Docket File
50-454/455/456/457

JAN 11 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: BYRON/BRAIDWOOD STATIONS, UNITS 1 AND 2, SAFETY EVALUATION REPORT, FSAR CHAPTER 7, INSTRUMENTATION AND CONTROL SYSTEMS

Plant Names: Byron and Braidwood Stations, Units 1 and 2
Docket Nos.: STN 50-454, 455, 456, 457
Applicant: Commonwealth Edison Company
Licensing Stage: OL
Responsible Branch: LB #1
Project Managers: S. Chesnut/ K. Kiper
Review Branch: ICSB
Review Status: Complete

On December 2, 1981 we provided a draft of our input for Chapter 7 of the Byron/Braidwood SER. Enclosed is a markup of the CRESS copy provided by the Project Manager, which serves as our final input to the SER. There are no further open items to be resolved with the applicant as noted in Section 7.1.3.1.

Confirmatory items, technical specification requirements and license conditions are also summarized in Section 7.1.3.2 through 7.1.3.4 respectively. TMI Action Plan Items are summarized in Section 7.1.6.

In that a number of typos were found in the CRESS copy, and several corrections and changes were made in the enclosure, we request that an updated CRESS copy be provided for review prior to issuance of the SER. As requested, a list of references used for our review of Chapter 7 is also attached.

Original Signed By
Themis P. Speis

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

Enclosures:
As stated

cc: See attached sheet

OFFICE	Contact: P. Bender X29448	ICSB/DSI PB	ICSB/DSI	ICSB/DSI	ADRS/DSI	
SURNAME		PBender:ct	TDunning	FRosa	TPSpeis	
DATE		1/ 8 /82	1/ 8 /82	1/11/82	1/11/82	

cc: B. Youngblood
K. Kiper
S. Chesnut
R. Mattson
T. Speis
F. Rosa
T. Dunning
E. Rossi
P. Bender
J. Elsbergas (ANL)
R. Capra

DISTRIBUTION:
Docket File
ICSB Reading File
P. Bender (PF)
Byron Subject File
Braidwood Subject File

OFFICE ▶							
SURNAME ▶							
DATE ▶							

7

7.1 Introduction

7.1.1 Acceptance Criteria

The instrumentation and control systems for the Byron/Braidwood stations have been reviewed. The bases for evaluation of the applicant's design, design criteria, and design bases are set forth in the Standard Review Plan (SRP), NUREG-0800 in Table 7-1, "Acceptance Criteria for Instrumentation and Control Systems 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 50.55 a(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. The acceptance criteria, consisting of the General Design Criteria (GDC) and IEEE Standard 279, are included in the Commission's regulations, and are applicable to the systems as identified in the SRP. In addition, the applicant has identified the guidelines, consisting of the Regulatory Guides and the industry codes and standards which are applicable to the systems. The acceptance criteria and guidelines identified by the applicant are provided in Table 7.1-1 and Appendix A 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 instrumentation and control systems important to safety, addressed in Section 7.1 of the FSAR, satisfy the requirements of GDC 1 and, therefore, are acceptable.

7.1.3 Specific Findings

7.1.3.1 Open Items

Total change to date

In the initial stages of this review a number of open items were identified for which additional information, ~~or~~ clarification, or design modification was required of the applicant. During the course of the staff's review a number of meetings were held with the applicant to resolve staff concerns. As a result of this effort, no open items remain to be resolved with the applicant on the review of Chapter 7 of the FSAR.

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 w'll not be addressed in supplements to this report unless an unexpected problem is revealed during the review of the documentation provided.

The Confirmatory Items and the sections of this report in which they are addressed are as follows:

~~(2) Water Level Measurement Errors (7.2.2.3)~~

(4) General Warning Alarm Trips (7.2.2.6)

~~(7) Steam Generator Level Control and Protection (7.3.2.1)~~

2. Compliance with IE Bulletin 80-06 (7.3.2.2)

~~(3) Auxiliary Feedwater Flow Control (7.3.2.7)~~

~~5~~ Test Jacks for P-4 Interlock Test (7.3.2.10)

~~6~~ Remote Shutdown Capability Test (7.4.2.2)

~~7~~ Steam Generator Pressure Control (7.4.2.3)

~~9~~ Interlocks for Reactor Coolant System Pressure Control During Low Temperature Operation (7.6.2.2)

~~8~~ Switchover from Injection to Recirculation Mode (7.6.2.3)

~~9~~ Boron Dilution Control (7.6.2.4)

~~10~~ Reactor Coolant System Loop Isolation Valve Interlocks (7.6.2.6)

~~(11) Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation (7.7.2.1)~~

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); ~~(5) Response Time Testing (7.3.2.6)~~ (4) Verification of the RTD Bypass Loop Flow (7.2.2.7); (5) Safety System Trip Setpoint Methodology (7.3.2.4).

7.1.3.4 Licensing Conditions

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

(1) Response Time Testing (7.2.2.5)

(2) Post-accident Monitoring (7.5.2.2)

7.1.3.5 Resolved Items of Concern

A number of concerns resulting from the staff's review have been fully resolved. The most important of these concerns are listed below. The sections in which they are discussed are shown in parentheses.

(1) Compliance to Regulatory Guides (7.1.7)

(2) Protection System Sensors and Cabling in Turbine Building (7.2.2.2)

~~(3) Water Level Measurement Errors (7.2.2.3)~~

~~(4) Steam Generator Level Control and Protection (7.3.2.1)~~

4 (5) Failure Mode and Effects Analysis (FMEA) Interface Requirements (7.3.2.3)

5 Auxiliary Feedwater Flow Controller Settings (7.3.2.5)

~~(6) Effect of the Auxiliary Feedwater Control Switch Position on the System~~

6 (7) Auxiliary Feedwater System Switchover to Essential Service Water (7.3.2.7)

~~(8) Containment High Radiation Monitor (7.3.2.10)~~

7 (9) Reset of Containment Ventilation Isolation Signal (7.3.2.10)

8 (10) Bypass of Inoperative Status Indication (7.5.2.1)

9 (11) Residual Heat Removal Isolation Valve Interlocks (7.6.2.1)

10 (12) Isolation of Nonqualified Systems from Essential Service Water (7.6.2.5)

(11) Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation (7.7.2.1)

12 (13) Failures of Rod Control System (7.7.2.2)

13 (14) High Energy Line Breaks and Consequential Control System Failures (7.7.2.3)

14 (15) Multiple Control System Failures (7.7.2.4)

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. The Remote Shutdown Instrumentation and Controls are discussed in Section 7.4.2.1.

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 applicants in NUREG-0737, "Clarification of TMI Action Plan Requirements." ~~The following Action Plan Items are applicable to the instrumentation and control systems important to safety at the Byron/Braidwood Stations.~~ The sections in which these items are addressed, are as follows:

II.D.3	Direct Indication of Relief and Safety Valve Position (7.5.2.3)
II.E.1.2	Auxiliary Feedwater System Automatic Initiation and Flow Indication (7.3.2.8)
II.E.4.2	Containment Isolation Dependability (7.3.2.11)
II.K.3.1	Installation and Testing of Automatic Power-Operated Relief Valve Isolation System (7.6.2.7)
II.F.1	Additional Accident Monitoring Instrumentation (7.5.2.4)

II.K.3.9 Proportional Integral Derivative Controller Modification (7.7.2.5)

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

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

7.1.7 Compliance with Regulatory Guides

Appendix A of the FSAR ~~(Reference in Table 1.8-1)~~ addresses application of Regulatory Guides. In many cases it was not clear as stated that the design conforms to the guidance of the Regulatory Guides or if exceptions are taken. In response to our concern, the applicant has revised Appendix A to more clearly indicate compliance or exceptions to all Regulatory Guides. Based on our review we find that acceptable conformance to the guidelines of the regulatory guides has been provided.

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. Each of the switches controls power to the undervoltage and shunt trip coils of both reactor trip breakers. 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 used for safety injection ~~(Section 7.5)~~ initiation.

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)	Reactor coolant pump breakers open	(2/4)
(12)	Low reactor coolant flow	(2/3 in any loop)
(13)	Reactor coolant pump bus undervoltage	(2/4)
(14)	Reactor coolant pump bus underfrequency	(2/4)
(15)	Low-low steam generator water level	(2/4 in any loop)

(16) Safety injection (see Section 7.3) (1/2)

(17) Turbine trip

close spacing

(a) Low auto stop oil pressure, or (2/3)

(b) Turbine stop valve close (4/4)

(18) General warning alarm (2/2)

(19) 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 Overpressure 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, axial neutron flux in the reactor, and the 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 axial neutron flux 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 above are not effective below or above certain power levels. The source range high neutron flux trip can be manually blocked when one of the two intermediate range channels ~~supersedes~~ reads above approximately 6×10^{-11} amperes (P-6 interlock). The intermediate range high neutron flux trip, and the power range high neutron flux low-setting trip can be manually blocked above approximately 10% power (P-10 interlock). All of the above blocks are automatically removed when the power level decreases below the set value. The pressurizer low pressure and high water level trips, reactor coolant pumps breaker open trip, low reactor coolant flow trip, reactor coolant pump bus undervoltage and underfrequency trips, and the turbine trip

are automatically blocked below approximately 10% power with the turbine impulse chamber pressure setpoint below set value (P-7 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 of the blocks above are automatically removed when the power increases above set value.

The Reactor Trip System includes provisions for testing the system operation. The testing is carried out in steps, a part of the system at a time, in a sequence that provides the necessary overlap to assure the complete system operability. All of the system can be tested at power, except for the manual reactor trip and the manual safety injection switches and the reactor coolant pump breakers. The manual trip switches have inputs in both reactor trip breakers and their actuation would trip the reactor. Opening a reactor coolant pump breaker would not trip the reactor directly because of the coincidence in the trip logic, but could result in a reactor trip due to low coolant flow. Also, the nuclear channel trips which are not effective above certain power levels are tested at reduced power levels and at shutdown. Bypassing of the trip functions during testing is required for the source and intermediate range nuclear channels that 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.

In addition to providing inputs to the Solid State Logic Protection System, analog signals of the protection channels are used for nonprotective functions,

such as control, remote indication, and computer monitoring. To protect from faults in the 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 resolution 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. The staff will include in the status technical specifications a requirement to periodically independently verify the operability of the undervoltage and shunt trip functions 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 this non-seismic turbine building are: (a) Turbine stop valve closure limit switches; (b) Turbine auto stop 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.

Of the three groups of components (items a, b, and c above) that provide inputs to the reactor trip system, the turbine stop valve closure limit switches, and the turbine impulse pressure transducers are seismically and environmentally qualified. The auto stop oil pressure switches are not environmentally qualified, ~~although~~ however in response to our concern, the applicant has stated his intent to obtain qualified switches. The cables for the two turbine trip inputs and the turbine impulse pressure input are routed in conduits through the turbine building. Although the conduits are identified as non-safety related, they have been treated, insofar as possible, as safety related. The conduit support system has been given special attention to ensure that the conduits are well supported and that mutually redundant cables are adequately separated.

As stated by the applicant, all of the circuitry in the turbine building, except for the environmental qualification of the auto stop oil pressure switches, complies with all requirements of IEEE Standard 279. Further, ~~the~~ circuit analysis shows that no credible fault in the portion of the trip circuitry in the turbine building would degrade the performance of the reactor trip system. 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. In response to our concern, the applicant has committed to evaluate the effect of high temperature on the reference legs of water level measurement systems following a high energy line break and to factor the measurement errors in the trip setpoints. The effects of environmental errors on level measurements will be reviewed as part of the staff review of setpoint methodology (see section 7.2.3.4).

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 applicant has committed to incorporate testing of the time constants ~~setpoints~~ in the station ~~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 a computer based system using process noise with the plant at power for sensor response time testing. The staff concluded that this method is acceptable during its review of the Callaway operating license application (Docket No. 50-483). However since there is only limited experience to date in the use of this technique for response time testing, the Callaway operating license will be conditioned to require the submittal of test results and conclusions through the first three fuel cycles to allow a more thorough review of the adequacy of this technology. During our review of this subject on the Byron/ Braidwood application, the applicant noted that Westinghouse is in the process of preparing a topical report to justify the adequacy of this method of

response time testing. If staff review and approval of the topical report does not occur prior to the issuance of the Byron operating license, conditions will be included in the license to require the submittal of test results and conclusions to permit further staff review of the experience with this technique for response time testing.

7.2.2.6 General Warning Alarm Trips

The General Warning Alarm System monitors various conditions, such as power supply output and test switch positions 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 in both trains, the reactor is automatically tripped.

The information presented in the FSAR did not identify the fact ~~allow the staff to positively conclude~~ that the General Warning Alarm System is incorporated in the Reactor Trip System. In response to our concern ~~question~~ the applicant has indicated that the design of the General Warning Alarm System is identical to that of the previously reviewed Callaway plant. This information is to be incorporated in the FSAR.

7.2.2.7 Verification of the RTD Bypass Loop Flow

note change to whole section

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.

the applicant has agreed to include in the Technical Specifications a requirement to perform the calibration at each refueling outage. Based on the applicant's commitment we consider this issue resolved subject to our confirmation of the Technical Specification revision.

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

This item deals with the modification proposed by some licensees to raise the power level at which the anticipatory trips are unblocked.

The applicant has not proposed a change in the interlock for the anticipatory reactor trip on turbine trip (the trip is active above approximately 10% of power); therefore this item is not applicable to Byron/Braidwood.

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

The Byron/Braidwood stations have an anticipatory reactor trip on turbine trip, which satisfies this item.

7.2.3 Conclusions

The RTS for Byron/Braidwood is functionally identical to the reactor trip systems reviewed and approved by the staff on previous operating license applications of which the Callaway application (Docket No. 50-483) is the most recent. Based on our prior review and approval of the standard design of the Westinghouse designed RTS including its conformance to the requirements of IEEE 279 and related General Design Criteria, we find the RTS for Byron/Braidwood to be acceptable subject to completion of the applicable confirmatory items and conditions noted in Sections 7.1.3.2, 7.1.3.3, and 7.1.3.4 of this report.

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 (EAS) systems. Also described are the control systems which regulate the operation of the ESF and EAS 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 and flows, steam line differential pressure, 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 as follows: ~~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.	Manual	(1/2)
b.	High containment pressure	(2/3)
c.	Low compensated steamline pressure	(2/3 in any steam line)
d.	Pressurizer low pressure	(1/3)

(2) Containment Spray and Containment Isolation, Phase B

a.	Manual (two sets, two switches per set)	(1/2 sets)
b.	Containment pressure high-high-high (Hi-3)	(2/4)

(3) Containment Isolation, Phase A

a.	Manual	(1/2)
b.	Automatic safety injection	See items b through d for function (1) above

(4) Steam Line Isolation

a.	Manual	(1/1 for any loop) (1/2 for all loops)
b.	Low steamline pressure (interlocked with loop stop valves)	(2/3 in any steamline)
c.	Containment pressure high-high (Hi-2)	(2/3)
d.	High steam pressure rate	(2/3 in any steamline)

(5) Feedwater Line Isolation

a.	Safety injection	(1/2)
b.	Steam generator level high-high (Hi-2)	(2/4 for any steam generator)
c.	Low T_{avg} and reactor tripped	(2/4)

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

7.2.1

Reactor Trip System in Section ~~7.2 above~~. 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 safeguard actuation and which can be tested without causing a plant upset. A continuity check is performed on the actuators of the untestable devices. To enable a 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 EAS System Operation

7.3.1.2.1 Auxiliary Feedwater System

The function of the Auxiliary Feedwater System (AFS) is to provide an adequate supply of ~~cooling~~ water to the steam generators in the event the main feedwater supply is not available. The AFS consists of two subsystems. One subsystem utilizes an electric-motor-driven pump which is powered from one of the emergency power systems supported by a diesel-generator. The other utilizes a pump that is driven directly by a diesel engine. All electrical equipment in each of the two subsystems is powered from a separate ESF bus. The water to the AFS is normally supplied from the condensate storage tanks. A backup source is available from the Essential Service Water System (ESWS) through two normally closed motor-operated valves in series for each pump.

A manual control switch is provided for each pump on the main control board and at the remote shutdown panel. ~~Also~~, The auxiliary feedwater flow ~~control valves~~ is automatically controlled ~~from manual controllers~~ which have setpoint stations at the main control board. The capability is provided to manually position the control valves from the remote shutdown panel to control flow. To start the pump and control flow ~~controls~~ at the remote shutdown panel, transfer switches (REMOTE/LOCAL), located at the remote shutdown panel, must be turned to the LOCAL position. The pumps are started automatically on either a low-low level in any steam generator, a safety injection

auxiliary feedwater pump requires contact closure from a pressure switch

signal, or a complete loss of offsite electrical power. Manual starting of the which monitors lube oil pressure. Under automatic safeguards start condition, the permissive from the lube oil pressure switch is not required. The pump is ~~stopped~~ tripped automatically on low-low pump suction pressure.

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. Additionally, a second pair of open/close indicating lights for each valve is provided on the monitor light panel (see Section 7.5.1).

7.3.1.2.3 Emergency Core Cooling System

The primary function of the Emergency Core Cooling System (ECCS) is to remove the stored and fission product decay heat from the reactor core during accident conditions. The ECCS is a two-train, fully redundant, engineered safety feature. Separate power sources are provided for each train from the ESF buses. The instrumentation and controls of one train are electrically independent and physically separate from the instrumentation and controls of the other train. Redundant as well as functionally independent variables are used to initiate safeguard signals (see Section 7.3.1.1). The safety injection signal initiates the following actions in the ECCS: (1) Starts centrifugal charging pumps; (2) Opens refueling water storage tank suction valves to charging pumps; (3) Opens safety injection containment isolation valves; (4) Closes normal charging path valves; (5) Closes charging pump miniflow valves; (6) Starts safety injection pumps; (7) Starts residual heat removal pumps; (8) Closes volume control tank outlet isolation valves. 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 the recirculation mode of operation (see Section 7.6.1.3).

7.3.1.2.4 Containment Spray System

The Containment Spray System (CSS) is designed to remove fission products, primarily elemental iodine, from the containment atmosphere following a loss-of-coolant accident. At the same time the spray water reduces the containment temperature and pressure. The CSS consists of two independent, 100% capacity, systems each powered from a separate ESF bus.

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 actuated automatically by the containment spray actuation signal from the ESFAS (see Section 7.3.1.1). Manual control switches are provided on the main control board. Indicating lights are provided on the main control board and on the ESF status boards (see Section 7.5.1) to show the status of the pumps and the position of the valves. Abnormal conditions in the pump and valve operation and in the spray water supply are alarmed on the main control board.

7.3.1.2.5 Reactor Containment Fan Cooler System

The function of the Reactor Containment Fan Cooler (RCFC) system is to cool and dehumidify the containment under normal and accident conditions. The RCFC system consists of two redundant trains each powered from a separate ESF bus. The instrumentation and controls of each redundant train are powered from the same ESF bus that powers the equipment in the train. Variables important to RCFC system operation are indicated in the control room, and alarms are provided to warn the operator of abnormal conditions.

The RCFC fans are started automatically at low speed upon receipt of an ESF actuation signal. For manual control of the RCFC system operation, switches are provided on the main control board and at the remote shutdown control panel.

7.3.1.2.6 Combustible Gas Control System

The Combustible Gas Control System controls the buildup of hydrogen gas within the containment. One hydrogen recombiner with associated controls is provided at each unit and is powered from one of the ESF buses. The hydrogen recombiners are portable units, allowing moving a recombiner from one unit to another if necessary. The recombiner control panel is located outside the containment. All controls, alarm, and readout instrumentation are located on this panel. After the recombiners are manually started, the system is designed to operate automatically.

7.3.1.2.7 Essential Service Water System

The Essential Service Water System (ESWS) supplies water to all essential heat loads. Two full-capacity service water loops are provided for each unit; each takes suction from different essential service water cooling tower basins at Byron, and the essential cooling pond at Braidwood. The two pumps and associated valves in each unit are powered from separate emergency power buses.

A manual control switch is provided for each pump on the main control board and at the remote shutdown panel. The switch on the remote shutdown panel is activated by turning a transfer switch (REMOTE/LOCAL), located on the remote shutdown panel, to LOCAL position. The pumps are started automatically by a safety injection signal provided that the suction valve is open. The pumps are stopped automatically by protective overcurrent relays, or by low suction pressure. One motor-operated isolation valve is provided in the suction line of each pump. The power source for the valve motor is supplied from the same power train as the associated pump.

7.3.1.2.8 Main Control Room HVAC System

The function of the Control Room HVAC System is to provide environmental conditions conducive to habitability and long component life in the control room under normal and abnormal station conditions. The system is comprised of two full-capacity ~~redundant~~ equipment trains. Instrumentation and controls for each train are completely independent of each other.

The instrumentation and control systems monitor radiation in the makeup air intakes, chlorine concentrations in the outside air intakes, and combustion products in the makeup air intakes, and take necessary action to ensure control room habitability. Also, alarms are actuated on the main control board on detection of high radiation or chlorine level, or combustion products. Temperature and pressure in the control room are also monitored and appropriate control actions are taken to maintain the temperature and pressure within established limits.

7.3.1.2.9 Auxiliary Building HVAC System

The Auxiliary Building HVAC System serves all areas of the auxiliary building including ESF cubicles, and Fuel Handling Building, but excludes the control room, computer room, and offices and laboratories which are served by independent HVAC systems. The Auxiliary Building HVAC System consists of redundant equipment having independent controls and instrumentation. The function of the HVAC system is the control radioactivity in the areas served and also to minimize the release of airborne activity.

The controls and instrumentation are powered from the ESF buses. The control system is interlocked with a high radiation signal from the radiation monitoring system to automatically route the exhaust air through normally bypassed charcoal filters and start booster fans. In case of fire in the charcoal filters, the associated booster fan will be tripped automatically by a signal from the fire detection system. Detection of combustion products in the air supply or exhaust ducts will actuate an alarm on the local control panel.

7.3.1.2.10 Essential Switchgear Rooms, Miscellaneous Electrical Equipment Rooms, and Battery Rooms Ventilation Systems

The function of the ventilation systems in the essential switchgear rooms, miscellaneous electrical equipment rooms, and the battery rooms is to remove heat generated by electrical equipment and prevent accumulation of hydrogen gas generated during charging of batteries. Ventilation fans are controlled from either the main control panel or the local control panel. Outside air and return air dampers are interlocked to open when running the ventilation fans

and are modulated by a temperature controller. Power to the instruments and controls is supplied from the same ESF buses that feed the associated HVAC equipment.

7.3.1.2.11 Diesel-Generator Facilities Ventilation System

Each of the four diesel-generator rooms and day tank rooms is provided with an independent ventilation system which provides continuous ventilation for the day tank room, and ventilation and a source of combustion air for the diesel-generator when it operates. The instruments and controls for the Diesel-Generator Facilities Ventilation System are not redundant, since redundant diesel-generators are provided. The instrumentation channels and logic circuits of each diesel-generator room ventilation system are, however, physically and electrically separated to prevent a failure in one diesel-generator room ventilation system affecting the other system. Diesel-generator room ventilating fans start automatically by the diesel-generator start sequence or manually by control switches in the main control room.

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 described in the FSAR, three steam generator level channels are used in two-out-of-three logic to isolate the feedwater on high-high (Hi-2) 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 demand 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 protection from two-out-of-three to two-out-of-two, and result 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. In

response to our concern the applicant has committed to provide a fourth channel and modify the logic such that protective action is initiated on 2 out of 4 logic. Based on this commitment we consider this issue resolved subject to our review of the FSAR amendment.

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 Byron/Braidwood design meets the requirements of IE Bulletin 80-06, the applicant stated that the requested reviews have been performed and a number of circuits were redesigned such that the requirements of IE 80-06 have been met. The applicant also stated that 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 added a statement of confirmation in the FSAR.

7.3.2.4 Safety System Trip Set Point Methodology

The methodology followed in setting the safety system trip points 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 been completed for the Byron/Braidwood plants. Since the primary function of this information is to confirm the adequacy of set points specified in the plant Technical Specifications, the staff will audit this information at the time the Technical Specifications are available for review.

delete

7.3.2.5 Effect of the Auxiliary Feedwater Control Switch Position on the System Operation

In our review of the auxiliary feedwater system we found that the pull-to-lock position of the auxiliary feedwater pump control switches disables the start of auxiliary feedwater pumps on safety actuation signal. In response to our concern on this fact, the applicant stated that if the switch is left in the pull-to-lock position, the system-inoperative light will be actuated on the equipment status display console. Based on this statement we consider this issue to be resolved.

7.3.2.~~6~~5 Auxiliary Feedwater Flow Controller Settings

that have setpoint stations

The auxiliary feedwater flow in each of the lines to the steam generators is maintained automatically at ~~the~~ a set level by ~~the~~ flow controllers located in the main control room, ~~and at the remote shutdown panel~~. We were concerned that no means are provided to insure that the flow control ~~loop are~~ is set to provide full flow of approximately 160 gpm after initiation of the feedwater system operation. In response to our concern the applicant committed to provide ~~that administrative procedures will require checking the controller settings to established interlocks to assure that they are at full flow settings. The staff, however, has taken position that~~ an alarm which is ~~required to be~~ actuated if any of the flow set points ~~settings~~ are not at the full-flow value when the auxiliary feedpumps are not running. The FSAR has been amended to reflect this design modification.

7.3.2.7 Auxiliary Feedwater Flow Controller Power Supply

delete

The auxiliary feedwater flow control instrumentation is powered from diesel-generator backed ESF buses. If a diesel generator would not start following a blackout requiring auxiliary feedwater, no power for the auxiliary feedwater flow control instrumentation would be available resulting in a loss of flow control. To eliminate this problem, we have requested the applicant to power the flow control instrumentation from the vital ac power inverters that are backed up by batteries.

→ continue 7.3.2.6 next page (insert)

insert

7.3.2.6 Auxiliary Feedwater Flow Control

A motor operated block valve is provided downstream of each auxiliary feedwater flow control valve. The block valve operates as a throttling control valve in that its control circuit does not seal-in on a momentary open or close command. The capability to control auxiliary feedwater flow with the block valve fulfills the safety function of the system in that the operation of the auxiliary feedwater flow control valves are dependent on the non-safety grade instrument system. The block valve is powered from a 480 volt essential bus. Instrument power for the flow indication and control is derived from a 480 to 120 volt instrument power transformer connected to the same essential bus supplying power to the block valve. This is in contrast to normal practice of supplying power to ESSENTIAL instrument control and indication systems from battery backed vital 120 volt ac power sources.

From an operability standpoint, this design does not introduce any concerns with respect to the "A" train of the auxiliary feedwater systems since the motor driven pump operability is dependent upon the same diesel EDG operator backed essential power train. However, with respect to the "B" train of the auxiliary feedwater system, the operability of the diesel driven auxiliary feed pump is not dependent upon the availability of the "B" train diesel generator backed essential buses. Thus, for events which lead to a loss of the "B" train essential buses, the diesel driven auxiliary feedwater pump would be operable. If these events were accompanied by a demand for auxiliary

feedwater, the operator may not recognize that the diesel driven pump is running and providing water to the steam generators since flow indication would indicate no flow on the loss of the "B" train power source. This could lead to an overcooling event that could be further complicated by a safety injection on low primary pressure, the most common cause of inadvertent safety injection.

For accident sequences with a loss of the "B" train power source, a faulted steam generator (feedwater or steam line break) presents an additional concern. In this case flow from the diesel driven auxiliary feed pump would not be limited to 160 gpm for each steam generator and again, with the loss of flow indication, the operator must recognize that the diesel pump is running and take action to trip the pump to terminate flow to the faulted steam generator.

Although not a design bases event the applicant has been requested to prepare emergency procedures for a total loss of AC power. In this event, the diesel driven pump is the source of auxiliary feedwater to permit safe shutdown. If the flow indication and controls were powered from battery backed 120 volt vital instrument buses, indication of flow would be available from the control room as well as flow control for as long as instrument air is available from the instrument air system.

~~In summary,~~ Therefore the staff concluded that there is a sufficient bases to require ~~plant~~ station modifications such that the steam generator flow indication and control instrumentation be powered from battery backed 120 volt vital instrument buses ~~This change will provide~~ and thus ensure a system which is more tolerant of potential failures that ~~could~~ would not

complicate the operator's ability to maintain the plant in a safe condition for such events.

~~We will report on the resolution of this open item in a supplement to this report.~~

The applicant agreed with our concern and committed to change the power source for the Train "B" Auxiliary Feedwater flow instruments from ESF Bus 12 to a battery backed supply. This issue is resolved subject to staff confirmation of an appropriate FSAR amendment.

7.3.2.7 Auxiliary Feedwater System Switchover to Essential Service Water

The normal supply of water to the auxiliary feedwater system is from the condensate tanks. In case this supply is not available, the water is supplied from the Essential Service Water System (ESWS). The automatic switchover is initiated when the pressure in the feedwater pump suction line drops to switchover setpoint (LO-2) while the safety injection signal is present. Although an alarm is sounded in the control room to warn of impending switchover when the LO-2 setpoint is reached, no clear indication was provided of actual switchover. In response to our concern, the applicant will provided an alarm to indicate that automatic switchover from the condensate storage tank to the ESWS has been initiated. ~~This item is resolved.~~

7.3.2.8 TMI 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~~ initiation of the auxiliary feedwater system, and (2) a reliable indication in the control room of the auxiliary feedwater flow.

~~Our review of the Byron/Braidwood design shows that:~~

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

(2) A single auxiliary feedwater flow indicator is provided in the control room for each steam generator. The flow instrumentation is powered from ESF buses (backed up by diesel generators). Therefore, we find that that the design of this system conforms to the Action Plan guidelines.

9
7.3.2.10 Test Jacks for P-4 Interlock Test

The Engineered Safety Features Actuation System includes a number of interlocks, designated "P", that perform various permissive and blocking functions depending on monitored conditions. Although as stated in the FSAR, the "P" interlocks are designed to meet the testing requirements of IEEE Standards 279-1971, and 338-1971, the P-4 interlock was found not to be fully testable. This was reported to the Commission by Westinghouse on November 7, 1979 and test procedures were recommended for all Westinghouse plants. In response to our concern with the Byron/Braidwood P-4 interlock testing, the applicant stated that test jacks will be provided at the reactor trip breakers to facilitate testing of the P-4 interlock. Based on this information we consider this issue resolved subject to confirmation that this modification has been implemented.

10
7.3.2.11 Containment Ventilation Isolation Radiation Monitors

Information provided in the FSAR indicates that radiation detectors that provide inputs to the containment ventilation isolation actuation logic, are not safety-related and are not redundant. In response to our concern, the applicant has stated that actually two redundant, Class 1E, safety-related radiation monitors are provided. One monitor provides a signal to protection system Train A, and the other to Train B. The information in the FSAR has been revised to reflect this statement.

10
7.3.2.12 Reset of Containment Ventilation Isolation Signal

The containment ventilation isolation actuation logic includes a retentive memory device with manual reset. This device receives a signal from an "OR" gate that has inputs from a containment radiation monitor and the safety injection actuation system. A high radiation or safety injection signal will generate a containment ventilation isolation actuation signal. This signal can be reset by operating a reset button. After the reset, providing that the initiating signal remains present, the logic will not respond to another initiation signal. In response to our concern the applicant modified the logic such that the reset of one actuation signal will not block the other signal from performing its protective action. The FSAR has been modified to show the revised system.

7.3.2.11 → use insert on next page

7.3.2.11 TMI ACTION PLAN ITEM II.E.4.2, ~~CONTAINMENT ISOLATION DEPENDABILITY~~ POSITIONS ~~(4)~~, ~~(6)~~ AND (7)

Action Plan Item II.E.4.2 Position (4) requires the design of control systems for automatic containment isolation valves ~~shall~~ be such that resetting the isolation signal will not result in the automatic reopening of containment isolation valves; Position (6) requires certain containment purge valves that do not satisfy specific operability criteria to be sealed closed in a defined manner; Position (7) requires containment purge and ventilation valves to close on a high radiation signal.

Based on our review of the instrumentation and control systems in this area, we find that the applicant has satisfied this item. See Section 6.2.4 of this report for a detailed discussion of the applicant's compliance with TMI Action Plan Item II.E.4.2.

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 (EAS) system and initiates operation of these systems. The ESF control system regulates the operation of the ESF system following automatic initiation by the protection system or manual initiation by the plant operator.

We have conducted an audit review of these systems for conformance to guidelines of the applicable Regulatory Guides and industry codes and standards. In Section 7.1 of this SER we concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon our audit review of the system design for conformance to the guidelines, we find that ~~upon satisfactory resolution of the open item identified in Section 7.3.2.8 and~~ 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 FSAR. 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 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 CRF Part 50 50.55a(h) subject to [redacted] completion of the applicable confirmatory items identified in Section 7.1.3.2 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

[redacted] Securing and maintaining a 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.~~
(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 ~~considered by the applicant as necessary~~ 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.

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

The equipment considered necessary for safe shutdown includes the following:

(1) Auxiliary feedwater pumps
(2) Centrifugal charging pumps
(3) Essential service water pumps
(4) Component cooling water pumps
(5) Reactor containment fan coolers
(6) Control room ventilation unit, including control room air inlet dampers
(7) Auxiliary feedwater control valves
(8) Atmospheric steam safety valves
(9) Steam generator PORV's

All of the equipment above is powered from ESF buses and can be controlled from both the main control room and the remote shutdown panel. Exceptions are the atmospheric steam safety valves which are self-actuated and require no power or controls. Important additional equipment that is available for safe shutdown and has controls both at the main control room and the remote shutdown panel, but is not powered from ESF buses, includes:

(1) Boric acid transfer pumps
(2) Primary water makeup pumps
(3) Charging flow control valve
(4) Letdown orifice isolation valves
(5) Power operated atmospheric steam relief valves
(6) Pressurizer heater control
(7) Emergency boration isolation valve.

and the steam generator PORV's which are being modified as noted in section 7.4.2.3 of this report.

7.4.1.2 Remote Shutdown

In addition to the controls and instrumentation in the main control room, selected duplicate controls and instrumentation are provided outside the control room to enable safe shutdown of the plant in case the main control room must be evacuated. The primary remote controls and instrumentation are at the remote shutdown panel that is located in the radwaste control area. This panel is divided into three sections; two sections for the two redundant ESF trains,

and one section for the nonsafety-related equipment. Separation between the sections is provided by physical barriers. The remote shutdown design meets the single failure criterion assuming no fire or accident conditions.

The remote shutdown panel is provided with the necessary controls and instrumentation to maintain the plant in a hot standby condition. The plant design also provides a capability for cold shutdown using the instrumentation and controls outside the main control room. ~~To accomplish this, however, certain modifications to the controls and instrumentation may be required.~~

Normal control of equipment and systems which have duplicated local controls and instrumentation, is accomplished in the main control room. In the event of a main control room evacuation, local control is established by use of selector switches that transfer the control from the main control room to the local controls. For the remote shutdown panel, switching to local control causes an annunciator alarm to sound in the main control room. Local control panel instrumentation such as analog indicators require no transfer as they are normally energized and operating.

7.4.2 Specific Findings

The concerns arising from our review and their resolution are as follows.

7.4.2.1 Remote Shutdown Instrumentation and Controls

~~From the information supplied in the FSAR, the staff could not conclude that the controls and instrumentation provided outside the main control room are sufficient to safely shut down the plant and to maintain it in this condition.~~ Analysis is being carried out to determine how the system meets the requirements of 10 CFR Part 50, Appendix R (shutdown capability for the analysis of fire hazards). See Section 9.5.1 of this report for a detailed discussion. Because changes in the system design of the remote shutdown system may be required based on the results of this analysis, the staff will review the final design prior to issuance of the Operating License. Any problems resulting from this review will be addressed in Section 9.5.1 or in a supplement to this report.

7.4.2.2 Remote Shutdown Capability Test

A concern raised by the staff regarding the remote shutdown capability, was a need for a test to verify design adequacy. In response to our concern, the applicant stated that the plant startup test program 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.

7.4.2.3 Steam Generator Pressure Control

Following initiation of the auxiliary feedwater system, the pressure in the steam generator is initially controlled by code safety valves following a reactor and turbine trip from full load. If the condenser is available, the bypass valves subsequently control steam generator pressure by dumping steam to the condenser when decay heat falls to approximately 40% of full load. If the condenser is not available, such as on the loss of offsite power, steam is vented to the atmosphere by the steam generator power operated relief valves (PORVs). For this case it is the staff's position that steam generator pressure control should be maintained by safety-grade systems without reliance on code safety valves for long-term pressure control.

The applicant has indicated that design changes are being ~~considered~~ implemented for the steam generator PORVs such that their operation would not be dependent on the nonsafety-grade instrument air system. Hydraulic operators will be provided for these valves. Power for two of the valve operators will be supplied from ESF Division 11 and the other two valve operators will be supplied from ESF Division 12. These operators will allow full control of valve position. This issue is resolved subject to confirmation of our review of these design modifications.

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. 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 th relevant requirements of General Design Criteria 2, 4, 13, 19, 34, 35, and 38 subject to ~~satisfactory resolution of open item~~ the completion of the confirmatory items identified in Section 7.1.3.2 of this report.

7.5 Information Systems Important to Safety

7.5.1 System Description

The function of the ~~Safety Related Display Instrumentation~~ Information Systems Important to Safety is to provide information to the reactor operator to enable him to perform required safety functions during normal, abnormal, and post-accident conditions.

continue with insert for 7.5.1

sert

7.5.1 System Description

The information systems important to safety are composed of display instruments which provide information to the operator to enable him to perform required manual safety functions, and to determine the effect of manual actions taken following a reactor trip ~~due to a Condition II, III, or IV event~~. Information is also displayed which the operator needs to maintain the plant in a hot standby condition or to proceed to cold shutdown within the limits of the technical specifications. The operator uses these information systems to monitor conditions in the reactor, the Reactor Coolant System, and in the containment and process systems throughout all normal operational conditions of the plant, including anticipated operational occurrences. The display systems include bypassed and inoperable status information, ESF monitors, and post-accident monitoring indications.

All safety function actuations are initiated automatically so that the plant operator is not required to ~~take a manual~~ initiate action to put the plant in a safe shutdown condition. All transmitted signals (including flow, pressure and temperature) which can cause a reactor trip are either indicated or recorded for each channel, including all neutron flux power range signals (top and bottom detector, algebraic difference and average of top and bottom detector signals). Any reactor trip will actuate an alarm and an annunciator. Such protective actions are indicated and identified down to the channel level.

Six monitor light panels are provided in the control room to provide the operator with the information necessary to quickly assess the status

of all remotely operated engineered safety feature (ESF) valves, motors or other essential components. Each monitor panel consists of an array of lights with a single light for each safety feature component monitored. When a monitor light is energized, the statement written on the window is true. Since all the lights in a particular grouping operate in the same manner, a component failure is readily apparent. A mechanism for testing light bulbs is provided in each light group.

The assignment of an ESF component . . . . .

(see next page)

7.5.1.1 Normal Operational Monitoring

The information available to the operator includes the following:

(1) Three indicating lights are provided for each pump control switch. They indicate pump stopped, pump automatic trip, and pump running.

(2) Two indicating status lights are provided for each valve control switch. They indicate valve closed and valve open, and both lights are on when the valve is in intermediate position.

(3) Monitor Lights

A light in the monitor light grouping is provided for each pump (running), and for each valve (open, closed), that is a part of the Engineered Safety Features (ESF) system. The assignment of a component to a light grouping is determined by that component's operation as follows:

(a) Group 1 lights monitor those components whose status is essential for advance readiness to actuate the Engineered Safety Features. These lights should all be dark during normal operation.

(b) Group 2 lights monitor those Engineered Safety Features components which must actuate during the injection phase of an accident. These lights should all light for an accident. Some of these lights may be lit during normal operation, for instance component cooling, centrifugal charging, and essential service water pumps and fans running.

(c) Group 3 monitors those valves required to close for Containment Isolation Phase A. They are separated to show pairs of redundant valves subject to closure by the A and B trains. These lights should all light for an accident. Some of these lights may be lit during normal operation, for instance sample line isolation valves.

(d) Group 4 monitors those components which must be changed to achieve the cold leg recirculation mode. The transition from injection mode

to cold leg recirculation is done manually by the plant operators. They use this group as a guide, realigning 18 valves and restarting the RHR pumps until all lights in this group are lit. Some of the lights may be lit during normal operation or nonaccident cooldowns, such as centrifugal charging and RHR pump lights.

5 ~~(e)~~ Group 5 monitors those components which must be changed to achieve the hot leg recirculation mode. The transition from cold leg recirculation to hot leg recirculation mode is done manually by the plant operators. They use this group as a guide, realigning eight valves and checking that the RHR pumps continue running until all lights in this group are lit. Some of the lights may be lit during normal operation or nonaccident cooldowns, such as centrifugal charging and RHR pump lights.

6 ~~(f)~~ Group 6 monitors those components which actuate on a high-high or a high-high-high containment pressure signal, including the containment spray system components, Containment Isolation Phase B components, and the main steam isolation valves. In nonaccident conditions, these lights will usually be all dark except during system testing or isolation of a steam generator.

~~A mechanism for testing light bulbs is provided in each light group.~~

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

(1) Nuclear Instrumentation - flux level and rate.

(2) Reactor Coolant System - coolant temperatures, pressures, and flow; pump current, frequency; overpower and overtemperature ΔT setpoints; pressurizer water level.

(3) Reactor Control System - rod position, demanded rod position and speed.

(4) Containment System - containment pressure.

(5) Feedwater and Steam Systems - main and auxiliary feedwater flow, steam flow and pressure, steam generator level and programmed level signal, turbine impulse chamber pressure, steam dump modulate 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 due to anticipated operational occurrences and accidents. 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) Steamline Pressure
(6) Steam Generator Water Level
(7) Refueling Water Storage Tank Level
(8) Boric Acid Tank 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 7.5.2.2 below).

~~7.5.1.3 Bypass or Inoperative Status Indication~~

The bypass/inoperability status of systems that are important to plant safety is displayed on the Equipment Status Display (ESD) panel in the control room. Indication is provided by means of a visual indicator on a system level, and an audible alarm. Information related to the status of various components of a

safety system is either directly wired or manually entered into the station computer. Software programming combines these inputs logically into a decision on whether the system is operable. For the systems selected, the time a system is not available generally is a limiting condition. Therefore, the logic decision includes timing functions which will determine when the time allowed for operation in a degraded condition expires.

Back-lighted pushbuttons on the ESD panel are used for system inoperable status indication. Yellow light corresponds to allowable operation in a degraded condition, while red signifies that the allowable time for operation in a degraded condition has expired. Upon receiving an alarm (flashing yellow or flashing red light plus an audible alarm), the operator acknowledges the alarm by depressing the pushbutton. This changes the flashing light to steady, silences the audible alarm, and transmits data back to the computer recording the alarm acknowledgment.

When the operator wishes to determine why the system condition is abnormal, he may interrogate the computer or physically check the system for failed component.

7.5.2 Specific Findings

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

7.5.2.1 Bypass or Inoperative Status Indication

As described in Section 7.5.1 above, the station computer is used to operate the bypass/inoperative status alarms of systems important to safety. We were concerned about the degree of reliability of the ~~CRT display used for the~~ system bypass indication and the associated software. In response to our concern the applicant stated that the ~~Process~~ Computer System used is a high reliability system that is provided with a dc battery back-up for its normal ac power source. A third independent power source (ac) may be selected in the event of a problem with the first two sources. Also, the ~~Process~~ Computer System includes four CPUs - one CPU serves as a back-up for any other CPU that may fail. ~~As concluded by the applicant~~, Further, the bypass/inoperable system meets the requirements of Regulatory Guide 1.47. On this basis, we conclude the system is acceptable.

7.5.2.2 Post-Accident Monitoring

Revision 2 to Regulatory Guide 1.97, "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant Environs Conditions During and Following an Accident," was issued in December 1980. In response to our question regarding implementation of R.G. 1.97 for the Byron/Braidwood design, the applicant stated that design changes in the post-accident monitoring system are presently being developed and will be submitted to the staff for review. The Operating License will be conditioned to require that the applicant comply with the recommendations of Regulatory Guide 1.97, Revision 2, or provide justification for any alternatives taken.

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

This Action Plan item requires providing a positive indication in the control room of the relief- and safety-valve position.

Direct, safety-grade position indication and alarm is provided in the control room for each of the pressurizer power operated relief valves, ~~relief isolation valves~~, and the safety relief valves. The position indication limit switches of the power operated relief valves, and the relief isolation valves are qualified per WCAP-8587, Rev. 2, March 5, 1979, "Environmental Qualification of Westinghouse Class 1E Equipment." The pressurizer safety relief position indication reed switches are qualified to IEEE Standard 323-1974. The review of the valve position indication is also included in the Byron station Control Room Design Review for NUREG-0700. Based on the above information we conclude that the design of this system conforms to the Action Plan guidelines.

sent 5.2.4 (next page)

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

sert

not caps

7.5.2.4 TMI ACTION PLAN ITEM II.F.1, ~~ADDITIONAL ACCIDENT~~ - MONITORING INSTRUMENTATION ~~POSITIONS (4), (5) AND (6)~~

Action Plan Item II.F.1 Position (4) requires a continuous indication of containment pressure in the control room; Position (5) requires a continuous indication of containment water level in the control room; and Position (6) requires a continuous indication of containment hydrogen concentration in the control room.

Based on our review, we find that the applicant has satisfied this item and adequately addressed the points of clarification ~~for this item~~ as stated in NUREG-0737. See Sections 6.2.1 and 6.2.5 of this report for a detailed discussion of the applicant's compliance with TMI Action Plan Item II.F.1.

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 ~~SRP~~ Standard Review Plan.

We have conducted an audit review of these systems for conformance to guidelines of the applicable Regulatory Guides and industry codes and standards. In Section 7.1.2 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 [illegible] of the open item identified in [illegible]~~ there is reasonable assurance that the systems conform to the applicable 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~~ these 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."

Our review also indicates that 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 completion of the licensing condition identified in Section ~~7.5.8~~ 7.1.3.4

7.6 Interlock Systems Important to Safety

7.6.1 System Description

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

7.6.1.1 Residual Heat Removal Isolation Valve Interlocks

The Residual Heat Removal System (RHRS) consists of two residual heat exchangers, two pumps, and the associated piping, valves, and instrumentation necessary for operational control. The inlet lines to the RHRS are connected 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 700 psig). The position of the valves in indicated on the main control board by lights actuated by the valve limit switches.

7.6.1.2 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 the RCS. To prevent injection of borated water at low pressure operation during shutdown and startup, each of the accumulators is provided with a motor-operated isolation valve in series with the check valves. The valve is closed by the operator shortly after the RCS is depressurized below the safety injection unblock 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") with the control switch in either the "AUTO" or "CLOSE" position.

(2) They open automatically whenever the RCS pressure is above the safety injection unblock pressure (~~P11~~ P-11 interlock) when the control switch is in the "AUTO" position.

(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 startup to prevent accidental closing. A light, actuated by the valve motor-operated limit switch, on the Group 1 monitor light box (see Section 7.5.1.1) is on if the valve is not fully open. An alarm, operated by the valve stem limit switch, is activated when a valve is not fully open with the system above the safety injection unblock pressure.

~~See Section~~ 5.4.7 for a discussion of conformance to RSB BTP 5-1.

Branch Technical Position

7.6.1.3 Switchover from Injection to Recirculation

The ~~change~~switch over 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 pump suction to the containment sump is accomplished automatically when the RWST level decreases below the low-low level setpoint following initiation of the safety injection. Four level measurement channels are provided and arranged in a two-out-of-four coincidence logic to open the two sump isolation valves. The RHR pumps continue to run during the switchover.

After receipt of the RWST auto switchover level signals and after the sump isolation valves are fully open, the operator closes the RWST ~~to RHR suction~~ isolation valves. 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 discharge.

Each of the four RWST level channels provides level indication in the control room and also generates high, low, low-low, and empty level alarms. The low-low level alarm automatically opens the sump isolation valves and alerts the operator to complete the switchover as described above.

7.6.1.4 Reactor Coolant System Loop Isolation Valve Interlocks

Each of the reactor coolant loops is provided with motor-operated stop valves which permit the loop to be isolated from the rest of the reactor cooling system (RCS). One stop valve is provided in the hot leg, and one in the cold leg of each loop.

The controls of the stop valves are interlocked to prevent an injection of a large amount of cold coolant resulting in a high reactivity insertion rate. The interlocks ensure that flow from the isolated loop to the remainder of RCS takes place through the relief line at a limited rate until the temperature and boron concentration in the isolated loop are brought into equilibrium with the

remainder of the system. The interlocks include stop valve position limit switches and differential pressure indicating switches in the relief line for flow monitoring.

7.6.1.5 Reactor Coolant System Pressure Control During Low Temperature Operation

The reactor coolant system (RCS) pressure control during low temperature operation includes automatic actuation logic for the two pressurizer power-operated relief valves (PORVs). The pressure control system functions by continuously monitoring reactor coolant temperature and pressure. The temperature is measured in each of the loops and the auctioneered lowest temperature signal is processed to generate a signal representing the allowable pressure. This reference signal is then compared with the actual measured pressure. An actuation signal to the PORVs will be generated if the measured pressure is higher than the reference pressure. Separate temperature and pressure monitoring channels are used for the actuation signal logic train for each of the two valves. The actuation signal from either train is effective only if the temperature is below an established level as determined by the temperature measurement channels of the other train.

7.6.2 Specific Findings

7.6.2.1 Residual Heat Removal Isolation Valve Interlocks

As discussed in Section 7.6.1.1 above, two motor operated valves are provided in series in each of the two residual heat removal pump suction lines to isolate the low-pressure residual heat removal system from the high-pressure reactor coolant system during normal operation. The two in-series isolation valves are powered from separate power sources and are separately and independently interlocked with pressure signals to prevent their opening above approximately 425 psig, and to close them automatically if the pressure increases to

approximately 700 psig. Also, the power source and pressure signal are common to one valve in each of the two suction lines.

The use of independently powered motor-operated valves in each of the two inlet lines, along with two independent pressure interlock signals, provides a system that meets the single failure criterion in regard to having at least one valve closed in each line to isolate RHRS when required. The system, however, does not meet the single failure criterion for opening at least one of the suction lines. One of the failures that would prevent opening of the isolation valves is a failure in one of the pressure monitoring channels providing interlocks to the valves. The other is a failure of an electrical power train. In either case, one of the two in-series valves in each of the suction lines could not be opened. In response to our concern, the applicant stated that such a failure is not considered to have an adverse safety impact. In such a situation, the auxiliary feedwater system and steam generator power-operated relief valves can be used to perform the safety function of removing residual heat. This allows the operator to take a necessary corrective action, such as bypassing the failed interlock, or restoring the power, or bringing in an alternate power source. [redacted] Based on our review we find the design acceptable.

7.6.2.2 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 7.6.1.5 above. In our review of the control logic of the automatic actuation system, we found that a failure resulting in a high output signal from either of the two auctioneers would prevent both relief valves from opening when needed. This is due to the fact that the output signal from an auctioneer is [redacted] used in the control logic to generate an actuation signal to the associated relief valve and also provides a permissive signal to the logic train of the other valve.

In response to our concern that the relief valve actuation system does not meet the single failure criterion, the applicant agreed to adopt the Westinghouse recommendation to remove the cross (*) below

7.6.2.3 Switchover from Injection to Recirculation Mode

As described in Section 7.6.1.3, the switchover from injection mode to recirculation mode is initiated when water level in the refueling water storage tank (RWST) reaches a preset trip point, and a safety injection signal ("S") has been received. The "S" signal is latched in by a retentive memory device and can be reset manually. If the "S" signal would be reset, no switchover to recirculation mode would be initiated even though it would be required by low water level in the RWST. We were concerned that the operator may not be aware of the situation, because no indication of "Reset" is provided. In response to our concern the applicant agreed to add an indication light to the RESET function. Based on this commitment we consider the issue resolved subject to confirmation of circuit revision.

7.6.2.4 Boron Dilution Control

One of the means of positive reactivity insertion to the reactor is the addition of unborated water into the reactor coolant system. A concern was raised about an inadvertent dilution resulting either from operator action or a mechanical failure in the makeup system. In our review of the FSAR we could find no information as to what means, if any, are provided to detect boron dilution and what steps would be taken to terminate it. In response to our concern the applicant will provide a boron dilution control system identical to that provided for the previously reviewed Callaway plant. This system involves upgrading the source range and intermediate range nuclear channels to meet the requirements of IEEE Standard 323-1974. In addition these channels will be modified to provide measurement of doubling time. Whenever a set limit of doubling time is reached, an alarm will be generated and valves in the CVCS will be automatically operated as required to prevent further dilution. We consider the issue resolved subject to confirmation that this new control system is incorporated and addressed in an FSAR revision.

connect and employ manual arming of the channels to meet the single failure criterion. An FSAR amendment will document this design change. We consider the issue resolved subject to confirmation of the FSAR revision.

7.6.2.5 Isolation of Non-Qualified Systems from Essential Service Water

The function of the Essential Service Water System (ESWS) is to supply water to the loads which are safety-related or essential to the safe shutdown of the reactor. To preserve system integrity in case of a seismic event, it is necessary to isolate nonseismically qualified loads. In response to our concern, the applicant stated that the only equipment that is nonseismically qualified and is supplied from the ESWS, are the Reactor Containment Fan Cooler System chillers. The isolation valves to the chillers are solenoid operated. The valves close on safety injection and fail closed on loss of power. Closed valve position is indicated on the monitor light box (see Section 7.5.1.1). As concluded by the applicant, a failure of the chiller system would not compromise the operation of ESWS. Based on this statement we consider the issue resolved.

7.6.2.6 Reactor Coolant System Loop Isolation Valve Interlocks

As described in Section 7.6.1.4 ~~#DDW~~, each reactor coolant loop is provided with two motor-operated stop valves. A requirement was imposed in the Construction Permit SER for the valve interlocks to conform to the requirements of IEEE Standards 279-1971 and 338-1971 or [redacted] lockout of power to the valve operators would be required to prevent accidental closing of the valves during operation. In response to this requirement, the applicant has agreed to remove the power to the reactor coolant loop isolation valve operators during operational modes 1, 2, 3, and 4. The power lockout will be controlled by administrative procedure. The FSAR will be revised to include this requirement. Based on the applicant's commitment we consider this issue resolved subject to our confirmation of the FSAR revision.

7.6.2.7 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 the 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

, "Report on Overall Safety Effect of Power Operated Relief Valve Isolation System",

response to item II.K.3.2 show that the probability of the PORV sticking open is sufficiently small.

Westinghouse

The applicant has stated that he agrees with the Westinghouse ~~determination~~ conclusions 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 guidance.

Our review included the interlock provided to prevent overpressurization of the primary coolant system during low temperature operation. The staff's position with regards to this interlock system is set forth in Branch Technical Position RSB 5-2, "Overpressurization Protection of Pressurized Water Reactors While Operating at Low Temperatures." (See section 7.6.2.2)

Space 5 5-2

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 completion of the confirmatory items identified in Section 7.1.3.2 of this report.

7.7 Control Systems

7.7.1 General

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.

7.7.2 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 bank 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 with each ~~of the channels uses~~ using a dual-section ionization chamber as a neutron flux detector. The currents from the ionization chambers are used to measure the power level, axial flux imbalance, and radial flux imbalance.

(b) Rod Position Monitoring System - Two separate systems are provided, digital rod position indication and the demand position indication system. The digital rod position indication system measures the actual position of each rod. The demand position indication 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 as a result of a comparison of any control rod position against the other rods in the bank.

(e) Rod Bottom Alarm - A local rod-at bottom alarm is generated for each of the rods by the Digital Rod Position Indication System. In addition, a control room annunciator is actuated when any rod is at bottom.

(4) Plant Control System Interlocks

(a) Rod Stops - Prevent abnormal power conditions which could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures. The interlocks are generated by signals from the neutron flux, overtemperature 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 overpressure ΔT measurement channels are used, and automatic

turbine load runback is initiated by an approach to an overpower or overtemperature condition.

(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) Presurizer 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.

(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 constant water level for normal power operation. 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 and/or the atmosphere to maintain an artificial load on the primary system. The rod control system can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions.

A demand signal for the load-rejection steam dump controller is generated if the difference between the reference average temperature based on turbine impulse chamber pressure and the measured 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 curcuit 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.

Space → Following a turbine trip, the load-rejection steam dump controller is deactivated and the turbine trip steam dump controller becomes active. The demand signal for this controller is generated if the difference between the measured 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 controller to regulate the rate of heat removal and thus gradually establish the equilibrium hot shutdown conditior.

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.

(9) Incore Instrumentation

The Incore Instrumentation includes the following systems:

(a) Thermocouples - Chromel-alumel thermocouples are used and located at fixed core outlet positions. The thermocouple readings are monitored by the plant computer. A backup readout is provided by an indicator with manual point selection located in the main control room.

(b) Movable Neutron Flux Detector System - Miniature fission chambers can be positioned in retractable guide thimbles for flux mapping of the

core. The controls, position indication, and flux recording for each detector are located in the control room.

(10) Boron Concentration Measurement System

The boron concentration measurement system employs a sample measurement device which contains a neutron source and neutron detector in a shielded tank. A coolant sample flow is maintained between the neutron source and the neutron detector. The neutron flux at the detector depends on the boron concentration in the coolant. Electronic circuitry converts the signal from the detector into a digital display of ~~ppm~~ boron concentration in parts per million (ppm).

(11) Main Steam Isolation Valve Control

Each steam generator main steamline is provided with a hydraulically operated isolation valve with a 4-inch air operated bypass around the valve. Both the isolation valves and the bypass valves will be closed automatically upon receipt of an isolation signal (see Section 7.3.1.1). Manual close-open controls for all valves are provided in the main control room. The main isolation valves may also be manually closed or opened from the remote shutdown panel. Means for proportional (throttling) control of the bypass valves are provided in the control room.

(12) Turbine-Generator Controls

The turbine is provided with a digital electrohydraulic control system. The controller generates a control signal which actuates hydraulic controls of the governor valves and the reheat steam interceptor valves. The control signal is based on comparison of signals representing turbine speed and first stage pressure with the reference signal representative of load demand. The turbine instrumentation and controls are located in the main control room.

(13) Main Condenser Controls

The following systems are provided:

(a) Condenser Water Level Control - Redundant water level instrument channels monitor and control water level in the hot well. Each channel includes a level transmitter, four level controllers, and three level switches. Each of the four controllers provides a pneumatic signal for the positioning of its associated control valves. These valves control the normal overflow, emergency overflow, normal makeup, and emergency makeup. Selection of one of the redundant controllers to drive each of the four control valves is made through a locally mounted, manually operated three-way valve.

(b) Condenser Vacuum Control - Two steam jet air ejectors are provided to maintain condenser vacuum at 3.5 inches Hg abs. at design conditions. Additionally, redundant hogging vacuum pumps are provided to establish initial vacuum conditions during startup. Controls for the vacuum pumps are on the main control board.

(14) Circulating Water System Controls

The circulating water system provides a supply of water to the main condenser to remove the cycle waste heat. Cooling of the heated circulating water is provided by the cooling towers at the Byron Station, and by the cooling pond for the Braidwood Station. Circulating water pumps are normally operated from the main control board.

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 Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation

A concern was raised in IE Bulletin 79-27, issued November 30, 1979, regarding the loss of a non-Class 1E power bus resulting in a consequential control system malfunction and significant loss of information to the operator. ~~We have requested~~ The applicant has provided the results of the Byron/Braidwood Station review as required by Bulletin 79-27 in an FSAR amendment. Based on our review we find the applicant's response in compliance with the requirements of this bulletin.

7.7.2.2 Failures of the Rod Control System

In our review we found that the FSAR did not include sufficient information to evaluate what design features are provided in the rod control system to limit reactivity insertion rates and incorrect sequencing or positioning of control rods resulting from a single failure within the system. In response to our concern the applicant stated that the Byron/Braidwood rod control system is the same as the generic system used for other current Westinghouse plants which have been previously reviewed, and has since incorporated the evaluation for such a rod control system in the FSAR.

7.7.2.3 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 then those analyzed in the Safety Analyses of Chapter 15. In response to the concern raised in Notice 79-22, the applicant submitted the results of his review of potential control systems failures. The information supplied is based on the Westinghouse generic review of this subject. In this review, four control systems were identified whose failure could impact the plant conditions. These systems are as follows:

(1) Automatic Rod Control System - Of concern is a failure in the neutron detector ouput in the low direction causing an automatic rod withdrawal following a steamline break.

(2) Main Feedwater Control System - A postulated problem is a malfunction of the main feedwater control system following a rupture of a small feedwater line. An assumption is made that this malfunction would result in closing the feedwater valves to all steam generators.

(3) Pressurizer PORV Control System - The potential problem involves the PORV valve failing to open due to the adverse environment resulting from a feedwater line rupture.

(4) Steam Generator POPV Control System - A failure of the PORV control system could result in a depressurization of the steam generators following the feedwater line break. The primary concern of such a failure is a loss of steam to a turbine driven auxiliary feedwater pump.

The four possible failures above have been investigated by the applicant and he has concluded that the accident sequences would not result in more limiting events than those presented in Chapter 15 of the Safety Analysis Report. Based on our review of the applicant's response we consider this item resolved.

7.7.2.4 Multiple Control System Failures

A concern ~~has been~~ was 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.

As stated by the applicant, 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.

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

Our review of control systems included the features of these systems for both manual and automatic control of the process systems. We find that the control