan Item II.E.1.2, Auxiliary Feedwater System Automatic Initiation and Flow Indication

Action Plan Item II.E.1.2 requires the following features:

(1) A reliable automatic initiation of the AFS

(2) A reliable indication in the control room of the AFS flow.

The staff's review of the Catawba AFS design shows that:

(1) Automatic initiation of the AFS is part of the ESFAS and the staff finds this aspect of the design acceptable.

(2) A single auxiliary feedwater flow indicator is provided in the control room for each steam generator. Highly reliable, battery-backed power sources are used to conform with Branch Technical Position ASB 10-1. The staff finds this acceptable.

Based on the above, the staff finds that the Catawba AFS satisfies the requirements of this item.

applicant, the staff believes that alternate sources for the indicator circuitry have not been selected at this time. The staff has expressed this concern to the applicant and will evaluate the applicant response in a supplement to this report.

7.3.2.7 Test of Engineered Safeguards P-4 Interlock

On November 7, 1979, Westinghouse notified the Commission of a potential 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. To minimize the possibility of accidental shorting or grounding of safety system circuits during testing of the P-4 interlocks, the staff required that suitable test jacks be provided to facilitate testing. The applicant is permanently installing a voltage indicator across the terminals. The staff finds this acceptable on confirmation of the installation. The staff has expressed this concern to the applicant and will evaluate the applicant's response in a supplement to this report.

7.3.2.8 Nondetectable Failure in Power Lockout Circuitry

Safety injection pump suction isolation valve (NI100B) and safety injection pump miniflow header to feedwater valve (NI147B) require power lockout to meet the single-failure criterion. The power lockout scheme for each valve uses an additional manually operated contactor, [illegible]. The staff concludes that a short of the [illegible] contacts for either "MAINTAINED" switch [illegible] (valve operation or power lockout) would constitute a nondetectable failure and thus violate the single-failure criterion. In response to the staff's concern, the applicant proposed a design change which would permit testing to verify the operability of the power lockout independent of the valve control switches. Further, the applicant confirmed in a December 8, 1982 letter that the circuitry will be tested in the valve closure direction at least once per refueling outage. The staff finds this acceptable.

7.3.2.9 Main Feedwater Isolation on High Doghouse Level

See Insert 4

Main feedwater lines entering a doghouse are isolated when a high level is sensed in that doghouse. Although those lines are safety grade, the applicant has not addressed or documented this isolation action in the FSAR. The staff has expressed concern that flooding within the doghouse may be a safety

Insert 4

7.3.2.9. Main Feedwater Isolation on High Doghouse Level

The containment penetration area for the main feedwater lines is called the doghouse. Two ~~is~~ separate doghouses are provided through which the feedwater lines for two steam generators run. Two water level switches are provided in each doghouse which are used to initiate feedwater isolation for line break protection in ~~the~~ the doghouses. Since the FSAR did not provide the design basis for this system, the staff inquired about ~~the~~ its safety significance. ~~This~~ In response, the applicant stated that the plant safety analysis relies on the protective action afforded by this system. Each level switch actuates a train of feedwater isolation logic. Since this system is not testable during power operation, the staff concludes that it does not conform to the regulatory requirements of GDC-21 and therefore, an acceptable finding ~~cannot~~ cannot be made at this time.

problem, and the applicant has confirmed that this feedwater isolation action is required for safety.

The logic for this isolation circuitry is one-out-of-one for each of the two trains. The applicant has indicated that this circuitry will be tested only during plant shutdowns. The staff has expressed its concern to the applicant about the testability and reliability of isolation circuitry. The staff will evaluate the applicant's response in a supplement to this report.

7.3.2.10 Switchover from Injection to Recirculation Mode

As described in Section 7.3.1.2.15, the switchover from injection mode to recirculation mode is initiated when water level in the RWST reaches a preset trip set point, and a safety injection signal ("S") has been received. The "S" signal is latched in by a retentive memory device that has an individual, manual reset. If the retentive memory device would be reset, no switchover to recirculation mode would be initiated even though it would be required by a low RWST water level. An indicator light is provided that lights when an "S" signal is received and remains lit until the operator resets the memory device. The staff finds this aspect of the design acceptable.

The staff, however, has expressed concern over the testing and manual switchover capabilities of the logic circuitry. The staff will evaluate the applicant's response in a supplement to this report.

7.3.2.11 Steam Generator Power-Operated Relief Valve Isolation

In discussions with the applicant, it was indicated that consideration was being given to implementing a safety-grade protective action that would initiate closure of the steam generator power-operated relief valves (PORVs) on the main steam isolation signal. The staff has expressed a concern that this may preclude the use of the PORVs for subsequent control of steam generator pressure for plant shutdown. The staff will evaluate the applicant's response in a supplement to this report.

7.3.2.12 Containment Pressure Control System

see insert 5

As described in Section 7.3.1.2.4 and 7.3.1.2.5, the CPCS provides four containment pressure sensor channels for each train of the containment spray system and the containment air return and hydrogen skimmer system to prevent manual and automatic operation of these ESF systems below a 0.25 psig containment pressure. The staff has expressed concern that a single failure may cause excessive containment depressurization; the staff will evaluate the applicant's response in a supplement to this report.

7.3.3 Conclusions

The review of the instrumentation and control aspects of the ESF systems included the 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.

The staff has conducted an audit review of these systems for conformance with guidelines of the applicable RGs and industry codes and standards as outlined in the SRP Section 7.3, Parts II and III. In Section 7.1 of this SER, the staff concluded that the applicant had adequately identified the guidelines applicable to these systems. Based on its audit review of the system design for conformance to the guidelines, the staff finds that upon satisfactory resolution of the ~~open items~~ concerns identified in Sections 7.3.2.1 ~~and~~, 7.3.2.5, ~~through~~ 7.3.2.9, and 7.3.2.11 ~~7.3.2.10~~ there is reasonable assurance that the systems conform with the applicable guidelines.

The staff review has included the identification of those systems and components for the ESFAS and ESF control systems that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based on its review, the staff concludes that the applitant 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

Insert 5

7.3.2.10 Containment Pressure Control System (CPCS)

As described in Sections 7.3.1.2.4 and 7.3.1.2.5, the CPCS provides four containment pressure sensor channels for each train of the containment spray system and the containment air return and hydrogen skimmer system to prevent manual and automatic operation of these ESF systems below a 0.25 psig containment pressure. The staff expressed concern that a single failure, affecting more than one of the four sensor channels associated with each train of the CPCS, could cause excessive containment depressurization. The applicant's response indicated that the independence of the four sensor channels within the same train is maintained by separating the sensors and cables per the protection channel separation criteria described in ~~FSAR~~ FSAR Section 7.3.2.2.3. Based on this, the staff finds this issue resolved subject to written confirmation of the separation applied to this installation.

Technical specifications will be required to include the CPCS and the low pressure interlocks.

7.3.~~2.11~~ Lockout of Manual Control by the Load Se~~quencer~~

During load sequencing, manual control of certain ESF loads is blocked by the sequencer. If the safety injection reset timer or the diesel sequencer sh~~ould fail~~, manual reset of the sequencer may be prevented or the sequence may not be completed. Under these conditions, the operator could be prevented from manually initiating ESF loads or manually tripping ESF loads unless he removes power from the sequencer in order to regain manu

7.3.2.11 ~~Lockout~~ Lockout of Manual Control by the Load Sequencer

Safety injection and/or loss of power will result in the automatic sequencing of required loads on the essential auxiliary power system. Under these conditions, the load sequencer removes manual capability to control loads and automatically starts each load in sequence. As noted in Section 8.4.8 of this SER, the load sequence can operate in an accelerated or dedicated sequence. The latter sequence permits loading of manually controlled loads within 12 minutes from the diesel generator start. For a safety injection, the capability to manually trip ~~each~~ any load which is started by the sequencer is not available until the operator resets safety injection and the load sequencer. Only by completing these actions can the operator regain manual control capability of sequenced loads. Based on our review, we conclude that a single failure could result in all loads being energized in sequence, but the operator would be unable to trip and subsequently restart any of the individual loads associated with a train of protection systems associated with one of the redundant essential buses. While single failure considerations could preclude the operability of one train of the safety system, the staff has not previously encountered a situation which would preclude manual control of all sequenced loads. Therefore, the safety significance of potential single failures for this aspect of the load sequencer design has not fully been evaluated. Further, the staff has not determined at this time whether any regulatory requirement or guidance provided in regulatory guides and industry standards should be applied to the failure modes of concern. The staff has requested

the applicant to address these concerns and therefore, we are not in a position to conclude that this aspect of the sequencer design is acceptable. The resolution of this issue will be addressed in a supplement to this report.

7.3.2.12 Auxiliary Feedwater Pump Suction Alignment Logic

As described in Section 7.3.1.2.1, the water supply to the auxiliary feedwater pumps is automatically transferred from the condensate supply to the NSW system under certain conditions. The logic circuitry for this transfer, shown in FSAR Figures 7.4.1 and 7.4.1.2, is complex and contains multiple coincidence logic and time delays. The staff has expressed concern about the testability of this circuitry during power operation. A requirement will be added to plant Technical Specifications to insure that this circuitry is tested.

7.3.2 (13) Undetectable Failure in On-Line Testing Circuitry for Engineered Safeguards Relays

On August 6, 1982, Westinghouse notified the staff of a potential undetectable failure in on-line 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 push buttons. If, after testing, a shunt is not provided for any proving lamp due to a switch contact failure, any subsequent safeguards actuation could cause the lamp to burn open prior to its associated slave relay being energized. This would then prevent actuation of any associated safeguards devices on that slave relay. Westinghouse has provided test procedures which ensure that the slave relay circuits operate normally when testing of the master relays is completed. The applicant stated that these additional test procedures will be performed and that a ~~permit~~ permanent circuit modification is being considered.

Until an acceptable circuit modification is installed, the staff will require technical specifications to include monthly tests (in lieu of quarterly) of any slave relay which has a proving lamp. These tests should be performed immediately following the monthly test of an associated master relay.

programs to demonstrate the capability of these systems and compcnents to survive applicable events. Therefore, the staff finds that the identification of the systems and components satisfies this aspect of the GDC 2 and GDC 4.

Based on its review, the staff concludes that the ESFAS conforms with the design bases requirements of IEEE Standard 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 FSAR. Therefore, the staff finds that the ESFAS satisfies the requirements of GDC 20.

The ESFAS adequately conforms with the guidance for periodic testing in RG 1.22 and IEEE Standard 338 as supplemented by RG 1.118. The bypassed and inoperable status indication adequately conforms to the guidance of RG 1.47. The ESFAS adequately conforms with the guidance on the application of the single-failure criterion in IEEE Standard 379 as supplemented by RG 1.53. Based on its review, the staff concludes that the ESFAS satisfies the requirement of IEEE Standard 279 with regard to the system reliability and testability. Therefore, the staff finds that the ESFAS satisfies the requirement of GDC 21.

The ESFAS adequately conforms with the guidance in IEEE Standard 384 as supplemented by RG 1.75 for the protection system independence. Based on its review, the staff concludes that the ESFAS satisfies the requirement of IEEE Standard 279 with regard to the systems independence. Therefore, the staff finds that the ESFAS satisfies the requirement of GDC 22.

Based on its review of the ESFAS, the staff concludes 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, the staff finds that the ESFAS satisfies the requirements of GDC 23.

Based on its review of the interfaces between the ESFAS and plant operating control systems, the staff concludes that the system satisfies the requirements of IEEE Standard 279 with regard to control and protection system interactions.

Therefore, the staff finds that the ESFAS satisfies the requirement of GDC 24.

The staff's conclusions, noted above, are based on the requirements of IEEE Standard 279 with respect to the design of the ESFAS. Therefore, the staff finds that the ESFAS satisfies the requirement of 10 CFR 50.55a(h) with regard to IEEE Standard 279.

The staff's review of the ESFAS and ESF control systems has examined the dependence of these systems on the availability of EAS systems. Based on its review and coordination with those having primary review responsibility of the EAS systems, the staff concludes that the design of the ESFAS and ESF control systems are compatible with the functional performance requirements of EAS systems. Therefore, the staff finds the interfaces between the ESFAS and ESF control systems and the EAS systems to be acceptable.

The staff's review of the ESF control systems included conformance with the requirements for testability, operability with onsite and offsite electrical power, and single failures consistent with the GDC applicable to these ESF systems. The staff concludes 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, the staff finds the ESF control systems meet the relevant requirements of GDC 34, 35, 38, and 41.

In summary, the staff concludes that the ESFAS and the ESF control systems will be acceptable and meet the relevant requirements of GDC 2, 4, 20 through 24, 34, 35, 38, and 41 and 10 CFR 50.55a(h), subject to resolution of the ~~open~~ concerns ~~items~~ identified in Sections 7.3.2.1 ~~and~~, 7.3.2.5, ~~through 7.3.2.10~~ 7.3.2.9, and 7.3.2.11 of this report.

short pg

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 that~~ The systems required for safe shutdown must:

(1) prevent the reactor from achieving criticality

(2) provide an adequate heat sink so 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
(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 also 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 also can 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 :

(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) condensate storage tank level

The above indicators are provided in the main control room and also on the remote shutdown panels.

The systems used for safe shutdown include the following:

(1) reactor coolant system
(2) main steam system
(3) auxiliary feedwater system
(4) chemical and volume control system
(5) component cooling water system
(6) nuclear service water system
(7) residual heat removal system
(8) supportive HVAC systems

7.4.1.1.1 Reactor Coolant System

The reactor coolant system (RCS) transfers core residual heat to the steam generators. The reactor core is at a lower elevation than the steam generators, ensuring that heat can be transported from the reactor core to the steam generators through 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 system can be placed in operation. Core residual heat and RCS sensible heat can be removed by use of the PORVs 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 chemical and volume control system (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, draining, and hydrostatic testing in the RCS

The safety-related part of the CVCS consists of two redundant, separate, and independent trains each of which is capable of supplying minimum emergency core cooling. In the event that system control must be transferred to the auxiliary shutdown complex, all ESF signals to the CVCS are defeated to allow for manual control.

7.4.1.1.5 Component Cooling Water System

The component cooling water system serves as an intermediate system and a second boundary between the RCS and the nuclear service water (NSW) system. The NSW system provides an ensured source of cooling water to the component cooling heat exchangers. Normal makeup to the component cooling water system is provided by the makeup demineralized water system. An ensured supply of makeup water is available from the NSW system. The component cooling water system consists of two independent subsystems--one subsystem for Unit 1 and another for Unit 2.

Each subsystem consists of two redundant trains. Each train consists of two component cooling pumps, one component cooling heat exchanger, one surge tank, one drain sump pump, and associated valves, piping, and instrumentation. Each train of component cooling equipment supplies cooling water to a corresponding

train of the following redundant engineered safety equipment:

(1) residual heat removal heat exchanger
(2) residual heat removal pump mechanical seal heat exchanger

Only one train of component cooling equipment is necessary to supply minimum requirements. All active system components considered vital to the operation of the system are redundant. Separate flow paths are used in piping that connects to the two trains of ESF equipment

7.4.1.1.6 Nuclear Service Water System

The NSW system instrumentation and controls monitor and control the operation of the NSW system to ensure a continuous supply of cooling water for essential systems and components under normal and accident conditions.

NSW is cooling water taken from either Lake Wylie or from the standby nuclear service water pond (SNSWP). This cooling water is pumped through heat exchangers in both units and returned to its source. The normal source of NSW is Lake Wylie. If water supply from Lake Wylie is lost as a result of a seismic event, the alternate source is the SNSWP, which contains sufficient water to bring the station safely to a cold shutdown following a LOCA. Two intake pits, A and B, receive water from the Lake Wylie intake structure through separate conduits. Isolation valves to Lake Wylie are closed and valves to the SNSWP are opened if a low level is sensed in either intake pit or if a phase B containment isolation signal is initiated. Each intake pit supplies suction to two pumps. The pumps that take suction from pit A are physically separated, by means of a concrete wall, from the pumps that take suction from pit B. Redundancy is fundamental in the system because either pit is capable of passing the flow needed for a simultaneous unit LOCA and unit cooldown. The operation of any two pumps on either or both supply lines is sufficient to supply all cooling water requirements for the two-unit plant for unit startup, cooldown, refueling, or postaccident operation.

7.4.1.1.7 Residual Heat Removal System

The residual heat removal system (RHRS) transfers heat from the primary coolant to the component cooling water system during plant cooldown and controls the temperature of the primary coolant during shutdown. During emergency conditions the RHRS serves as part of the emergency core cooling system and containment spray system. The RHRS consists of two redundant, separate, and independent trains each of which is capable of maintaining its design cooling function even with major single failures such as failure of an RHRS pump, valve or heat exchanger.

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 auxiliary shutdown control panels and the auxiliary feedwater pump turbine control panel. Each of the two auxiliary shutdown panels is located in a separate locked room to restrict access. Both shutdown panels are required for hot shutdown. Selector switches on the auxiliary shutdown panels allow the operator to transfer control of the equipment required for shutdown from the control room to the shutdown panels. Transfer of this control is alarmed in the control room. A loss-of-control-room test will be conducted to demonstrate the remote shutdown capability. Cold-shutdown conditions can be reached from outside the control room with some temporary instrumentation and control modifications.

7.4.2 Specific Findings

The concerns arising from the staff's review and their status follow.

7.4.2.1 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 to obtain safe shutdown upon loss of any Class 1E

or non-Class 1E bus supplying power to safety- or nonsafety-related instruments and controls. This issue was addressed for operating reactors through IE Bulletin 79-27.

The applicant has conducted a review using the guidelines of IE Bulletin 79-27 and stated that no design modifications are required. The applicant also has committed to develop or revise procedures to meet the requirement of IE Bulletin 79-27. The staff finds this acceptable.

7.4.2.2 Remote Shutdown Instrumentation and Controls

See Insert A

From the information provided by the applicant, the staff believes that design inadequacies may exist because, on transfer of control from the control room to the remote shutdown stations, automatic actions occur, safety signals are bypassed, and control and interlocks established in the control room are defeated. The staff believes that the power sources also may be inadequate for certain sequences of events. The staff has expressed its concern to the applicant; the staff will evaluate the applicant's response in a supplement to this report.

7.4.2.[illegible] Remote Shutdown Capability Test

Another concern raised by the staff, regarding the remote shutdown capability, was a need for a test to verify design adequacy. The applicant conducts a plant startup test program that includes a one-time demonstration to maintain a safe shutdown condition from outside the control room. The test is to be carried out with the plant initially above 10% power. Subject to confirmation that this test has been successfully completed, the staff considers this item to be resolved.

7.4.2.3 Testability of Circuitry for Transfer of NSW Suction from Lake Wylie to SNSWP

The transfer of NSW suction from Lake Wylie to the SNSWP on low pit level uses one-out-of-four logic (one-out-of-two logic until Unit 2 is in service) to effect the transfer. The staff has expressed

Insert A

7.4.2.2 Remote Shutdown Instrumentation and Controls

GDC-19, "Control Room," requires that equipment at appropriate location outside the control room be provided to achieve a safe shutdown condition. To meet GDC-19 (as interpreted in SRP Section 7.4 the following are required:

(1) Redundant safety grade capability to achieve and maintain hot shutdown from a location or locations remote from the control room, assuming no fire damage to any required system and equipment and assuming no accident has occurred. The remote shutdown equipment should be seismically and environmentally qualified and capable of maintaining functional operability under all service conditions postulated to occur (including abnormal environments such as loss of ventilation).

(2) Credit may be taken for manual actions (exclusive of continuous control) of systems from locations that are reasonably accessible from the Remote Shutdown Stations. Credit may not be taken for manual actions involving jumpering, rewiring, or disconnecting circuits.

(3) Redundant safety grade capability for attaining subsequent cold shutdown through the use of suitable procedures.

(4) Loss of offsite power should not negate shutdown capability from the Remote Shutdown Stations. The design and procedures should be such that following activation of control

from the remote shutdown location, a loss of offsite power will not result in subsequent overloading of essential buses or diesel generators. Manual restoration of power to shutdown loads is acceptable provided that sufficient information is available such that it can be performed in a safe manner.

(5) Manual transfer of control to the remote location(s) should not disable any automatic actuation of ESF functions or change the operating status of equipment while attaining or maintaining shutdown, other than where ESF features can be manually placed in service to achieve and maintain shutdown. It is permissible to disable automatic low pressure injection actuation in this manner when necessary to enable control of the RHR system from the remote location and while operating this system to effect cold shutdown from hot shutdown.

During the staff's review of the Catawba remote shutdown instrumentation and control, the following concerns were identified:

(1) Components, such as indication of plant parameters by sensors provided solely for the remote shutdown system are not seismically qualified.

(2) Independence of some redundant instrument systems which provide indication on separate remote shutdown panels is not

maintained to the same degree as required for redundant safety grade systems.

(3) Components may not be environmentally qualified for conditions such as loss of ventilation.

(4) All automatic actions are bypassed when control is transferred to the remote locations. This defeats automatic sequencing of shutdown loads onto emergency power sources.

(5) Some components required for ~~safe~~ safe shutdown are supplied instrument power from a bus which is load shed on a safety injection signal. This introduces the concern that either a loss of off-site power or delay of operator action to control auxiliary feedwater could lead to overcooling and subsequent SI with loss of power to remote shutdown components.

The staff has requested the applicant to response to the above concerns and will evaluate his response in a supplement to this report.

The applicant will conduct a plant start up test program that includes a one-time demonstration to maintain a safe shutdown condition from outside the control room. The test is to be carried out with the plant initially at 10% power. Subject to ~~confirmatory~~ confirmation that this test has been successfully completed, the staff finds this acceptab

concern on the testability of this transfer circuitry during power operation. Because the applicant has not ~~shown~~ developed a periodic test method, the staff will review this information during its review of plant Technical Specifications ~~review~~.

See Insert 6

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 adequate residual heat removal.

The staff has conducted an audit review of these systems for conformance to guidelines of the applicable Regulatory Guides and industry codes and standards as outlined in SRP Section 7.4, Parts II and III. In Section 7.1 of this SER, the staff concluded that the applicant had adequately identified the guidelines applicable to these systems. Based on its audit review of the systems designs for conformance to the guidelines, the staff finds that upon satisfactory resolution of the concerns identified in Sections 7.4.2.2 and 7.4.2.4 there is reasonable assurance that the systems conform fully to the applicable guidelines.

The staff review has included the identification of those systems and components required for safe shutdown that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based on the review, the staff concludes 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, the staff finds that the identification of these systems and components satisfies this aspect of the GDC 2 and 4.

Based on its review, the staff concludes that instrumentation and controls have been provided to maintain variables and systems that 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, the staff finds that the

Insert 6

7.4.2.4 Loss of Both RHR Trains Due to a Single Instrument Bus Failure

When the RHR system is used for decay heat removal, a single instrument bus failure will cause an RHR suction valve to close in each RHR train. The staff has required that the applicant provide the basis that this design does not pose a safety significant issue. The staff will address the applicant's response in a supplement to this report.

7.4.2.5 Control Switches for RHR Miniflow Valves

The control switches for the miniflow valves for the RHR pumps are uniquely configured. Both switches have a neutral position which prevents the valves from automatically opening to protect the RHR pumps on low flow conditions. The staff ~~has~~ expressed its concern that if the control switches are left in the neutral position, the miniflow valves will not respond to an automatic open signal required for RHR pump protection. This appears to be a means by which both pumps could be damaged on a safety injection signal if the minimum flow protection is not in the automatic mode.

The applicant has indicated that design changes will be implemented to alleviate this concern. This issue is resolved subject to staff confirmation that design modifications have been acceptably implemented.

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 with (1) 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) a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures. Therefore, the staff concludes that the systems required for safe shutdown satisfy the requirements of GDC 19, "Control Room."

The staff 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 this review and coordination with those having primary review responsibility for the EAS systems, the staff concludes that the design of EAS systems is compatible with the functional performance requirements of the systems reviewed in this section. Therefore, the staff finds the interfaces between the design of safe shutdown systems and the design of EAS systems to be acceptable.

The 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 GDC applicable to safe shutdown systems. The staff concludes 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, the staff finds that these systems meet the relevant requirements of GDC 34, 35, and 38.

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

38 subject to satisfactory resolution of ~~open items~~ concerns identified in Sections 7.4.2.2 and 7.4.2.4 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 postaccident monitoring and normal operating conditions. Engineered Safety Features (ESFs) bypass indicators and the monitor light panels provide information during all operating conditions. The information is displayed 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 ~~item~~ provided include the following: ~~functions~~

(1) reactor trip
(2) engineered safety features
(3) safe shutdown.

7.5.1.1 Normal Operational Monitoring

The following display instrumentation is available to the operator for monitoring conditions in the reactor, the reactor coolant system, the containment, and the process systems throughout all normal operating conditions of the plant, including anticipated operational occurrences:

single space

(1) source range flux level and startup rate
(2) intermediate range flux level and startup rate
(3) power range flux level and flux distribution
(4) $T_{average}$ (one per loop)
(5) ΔT (one per loop)
(6) overpower ΔT set point
(7) overtemperature ΔT set point
(8) pressurizer pressure
(9) pressurizer level
(10) primary coolant flow
(11) reactor coolant pump current
(12) system wide range pressure
(13) demanded rod speed
(14) auctioneered $T_{average}$
(15) $T_{reference}$
(16) control rod position
(17) control rod bank demanded position
(18) containment pressure
(19) auxiliary feedwater flow
(20) steam generator level, narrow range
(21) steam generator level, wide range
(22) programmed steam generator level
(23) main feedwater flow
(24) magnitude of signal controlling main and bypass feedwater control valves
(25) steam flow
(26) steamline pressure
(27) steam dump modulate signal
(28) turbine impulse chamber pressure

Eight monitor light panels are provided in the control room to enable the operator to quickly assess the status of all remotely operated ESF valves, motors, fans, etc.

Each monitor light panel consists of an array of white lights, one for each ESF component monitored. The monitor lights normally are not energized when the monitored component is in the position or mode required for normal power operation. An energized light on the monitor light panel normally indicates that the monitored component is in its safety position or mode.

The eight monitor light panels are arranged to monitor particular groupings of components as follows:

(1) Grouping 1 Panel monitors those components that are normally in their safety positions and receive an ESFAS signal to ensure correct positioning (containment isolation valves excepted).

(2) Grouping 2 Panel monitors those components that are normally positioned for safety injection but are realigned for recirculation.

(3) Grouping 3 Panel monitors those components that are aligned for safety injection by an ESFAS signal and are realigned for recirculation.

(4) Grouping 4 Panel monitors those components that are aligned for safety injection by an ESFAS signal and are not realigned for recirculation (containment isolation valves excepted).

(5) Grouping 5 Panel monitors those components that are normally aligned for safety injection and cold leg recirculation, but must be realigned for hot leg recirculation.

(6) Grouping 6 Panel monitors upper head injection (UHI) isolation valves (monitor lights are energized after closure of UHI isolation valves on accumulator low liquid level).

(7) Grouping 7 Panel monitors those components that are normally aligned for safety injection with power removed.

(8) Grouping 8 Panel ~~[illegible]~~ monitors containment isolation components that receive an ESFAS signal.

7.5.1.2 Postaccident Instrumentation

In addition to the instrumentation for normal operational monitoring, instrumentation channels are provided to enable the operator to perform manual safety functions, to determine the effects of manual actions taken, and to maintain safe shutdown following a reactor trip. This instrumentation, designated as the postaccident monitoring system (PAMS), monitors the following variables:

(1) wide range T_{hot} and T_{cold}
(2) pressurizer water level
(3) primary system wide range pressure
(4) containment pressure
(5) steamline pressure
(6) steam generator water level
(7) refueling water storage tank level
(8) boric acid tank level
(9) containment radiation level
(10) containment hydrogen concentration
(11) containment sump level

The requirements applied to this system include redundancy, separation, and independent power sources to meet the single-failure criterion; capability for verifying operability; and isolation from nonsafety systems. One of the channels used to monitor each parameter also is recorded. The recorders are qualified to be operable following (not during) a seismic event. This system ~~is currently under~~ will be reviewed for ~~redesign as needed to comply~~ conformance with the recommendations of RG 1.97, Revision 2 (see Section 7.5.2.1 below) as part of the applicant's overall emergency response capability.

7.5.1.3 Bypass or Inoperative Status Indication

Automatic function level bypass indication is provided in the control room for each safety-related function designed to perform automatically if it is expected that the function will be bypassed or deliberately made inoperable more than once per year when it is normally required to be operable. The

indication of bypassed or inoperable status for safety-related functions conforms with the recommendations of RG 1.47, Revision 0.

The function bypass alarms receive their inputs from valve position limit switches, circuit breaker auxiliary contacts, switch contacts, relays, and so forth indicative of function inoperability. Means for manual actuation of each bypass alarm also are provided in the control room. ~~The operator does not have the capability to disable any of the automatic function level bypass alarms.~~

A separate bypass alarm system is provided for each Catawba unit. Alarm window terminology is explicit as to the safety function affected.

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 room for each train of the following safety-related functions:

(1) annulus ventilation
(2) auxiliary building ventilation
(3) auxiliary feedwater pumps (motor-driven)
(4) auxiliary feedwater pump (turbine-driven)
(5) chemical and volume control system (charging/injection)
(6) component cooling
(7) containment air return and hydrogen skimmer
(8) containment isolation
(9) containment penetration valve injection water
(10) containment pressure control
(11) containment spray
(12) control room ventilation and chilled water
(13) diesel building ventilation
(14) diesel generator
(15) diesel generator room sump drainage
(16) groundwater drainage
(17) nuclear service water
(18) nuclear service water pump structure ventilation

(19) reactor trip
(20) residual heat removal (injection)
(21) residual heat removal (spray)
(22) safety injection
(23) safety injection (accumulator)
(24) spent fuel pool cooling
(25) upper head injection

7.5.2 Specific Findings

7.5.2.1 Postaccident Monitoring System

The postaccident monitoring system (PAMS) provides information readouts to enable the operator to perform required manual functions and to determine the effect of manual actions taken following a reactor trip. The applicant developed PAMS design criteria using applicable requirements of IEEE Standard 279-1971. These include the requirements for redundancy (either duplicate or functionally related channels), isolation, separation, Class 1E power, qualification, and the capability for verifying the operability of the monitoring channels.

The staff find that the safety-related display instrumentation is acceptable for initial plant operation. For the long term, the staff will evaluate conformance with RG 1.97 (Revision 2) in conjunction with ~~other emergency control~~ emergency response capability ~~room design~~ improvements on a schedule consistent with ~~forthcoming~~ implementation requirements for Supplement 1 to NUREG-0737.

7.5.2.2 TMI-2 Action Plan Item II.D.3, Direct Indication of Relief and Safety Valve Positions

This action plan item requires position indication in the control room for the relief and safety valves.

Seismically and environmentally qualified safety-grade position indication is provided in the control room for each of the pressurizer power-operated relief valves (PORVs) and the safety valves. The ~~PORV~~ positions of the PORVs are detected by stem-mounted limit switches. A control room computer alarm (nonsafety grade) also

is activated upon opening of a PORV. The safety-valve positions are detected by an acoustic flow detector system that senses vibrations caused by flow through the valve indicating that the valve is not fully closed. A safety-grade indicator light and a nonsafety-grade annunciator are provided in the control room to indicate flow through any of the three valves. A bar graph monitor is provided in the electrical penetration room that can be used to determine which valve is open. Based on the above information, the staff concludes that the design of this system conforms with the TMI-2 Action Plan Item II.D.3 guidelines.

7.5.2.3 TMI-2 Action Plan Item II.F.1, Additional Accident Monitoring Instrumentation

Positions (4), (5), and (6) of this action plan item require installation of a containment pressure monitor, containment water level monitor, and containment hydrogen concentration monitor.

Continuous indication and recording of the containment pressure is provided in the control room with a measurement and indication range extending from -5 psig to 60 psig. Two redundant channels of indication are provided with two channels recorded. The instrumentation is powered from the 120-V ac vital instrumentation and control power system and is seismic Category I.

The containment emergency recirculation sump for Catawba encompasses the entire floor of the lower containment. Redundant safety-grade level instrumentation is provided to measure emergency recirculation sump level. The range of this instrumentation is 0-20 ft (approximately 1,000,000 gal). Continuous indication from each redundant differential pressure transmitter is provided in the control room with two channels recorded. The instrumentation is powered from the 120-V ac vital instrumentation and control power system and is seismic Category I.

Continuous indication and recording (one channel) of the containment hydrogen concentration is provided in the control room. The hydrogen monitoring system consists of two redundant analyzer systems with a range of 0-30% hydrogen by

volume. These analyzers are powered from redundant Class 1E power supplies. Each analyzer has a local control panel indicator and alarm and a separate control room indicator and alarm. The system is seismic Category I.

Based on ~~the above information~~ our review, ~~the staff~~ we concludes that the design of these monitors conform with the TMI-2 Action Plan Item II.F.1 guidelines.

7.5.2.4 Freeze Protection for Instrumentation Sensing and Sampling Lines

In the past there have been many occurrences of frozen instrumentation and sampling lines. IE Bulletin 79-24 requested a review of plant designs to ensure that adequate measures had been taken to prevent safety-related process, instrument and sampling lines from freezing during extremely cold weather. The applicant has used heat tracing to provide the required freeze protection. An independent monitoring system with a control room annunciator is provided. A portable monitor (thermocouple) is used to periodically check the operation of the permanently installed monitors. The staff finds this design to be consistent with the function's importance to safety and, therefore, acceptable.

The staff will include a requirement to periodically test these circuits in the plant Technical Specifications.

7.5.2.5 Instrumentation Used To Initiate Safety Functions

See Insert 7

~~The staff requires that instrumentation provided to perform safety functions such as isolating nonseismic portions of systems, closing valves when tank levels reach low level set points, and similar functions should be provided with alarms and indicators commensurate with the importance of the safety function and should be testable without interfering with normal plant operations. The staff position on these instrument channels also requires that the following should be provided:~~

~~(1) an indicator in the control room to provide the operator information on the process variable being monitored that also can be used for periodic surveillance checks of the instrument transmitter~~

Insert 7

7.5.2.5 Instrumentation Used to Initiate Safety Functions

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

a) An indicator in the control room to provide the operator information on the process variable being monitored which can also be used for periodic surveillance checks of the instrument transmitter.

b) An alarm to indicate to the operator that a specific safety function has been actuated.

c) Indicator lights or other means to inform the operator which specific instrument channel has actuated the safety function.

d) Rod positions, pump flows, or valve positions to verify that the actuated safety equipment has taken the action required for the safety function.

e) The capability for testing each safety function without interfering with normal plant operations and without lifting instrument leads or using jury rigs. The capability for testing should include the transmitter where indicators are not provided to perform operability checks of the transmitters.

During recent reviews, it has been found that one or more of the features above was not provided for certain instrumentation used to initiate safety functions. The staff position is that instrumentation provided to perform safety functions such as isolating non-seismic

portions of systems, closing valves when tank levels reach low-level setpoints, and similar functions should be provided with alarms and indicators commensurate with the importance of the safety function and should be testable without interfering with normal plant operations. The applicant was requested to provide the staff with a list of all instrument channels which perform a safety function where one or more of the features listed in (a) through (e) ~~of the concern~~ above are not currently provided. For each of these instrument channels, the applicant was requested to indicate which of the features (a) through (e) are ~~or~~ not currently provided. Since the majority of items covered by the staff's position are related to interfaces with the plant operators, the applicant requested that his response to address these concerns be delayed such that it may be integrated into the control room design review.

The staff has performed an audit review of instrumentation which performs safety functions. As a result of this review, we have identified that the containment pressure transmitters used for the Containment Pressure Control System do not have indicators to facilitate surveillance checks. In response to this concern the applicant provided a commitment to install analog indicators which will permit verification of the operability of the pressure measurement channels. The staff will include a requirement in the plant Technical Specifications that a channel check be performed on a daily basis for these channels.

~~With regards to the applicant's ongoing control room design review program, he is to address the staff's concerns related~~

Based on the applicant's commitment to address the staff's concerns related to indication, alarm and test features as part of his ongoing control room design review program, the staff considers this a confirmatory item and will address the resolution of this matter in a supplement to this report if any future problems are identified.

7.5.2.6 Upper Head Injection Level Indication

Level indication is provided over a narrow range for the UHI accumulator surge tank. The only means to estimate the volume of water in the accumulator from the control room is by reading the nitrogen accumulator pressure. Since accumulator level measurements are required by R.G. 1.97, Rev. 2 this aspect of the system design will be addressed at the time that conformance to the regulatory guide is reviewed. As noted in Section 7.5.2.1, this is to be considered in the context of the plant's emergency response capability as specified in Supplement 1 to NUREG-0737.

(2) an alarm to indicate to the operator that a specific safety function has been actuated

(3) indicator lights or other means to inform the operator which specific instrument channel has actuated the safety function

(4) rod positions, pump flows, or valve positions to verify that the actuated safety equipment has taken the action required for the safety function

(5) design features to allow test of the instrument channel and actuated equipment without interfering with normal plant operations and without lifting instrument leads or using jury rigs (the capability for testing should include the transmitter where indicators are not provided to perform operability checks of the transmitters.)

The staff has requested the applicant to review all instrument channels that perform a safety function, to list those channels that do not have all of the above features, and to identify the features that are not provided. The staff will evaluate the applicant's response in a supplement to this report.

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 also has included the applicant's analyses of the manner in which the design of information systems conforms with the acceptance criteria and guidelines that are applicable to these systems as noted in the SRP.

The staff has conducted an audit review of these systems for conformance with guidelines of the applicable Regulatory Guides and industry codes and standards

as outlined in SRP Section 7.3, Parts II and III. In Section 7.1 of this SER, the staff concluded that the applicant had adequately identified the guidelines applicable to these systems. Based on the audit review of the systems designs for conformance to the guidelines, the staff finds that on satisfactory resolution of the ~~open items~~ concerns identified in Sections 7.5.2.1 ~~and~~ 7.5.2.5, and 7.5.2.6 there is reasonable assurance that the systems conform with the guidelines applicable to them.

The staff review has included the identification of those systems and components of the information systems that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based on its review, the staff concludes 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, the staff finds that the identification of these systems and components satisfies this aspect of GDC 2 and 4.

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

The staff concludes that the information systems important to safety include appropriate variables and that their range and accuracy are consistent with the plant safety analysis. Therefore, the staff finds 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, the staff finds that conformance with 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 GDC 2, 4, 13 and 19 subject to satisfactory resolution of ~~open items~~ concerns identified in Sections 7.5.2.1, ~~and~~ 7.5.2.5, and 7.5.2.6

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 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 to the hot legs of two reactor coolant loops, and the return lines are connected to the cold legs.

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. Interlocks prevent opening of the 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 600 psig). The position of the valves is indicated on the main control board by lights actuated by the valve limit switches.

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 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 the 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 set point.

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

(1) The valves open automatically on receipt of a safety injection signal ("S").

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

(3) The valves 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 also is disconnected after the valves are opened during normal power operation to prevent accidental closing. A light, actuated by the valve motor-operated limit switch, on the control room monitor light panel is on if the valve is not fully open. An alarm, operated by both the valve motor operator limit switch and valve stem limit switch, is activated when a valve is not fully open with the system above the safety injection unblock pressure.

7.6.1.3 Upper Head Injection Interlocks

The UHI system includes two accumulators, one filled with borated water, the other filled with pressurized nitrogen gas. During normal plant operation, the contents of the accumulators are separated by a membrane in the line connecting them and their pressure is maintained at equilibrium through a surge tank. Should the RCS pressure fall below the accumulator pressure, the check valves

in the two lines connecting the water accumulator to the RCS will open and the water will be forced into the RCS.

Each of the two redundant UHI lines are provided with two series, hydraulically operated isolation valves. These valves close to prevent nitrogen gas from entering the reactor coolant following the injection of the borated water from the accumulator. The valves are normally open during operation, and each valve is closed by a separate and independent low level signal and a separate hydraulic accumulator. Manual controls are provided in the control room to close the valves during shutdown and open the valves during startup. Following valve closure, a motor-driven gagging device is inserted in the valve operator to prevent reopening on the valve on loss of hydraulic pressure to the valve operator. In the event of an accident requiring UHI, the safety injection signal automatically engages the gagging devices when the isolation valves are closed. Open and closed valve position indication is provided in the control room. A separate light is provided for each valve to indicate when the valve is not fully open. A stem mounted limit switch on each accumulator isolation valve actuates an alarm in the control room if the valve is not fully open when the reactor coolant pressure is raised above the safety injection unblock pressure (P-11).

7.6.1.4 Reactor Coolant System Overpressure Protection System for Low Pressure/Temperature, Water Solid Conditions

The reactor coolant system overpressure protection system prevents the RCS from overpressurization during periods of water solid operation during startup and shutdown. The maximum RCS pressure is limited by providing a low-pressure set point interlocked with reactor coolant temperature to ~~actuate the~~ actuate two of the pressurizer PORVs. Keylock switches, located on the main control board, enable the low-pressure set point for each train of PORV actuation. When plant conditions require low temperature overpressure protection, an annunciator is provided to alert the operator. When the low-pressure set point is enabled, any pressure excursion above the set point will cause actuation of the PORVs if the ~~pressure~~ primary coolant temperature is below the temperature set point. If the system temperature rises above the temperature set point, the RCS overpressure

protection system is automatically disarmed and an annunciator alerts the operator to return the keylock switches to their normal positions. Separate wide-range temperature and pressure transmitters are provided for each train of PORV actuation.

7.6.1.5 Diesel Generator Cooling Water System Interlocks

The diesel generator cooling water system maintains diesel engine temperature within the design operating range. Each diesel generator is provided with a train of cooling water. If the temperature of a train of cooling water exceeds a predetermined set point, that train's diesel engine automatically shuts down. This interlock is automatically bypassed by a diesel emergency start signal. Alarms are provided locally and in the control room for high and low water temperature, low water pressure, and low standpipe level.

7.6.1.6 Diesel Generator Lubricating Oil System Interlocks

The diesel generator lubricating oil system pumps ~~lubricating~~ oil from the lube oil tank to the diesel generator and provides a gravity drain from the diesel engine crankcase back to the ~~sump~~ lube oil tank. Each diesel generator is provided a separate lube oil system, including interlocks to prevent starting or to shut down the engine on low lube oil pressure, low-low lube oil pressure, low turbo oil pressure, high lube oil outlet pressure, or high main bearing temperature. All of these interlocks, except the low-low lube oil pressure, are automatically bypassed by an emergency start signal. This low-low oil pressure interlock uses three pressure switches with two-out-of-three logic and is bypassed for a sufficient time to allow diesel engine starting. Alarms are provided locally and in the control room for high or low oil inlet temperature, high or low oil outlet temperature, low oil pressure, or low lube oil sump tank level.

7.6.2 Specific Findings

7.6.2.1 Interlocks for Reactor Coolant System Pressure Control During Low Temperature Operation

The generation of actuation signals to open the pressurizer PORVs to prevent the reactor coolant system pressure from exceeding allowable limits during low temperature operation is described in Section 7.6.1.4.

In its review of the control logic, the staff was concerned about incorrect mode selector switch positions not being sensed by the "Low Pressure Mode Operation Alert" alarm actuating logic. The applicant has agreed to modify this logic by providing an input from the mode selector switch to the alarm logic ~~to rectify the staff's concern~~. Based on this commitment the staff considers the issue resolved subject to confirmation of ~~circuit revision~~ installation of circuit modification.

7.6.2.2 Upper Head Injection Automatic Termination

see Insert B

Termination of the injection by the UHI system is effected automatically by the use of local level switches. With this design, the staff believes surveillance of the system is difficult, if not impractical, during power operation and, therefore, greatly reduces the confidence in the system's ability to perform its required safety function. The staff has expressed this concern to the applicant; the staff will evaluate the applicant's response in a supplement to this report.

7.6.2.3 Upper Head Injection Manual Control

see Insert B

The valves used to terminate UHI utilize hydraulic accumulators to effect automatic fast closure. Manual closure is provided only by the use of a nonsafety-grade hydraulic pump closing one of the four valves at a time. This means of manual closure is a slow process. The staff believes that operator action may be required for small- and intermediate-break LOCAs to prevent the UHI system from maintaining reactor coolant pressure and thereby leading to severe subcooling transients. The staff has expressed this concern to the applicant.

Insert 8

7.6.2.2. Upper Head Injection Termination

Termination of injection by the UHI system is effected ~~by~~ automatically by the use of local level indicating switches. Surveillance testing to determine the operability of these components requires simulation of the differential pressures corresponding to those produced by changes in level of the UHI water accumulator. Since during operation, the water level in the accumulator is above the upper level sensing tap (reference leg), normal full range indicated level corresponds to zero differential pressure at the level indicating switch. The conditions existing following surveillance when the instrument is returned to service do not provide an indicated level that conclusively verifies it was placed in service. The indicated level of an in-service device is the same as that which would be obtained if the equalizing valve between the level sensing lines were left open. Therefore, the surveillance procedures and test frequencies for these devices will be reviewed during technical specification review to assure that they are adequate for the safety function.

7.6.2.3 Upper Head Injection Manual Control

The valves used to terminate UHI utilize hydraulic accumulators to effect automatic fast closure. For large break LOCA's, interlocks provide fast closure of these accumulator isolation valves to terminate UHI ~~injection~~ and preclude introduction of nitrogen into the reactor vessel. Manual closure is provided only by use of a non-safety grade hydraulic pump closing one of the four valves at a time. This means of manual closure is a slow process

requiring on the order of 90 seconds of operator time per valve.

Since the plant safety analysis is based on automatic termination of VHI, this aspect of the design conforms to the regulatory requirements for protection systems. The staffs interpretation of Section 4.17 of IEEE Standard 279 is that manual initiation of the protective action to terminate VHI should also be provided in conformance to the requirements of this standard. On that the design does not satisfy these ~~requirements~~ regulatory requirements, the staff do~~es~~ not find this aspect of the VHI system design to be acceptable. The resolution of this matter will be addressed in a supplement to this report.

7.6.2.4 Key-Locked Switches Used to Override Isolation of Control Room Area HVAC System.

Isolation valves in the air intakes of the control room area HVAC system are closed by signals from chloride and radiation monitors and smoke detectors. A key-locked switch is used for each isolation valve which blocks the isolation signal and ~~permits~~ permits the isolation valve to be opened. This feature permits the operator to override the isolation of the air intakes due to a faulty monitor or detector. The staff expressed the concern that such action could preclude isolation of the air intake by non-failed monitors or detectors. The applicant subsequently proposed modifications that would ~~permit~~ provide the capability to block isolation signals from a failed detector or monitor but would not preclude closure of of the isolation valves due to a subsequent isolation signal. The staff finds the proposed changes resolve the staff's concern sujject

to confirmation that they have been implemented.

The staff will evaluate the applicant's response in a supplement to this report.

7.6.2.4 Upper Head Injection Level Indication

Level indication is only provided for the UHI accumulator surge tank and not for the accumulator itself. The staff believes the UHI accumulator level indication would be useful to confirm that safety actions have been taken and to aid in the manual closure capability discussed in Section 7.6.2.3. The staff has expressed this concern to the applicant. The staff will evaluate the applicant's response in a supplement to this report.

7.6.2.5 Cold-Leg Accumulator Valve Interlocks and Position Indication

A motor-operated isolation valve is provided between each safety injection tank and the reactor coolant (primary) system. The valve opens automatically when either the primary coolant system pressure exceeds the safety injection unblock pressure as specified in the Technical Specifications or when the safety injection signal ("S") 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 also is disconnected after the valves open during normal power operation to prevent accidental closing. Gear and stem limit switches are separately powered. The valve position indication in the control room is redundantly available regardless of the power lockout to the valve.

The staff concludes that the design of the cold-leg accumulator isolation valve interlocks and the valve position indication is in accordance with the requirements of BTP ICSB 4 and is acceptable.

7.6.2.6 TMI-2 Action Plan 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 PORV block valve to protect against a small-break LOCA. 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 control 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.

The applicant has stated agreement with the Westinghouse determination that an additional block valve closure system would add little protection against a PORV failure. If the staff does not accept the Westinghouse conclusions, it will ~~address this item in a supplement to this report~~ require any necessary modifications to the Catawba system.

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 GDC 2 and 4, as discussed in the following paragraph.

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 regard to this interlock system is set forth in BTP ICSB-3, "Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System." Based on its review, the staff concludes that the design of this system adequately complies with the staff's guidelines.

This review included the interlock provided to prevent overpressurization of the primary coolant system during low temperature operation. The staff's position with regard to this interlock system is set forth in BTP RSB 5-2, "Overpressurization Protection of Pressurized Water Reactors While Operating at Low Temperatures." Based on the review, the staff concludes that the design of this system adequately complies with the staff's guidelines subject to confirmation of circuit revision (see Section 7.6.2.1).

This review included the interlocks for the ECCS accumulator valves. The staff's position with regard to this interlock system is set forth in BTP ICSB-4, "Requirements of Motor Operated Valves in the ECCS Accumulator Lines." Based on the review, the staff concludes that these interlocks adequately comply with the staff's guidance.

Based on the review of the interlock systems important to safety, the staff concludes that their design bases are consistent with the plant safety analysis and the systems importance to safety. Further, the staff concludes that the aspects of the design of these systems with respect to single failures, redundancy, independence, qualification, and testability are adequate to ensure that the functional performance requirements will be met.

The review has included the identification of those systems and components of interlock systems important to safety that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based on the review, the staff concludes 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, the staff finds that the identification of the systems and components satisfies this aspect of GDC 2 and 4.

In summary, the staff concludes that the interlock systems important to safety are acceptable subject to satisfactory resolution of ~~open items~~ concerns identified in Sections 7.6.2.3 ~~through~~ and 7.6.2.6 of this report, ~~and the generic concern identified in Section 7.6.2.5~~.

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

(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 Description

(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 a control bank 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 five shutdown banks are moved to the fully withdrawn position by manual control before 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 in a group move simultaneously. There is individual position indication for each rod control cluster assembly.

(3) Plant Control Signals for Monitoring and Indication

(a) Nuclear Instrumentation Power Range System--Four channels are provided, with each using 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--The 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 a preset limit is exceeded by any shutdown rod or whenever an individual control rod position deviates from the bank demand position by 12 steps.

(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 that 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 ΔT, overpower ΔT, 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 ΔT and overpower ΔT measurement channels are used to initiate automatic turbine load runback when an overpower or overtemperature condition is approached.

(c) Turbine Loading Stop--Limits turbine loading in a power transient resulting from a reduction in reactor coolant temperature. The interlock is cleared by an increase in coolant temperature that is accomplished by reducing the boron concentration in the coolant.

(5) Pressurizer Pressure Control

The RCS 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 a result of heat losses, including heat losses a result of 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 set point 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 demand 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 that maintains a programmed water level, which is a function of neutron flux. The three-element feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the water level signal, the programmed level, and the pressure-compensated steam flow signal. The feedwater pump speed is varied to maintain a programmed pressure differential between the steam header and the feed pump discharge header.

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

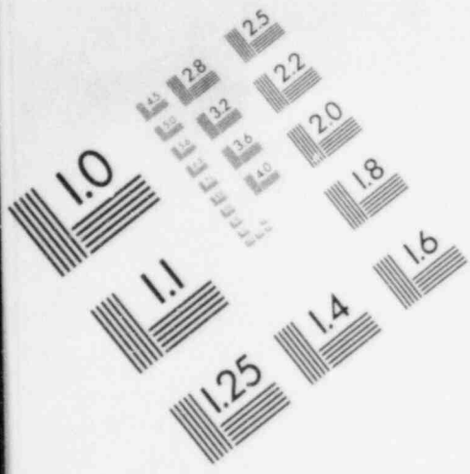
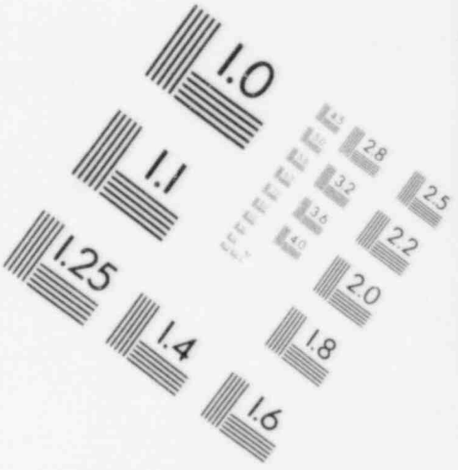
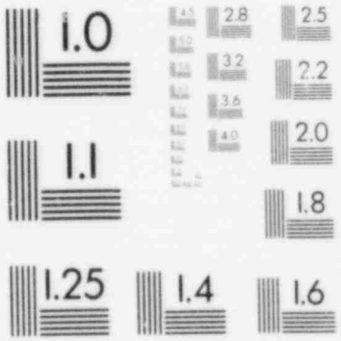
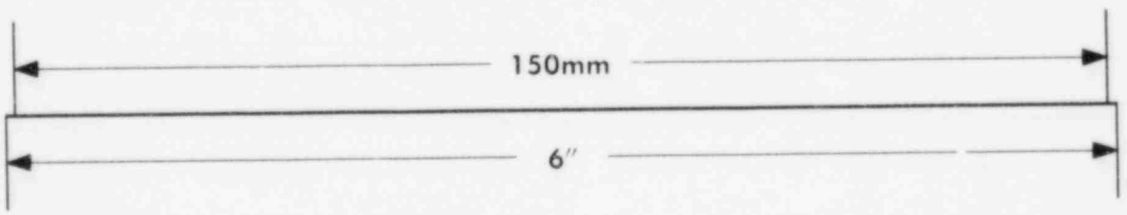
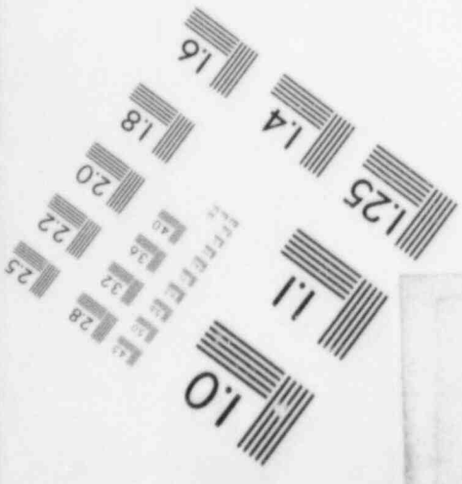


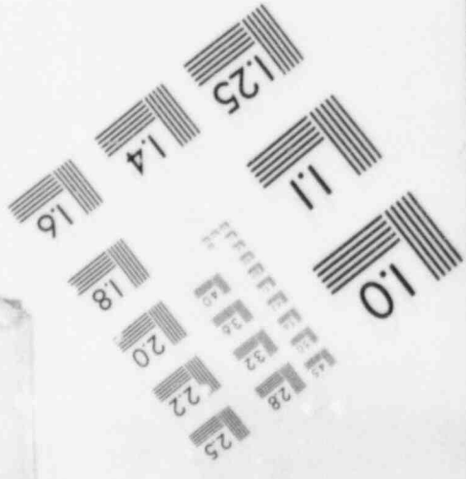
IMAGE EVALUATION TEST TARGET (MT-3)











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.

(8) Steam Dump Control System

The steam dump system, together with the rod control system, is designed to accept a 50% loss of net load without tripping the reactor. The system functions automatically by bypassing steam directly to the condenser to maintain an artificial load on the primary system. In the event load rejection exceeds 50%, main steam also is dumped to the atmosphere. 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 condensers based on measured steam pressure. This controller operates a portion of the same steam dump valves to the condenser that are used following load rejection or plant trip.

7.7.2 Specific Findings

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

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

The applicant submitted information discussing design features that limit rod speeds and malpositionings. A conclusion of the applicant's review is that even in the unlikely event of simultaneous multiple failures in the rod control system the rod speed is limited to 100 steps per minute by mechanical limitations of the drive mechanism and that this speed has been verified by tests. The consequences of positive reactivity insertion rates, which include the rod speed of 100 steps per minute, are bounded by FSAR Chapter 15 analyses. A further conclusion is that no single failure within the rod control system can cause either reactivity insertions or malpositionings of control rods that can result in core thermal conditions not bounded by FSAR Chapter 15 analyses. The staff finds the applicant's response acceptable.

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 FSAR Chapter 15. The applicant was requested to perform a review to determine what,

if any, design changes or operator actions would be necessary to ensure that high-energy-line breaks will not cause control system failures to complicate the event beyond the FSAR Chapter 15 safety analyses. The applicant has not completed this review. The staff will evaluate the applicant's response in a supplement to this report.

7.7.2.3 Multiple Control System Failures

A concern has been raised that if two or more control systems receive power or sensor information from common power sources or common sensors (including common headers or impulse lines), failures of these power sources or sensors, or rupture/plugging of a common header or impulse line, could result in transients more severe than considered in plant safety analyses.

The applicant has conducted a review to identify power sources, sensors, or sensor impulse lines that provide power or signals to two or more control systems. The effects of the failures of each of these power sources, sensors, or sensor impulse lines were analyzed. The analysis was conducted for all five major NSSS control systems: (1) reactor control system, (2) steam dump system, (3) pressurizer pressure control system, (4) pressurizer level control system, and (5) feedwater control system. The initial conditions for the analysis were assumed to be anywhere within the full operating power range of the plant (0-100%) where applicable.

The results of the analysis indicate that for any of the postulated events considered--including (1) loss of any single instrument, (2) break of any single instrument line, and (3) loss of power to all systems powered by a single power supply system (i.e., single invert -)--the Condition II accident analyses given in Chapter 15 of the FSAR are bounding. Based on the results of the applicant's review, the staff considers this item resolved.

7.7.2.4 TMI-2 Action Plan Item II.K.3.9, Proportional Integral Derivative Controller Modification

This action plan item calls for implementation of a Westinghouse recommendation

Insert 9

if any, design changes or operator actions would be necessary to ensure that high-energy-line breaks will not cause control system failures to complicate the event beyond the FSAR Chapter 15 safety analysis.

The applicant has completed this review and provided a response in a November 23, 1982, letter. The analysis was conducted for four non-safety 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 results of the analysis indicate that the pressurizer PORV control system and the main feedwater control system do not contain non-safety grade control equipment which can be exposed to environments resulting from a high-energy-line break. The steam generator PORV control system and automatic rod control system contain non-safety grade components which can be exposed to high-energy-line break environments. But for these components, the analysis concluded that the present design employs sufficient temperature ~~[illegible]~~ withstanding capability, safety grade overrides and other design features to provide adequate assurance that high-energy-line breaks will not cause control system failures to complicate the event beyond the Chapter 15 analysis. Based on the results of the applicant's review, the staff considers this issue resolved.

to modify the PORV proportional integral derivative controller to prevent derivative action from opening the PORV. Two options are provided.

The applicant has satisfied this requirement by implementing the option of setting the derivative time constant equal to zero.

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 GDC 13 and 19. This conclusion is based on the following.

Based on its 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, the staff concludes that the control systems are capable of maintaining system variables within prescribed operating limits. Therefore, the staff finds that the control systems satisfy this aspect of GDC 13.

The staff review of control systems included the features of these systems for both manual and automatic control of the process systems. The staff concludes that the features for manual and automatic control facilitate the capability to maintain plant variables within prescribed operating limits. The staff finds that the control systems permit actions that can be taken to operate the plant safely during normal operation, including anticipated operational occurrences. Therefore, the control systems satisfy GDC 19 with regard to normal plant operations.

The conclusions of the analysis of anticipated operational occurrences and accidents as presented in FSAR Chapter 15 have been used to confirm that plant safety is not dependent on the response of the control systems. The staff

concludes that failure of the systems in themselves or as a consequence of supporting systems failures, such as power sources, does not result in plant conditions more severe than those bounded by the analysis of anticipated operational occurrences.

Finally, the staff has 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, [redacted] The staff finds that the control systems are not relied upon to ensure plant safety and are, therefore, acceptable.

In summary, the staff concludes that the control systems are acceptable [redacted]

CATEGORIZATION OF SPECIFIC FINDINGS RESULTING FROM ICSB REVIEW OF CATAWBA NUCLEAR STATION UNITS 1 & 2

OPEN ITEMS

(1) Testing the Reactor Trip Breakers and Manual Trip Switches (7.2.2.1)*

(2) Main Feedwater Isolation on High Doghouse Level (7.3.2.9)

(3) Lockout of Manual Control by the Load Sequencer (7.3.2.11)

(4) Remote Shutdown Instrumentation and Controls (7.4.2.2)

(5) Loss of Both RHR Trains Due to a Single Instrument Bus Failure (7.4.2.4)

(6) Upper Head Injection Manual Control (7.6.2.3)

CONFIRMATORY ITEMS

(1) Steam Generator Level Control and Protection (7.3.2.1)

(2) Compliance With IE Bulletin 80-06 (7.3.2.2)

(3) Test of Engineered Safeguards P-4 Interlock (7.3.2.7)

(4) Containment Pressure Control System (7.3.2.10)

(5) Remote Shutdown Instrumentation and Controls (7.4.2.2)

(6) Control Switches for RHR Miniflow Valves (7.4.2.5)

(7) Instrumentation Used to Initiate Safety Functions (7.5.2.5)

(8) Interlocks for Reactor Coolant System Pressure Control During Low Temperature Operation (7.6.2.1)

(9) Key-Locked Switches Used to Override Isolation of Control Room Area HVAC System (7.6.2.4)

TECHNICAL SPECIFICATION ITEMS

(1) Water Level Measurement Errors (7.2.2.3)

(2) Lead, Lag, and Rate Time Constant Set Points Used in Safety System Channels (7.2.2.4)

(3) Verification of the Resistance Temperature Detectors Bypass Loop Flow (7.2.2.6)

(4) TMI-2 Action Plan Item II.K.3.10, Proposed Anticipatory Trip Modification (7.2.2.7)

(5) Turbine Trip Following A Reactor Trip (7.2.2.9)

(6) Safety System Trip Set Point Methodology (7.3.2.4)

(7) Containment Pressure Control System (7.3.2.10)

(8) Auxiliary Feedwater Pump Suction Alignment Logic (7.3.2.12)

(9) Undetectable Failure in On-Line Testing Circuitry for Engineered Safeguards Relays (7.3.2.13)

(10) Testability of Circuitry for Transfer of NSW Suction from Lake Wylie to SNSWP (7.4.2.3)

(11) Freeze Protection for Instrumentation Sensing and Sampling Lines (7.5.2.4)

(12) Instrumentation Used to Initiate Safety Functions (7.5.2.5)

(13) Upper Head Injection Termination (7.6.2.2)

LICENSING CONDITION

(1) TMI-2 Action Plan Item II.K.3.1, Installation and Testing of Automatic Power - Operated Relief Valve Isolation System (7.6.2.6)

TMI-2 ACTION PLAN ITEMS

(1) TMI-2 Action Plan Item II.K.3.10, Proposed Anticipatory Trip Modification (7.2.2.7)

(2) TMI-2 Action Plan Item II.K.3.12, Confirm Existence of Anticipatory Trip Upon Turbine Trip (7.2.2.8)

(3) TMI-2 Action Plan Item II.E.1.2, Auxiliary Feedwater System Automatic Initiation and Flow Indication (7.3.2.6)

(4) TMI-2 Action Plan Item II.D.3, Direct Indication of Relief and Safety Valve Positions (7.5.2.2)

(5) TMI-2 Action Plan Item II.F.1, Additional Accident Monitoring Instrumentation (7.5.2.3.)

(6) TMI-2 Action Plan Item II.K.3.1, Installation and Testing of Automatic Power-Operated Relief Valve Isolation System (7.6.2.6)

(7) TMI-2 Action Plan Item II.K.3.9, Proportional Integral Derivative Controller Modification (7.7.2.4)

*The SER sections which address these items are indicated in parentheses following each item.

Docket
File
50-400/401

5.

SEP 13 1983

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 - SHEARON HARRIS UNITS 1 & 2

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

The enclosed Safety Evaluation Report (SER) was prepared by the Instrumentation and Control Systems Branch. This SER reflects the results of our review of the information presented in the Shearon Harris Safety Analysis Report (FSAR) through Amendment 9.

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 four open items, three confirmatory items and four technical specification items listed in Section 7.1.4 of the SER.

Original signed by
R. Wayne Houston

DESIGNATED ORIGINAL

Certified By Cheryl Thompson

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

Enclosure:
As stated

cc: R. Mattson
G. Knighton
B. Buckley
R. Capra

DISTRIBUTION:
Docket File
ICSB R/F
H. Li (PF)(2)
T. Dunning
F. Rosa
AD/RS Rdg.
Shearon Harris S/F

Contact:
H. Li, ICSB
X29452

8309220267 ~~830918~~
~~CF ADOCK 05000400~~
~~CF~~

OFFICE	ICSB/DSI	ICSB/DSI	ICSB/DSI	AD/RS/DSI			
SURNAME	HLi:ct	TDunning	FRosa	RWHouston			
DATE	9/6/83	9/9/83	9/12/83	9/13/83			

NRC FORM 318 (10-80) NRCM 0240

OFFICIAL RECORD COPY

7 INSTRUMENTATION AND CONTROLS

DESIGNATED ORIGINAL

Certified By Cheryl Thompson

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 Harris Units 1 and 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 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

Harris uses a Westinghouse NSSS with balance-of-plant (BOP) design provided by Ebasco. Many safety-related instrumentation and control systems are similar to those at North Anna, Beaver Valley, and Virgil Summer, and have been previously reviewed and approved by the staff. The staff concentrated its review on those areas where the Harris design differs from previously reviewed designs and on those areas that have remained of concern during reviews of other similar plants. Several meetings have been 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 RGs 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 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 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 subsequent version of this report. The applicable sections of this report that address these items are indicated in parentheses following each open item.

(1) Generic Westinghouse design modification for automatic reactor trip using shunt coil trip attachment (7.2.2.4)

(2) loss of non-Class 1E instrumentation and control power system bus during operation (IE Bulletin 79-27) (7.5.2)

(3) control system failure caused by malfunctions of common power source or instrument line (7.7.2)

(4) control system failure caused by high energy line breaks (7.7.2)

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 that address these items are noted in parentheses.

(1) Solid-state logic protection system test circuit (7.3.3.11)

(2) testing for remote shutdown operation (7.4.2.2)

(3) RCS Overpressure protection During Low Temperature Operation (7.6.2.2)

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) Trip setpoint and margins (7.2.2.2)

(2) Response-time testing (7.2.2.3)

(3) Spare component cooling water pump (7.3.3.9)

(4) Spare charging pump (7.3.3.10)

7.1.4.4 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.

7.1.4.5 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 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 (7.5.2.2)

(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.F.3 - Instrumentation for Monitoring Accident Conditions (7.5.2.2)

(5) II.K.3.9 - Proportional Integral Derivative Controller Modification (7.7.2.3)

(6) II.K.3.12 - Confirm Existence of Anticipatory Reactor Trip Upon Turbine Trip (7.2.2.5)

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 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, 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 7.2.2.4 of this report.

The reactor trips listed below are provided in the Harris 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 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 coincident 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 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 ΔT trip protects against excessive power (fuel rod rating protection). The setpoint for this trip is continuously calculated by analog circuits to compensate for the effects of temperature and axial neutron flux difference.

The pressurizer low pressure trip is used to protect against low pressure that could lead to DNB. The reactor is tripped when the pressurizer pressure (compensated for rate of change) falls below a preset limit. This trip is blocked below approximately 10% 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 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% 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 38% 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 approximately 70% of rated 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 second 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% 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% 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 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.

A general warning alarm in both solid-state protection system trains initiates a reactor trip. The general warning alarm is provided for each train of the solid-state protection system and is activated when the corresponding train is being tested or is otherwise inoperable. The trip resulting from the general warning alarm in both trains provides protection for conditions under which both trains of the protection system may be 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 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 nonprotective 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 (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 personnel performed tests to demonstrate that credible faults or electrical interference in cables associated with the 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 conducted by Westinghouse on the 7300 series process control system and are described 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 tests. 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 on the basis of 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 psi (absolute)

(3) fuel rod maximum linear power of 18.0 kW 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 the staff's review of the plant Technical Specifications and will be completed before the operating license is issued. 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). This information will be provided for review with the applicants proposed Technical Specifications.

7.2.2.3 Response-Time Testing

To ensure that the response time of each protective function of the reactor trip system and the engineered safety features actuation system (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.

7.2.2.4 Generic Westinghouse 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 has not however, provided a response to Generic Letter 83-28 which established the requirements for this modification. The resolution of this matter will be addressed in a supplement to this report.

7.2.2.5 TMI Action Plan Items II.K.3.12 Confirm Existence of Anticipatary Reactor Trip on Turbine Trip.

The Shearon Harris design includes an anticipatory reactor trip on a turbine trip. Two out of three logic from trip fluid pressure signals or by all closed signals from the turbine steam stop valves will cause a direct reactor trip above 10 percent of rated thermal power (P-7 interlock). The staff finds that the applicant's compliance with the Action Plan guidelines for this item is acceptable.

7.2.3 Evaluation Conclusion

The staff has conducted an audit review of the RTS for conformance to guideline of the applicable Regulatory Guides and industry codes and standards. In Section 7.1 of this SER, the staff concluded that the applicant had adequately identified the guidelines applicable to these systems. Based on its audit review of the design for conformance to the guidelines, the staff finds that there is reasonable assurance that the systems will conform to the guidelines applicable to them. The scope of the review included the FSAR descriptive information; electrical, instrumentation, and control drawings; and piping and instrumentation diagrams. In addition, meetings with the applicant, architect/engineer, and the NSSS supplier were held. These meetings provided a forum for information exchange and the answering of staff questions.

Staff review has included the identification of those systems and components for the RTS that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based on its review, the staff concludes that the applicant has identified the systems and components consistent with the design bases for the RTS. Section 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, the staff finds that the identification of the systems and components satisfies this aspect of GDC 2 "Design Bases for Protection Against Natural Phenomena," and 4 "Environmental and Missile Design Bases".

Based on its review, the staff concludes that the RTS conforms to the design-bases requirements of IEEE Std 279. The RTS includes the provision to sense accident conditions and anticipated operational occurrence and initiate reactor shutdown consistent with the analyses presented in Chapter 15 of the SAR. Therefore, the staff finds 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 1.22, "Periodic Testing of Protection System Actuation Functions," and IEEE Std 338 as supplemented by Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection System." The bypassed and inoperable status indication addequately conforms to the guidance of Regulatory Guide 1.47, "By passed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." The RTS adequately conforms to the guidance on the application of the single-failure criterion in IEEE Std 379, as supplemented by Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." Based on its review, the staff concludes that the RTS satisfies the requirements of IEEE Std 279 with regard to system reliability and testability. Therefore, the staff finds that the RTS satisfies the requirements of GDC 21, "Protection System Reliability and Testability."

The RTS adequately conforms to the guidance in IEEE Std 384 as supplemented by Regulatory Guide 1.75 for protection system independence. Based on its review, the staff concludes that the RTS satifies the requirements of IEEE Std 279 with

regard to independence of systems and hence satisfies the requirement of GDC 22, "Protection System Independence."

Based on its review of failure modes and effects for the RTS, the staff concludes 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, the staff finds that the RTS satisfies the requirements of GDC 23, "Protection System Failure Modes."

Based on its review of the interface between the RTS and plant-operating control systems, the staff concludes that the system satisfies the requirements of IEEE Std 279 with regard to control and protection system interaction. Therefore, the staff finds that the RTS satisfies the requirements of GDC 24, "Separation of Protection and Control Systems."

Based on its review of the RTS, the staff concludes 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 ensure that fuel design limits are not exceeded for such events. Therefore, the staff finds that the RTS satisfies the requirements of GDC 25, "Protection System Requirements for Reactivity Control Malfunction."

The staff's conclusions, noted above, are based on the requirements of IEEE Std 279 with respect to the design of the RTS. Therefore, the staff finds that the RTS satisfies the requirements of 10 CFR 50.55a(h) with regard to IEEE Std. 279.

The review of the RTS has examined the dependence of this system on the availability of essential auxiliary support (EAS) systems. Based on its review, the staff concludes that the design of the RTS is compatible with the functional performance requirements of EAS systems. Therefore, it finds the interfaces between the RTS design and the design of the EAS systems acceptable.

7.3 Engineered Safety Features Systems

7.3.1 System Description

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

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 a NSSS designed by Westinghouse and the BOP designed by Ebasco.

There are seven ESFAS actuation functions in the Harris design. The initiation signals for each of the ESFAS functions are listed below. The numbers in parentheses after each initiation channel indicate the coincident logic; 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 steamline pressure (2/3 in any line)

(c) high containment pressure (HI-1) (2/3)

(d) manual actuation (1/2)

(2) containment isolation phase A actuation (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 steamline 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

(1) onsite power supply system

(2) emergency service water system

(3) component cooling water system

(4) essential services chilled water system

(5) 120-V ac plant protection power system

(6) safety-related 125-V dc power system

(7) control room air conditioning system

(8) reactor auxiliary building (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 pumphouse 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) 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 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 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 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 interlocks described below. 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 the RWST level (two out of four) reaches a low-low level setpoint in conjunction with an 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 RWST 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 Actuation

The function of the containment isolation system (CIS) is to isolate nonessential lines that pass through the containment boundary. The CIS is designed to limit the release of radioactivity from the containment during abnormal events and accidents.

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 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, which 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 Actuation

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

The containment spray system (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 sodium hydroxide to mix with the spray. For the recirculation phase, the spray pump suction is automatically switched from the 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 Steamline Isolation Actuation

The main steamline isolation signal is generated on low steamline pressure or high-high containment pressure. A manual block permissive is provided for the low steamline pressure signal for use during normal plant cooldowns and heatups. A high rate of steamline pressure decrease is used to initiate main steam isolation when the low steamline pressure signals are blocked during normal plant startup and shutdown. The block of the low steamline 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 steamline 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 online 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 a reactor trip. On 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 (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. The motor-driven supply is independent of the turbine-driven supply for each steam generator. The two supplies connect in the containment at the auxiliary feedwater nozzle on the steam generator. The auxiliary feedwater (AFW) 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. The pump can be manually aligned by remote control to take suction from the emergency service water system.

The AFWS can be manually initiated and controlled from the main control board or the auxiliary shutdown panel. The AFWS control is addressed in Section 7.4

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

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 the hydrogen purge system. The hydrogen monitoring system has redundant and separate hydrogen analyzers located outside containment. Each analyzer is powered from an independent onsite power source. Two hydrogen recombiners are manually controlled and are located inside containment. The design meets functional requirements in the post-accident 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 that 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 208/120-V power panels. The dc power system consists of two safety-related 125-V batteries, one nonsafety-related 125-V battery, and one nonsafety-related 250-V battery, each with its own battery chargers and dc load center. There are four 120-V ac safety-related power distribution panels for safety-related vital instrumentation and control loads. Each power panel has a 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 the main reservoir or the auxiliary reservoir. The emergency service water system is designed to seismic Category I requirements. The nonsafety-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% 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 with 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% systems, which are powered from redundant emergency buses. The nonessential portions of the chilled water system are automatically isolated from the essential portions on receipt of a safety injection actuation signal.

7.3.2.12 Control Room Area Ventilation System

The control room area ventilation system is designed to (1) maintain suitable control room temperature and humidity for continuous plant operation; (2) detect radioactive material, chlorine, or smoke in the control room; and (3) automatically isolate the control room on detection of the above hazardous conditions. The control room area ventilation system serves both the Units 1 and 2 control rooms. The system consists of four 50% capacity air-handling units, four 50% capacity exhaust fans, four 50% capacity purge fans, and two 100% capacity filtration systems.

7.3.2.13 ESF Ventilation System

The ESF ventilation system consists of auxiliary building ESF equipment cooling, switchgear room ventilation, fuel oil transfer pumphouse 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 equipment 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 when negative containment building pressure is between 0.25 and 2.5 in. 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 TMI Action Plan 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 are included in the plant Technical Specifications. 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 indications for two steam generators are powered from the Class 1E channel A power source, and those for the other steam generators from the channel B power source. The staff concludes that the Harris design satisfies the requirements of TMI Action Plan Item II.E.1.2.

7.3.3.2 System Level ESF Manual Initiation Capability

IEEE 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 on the operation of a minimum of equipment. In the 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, fuel-handling building ventilation isolation, RAB ventilation isolation, and auxiliary feedwater isolation. By a letter dated July 1, 1983, the applicant has addressed the manual initiation capabilities for each of the above systems. The staff has reviewed the design and finds it acceptable.

7.3.3.3 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.

In response by letter dated July 15, 1983, the applicant committed to incorporate a built in test features which will consist of the addition of two voltmeters and two selector switches to the reactor trip switchgear assembly wired to the P-4 contact matrix. The staff finds this modification is acceptable and eliminates the identifed concern.

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. The applicant has stated that the requested reviews have been performed and that safety-related equipment will remain in its associated emergency mode following reset. Confirmatory tests requested by the Bulletin will be performed to verify the conclusion of this review. The staff finds this acceptable.

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

The staff requested that the applicant 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. By a letter dated July 15, 1983, the applicant has committed to insulate the steam generator reference legs as a permanent solution to the heat up concern addressed in IE Bulletin 79-21. The staff finds this acceptable.

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. By a letter dated July 15, 1983, the applicant has committed to add a fourth steam generator level channel. A two-out-of-four high-high steam generator water level signal will then used to initiate turbine trip and feedwater isolation in place of the existing two-out-of-three logic. The staff finds this acceptable.

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. 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. The applicant has modified the design to provide redundant class-IE level indicators for the spray additive tank, and provide testing capability for tank isolation valves. The staff finds that these design modifications acceptable.

7.3.3.8 Non-Class 1E Inputs to Class 1E Control Circuits

In response to a staff request, the applicant provided a list of non-Class 1E control signals that are used as inputs to Class 1E control circuits. The applicant stated that all of non-Class 1E signals are through an isolation device before signals are input to Class 1E control circuits. Failure of non-class IE input will not affect the class IE control circuits. The staff has audited the schematic drawings and finds the design acceptable.

7.3.3.9 Spare Component cooling water (CCW) pump

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 safety train separation of in the electrical power supplies and control circuits. The applicant was requested to revised the proposed Technical Specifications to include the testing of the Spare pump breaker and the CCW surge tank level instruments.

7.3.3.10 Spare Charging Pump

A spare charging pump is provided to allow continued plant operation when one of the two charging pumps is out of service. The spare pump can replace either pump in the redundant safety injection trains and still maintain the required safety train separation of electrical power supplies and control circuits. The

applicant was requested to revised the proposed Technical Specification to include the testing of the spare pump breaker.

7.3.3.11 Solid-State Logic Protection System test circuits

On August 6, 1982, 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-V ac to 15-V dc 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. On 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 not 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 applicant has proposed a circuit modification developed by the equipment vendor (Westinghouse) to resolve the concern. Based on a review of the proposed modification the staff finds it acceptable.

7.3.3.12 Failure Modes and Effects Analyses of ESFAS

The description of the ESFAS analysis, which is provided in FSAR Section 7.3.2.1, is incomplete. It does not provide all of the information required by RG 1.70, Section 7.3.2, which demonstrates how the requirements of the GDC and IEEE 279-1971 are satisfied and the extent to which the recommendations of the applicable RGs are satisfied. The applicant has referred to the failure modes and effects analysis (FMEA) 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 Westinghouse Topical Report

(3) has met the interface requirements

In FSAR Amendment 9, the applicant confirms that the Shearon Harris Nuclear Power Plant complies with the interface requirements of Appendix B of WCAP 8584/8760. This FMEA together with the assumption of compliance to the interface requirements of Appendix B and the considerations of Appendix C is applicable to engineered safety features equipment within NSSS and BOP scope and design changes subsequent to the design analyzed. The staff finds this acceptable.

7.3.4 Evaluation Conclusion

The review of the instrumentation and control aspects of the ESF systems included the ESFASs and the ESF control systems. The ESFAS detects a plant condition requiring the operation of an ESF system and/or essential auxiliary supporting (EAS) system and initiates operation of these systems. The ESF control systems regulate the operation of the ESF systems following automatic initiation by the protection system or manual initiation by the plant operator.

The staff concludes that the FSFAS and the ESF control systems are acceptable and meet the relevant requirement of GDC 2, 4, 20 through 24, 34, 35, 38, and 41 and 10 CFR 50.55a(h). This conclusion is based on the following:

The staff has conducted an audit review of these systems for conformance to guidelines of the Regulatory Guides and industry codes and standards applicable to these systems. In Section 7.1 of this SER, the staff concluded that the applicant had adequately identified the guidelines applicable to these systems. Based on its audit review of the system design for conformance to the guidelines, the staff finds that there is reasonable assurance that systems conform fully to the guidelines applicable to these systems.

The staff's review has included the identification of those systems and components for the ESFAS and ESF control systems that are designed to survive the

effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based on its review, the staff concludes that the applicant has identified those systems and components consistent with the design bases for those 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 thse events. Therefore, the staff finds that the identification of these systems and components satisfies this aspect of GDC 2 and 4.

Based on its review, the staff concludes that the ESFAS conforms to the design-bases requirements of IEEE Std 279 and that the system includes the provision to sense accident conditions and anticipated operational occurrence to initiate the operation of ESF and EAS systems consistent with the accident analysis presented in Chapter 15 of the SAR. Therefore, the staff finds that the ESFAS satisfies the requirements of GDC 20.

The ESFAS conforms to the guidelines for periodic testing in Regulatory Guide 1.22 and IEEE Std 338, as supplmented by Regulatory Guide 1.118. The bypassed and inoperable status indication conforms to the guidelines of Regulatory Guide 1.47. The ESFAS conforms to the guidelins on the application of the single-failure criterion in IEEE Std 379, as supplemented by Regulatory Guide 1.53. Based on its review, the staff concludes that the ESFAS meets the criteria of IEEE Std 279 with regard to the system's reliability and testability. Therefore, the staff finds that the ESFAS satisfies the requirement of GDC 21.

The ESFAS conforms to the guidelines in IEEE Std 384, as supplemented by Regulatory Guide 1.75, for the protection system independence. Based on its review, the staff concludes that the ESFAS satisfies the requirement of IEEE Std 279 with regard to the system's independence. Therefore, the staff finds that the ESFAS satisfies the requirement of GDC 22.

Based on its review of the analysis for the ESFAS, the staff concludes that the system is designed with due consideration of safe failure modes if conditions such as disconnection of the system, loss of energy, or postulated adverse environment are experienced. Therefore, the staff finds that the ESFAS satisfies the requirements of GDC 23.

Based on its review of the interfaces between the ESFAS and plant operating control systems, the staff concludes that the system satisfies the requirements of IEEE Std 279 with regard to control and protection system interactions. Therefore, the staff finds that the ESFSA satisfies the requirement of GDC 24.

The staff's conclusions noted above are based on the requirements of IEEE Std 279 with respect to the design of the ESFAS. Therefore, it finds that the ESFAS satisfies the requirement of 10 CFR 5).55a(h) with regard to IEEE Std 279.

The staff's review of the ESF control systems included cnformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures consistent with the GDC applicable to these ESF systems. The staff concludes 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 single-failure criterion and, therefore, meet the relevant requirements of GDC 34, 35, 38, and 41.

7.4 Systems Required for Safe Shutdown

7.4.1 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 (1) control the reactor coolant system temperature and pressure, (2) borate the reactor coolant, and (3) 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 power-operated relief valves (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) 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 heating, ventilation, and air conditioning 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 operator 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 1E 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 AFWS includes the following considerations:

(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 posttrip control from auxiliary shutdown panel

Steam generator level is operator controlled by positioning the AFW regulating valves. The two motor-driven pumps and their associated controls are redundant and powered from safety train A and B, respectively. The AFW 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. Operator speed control can be performed at the main control board or the auxiliary control panel.

During plant cold shudown, the main steam PORVs are automatically controlled by steamline pressure with remote operator adjustment of the pressure setpoint from the control room or the auxiliary shutdown panel. Operator adjustment of the AFW flow rate and steam generator pressure setpoint is used to control the cooldown rate.

A system is provided to terminate AFW to a faulted steam generator. A comparison of the differential pressures between all steam generators is made and used in conjunction with the main steam isolation signal (MSIS) to determine a steam line break and terminate auxiliary feedwater flow to the faulty steam generator. The steam generator pressure mismatch signal and MSIS are combined in a coincidence logic to develop a steam generator available signal (SGSAS). A SGAS will perform the following actions:

a. Open the auxiliary feedwater regulating and pump discharge valves to the intact steam generator.

b. Close the auxiliary feedwater regulating and pump discharge valves to the faulty steam generator.

When in a shutdown condition, manual initiation of the selected auxiliary feedwater pumps is required. This can be accomplished by using the manual control switches provided on the main control board or the auxiliary shutdown panel. Auxiliary feedwater flow indication, pump suction and discharge pressures, AFW turbine speed, valve positions, steam generator level control, and level indications are provided on the main control board and the auxiliary shutdown panel. The staff finds that the design of the Auxiliary feedwater control is acceptable.

7.4.2 Specific Findings

7.4.2.1 Capability to Achieve Cold Shutdown

The Harris design uses the steam generator PORVs in conjunction with the AFWS 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 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 identified a concern that the PORV may not function under a postulated steamline break accident in the steam tunnel; therefore, the plant may not be able to achieve cold shutdown. By letter dated July 1, 1983, the applicant has committed that the main steam power oprated relief valve operators will be qualified to function under a postulated steam line break in the steam tunnel. The staff finds this acceptable.

7.4.2.2 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 Findings

The review of systems required for safe shutdown included the sensors, circuitry, redundancy features, and actuated devices that prevent the reactor from returning to criticality and provide means for adequate residual heat removal. The review included the FSAR descriptive information, logic diagrams, single-line diagrams, schematic diagrams, and piping and instrumentation diagrams.

The staff has conducted an audit review of these systems for conformance to guidelines of the applicable Regulatory Guides and industry codes and standards. In Section 7.1 of this SER the staff concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon its audit review of the system designs for conformance to the guidelines, the staff finds that there is reasonable assurance that the systems conform to the applicable guidelines.

The staff review has included the identification of those systems and components required for safe shutdown that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles.

Based upon its review, the staff concludes 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, the staff finds that the identification of these systems and components satisfies this aspect of GDC 2, "Design Bases for Protection Against Natural Phenomena," and 4, "Environmental and Missile Design Bases."

Based on its review, the staff concludes that instrumentation and controls have been provided to maintain variables and systems that can effect 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, the staff finds that the systems required for safe shutdown satisfy the requirements of GDC 13, "Instrumentation and Control."

Instrumentation and controls have been provided within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown including a shutdown following an accident. Equipment at appropriate locations outside the control room has been provided with (1) a design capability for prompt hot shutdown of the reactor, including instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

Staff 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 its review and coordination with those having primary review responsibility for the EAS systems, the staff concludes that the designs of EAS systems are compatible with the functional performance requirements of the systems reviewed in this section. Therefore, it finds the interfaces between the designs of safe shutdown systems and the design of EAS systems acceptable.

Staff 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 GDC applicable to safe shutdown systems. The staff concludes that, in general, 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 or the single-failure criterion.

In summary, the staff concludes that the systems required for safe shutdown are acceptable and meet the relevant requirements of GDC 2, 4, 13, and 19, and the guidelines of Regulatory Guides 1.47, 1.53, and 1.62 subject to the closeout of the confirmatory items noted in Section 7.4.2.

7.5 Information Systems 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 post-accident monitoring. The display system also includes bypassed and inoperable status information.

The following information systems are provided:

(1) plant process display instrumentation
(2) reactor trip system monitoring
(3) ESF 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 Harris design is in conformance with RG 1.47. The bypass indication on the bypass panel is arranged for the ESF and the EAS system on a train basis. The system bypass indication will be indicated automatically whenever an ESF system is bypassed or becomes inoperable as a result of loss of control power or a valve not being in its proper position. A bypassed or inoperable condition can be actuated or reset manually by the operator by depressing the system window pushbutton. The

subsystem level bypassed and inoperable status will be monitored by the plant computer system.

The post-accident 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 120-V ac instrument buses, which are normally energized from the onsite emergency buses. 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) steamline pressure
(6) steam generator water level (wide 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 Specific Findings

7.5.2.1 Loss of Non-Class 1E 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 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. Base on a review of the applicant response to this matter, additional information has been requested to support the applicant's conclusion for this review.

7.5.2.2 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 valve positions are displayed on the Emergency Response Facility Information System (ERFIS) CRT located on the main control board. The resistance temperature detectors (RTDs) are provided as the backup device to detect any valve seat leakage. If there is any leakage, the RTDs will actuate on annunciator on the main control board. The valve position indicating switch will be seismically and environmentally qualified. The staff finds that the applicants compliance with the Action Plan guidelines for this item is acceptable.

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

Position (4), (5), and (6) of this action plan item require installation of a containment pressure monitor, containment water level monitor, and containment hydrogen concentration monitor.

The Shearon Harris design includes containment pressure monitoring and containment water level monitoring instrumentation as required by NUREG-0737 Item II.F.1 Attachments 4, "Containment Pressure Monitor," and 5, "Containment Water Level Monitor." Continuous indication, display, and, if desired, recording of containment pressure over a range of -5 to 135 psig will be provided in the main control room by redundant Class 1E pressure transmitters. Continuous Class 1E indication of containment water level from the bottom of the containment sump to the top of the sump (narrow range) and from the bottom of containment to the elevation equivalent to 600,000 gallons (wide range) will also be provided in the main control room from redundant instrumentation channels. The staff has reviewed the accuracies of the containment pressure and water level instrumentation and found them acceptable. In addition, the applicant has stated that the containment pressure monitoring channels shall meet the design and qualification criteria of Regulatory Guide 1.97, Revision 2, and, for the containment water level instrumentation, qualification will be in accordance with the criteria for Class 1E transmitters located inside containment and the narrow range monitors will meet the requirements of Regulatory Guide 1.89.

The hydrogen monitoring system has a range of 0-10 percent hydrogen concentration by volume with an accuracy of ± 2 percent of full scale. The system has redundant recorders for containment hydrogen concentration on the control panels with alarms for hydrogen analyzer malfunction, loss of power, and high hydrogen concentration (i.e., greater than 3.0%) in the main control room. The applicant has also stated the hydrogen monitoring system is capable of continuous indication of containment hydrogen concentration within 30 minutes of the initiation of safety injection. Based on the staff's review of the post-accident hydrogen monitoring system, we find that the requirements of NUREG-0737 Item II.F.1, Attachment 6, "Containment Hydrogen Monitor" have been met.

II.F.3--Instrumentation for Monitoring Accident Conditions (RG 1.97, Revision 2)

The Commission has instructed the staff to use SECY-82-111 (Supplement 1 of NUREG-0737) in the implementation of emergency response capability (including requirements for post-accident monitoring). Therefore, conformance to the guidelines of RG 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 completion 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."

7.5.3 Evaluation 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 status to be indicated, function control 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-related systems. The review has also included the applicable acceptance criteria and guidelines and design bases, including those for indication of bypassed or inoperable safety-related systems. The review has also included the applicant's analyses of the manner in which the design of information systems conforms to the acceptance criteria and guidelines that are applicable to these systems as noted in the SRP.

The staff concludes that the information systems important to safety are acceptable and meet the requirements of GDC 2, 4, 13, and 19. This conclusion is based on the following.

The staff has conducted an audit review of these systems for conformance to guidelines of the Regulatory Guides and industry codes and standards applicable to these systems. In Section 7.1 of this SER, the staff concluded that the applicant had adequately identified the guidelines applicable to these systems. Based on its audit review of the system design for conformance to the guidelines, the staff finds that there is reasonable assurance that these systems conform to the guidelines applicable to these systems.

Staff review has included the identification of those systems and components for the information systems that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based on

its review, the staff concludes that the applicant has identified those systems and components consistent with the design basis for those systems. Sections 3.10 and 3.11 of this SER address the qualificaiton programs to demonstrate the capability of these systems and components to survive these events. Therefore, it finds that the identification of these systems and components satisfies this aspect of GDC 2 and 4.

The staff concludes that the information systems important to safety, including the accident monitoring instrumentation, are consistent with the plant safety analysis and show substantial compliance with the guidelines of Regulatory Guide 1.97, Revision 2. Therefore, the staff finds that the information systems satisfy the requirements of GDC 13 for monitoring variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions. Further, the staff finds that conformance to GDC 13 and the applicable guidelines satisfies the requirements of GDC 19, 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 GDC 2, 4, 13, and 19.

7.6 Interlock Systems Important to Safety

7.6.1 Description

This section addresses the safety-related interlocks that

(1) prevent the overpressurization of low pressure systems

(2) prevent the overpressurization of the primary coolant system during low temperature operation

(3) ensure the availability of ECCS accumulators

(4) automatically open sump isolation valves for the recirculation mode of operation

The objectives of the review have 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 System Isolation Valves Interlock

The residual heat removal 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 it from opening if RCS pressure is greater than 425 psig and to automatically close it if RCS pressure exceeds 750 psig. Valve position indication is provided in the control room.

The redundant valve interlock design includes independence, separation, and diversity and satisfies BTP ICSB 3, "Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System," and therefore is acceptable.

7.6.2.2 RCS Overpressure Protection During Low Temperature Operation

The overpressure protection during low temperature operation is provided by automatic actuation of the pressurizer PORVs. In its review of the automatic control logic for these valves, the staff found that a failure resulting in a high output signal from either of the two auctioneers would prevent both of the valves from opening when needed. Because no indication of the auctioneered safety output signals is provided to the operator, such a failure could remain undetected. Furthermore, even if such a failure would be detected, the system would remain inoperative because no capability to manually arm the system to replace a failed permissive signal from the auctioneer is provided. By letter

dated July 1, 1983, the applicant has committed to install switches on the main control board for the operator to manually arm this system. The manual arming will be included in the operating procedure when the reactor coolant temperature is equal to or below the set point and before beginning the filling operation. The system arming will be reset when the system is brought back above the system temperature set point for arming. The staff will define the arming set point in the Technical Specifications, and the instruments for overpressure protection will be under periodic surveillance test. The staff finds this design acceptable subject to its review of the updated drawings and FSAR descriptions to be submitted by the applicant.

7.6.2.3 Accumulator Isolation Valve Interlock

A motor-operated isolation valve is provided at each accumulator outlet. These valves are normally open during 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 so that they

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

(2) 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 ensure 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 a valve motor limit switch, and the other set is actuated by a valve stem limit switch. An alarm will also sound when either of the limit switch senses that the valve is not fully open. The valve position indicating lights operated by valve motor limit switch is located

at the control module for each valve. These lights are powered by separate Class 1E, 120 V AC power supply which will not be affected by the power removal from the valve motor circuit breakers. The valve position indicating lights operated by stem limit switch is located at safeguard light box which is powered from 125 V DC power supply. The staff finds that the design satisfies the Branch Technical Position ICSB-4 and therefore is acceptable.

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 RWST levels reach the low-low level setpoint after safety injection actuation. The valve cannot be closed as long as a safety injection (SI) signal is present. The interlock from an SI signal can be removed by a reset switch, which is separate from the system level SI 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 if 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

The staff conlcudes that the design of the interlock systems important to safety is acceptable and meets the relevant requirements of GDC 2 and 4. 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 regard to this interlock system in BTP ICSB-3, "Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System." Based on its review, the staff concludes that the design of this system satisfies the staff's guidelines.

Staff review included the interlock for the ECCS accumulator isolation valve. The staff's position with regard to this interlock system is BTP ICSB-4,

"Requirements of Motor Operated Valves in the ECCS Accumulatory Lines." Based on it sreview, the staff concludes that these interlocks satisfy the staff's guidelines. Based on its review of the interlock systems important to safety, the staff concludes that the systems design bases are consistent with the plant safety analysis and their importance to safety. Further, the staff concludes that the aspects of the design of those systems with respect to single failures, redundancy, independence, qualification, and testability are adequate to ensure that the functional performance requirements of these systems will be met and that they meet the applicable requirements of GDC 2 and 4.

7.7 Control Systems

7.7.1 Description

The plant control systems that are not relied on to perform safety functions but that 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 resulting from 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 ±3.5F° of the programmed temperature. The automatic rod control is performed between 15 and 100% 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 reactor coolant 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 reactor coolant 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 setpoint, and the steam flow signal. An override signal closes all feedwater valves when the reactor coolant T_{avg} is below setpoint and the reactor has tripped. During startup or low power operation, a feed-forward control scheme 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% 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 reference reactor coolant average temperature (based

on turbine impulse chamber pressure) and the measured reactor coolant average temperature exceeds a preset value. To prevent actuation of steam dump as a result of a 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.

A freeze protection system is provided to ensure that instrumentation sensing and sampling lines for systems important to safety are protected from freezing during extremely cold weather.

The freeze protection system is designed to protect preselected piping systems exposed to ambient temperatures between 40°F and -2°F. Two thermostats are connected in parallel to turn on and turn off the heating devices. The thermostats are preset to turn on at 40°F and off at 45°F. Redundancy for the freeze protection system is provided for the systems which are critical to the safe operation and essential for safe shutdown of the plant.

7.7.2 Specific Findings

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

7.7.2.2 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 if certain nonsafety-grade control equipment were subjected to the adverse environment of a high energy line break, it 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 a consequence more severe than those of the FSAR 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.

7.7.2.3 TMI Action Plan Item

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

Westinghouse recommended that the derivative time constant in the pressurizer PORV PID controller be set to off. This action removes the derivative action from the controller so that the actuation signal to this valve is no longer sensitive to the rate of change of pressurizer pressure. The applicant has implemented this recommendation. The staff finds that the applicant's compliance with the Action Plan guidelines for this item is acceptable.

7.7.3 Evaluation Conclusions

The control systems used for normal operation, which are not relied on to perform safety functins 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 GDC 13 and 19. This conclusion is based on the following:

On the basis of its 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, the staff concludes that the control systems are capable of maintaining system variables within prescribed operating limits. Therefore, it finds that the control systems satisfy this aspect of GDC 13.

Staff review of control systems included features of these systems for both manual and automatic control of the process systems.

The staff concludes that the features for manual and automatic control facilitate the capability to maintain plant variables within prescribed operating limits. It finds that the control systems permit actions that can be taken to operate the plant safely during normal operation, including anticipated operational occurrences, and, therefore, the control systems satisfy GDC 13 with regard to normal plant operations.

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

The staff has also requested a review by the applicant to determine whether the harsh environments associated with high-energy line breaks might cause control system malfunctions and result in consequences more severe than those of Chapter 15 analyses or beyond the capability of operators or safety systems.

The staff will report on the resolution of these issues in a supplement to this report.