Docket
File
50-413/414

JUN 30 1982

MEMORANDUM FOR: Robert L. Tedesco, 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, DRAFT SAFETY EVALUATION REPORT, FSAR SECTION 7, INSTRUMENTATION AND CONTROL SYSTEMS

Plant Name: Catawba Nuclear Station, Units 1 and 2
Docket No.: 50-413/414
Licensing Status: OL
TAC No.: 05000413
Responsible Branch: LB #4
Project Manager: K. Jabbour
Review Branch: ICSB
SER Completion Date: January, 1983

Enclosed is the draft Safety Evaluation Report (SER) input for the Catawba Nuclear Station, Units 1 and 2, prepared by the Instrumentation and Control Systems Branch (ICSB) with assistance from our consultant at Argonne National Laboratories (ANL).

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 sixteen open items for which ICSB has primary review responsibility. These open items are listed in Section 7.1.3.1 of the SER.

An open item resolution meeting with the applicant will be held in August 1982. We therefore expect to resolve most of these open items prior to issuing our SER due in January 1983.

Please note that Section 7.1.3 of the SER lists not only Open Items, but also Confirmatory Items and Technical Specification Items. SSER input will not discuss Confirmatory Items unless a problem is found when final

See ~~Attachments to Mo~~ SER Docket.

Contact:
F. Burrows, ICSB
X29455

Original signed by Themis P. Speis

8207190502 820630
CF ADOCK 05000413
CF

XA

OFFICE							
SURNAME							
DATE							

NRC FORM 318 (10-80) NRCM 0240

OFFICIAL RECORD COPY

documentation is submitted by the applicant. TMI-2 Action Plan Items related to Instrumentation and Control are identified in Section 7.1.6.

The enclosed draft SER is applicable to both units at Catawba Nuclear Station.

Original Signed By
Themis P. Speis

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

cc w/enclosure:
K. Jabbour
J. Elsbergas (ANL)

cc w/o enclosure:
R. Mattson
E. Adensam
T. Speis
F. Rosa
T. Dunning
C. Rossi
R. Capra
F. Burrows

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

OFFICE	ICSB/DSI	ICSB/DSI	ICSB/DSI	ADRS/DSI			
SURNAME	FBurrows:ct	TDunning	FRosa	TPSpeis			
DATE	6/28/82	6/29/82	6/28/82	6/29/82			

NRC FORM 318 (10-80) NRCM 0240

OFFICIAL RECORD COPY

7.0 Instrumentation And Controls

7.1 INTRODUCTION

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

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 Stations Unit 1 and Unit 2. The acceptance criteria used as the basis for our evaluation are set forth in the Standard Review Plan (SRP), NUREG-0800, in Table 7-1, "Acceptance Criteria for Instrumentation and Control Systems Important to Safety," and Table 7-2, "TMI Action Plan Requirements for Instrumentation and Control Systems Important to Safety." These acceptance criteria include the applicable General Design Criteria (Appendix A to 10 CFR Part 50), and IEEE Standard 279, "Criteria for Protection Systems for Nuclear Power Generating Stations(10 CFR Part 50.55a(h)).

Guidelines for implementation of the requirements of the acceptance criteria are provided in the IEEE Standards, Regulatory Guides (RGs), and Branch Technical Positions (BTPs) of the Instrumentation and Control Systems Branch (ICSB) identified in Section 7.1 of the SRP. Conformance to the acceptance criteria provides the bases for concluding that the instrumentation and control systems meet the requirements of 10 CFR Part 50.

7.1.2 General Findings

The applicant has identified the instrumentation and control systems important to safety and the acceptance criteria which are applicable to those systems as identified in the SRP. The applicant has also identified the guidelines, including the Regulatory Guides and the industry codes and standards, which are applicable to the systems. The acceptance criteria and guidelines identified by the applicant are provided in Section 7.1.2 of the Final Safety Analysis Report (FSAR).

Based on the review of Section 7.1 of the applicant's FSAR, we conclude that the implementation of the identified acceptance criteria and guidelines satisfies the requirements of

General Design Criterion (GDC) 1, "Quality Standards and Records," with respect to the design, fabrication, erection, and testing to quality standards commensurate with the importance of the safety functions to be performed. We find that the Nuclear Steam Supply System (NSSS) and the Balance of Plant (BOP) instrumentation and control systems important to safety, addressed in Section 7.1 of the applicant's FSAR, satisfy the requirements of GDC 1 and, therefore, are acceptable.

7.1.3 Specific Findings

7.1.3.1 Open Items

The staff's conclusions noted herein are applicable to the instrumentation and control systems important to safety with the exception of the open items listed below. The staff has not completed its review of these items. The resolution of these items will be addressed in a supplement to this report. The applicable sections of this report which address these items are indicated in parentheses following each open item.

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

(2) Auxiliary Feedwater System (7.3.2.5)

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

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

(5) Non-Detectable Failure in Power Lockout Circuitry (7.3.2.8)

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

(7) Switchover from Injection to Recirculation Mode (7.3.2.10)

(8) Steam Generator PORV Isolation (7.3.2.11)

(9) Containment Pressure Control System (7.3.2.12)

(10) Remote Shutdown Instrumentation and Controls (7.4.2.2)

(11) Instrumentation Used To Initiate Safety Functions (7.5.2.5)

(12) Upper Head Injection Automatic Termination (7.6.2.2)

(13) Upper Head Injection Manual Control (7.6.2.3)

(14) Upper Head Injection Level Indication (7.6.2.4)

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

(16) High Energy Line Breaks and Consequential Control System Failures (7.7.2.2)

7.1.3.2 Confirmatory Items

In a number of areas the applicant has committed to make design changes or to provide additional documentation to address concerns raised by the staff during its review. Based upon information provided during meetings and discussions with the applicant, the staff has concluded that the technical issues have been resolved in an acceptable manner. However, the applicant must formally provide final documentation of these items. The staff will confirm that final documentation is provided prior to issuance of the operating license. The staff's conclusions on the confirmatory items will not be addressed in supplements to this report unless an unexpected problem is revealed during the review of documentation provided.

The confirmatory items and the sections in which they are addressed are as follows:

(1) Compliance with IE Bulletin 80-06 (7.3.2.2)

(2) Failure Modes and Effects Analysis (FMEA) Interface Requirements (7.3.2.3)

(3) Remote Shutdown Capability Test (7.4.2.3)

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

7.1.3.3 Technical Specification Items

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

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

(2) Water Level Measurement Errors (7.2.2.3)

(3) Lead, Lag, and Rate Time Constant Setpoints Used in Safety System Channels (7.2.2.4)

(4) Response Time Testing (7.2.2.5)

(5) Verification of RTD Bypass Loop Flow (7.2.2.7)

(6) TMI-2 Action Plan Item II.K.3.10, Proposed Anticipatory Trip Modification (7.2.2.8)

(7) Turbine Trip Following A Reactor Trip (7.2.2.10)

(8) Safety System Trip Setpoint Methodology (7.3.2.4)

(9) Testability of Circuitry for Transfer of NSW Suction from Lake Wylie to SNSWP (7.4.2.4)

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

7.1.4 Site Visit

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

7.1.5 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 (10 CFR Part 50, Appendix R) are discussed in Section 9.5.1 of this report.

7.1.6 TMI-2 Action Plan Items

The TMI Action Plan was developed to provide a comprehensive and integrated plan for actions now judged necessary to correct or improve the regulation and operation of nuclear facilities based on the experience from the accident at TMI-2. Guidance

on implementation of the Action Plan was provided to the applicants in NUREG-0737, "Clarification of TMI Action Plan Requirements." All items related to instrumentation and control have been resolved except for items II.E.1.2 and II.K.3.1. The specific items and sections of the report addressing each item area are indicated below:

(1) II.D.3 Direct Indication of Relief and Safety Valve Position (7.5.2.2)

(2) II.E.1.2 Auxiliary Feedwater System Automatic Initiation and Flow Indication (7.3.2.6)

(3) II.F.1 Additional Accident Monitoring Instrumentation - Positions 4, 5, and 6 (7.5.2.3)

(4) II.K.3.1 Installation and Testing of Automatic Power-Operated Relief Valve Isolation System (7.6.2.6)

(5) II.K.3.9 Proportional Integral Derivative Controller Modification (7.7.2.4)

(6) II.K.3.10 Proposed Anticipatory Trip Modification (7.2.2.8)

(7) II.K.3.12 Confirm Existence of Anticipatory Reactor Trip Upon Turbine Trip (7.2.2.9)

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. In order 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 are also 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 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 Reactor Trip System 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 setpoint 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 setpoint 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, test switch position, etc., 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 Reactor Trip System 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 assure 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 which 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 non-trip 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 non-protective functions, such as control, remote indication, and computer monitoring. To protect from faults in the non-safety 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

The concerns arising from our review of the Reactor Trip System and their status are as follows:

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 since 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.

7.2.2.2 Protection System Sensors and Cabling in Non-Seismic Structures

Protection system trip circuit inputs that are located in non-seismic turbine building, are:

(a) Turbine stop valve closure limit switches

(b) Turbine control valve oil pressure switches

(c) Turbine impulse pressure transducers.

Items (a) and (b) above provide inputs to the reactor trip on turbine trip circuit, item (c) 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 the Branch Technical Position ICSB 26, requires that all reactor trips, including the anticipatory trips, should meet the requirements of IEEE Standard 279. It also requires that no credible fault, such as grounding or shorting in the portion of the trip circuitry in the non-seismic 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. Since no credit is taken in the safety analysis for these inputs to the 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 non-seismic area, they have been treated, insofar as possible, as safety related and mutually redundant cables are adequately separated. Isolators are 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 Branch Technical Position ICSB 26.

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 due to a high energy line break. For such an accident, the steam generator water level provides the primary trip function and the trip setpoints 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 assure that measurement errors are factored into the basis for establishing trip setpoints. The applicant intends to use insulation on the reference legs to minimize above errors. The staff finds this approach acceptable and will insure that any environmental errors are taken in account during our review of setpoint methodology and technical specifications.

7.2.2.4 Lead, Lag, and Rate Time Constant Setpoints Used In Safety System Channels

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

7.2.2.5 Response Time Testing

To assure 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.

7.2.2.6 Trip of Reactor Coolant Pump Breakers on Underfrequency

The staff asked the applicant to provide justifications that tripping the reactor coolant pump breakers on underfrequency is not a safety function and, thus, the reactor coolant pump breakers do not have to be designed and qualified to meet the criteria applicable to equipment performing a safety function. The 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.

7.2.2.7 Verification of the RTD Bypass Loop Flow

The reactor coolant system hot and cold leg resistance temperature detectors used for reactor protection are located in reactor coolant bypass loops. A bypass loop from upstream of the steam generator to downstream of the steam generator is used for the hot leg resistance temperature detector and a bypass loop from downstream of the reactor coolant pump to

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

7.2.2.8 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 Catawba. A decision to trip the reactor following turbine trip at different power levels would involve only bistable setpoint changes and not instrument hardware changes. The staff finds that the design therefore is acceptable. The

specific power level setpoint below which a reactor trip following a turbine trip is blocked will be reviewed and specified in the plant technical specifications.

7.2.2.9 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.

7.2.2.10 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 which traverse non-seismic qualified structures are isolated from the Solid State Protection System. The circuits are fully testable during full power operation. The staff finds this design to be consistent with the function's importance to safety and, therefore, acceptable.

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

7.2.3 Evaluation Findings

We have conducted an audit review of the Reactor Trip System (RTS) for conformance to guidelines of the applicable regulatory guides and industry codes and standards as outlined in the Standard Review Plan, Section 7.2, Part II and III. In Section 7.1 of this SER, we concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon our audit review of the design for conformance to the guidelines, we find that there is reasonable assurance that the systems will conform to the applicable guidelines.

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

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

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

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

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

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

Based on our review of the Reactor Trip System, we conclude that the system satisfies the protection system requirements for malfunctions of the reactivity control system, such as accidental withdrawal of control rods. Section 15 of the SAR addresses the capability of the system to assure that fuel design limits are not exceeded for such events. Therefore, we find that the RTS satisfies the requirements of GDC-25, "Protection System Requirements for Reactivity Malfunction".

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

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

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

7.3 Engineered Safety Features 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 which 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 Engineered Safety Features (ESF) and the auxiliary support systems equipment. Typical accidents that require actuation of the ESF systems are a loss of primary coolant and steam line breaks. The plant variables that are monitored by the analog circuitry of the ESFAS include pressurizer pressure, steam line 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 Engineered Safety Features system equipment.

The ESFAS signals and the plant conditions that generate these signals are shown below. 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 steam line)

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 (non-redundant and not part of ESFAS)	(1/1)
c.	Manual	(1/2)

(4) Steam Line 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 generator)
c.	Low Tavg (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 4160V 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

(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 Reactor Trip System 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 which require safeguards actuation and which 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 is also 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 which 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 which 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 which 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 which releases radioactive material inside the containment. The containment isolation system is actuated automatically by signals from the ESFAS system (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 safety injection (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 engineered safety feature. 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) Start centrifugal charging pumps
(2) Valves in the centrifugal charging pumps suction header isolate the volume control tank and align to the refueling water storage tank
(3) Boron injection tank (BIT) suction and discharge parallel isolation valves open
(4) Close normal charging path valves

(5) BIT recirculation loop is isolated and the recirculation pumps stop

(6) Start safety injection pumps

(7) Start residual heat removal pumps

(8) Refueling water storage tank recirculation is terminated and the makeup line to the spent fuel pool is isolated

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 (CSS)

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 LOCA, a main steam line 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 operates in three sequential modes:

1) Spraying a portion of the contents of the RWST into the containment atmosphere using the containment spray pumps;

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

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 depressurivation 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 120V 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) assure 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, associated piping and valves and two independent, 100% capacity air return fans and 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 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 above, 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; (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 read-outs 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 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 System (NSW) supplies cooling water to safety and non-safety 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 with pump suction and discharges 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 Standby Nuclear Service Water Pond and the NSW pumps are started. Additionally, the crossover valves between NSW trains and the isolation valves for non-essential

heat exhangers are closed, and isolation valves for safety-related heat exchangers are automatically opened.

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 read-outs 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 due to 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 Steam Line Isolation

An automatically operated main steam isolation valve is installed in each main steam line 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 steam line isolation on low compensated steam line pressure. This allows steam line isolation on high negative pressure rate during normal plant heatups and cooldowns. The block of the low steam line pressure is automatically removed and the high rate is automatically blocked when the pressurizer pressure is above the P-11 setpoint.

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 seconds. Control air is supplied to the main steam isolation valves through two series (one train A and one train B) 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 non-safety 120 VAC and loss of offsite power will close the main steam isolation valves. The isolation valves are periodically tested to 10% of full stroke.

7.3.1.2.11 Emergency Diesel Generators

Each train of the 4160 VAC 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 are also provided for the diesels which are 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 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 post-accident conditions. The system is divided into two 100% capacity, redundant trains that are interlocked such 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 insures 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 HVAC. 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 assure that proper temperatures are maintained in the Auxiliary Building (except 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 Engineered Safety Features. Upon receipt of a Safety Injection (via sequencer) signal all non-essential 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 bypass 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 access in the Diesel Building. The system consists of two subsystems for each enclosure: (1) Normal Ventilation System and (2) Emergency Ventilation System. The Normal Ventilation System operates only during normal plant operations and its fan is cycled off and shutoff damper is closed when its associated diesel is started. The Emergency Ventilation System fans automatically start when the diesel starts 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 such that no single failure can effect 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 residual heat removal (RHR) pumps deliver water to the Reactor Coolant System from the refueling water storage tank (RWST). During the recirculation mode the water is taken from the containment sump. The transfer of the RHR pump suction to the containment sump is accomplished automatically when the RWST level decreases below the low level setpoint 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 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 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, make-up, 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

The concerns arising from our review and their status are as follows:

7.3.2.1 Steam Generator Level Control and Protection

As listed in Section 7.3.1.1 above, 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 on "Control and Protection System Interaction," since the remaining protection system would not meet the single failure criterion. We expressed our concern on this deficiency to the applicant and we will evaluate his response in a supplement to this report.

7.3.2.2 Compliance with IE Bulletin 80-06

IE Bulletin 80-06 requests a review of the Engineered Safety Features, with the objective of ensuring that no device will change position solely because of the reset of the actuation signal. In response to our question on how the Catawba design meets the requirements of IE Bulletin 80-06, the applicant has performed the requested review which did not identify any component which 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 80-06, will be conducted as part of the preoperational tests. Based on this commitment we consider 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 the Westinghouse Topical Report WCAP-8584, "Failure Mode and Effects Analysis (FMEA) of the Engineered Safety Features Actuation System," as the supporting document of FMEA for ESFAS equipment within the Westinghouse scope of supply. We 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 that a statement of confirmation will be added to the FSAR. Based on the applicant's response,

we consider this matter resolved subject to confirmation of the FSAR revision.

7.3.2.4 Safety System Trip Setpoint Methodology

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

7.3.2.5 Auxiliary Feedwater System

During our review of the Auxiliary Feedwater System for Catawba we have been concerned with several instrumentation and control features provided. These concerns are centered on the use of non-safety grade equipment and systems, the design may not meet the single failure criteria, and manually operated valves may block automatic initiation. We have expressed our concerns to the applicant and will evaluate his 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 Auxiliary Feedwater System, and (2) a reliable indication in the control room of the auxiliary feedwater flow.

Our review of the Catawba design shows that:

(1) Automatic initiation of the Auxiliary Feedwater System is part of the Engineered Safety Features Actuation System. We have expressed some concerns (see 7.3.2.5 above) on this area of the auxiliary feedwater design, and we will address the licensee 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 applicant, the staff believes that power sources for the indicator circuitry have not been selected at this time. We have expressed our concern and will evaluate his 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 which could exist in the engineered safeguards P-4 interlocks. Test procedures were developed to detect failures which might occur. The procedures require the use of voltage measurements at the terminal blocks of the reactor trip breaker cabinets. In order to minimize the possibility of accidential shorting or grounding of safety system circuits during testing, the staff position was that suitable test jacks be provided to facilitate testing of the P-4 interlocks. We have expressed our concern on this to the applicant and we will evaluate his response in a supplement to this report.

7.3.2.8 Non-Detectable 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 (M2). The staff believes a short of the 1-2 contacts for either "MAINTAINED" switch (NI65 or NI73) would constitute a non-detectable failure and thus violate the single falure criteria. We have expressed our concern on this to the applicant and will evaluate his response in a supplement to this report.

7.3.2.9 Main Feedwater Isolation on High Doghouse Level

Main feedwater lines entering a doghouse are isolated when a high level is sensed in that doghouse. Although safety-grade, the applicant does not take credit nor provides documentation for this isolation action in the FSAR. The staff has expressed concern that flooding within the doghouse may be a safety 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 only be tested during plant shutdowns. The staff has expressed concern about the testability and reliability of the above circuitry. We 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 above, the switchover from injection mode to recirculation mode is initiated when water level in the refueling water storage tank (RWST) reaches a preset trip setpoint, and a safety injection signal ("S") has been received. The "S" signal is latched in by a retentive memory device which 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 which lights when a "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. We will evaluate the applicant's response in a supplement to this report.

7.3.2.11 Steam Generator PORV Isolation

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

7.3.2.12 Containment Pressure Control System

As described in Section 7.3.1.2.4 and 7.3.1.2.5 above, the Containment Pressure Control System (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 and we 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 Engineered Safety Feature (ESF) Systems included the Engineered Safety Features Actuation System (ESFAS) and the ESF control systems. The ESFAS detects a plant condition requiring the operation of an ESF system and/or essential auxiliary support system and initiates operation of these systems. The ESF control system regulates the operation of the ESF system following automatic initiation by the protection system or manual initiation by the plant operator.

We have conducted an audit review of these systems for conformance to guidelines of the applicable Regulatory Guides and industry codes and standards as outlined in the Standard Review Plan, Section 7.3, Parts II and III. In Section 7.1 of this SER we concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon our audit review of the system design for conformance to the guidelines, we find that upon satisfactory resolution of the open items identified in Sections 7.3.2.1 and 7.3.2.5 through 7.3.2.12 there is reasonable assurance that the systems conform to the applicable guidelines.

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

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

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

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

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

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

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

Protection and Control Systems."

Our conclusions noted above are based upon the requirements of IEEE-279 with respect to the design of the ESFAS. Therefore, we find that the ESFAS satisfies the requirement of 10 CFR Part 50.55a(h) with regards to IEEE-279.

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

Our review of the ESF control systems included conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures consistent with the General Design Criteria applicable to these ESF systems. We conclude that the ESF control systems are testable and are operable on either onsite or offsite power (assuming only one source is available) and that the controls associated with redundant ESF systems are independent and satisfy the requirements of the single failure criterion. Therefore, we

find the ESF control systems meet the relevant requirements of GDC-34, "Residual Heat Removal," GDC-35, "Emergency Core Cooling," GDC-38, "Containment Heat Removal," and GDC-41, "Containment Atmosphere Cleanup."

In summary, the staff concludes that the ESFAS and the ESF control systems will be acceptable and meet the relevant requirements of General Design Criteria 2, 4, 20 thru 24, 34, 35, 38, and 41 and 10 CFR Part 50.55a(h) subject to resolution of the open items identified in Sections 7.3.2.1 and 7.3.2.5 through 7.3.2.12 of this report.

7.4 Systems Required for Safe Shutdown

7.4.1 System Description

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

7.4.1.1 Safe Shutdown Systems

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

(1) Prevent the reactor from achieving criticality, and

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

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

(1) Boration

(2) Adequate supply of auxiliary feedwater, and

(3) Residual heat removal.

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

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

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

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

The monitoring indicators for maintaining hot standby are as follows:

(1) Water level for each steam generator

(2) Pressure for each steam generator

(3) Pressurizer water level

(4) Pressurizer pressure

(5) Primary coolant hot and cold leg temperatures

(6) Auxiliary feedwater flow for each steam generator

(7) 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 (RCS)

(2) Main Steam System

(3) Auxiliary Feedwater System

(4) Chemical and Volume Control System (CVCS)

(5) Component Cooling Water System (CCWS)

(6) Nuclear Service Water System (NSW)

(7) Residual Heat Removal System (RHR)

(8) Supportive HVAC Systems

7.4.1.1.1 Reactor Coolant System

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

7.4.1.1.2 Main Steam Sy tem

The main steam system consists of main steam piping, power-operated atmospheric steam relief valves (PORVs), safety valves, and main steam isolation valves. The system is used for maintaining a hot standby condition and for plant cooldown to the temperature and pressure at which the RHR can be placed in operation. Core residual heat and RCS sensible heat can be removed by use of the PORV's if the main condenser is not in service.

7.4.1.1.3 Auxiliary Feedwater System

See Section 7.3 for a discussion of the Auxiliary Feedwater System.

7.4.1.1.4 Chemical and Volume Control System

The CVCS is designed to:

1. Maintain a predetermined water level in the pressurizer.
2. Maintain seal water injection flow to the reactor coolant pumps.
3. Control reactor coolant water chemistry conditions, radioactivity level, and soluole chemical neutron absorber concentration.

4. Provide emergency core cooling.
5. Provide means for filling, draining, and hydrostatic testing in the reactor coolant system.

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.

1.1.5 Component Cooling Water System

The Component Cooling Water System serves as an intermediate system and a second boundary between the Reactor Coolant System and the Nuclear Service Water System. The Nuclear Service Water System provides an assured 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 assured supply of makeup water is available from the Nuclear Service Water 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:

a. Residual heat removal heat exchanger

b. 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 which connects to the two trains of Engineered Safety Features equipment.

7.4.1.1.6 Nuclear Service Water System

The Nuclear Service Water (NSW) System instrumentation and controls monitor and control the operation of the NSW System in order to assure a continuous supply of cooling water for essential systems and components under normal and accident conditions.

Nuclear Service Water 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 due to a seismic event, the alternate source is 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 safety injection signal is initiated. Each intake pit supplies suction to two pumps. The pumps which take suction from pit A are physically separated from the pumps which take suction from pit B by means of a concrete wall. Redundancy is fundamental in the system in that 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 start-up, cooldown, refueling, or post-accident 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 are as follows:

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 non-safety-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 concluded that no design modifications are required. The applicant has also 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

From the information provided by the applicant, the staff believes that design inadequacies may exist in that 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 may also be inadequate for certain sequences of events. We have expressed our concern to the applicant and will evaluate his response in a supplement to this report.

7.4.2.3 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 which 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 we consider this item to be resolved.

7.4.2.4 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 utilizes one-out-of-four logic to effect the transfer. We have expressed our concern on the testability of this transfer circuitry during power operation. Since the applicant has not chosen a periodic test method, the staff will review this information during technical specifications review.

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.

We have conducted an audit review of these systems for conformance to guidelines of the applicable Regulatory Guides and industry codes and standards as outlined in the Standard Review Plan, Section 7.4, Parts II and III. In Section 7.1 of this SER we concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon our audit review of the systems designs for conformance to the guidelines we find that there is reasonable assurance that the systems conform fully to the applicable guidelines.

Our review has included the identification of those systems and components required for safe shutdown which are designed to survive the effects of earthquakes, other natural phenomena,

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

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

Instrumentation and Controls have been provided within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown including a shutdown following an accident. Equipment at appropriate locations outside the control room has been provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures. Therefore, we conclude that the systems required for safe shutdown satisfy the requirements of GDC-19, "Control Room."

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

acceptable.

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

In summary, the staff concludes that the systems required for safe shutdown are acceptable and meet the relevant requirements of General Design Criteria 2, 4, 13, 19, 34, 35, and 38 subject to satisfactory resolution of open item identified in Section 7.4.2.2 of this report.

7.5 Information Systems Important to Safety

7.5.1 System Description

Indicators, annunciators, recorders, and lights are used to provide information to the operator during post-accident monitoring and normal operating conditions. Engineered Safety Features (ESF) 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 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:

(1) Source Range Flux Level and Start-Up Rate

(2) Intermediate Range Flux Level and Start-Up Rate

(3) Power Range Flux Level and Flux Distribution

(4) $T_{average}$ (one per loop)

(5) ΔT (one per loop)

(6) Overpower ΔT Setpoint

(7) Overtemperature ΔT Setpoint

(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) Steam-Line 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 engineered safety features valves, motors, fans, etc.

Each monitor light panel consists of an array of white lights, one for each engineered safety feature 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:

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

Grouping Two Panel - components that are normally positioned for safety injection but are realigned for recirculation.

Grouping Three Panel - components that are aligned for safety injection by an ESFAS signal and are realigned for recirculation.

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

Grouping Five Panel - components that are normally aligned for safety injection and cold leg recirculation, but must be realigned for hot leg recirculation.

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

Grouping Seven Panel - components that are normally aligned for safety injection with power removed.

Grouping Eight Panel - containment isolation components that receive an ESFAS signal.

7.5.1.2 Post-Accident 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 Post-Accident 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) Steam-Line 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 single-failure criterion; capability for verifying operability; and isolation from non-safety systems. One of the channels used to monitor each parameter is also recorded. The recorders are qualified to be operable following (not during) a seismic event. This system is currently under review for redesign as needed to comply with the recommendations of Regulatory Guide 1.97, Revision 2 (see Paragraph 7.5.2.1 below).

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 to the recommendations of Regulatory Guide 1.47, Revision 0.

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

The concerns resulting from our review and their status are as follows:

7.5.2.1 Post-Accident Monitoring System

The Post-Accident Monitoring System (PAMS) provides the operator information readouts to enable him 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.

We find that the safety related display instrumentation is acceptable for initial plant operation. For the long term, the staff will evaluate conformance to R.G. 1.97 (Rev. 2), "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following

an Accident", in conjunction with other emergency control room design improvements on a schedule consistent with forthcoming implementation requirements.

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.

Safety-grade, seismically and environmentally qualified, position indication is provided in the control room for each of the pressurizer power operated relief valves (PORV) and the safety valves. The PORV positions are detected by stem-mounted limit switches. A control room computer alarm (non-safety grade) is also activated upon opening of a PORV. The safety valve positions are detected by an acoustic flow detector system which senses vibrations caused by flow through the valve indicating that the valve is not fully closed. A safety-grade indicator light and a non-safety 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 which can be used to determine which valve is open. Based on the above informa-

tion we conclude that the design of this system conforms to the Action Plan 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 VAC 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 feet (approximately 1,000,000 gallons). Continous indication from each redundant differential pressure

transmitter is provided in the control room with two channels recorded. The instrumentation is powered from the 120 VAC Vital Instrumentation and Control Power System and is seismic Category I.

Continous 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 we conclude that the design of these monitors conform to the Action Plan 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 No. 79-24 requested

a review of plant designs to assure 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

The staff requires 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 staff position on these instrument channels is further that the following should be provided:

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) 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.

We have requested the applicant to review all instrument channels which perform a safety function, to list those channels which do not have all of the above features, and to identify the features that are not provided. We 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 has also included the applicant's analyses of the manner in which the design of information systems conforms to the acceptance criteria and guidelines which are applicable to these systems as noted in the staff's Standard Review Plan.

We have conducted an audit review of these systems for conformance to guidelines of the applicable Regulatory Guides and industry codes and standards as outlined in the Standard Review Plan, Section 7.3, Parts II and III. In Section 7.1 of this SER, we concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon our audit review of the systems designs for conformance to the guidelines, we find that upon satisfactory resolution of the open items identified in Sections 7.5.2.1 and 7.5.2.5 there is reasonable assurance that the systems conform to the guidelines applicable to them.

Our review has included the identification of those systems and components of the information systems which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based upon our review, we conclude that the applicant has identified those systems and components consistent with the design bases for the systems. Sections 3.10 and 3.11 of this SER address the qualification programs to demonstrate the capability of these systems and components to survive applicable events. Therefore, we find that

the identification of these systems and components satisfies this aspect of GDC-2, "Design Bases for Protection Against Natural Phenomena," and GDC-4, "Environmental and Missile Design Bases."

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

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

In summary, the staff concludes that the information systems important to safety are acceptable and meet the requirements of General Design Criteria 2, 4, 13 and 19 subject to satisfactory resolution of open items identified in Sections 7.5.2.1 and 7.5.2.5.

7.6 Interlock Systems Important to Safety

7.6.1 System Description

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

7.6.1.1 Residual Heat Removal Isolation Valve Interlocks

The Residual Heat Removal System (RHRS) consists of two residual heat exchangers, two pumps, and the associated piping, valves, and instrumentation necessary for operational control. The inlet lines to the RHRS are connected 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 reactor coolant system (RCS) by two check valves in series. Should the RCS pressure fall below the accumulator pressure, the check valves open and borated water is forced into RCS. To prevent injection of borated water at low pressure operation during shutdown and startup, each of the accumulators is provided with a motor-operated isolation valve in series with the check valves. The valve is closed by the operator shortly after the RCS is depressurized below the safety injection unblock setpoint.

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

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

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

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

After the RCS pressure is decreased during shutdown and the motor-operated isolation valves are closed, power to the valves is disconnected to prevent accidental operation. The power to the valves is also disconnected after the valves are opened during normal power operation to prevent accidental closing. 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 (UHI) Interlocks

The Upper Head (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 Reactor Coolant System (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 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 (RCS) 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 setpoint interlocked with reactor coolant temperature to activate the two pressurizer power-operated relief valves (PORV's). Key-lock switches located on the main control board, enable the low pressure setpoint for each train of PORV. When plant conditions require low temperature overpressure protection, an annunciator is provided to alert the operator. When the low pressure setpoint is enabled, any pressure excursion above the setpoint will cause actuation of the PORV's if the plant temperature is below the temperature setpoint. If the system temperature rises above the temperature setpoint, the RCS Overpressure Protection System is automatically disarmed and

an annunciator alerts the operator to return the key-lock 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 setpoint, 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 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 employs 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

The concerns resulting from our review and their status are as follows:

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

The generation of actuation signals to open the pressurizer power-operated relief valves to prevent the reactor coolant system pressure from exceeding allowable limits during low temperature operation, is described in Section 7.6.1.4 above.

In our review of the control logic, we were 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 his logic to rectify our concern. Based on this commitment we consider the issue resolved subject to confirmation of circuit revision.

7.6.2.2 Upper Head Injection Automatic Termination

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. We have expressed our concern on this to the applicant and will evaluate his response in a supplement to this report.

7.6.2.3 Upper Head Injection Manual Control

The valves used to terminate UHI utilize hydraulic accumulators to effect automatic fast closure. Manual closure is only provided by the 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. The staff believes that operator action may be required for small and intermediate break LOCA's to prevent the UHI system from maintaining reactor coolant pressure and thereby leading to severe subcooling transients. We have expressed our concern on this to the applicant and will evaluate his 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. We have expressed our concern on this to the applicant and will evaluate his 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 is also 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.

We conclude that the design of the cold leg accumulator isolation valve interlocks and the valve position indication is in accordance with the requirements of Branch Technical Position 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 loss-of-coolant accident. The system would automatically close the block valve when the reactor coolant system pressure decays after the PORV opens. The staff requirements provide, however, that such a 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 that he agrees 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, we will address this item in a supplement to this report.

7.6.3 Conclusions

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

The review of the interlock systems important to safety included the interlocks to prevent overpressurization of low pressure systems when connected to the primary coolant system. The staff position with regards to this interlock system is set forth in Branch Technical Position ICSB-3, "Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System."

Based on our review, we conclude that the design of this system adequately complies with the staff's guidelines.

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

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

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

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

In summary, the staff concludes that the interlock systems important to safety are acceptable subject to satisfactory resolution of open items identified in Sections 7.6.2.2 through 7.6.2.4 of this report and the generic concern identified in Section 7.6.2.6.

7.7 Control Systems

The general design objectives of the Plant Control System are:

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

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

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

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

(3) Plant Control Signals for Monitoring and Indication

(a) Nuclear Instrumentation Power Range System

Four channels are provided. Each of the channels uses a dual-section ionization chamber as a neutron flux detector. The currents from the ionization chambers are used to measure the power level, axial flux imbalance, and radial flux imbalance.

(b) Rod Position Monitoring System

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

(c) Control Bank Rod Insertion Monitoring

Provides warning to the operator of excessive rod insertion. The "low" alarm alerts the operator of an approach to the rod insertion limits requiring boron addition by following normal procedures

with the Chemical and Volume Control System. The "low-low" alarm alerts to a need for immediate action to add boron by any one of several alternate methods.

(d) Rod Deviation Alarm

The rod deviation alarm is generated by the Digital Rod Position Indication System whenever 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 which could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures. The inter-

locks 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 which is accomplished by reducing the boron concentration in the coolant.

(5) Pressurizer Pressure Control

The Reactor Coolant System pressure is controlled by using either the heaters (in the water region) or

the spray (in the steam region) of the pressurizer plus steam relief for large transients. The electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater group is proportionally controlled to correct small pressure variations. These variations are due to heat losses, including heat losses due to a small continuous spray. The remaining (backup) heaters are turned on when the pressurizer pressure control signal demands approximately 100 percent proportional heater power.

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

(6) Pressurizer Water Level Control

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

A programmed pressurizer water level is maintained by the Chemical and Volume Control System. During normal plant operation, the charging flow varies to produce the flow 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 which 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 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 is also 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 which are used following load rejection or plant trip.

7.7.2 Specific Findings

The concerns arising from our review of the control systems and their status are as follows:

7.7.2.1 Design Features Limiting The Consequences Of Single Failures In The Rod Control System

The staff requested 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 which 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 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 which can result in core thermal conditions not bounded by 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 non-safety-grade or control equipment, if subjected to the adverse environment of a high energy line break, could malfunction and cause the plant conditions to be more severe than those analyzed in the Safety Analyses of Chapter 15. The applicant was requested to perform a review to determine what, if any, design changes or operator actions would be necessary to assure that high energy line breaks will not cause control system failures to complicate the event beyond the Chapter 15 Safety Analyses. The applicant has not completed his review. We will evaluate his 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 which 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 (i.e., 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 inverter), the condition II accident analyses given in Chapter 15 of the FSAR are bounding. Based on the results of the applicant's review, we consider 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 to modify the PORV PID 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 General Design Criteria 13, "Instrumentation and Control", and GDC-19, "Control Room". This conclusion is based on the following:

Based on our review of the plant transient response to normal load changes and anticipated operational occurrences, such as reactor trip, turbine trip, upsets in the feedwater and steam bypass systems, we conclude that the control systems are capable of maintaining system variables within prescribed operating limits. Therefore, we find that the control systems satisfy this aspect of GDC-13, "Instrumentation and Control".

Our review of control systems included the features of these systems for both manual and automatic control of the process systems. We conclude that the features for manual and automatic control facilitate the capability to maintain plant variables within prescribed operating limits. We find that the control systems permit actions which can be taken to operate the plant safely during normal operation, including anticipated operational occurrences; therefore, the control systems satisfy GDC-19, "Control Room", with regards to normal plant operations.

The conclusions of the analysis of anticipated operational occurrences and accidents as presented in Chapter 15 of the FSAR have been used to confirm that plant safety is not dependent upon the response of the control systems. We conclude that failure of the systems of themselves or as a consequence of supporting systems failures, such as power sources, do not result in plant conditions more severe than those bounded by the analysis of anticipated operational occurrences.

Finally, we have confirmed that the consequential effects of anticipated operational occurrences and accidents do not result in control system failures that would cause plant con-

ditions more severe than those bounded by the analysis of these events pending satisfactory resolution of open item in Section 7.7.2.2. We find that the control systems are not relied upon to assure plant safety and are, therefore, acceptable.

In summary, the staff concludes that the control systems are acceptable subject to satisfactory resolution of the open item identified in Section 7.7.2.2 of this report.