Department of Energy
Washington, D.C. 20545

Docket No. 50-537
HQ:S:82:147

DEC 14 1982

Mr. Paul S. Check, Director
ATTN: J. L. Mauch, ICSB
CRBR Program Office
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Check:

INSTRUMENTATION (CHAPTER 7) WORKING MEETINGS - ADDITIONAL INFORMATION

References: (1) J. R. Longenecker to P. S. Check, Subject: Meeting Summary for Instrumentation (Chapter 7) Working Meeting, September 21 and 22, 1982, dated September 24, 1982

(2) J. R. Longenecker to P. S. Check, Subject: Meeting Summary for Instrumentation (Chapter 7) Working Meeting, November 18 and 19, 1982, dated November 29, 1982

Enclosed is the additional information requested during the subject meetings for which response dates of December 10, 1982, were projected. The amended Preliminary Safety Analysis Report (PSAR) pages will be incorporated into a future PSAR revision.

Three items that were due December 10 are not complete at this time. These items are identified in the enclosure and will be submitted by December 17.

Any questions regarding the information provided or further activities can be addressed to Mr. R. Rosecky (FTS 626-6149) or Mr. A. Meller (FTS 626-6355) of the Project Office Oak Ridge staff.

D001
S
1/40

Sincerely,

Joseph C. Bartley for
John R. Longenecker
Acting Director, Office of
Breeder Demonstration Projects
Office of Nuclear Energy

Enclosure

cc: Service List
Standard Distribution
Licensing Distribution

Enclosure

Instrumentation and Control (Chapter 7) September 21 and 22, and November 18 and 19 Working Meetings Action Items due to NRC December 10, 1982.

September Item (November Item)

6*
96 (1)
54 (4)*
46 (7)
84 (9)
42 (10)*
17, 18, (12)
4, 17, 18 (13)
69, 70 (18)
67 (19)

* Items not complete at this time; expected submittal date is December 17.

SEPTEMBER ITEM 96, NOVEMBER ITEM (1)
RESPONSE TO QUESTION 421.19

NRC CONCERN:

1. Document that when in test of a protection channel, and common part of protection system fails, the damage levels do not exceed those of the anticipated operational occurrence. Update Ch. 7.2.15.

2. App. B QA, OBE Seismic Qualification, and periodic test criteria should apply to the median selectors. A greater than OBE occurence requires retest commitment in the tech specs.

3. Indicate that the Q421.19 analyses submitted applies to "PPS channel under test" situation.

RESOLUTION:

The revised response to Question 421.19 is provided.

1. Revised Section 7.2.15 indicates that, when in test, the shutdown systems limit the core transients to limits no greater than those associated with normal operation of the shutdown system.

2. Although not stated in the PSAR, the median select circuit is being designed and fabricated under an ANSI N45.2 QA program and thus meets the 10CFR50 Appendix B requirements. The median select circuit is being designed to be functional after an OBE.

3. The response to Q421.19 discusses the situation of "PPS channel under test" in the following sections: "Loss of Any Single Instrument" and "Loss of Power to a Protection Separation Group."

Question CS421.19

A number of concerns have been expressed regarding the adequacy of safety systems in mitigation of the kinds of control system failures that could actually occur at nuclear plants, as opposed to those analyzed in PSAR Chapter 15 safety analyses. Although the Chapter 15 analyses are based on conservative assumptions regarding failures of single control systems, systematic reviews have not been reported to demonstrate that multiple control system failures beyond the Chapter 15 analyses could not occur because of single events. Among the types of events that could initiate such multiple failures, the most significant are in our judgement those resulting from failure or malfunction of power supplies or sensors common to two or more control systems.

To provide assurance that the design basis event analyses adequately bound multiple control system failures you are requested to provide the following information:

1) Identify those control systems whose failure or malfunction could seriously impact plant safety.

2) Indicate which, if any, of the control systems identified in (1) receive power from common power sources. The power sources considered should include all power sources whose failure or malfunction could lead to failure or malfunction of more than one control system and should extend to the effects of cascading power losses due to the failure of higher level distribution panels and load centers.

3) Indicate which, if any, of the control systems identified in (1) receive input signals from common sensors, common hydraulic headers, or common impulse lines.

The PSAR should verify that the design criteria for the control systems will be such that simultaneous malfunctions of control systems which could result from failure of a power source, sensor, or sensor impulse line supplying power or signals to more than one control system will be bounded by the analysis of anticipated operational occurrences in Chapter 15 of the Final Safety Analysis Report.

Response — Replace with revised response

The design criteria for the Plant Protection System prohibits control system malfunctions from endangering plant safety. Therefore, there are no control system failures or malfunctions that seriously impact plant safety because of protection provided by the Plant Protection System (PPS). Failure in the following control systems could, however, cause a reactor scram to occur: Supervisory Control, Reactor Control, PHTS and IHTS Sodium Flow Control, PHTS and IHTS Pump Speed Control, Drum Level Control and Turbine Control. The Chapter 15 analysis envelopes the failure of multiple control systems due to loss of power since:

1) For loss of offsite power, the PPS trips the control rods upon loss of power to the sodium pumps. Action of the control system is irrelevant.

2) Primary rod control has redundant MG sets powered from non-UPS normal A and B sources. Loss of A or B does not affect rod motion. For loss of A and B, a PPS trip occurs due to steam/feedwater mismatch resulting from a turbine/generator trip.

3) Failure of electrical power (non-UPS normal A) to the Supervisory Control and Reactor Control Systems will not result in primary control rod withdrawal. The control rod rate circuit will produce a zero rod rate signal with zero power available. The worse that can happen on the loss of non-UPS normal electrical power is a reduction in coolant flow which is enveloped in the Chapter 15 analysis.

4) For Supervisory Control, Reactor Control, PHTS Sodium Flow control and IHTS Sodium Flow Control, the design provides for controllers in different cabinets each with redundant power supplies to eliminate power supply failures affecting several controllers.

Superheater exit steam flow sensors are shared by the Supervisory Control and Drum Level Control Systems, but median select circuits are used to prevent single sensor failures form causing an abnormal condition and resulting reactor scram. Loss of power to the median select circuits will result in a lowering of the steam drum level and a reduction in reactor power. The Plant Protection System will trip the reactor on a "low steam drum level" trip. The loss of power to the median select causes the superheater exit steam flow signal to go to zero indicating zero steam flow. This causes the steam drum level control system to close the feedwater control valves resulting in a decrease in the steam drum level. It also causes the supervisory control system to decrease reactor power in order to keep reactor power equal to plant thermal power as indicated by the superheater exit steam flow signal.

REPLACE WITH REVISED RESPONSE

Response

The design criteria for the Plant Protection System requiresthat control system malfunctions do not as a consequence compromise the capability of plant systems to maintain the plant in a safe condition. Accordingly, the Plant Protection System has been designed to provide continuing protection in the event of control system failures and malfunctions. The Plant Protection System is designed as a safety related system and includes redundant instrument channels, qualified to safety grade requirements. Where control actions are accomplished by plant control systems, functions important to safety are monitored through the Plant Protection System. Thus, the Plant Protection System through its redundant sensory channels will sense and respond appropriately to the consequential effects of control system failures or malfunctions. This includes failures or malfunctions within one control system that directly affect the functioning of other control systems, e.g., loss of a power supply common to several control systems, or shared sensor inputs.

Evaluation of the application of these design criteria applied to CRBRP Plant Protection System and Plant Control System involves analysis of postulated events which could propagate the effects of failures or malfunctions through more than one control system. Events which are considered to cause or result in such propagation are:

1) Loss of a single instrument

2) Break of a single instrument line

3) Loss of power supply for all systems provided from a common power source (e.g., a single inverter supplying several systems).

CRBRP control systems which may affect functions important to safety are:

A) Supervisory Control
B) Reactor Control
C) PHTS and IHTS Sodium Flow Control
D) PHTS and IHTS Pump Speed Control
E) Steam Drum Level Control
F) Turbine Control
G) Bypass Valve Control

Analysis of such events have been conducted for the control systems above. These analyses show that for postulated events considered in 1) thru 3) above the plant is maintained in a safe condition and no conditions result which are worse than those addressed in the PSAR Chapter 15, Accident Analyses.

The analyses assume initial conditions to be anywhere within the full operating power range of the plant (i.e., 0-100%), where applicable.

The results of the analyses indicate that, for any of the postulated events considered in 1) thru 3) above, the accident analyses in Chapter 15 of the PSAR are bounding.

22

Loss of Any Single Instrument

Median select circuits are used by most of the control systems itemized above to provide the median (or middle) of three sensors as the control feedback signal. For systems using median select circuits the failure of one sensor will not result in loss of control. The analysis in this section, however, goes beyond a sensor failure for these systems and considers a failure in the controller circuitry such that the feedback signal fails high or low. Table 1, Loss of Any Controller Feedback Signal, is an evaluation of the effect on the control systems and the plant caused by loss of the feedback signal either high or low. For control action in the unsafe direction, the bounding PSAR accident is listed. Where no control action occurs or where control action is in a safe direction, no bounding accident is given. This table clearly shows that for the feedback signal failing high or low, events in Chapter 15 of the PSAR are bounding. Control systems that don't use median select circuits are discussed below.

The turbine EHC speed control as well as primary and intermediate pump speed control systems use auctioneering circuits rather than a median select circuit. The circuits are designed such that one sensor failure will not affect control. Two failures are required for loss of the control function. Even though one sensor failure has no effect, this analysis considers failure of the feedback signal high or low. Plant effects and bounding events are given in Table QCS421.19-1.

The turbine EHC flow control and bypass valve position control systems do not use median select circuits but rather single sensors for the feedback signal. For these systems the failure of one sensor will result in a plant disturbance. Plant effects and the bounding event for failure of the feedback signal high or low is provided in Table QCS421.19-1.

The analysis in Table 1 also covers the case of a sensor failure while testing a redundant PPS channel. Control systems that use buffered PPS signals all have median select circuits. For the worst case, the median select circuit would choose one of the failed input signals as the controller feedback. The resulting transient is the same as that in Table 1 where the feedback signal downstream of the median select is assumed to be failed high or low.

Common Sensors Used By Control Systems

There are two cases where common sensors are used by control systems. The Supervisory Control and Bypass Valve Pressure Control systems both use pressure sensors in the main steam header. Each system has its own median select circuit, and the two systems are not in operation at the same time, therefore, failure of a common sensor will not result in loss of control.

The second case involves the Supervisory and Steam Drum Level Control systems. Both systems use superheater steam flow sensors and a common median select circuit in each loop. Since median select circuits are used in each loop, the failure of a single sensor will not result in loss of control in either control system. In the event the median select circuit fails low, the NSSS power is reduced by the supervisory controller and feedwater in the affected loop is reduced by the drum level controller. A reactor scram and SGAHRS initiation results due to low drum level. The bounding event is Loss of Normal Feedwater (PSAR Section 15.3.1.6). In the event the median select fails high, NSSS power is increased but limited to 100% power by a reactor control limiter and feedwater increases until a high drum level condition results in isolation of the main feedwater and a reactor trip. The Chapter 15 bounding event is not applicable for this case.

Break of Any Single Instrument Line

The break of an instrument line common to more than one control system is not applicable to CRBRP. There are only two cases in which sensors are common to more than one control system and the common point is at the transmitter or median select output. These two cases were addressed in the previous section.

Loss of Power to a Protection Separation Group

This section analyzes the effects [illegible]ol systems caused by the loss of an inverter powering a protectio[illegible] If the bus to protection channel A, B or C fails low, then th[illegible]ed PPS channel will trip and the following PPS buffered signals used by the control systems will drop to zero: Channel A, B or C corresponding to the failed bus for reactor flux, primary sodium flow, intermediate sodium flow, steam drum level, superheater steam flow and feedwater flow. Since median select circuits are used to provide the median of the three buffered PPS signals as the controller feedback signal, there will be no loss of control and no effect on the plant. Chapter 15 accident analysis is not applicable.

The following describes the effects in the event power is lost to a redundant protection channel while a PPS channel is under test:

1) If an inverter fails with power lost to the PPS logic, the channel under test is tripped during test satisfying the 2/3 trip logic, and a reactor scram will occur.

2) If a bus fails such that power is lost to a sensor or transmitter but not to the PPS logic, the controller feedback signal in the worst case will be low as a result of two input signals low. (One due to power failure and one due to channel test condition.

Loss of Power to Control Systems

This section examines the effects on the control systems caused by loss of a bus powering these systems. Most of the control systems are supplied by primary and alternate sources of power and have redundant power supplies in the cabinets. The alternate power source will supply power in the event of a failure of the primary source. Thus, total loss of power requires failure of both power sources and is unlikely. For these control systems, loss of one supply will not result in loss of the control function and the Chapter 15 accident analysis, therefore, is not applicable. Control systems that are powered from one source are discussed below.

For the primary rod controller, there is some circuitry that is not powered from redundant supplies. In the event Non-1E UPS system A bus fails low, all rod position displays will be lost and rod movement in group or single modes will be inhibited. No plant disturbance results since primary rods are powered from redundant MG sets and remain stationary. Plant operation will proceed in accordance with technical specification limits.

For the primary and intermediate speed control systems, loss of either Non-Class 1E 13.8 KV, 480 VAC or 120 VAC buses feeding the pump drive equipment will lead to a pump trip followed by a reactor scram. The bounding event is Spurious Primary Pump Trip (PSAR 15.3.1.2).

Besides the loss of power to control systems from the loss of a power distribution bus, there is a chance of having an electrical fault on one of the control system circuit cards. The control systems are designed so that each card is used in only one control system. A circuit card failure cannot directly impact more than one control system. A failure on a control card would cause the controller to generate either an "off" or a "full on" output, depending on the type of failure. This result would be similar to having the feedback signal fail high or low. Therefore, the failure of or loss of power in any control system circuit card would be bounded by the Loss of Any Controller Feedback signal analysis described in Table QCS421.19-1.

or "as is" or "between off and full on"

Conclusions

The preceding sections have shown that failures of individual sensors, loss of controller feedback signals, breaks in instrument lines and loss of power to protection channels and control systems all result in events which are bounded by Chapter 15 of the PSAR or result in events with no control or plant impact. Therefore, the PSAR Chapter 15 Accident Analysis adequately bounds the consequences of these fundamental failures.

Table QCS421.19-1. Loss of Any Controller Feedback Signal

Feedback Signal	System	Assumed Failure Direction	Effect	Bounding Event
Reactor Flux	Reactor Control	Lo	Control rods are withdrawn if flux control in auto until high flux or flux-to-flow deviation rod blocks stop rod motion.	Bounding event is Maloperation of Reactor Plant Controllers (PSAR Section 15.2.2.3).
		Hi	Control rods are inserted if flux control in auto.	Not applicable.
Core Exit Temperature	Reactor Control	Lo	Control rods are withdrawn if core exit temperature control in auto until high flux or flux-to-flow deviation rod blocks stop rod motion.	Bounding event is Maloperation of Reactor Plant Controllers (PSAR Section 15.2.2.3).
		Hi	Control rods are inserted if core exit temperature control in auto.	Not applicable.
Turbine Inlet Temperature	Turbine Inlet Temperature Control	Lo	Control rods are withdrawn if turbine inlet temperature control in auto until high flux or flux-to-flow deviation rod blocks stop rod motion.	Bounding event is Maloperation of Reactor Plant Controllers (PSAR Section 15.2.2.3).
		Hi	Control rods are inserted if turbine inlet temperature control in auto.	Not applicable.

QCS421.19-6

26

Table QCS421.19-1 (Continued)

Feedback Signal	System	Assumed Failure Direction	Effect	Bounding Event
Turbine Inlet Pressure	Turbine Inlet Pressure Control	Lo	Intermediate pump speed in all loops increases if turbine inlet pressure control in auto.	Not applicable
		Hi	Intermediate pump speed in all loops decreases if turbine inlet pressure control in auto.	Bounding event is Loss of Off-Site Electrical Power (PSAR Section 15.3.1.1).
Superheater Steam Flow	Unit Load Control (Load Programmer)	Lo	Setpoints to all NSSS control systems will decrease to 40% of design.	Not applicable.
		Hi	Setpoints to all NSSS control systems will increase to 100% of design.	Bounding event is Maloperation of Reactor Plant Controllers (PSAR Section 15.2.2.3).
Primary Sodium Flow	Primary Sodium Flow Control	Lo	Primary pump speed increases if primary flow control in auto mode.	Not applicable.
		Hi	Primary pump speed decreases if primary flow control in auto mode.	If flow controller output change is greater than 10%, pump speed does not change due to speed control mode transfer to manual (open loop). If flow controller output change is less than 10% pump speed decreases ove time. Hence, bounding event is Spurious Primary Pump Tri (PSAR 15.3.1.2).

27

Table QCS421.19-1 (Continued)

Feedback Signal	System	Assumed Failure Direction	Effect	Bounding Event
Intermediate Sodium Flow	Intermediate Flow Control	Lo	Intermediate pump speed increases if intermediate flow control in auto mode.	Not applicable.
		Hi	Intermediate pump speed decreases in affected loop if intermediate flow control in auto mode. Pressure control increases pump speed in other loops.	If flow controller output change is greater than 10%, pump speed does not change due to speed control mode transfer to manual (open loop). If flow controller output change is less than 10% pump speed decreases over time. Hence, bounding event is Loss of Off-Site Electrical Power (PSAR Section 15.3.1.1).
Primary Speed	Primary Speed Control	Lo	Speed control automatically transfers to open loop control. No plant disturbance.	Not applicable.
		Hi	Same as above.	Not applicable.
Intermediate Speed	Intermediate Speed Control	Lo	Speed control automatically transfers to open loop control. No plant disturbance.	Not applicable.
		Hi	Same as above.	Not applicable.

Table QCS421.19-1 (Continued)

Feedback Signal	System	Assumed Failure Direction	Effect	Bounding Effect
Steam Drum Level	Steam Drum Level Control	Lo[1]	Main feedwater flow increases if steam drum level control is in auto. Increase in feedwater flow results in a high drum level and isolation of feedwater. Reactor trips upon isolation of main feedwater.	Not applicable.
		Hi[2]	Main feedwater flow decreases if steam drum level control in auto. Reactor scram and SGAHRS initiation result due to low drum level.	Bounding event is Loss of Normal Feedwater (PSAR Section 15.3.1.6).
Flow Reference Trim	Turbine EHC Speed Control	Lo	Turbine steam flow decreases as control valves close. NSSS follows steam flow if in supervisory control mode.	Not applicable.
		Hi	Turbine steam flow increases as all control valves open. NSSS follows steam flow up to 100% power (high flux limiter in reactor control) if in supervisory control mode. At 100% power, mismatch condition results in cooldown of the NSSS followed by a turbine trip on low pressure.	Bounding event is Turbine Trip (PSAR Section 15.3.1.5)

[1] Same effect for feedwater flow feedback failing low or superheater steam flow feedback failing high.

[2] Same effect for feedwater flow feedback failing high or superheater steam flow feedback failing low.

Table QCS421.19-1 (Continued)

Feedback Signal	System	Assumed Failure Direction	Effect	Bounding Event
Valve Position	Turbine EHC Flow Control	Lo	Turbine steam flow initially increases as affected control valve opens. Increase in flow is minimized by other 3 control valves closing to compensate. Disturbance on NSSS is small and bounded by normal plant transients.	Not applicable.
		Hi	Turbine steam flow initially decreases as affected control valve closes. Decrease in flow is minimized by the other 3 control valves opening to compensate. At 100% power, flow decrease continues due to limited compensation (valves fully open). NSSS follows steam flow if in supervisory control mode.	Not applicable.
Valve Position	Bypass Valve Control	Lo	Steam flow increases and pressure decreases as affected valve opens. If in load error mode, turbine trips on low pressure. If in pressure mode, other valves close to compensate; Possible turbine trip.	Bounding event is Turbine Trip (PSAR Section 15.3.1.5)
		Hi	Steam flow decreases and pressure increases as affected valve closes. If in load error mode, NSSS follows steam flow reduction. If in presure mode, other valves open to compensate	Not applicable.

Table QCS421.19-1 (Continued)

Feedback Signal	System	Assumed Failure Direction	Effect	Bounding Event
Pressure	Bypass Valve Control	Lo	Valves close increasing turbine inlet pressure and decreasing steam flow.	Bounding event is Failure of Steam Bypass System (PSAR Section 15.3.2.4).
		Hi	Valves open decreasing turbine inlet pressure and increasing steam flow with possible turbine trip on low pressure.	Bounding event is Turbine Trip (PSAR Section 15.3.1.5).

September ITEM 46, RELATIONSHIP OF PHTS, IHTS
November Item (7) AND SGS WITH DHRS

NRC CONCERN:

Add to the PSAR a summary of DHRS instrumentation and control design criteria and how it is independent and separate from the SGAHRS I&C. Verify in PSAR that DHRS I&C is safety-related and separate from SGAHRS I&C.

RESPONSE:

The SGAHRS consists of three redundant systems, each system is powered from its respective Class 1E redundant power division 1, 2 or 3. The equipment and power supplies of the three divisions are physically and electrically independent such that the loss of any one division will not prevent the other divisions from performing their safety functions.

The DHRS equipment is powered from Class 1E, Divisions 1 and 2. The DHRS equipment of the two redundant divisions and their respective power supplies are physically and electrically independent.

In general, the cables, raceways and other equipment of the SGAHRS and DHRS are located in different areas of the plant, except in the control building and the steam generator building where the cables of the same safety division of SGAHRS and DHRS share common raceways. However, the cables and raceways of redundant divisions are physically and electrically separated such that the loss of one safety division will not prevent the other divisions from performing their safety functions.

The PSAR Sections 7.6.3 and 7.4 will be revised as attached, to include the above description.

(c) The PACC outlet louver opens automatically whenever the inlet louver is not fully closed. When the outlet louver is fully open, the PACC blower may be started either automatically or manually.

7.4.1.1.5 Redundancy/Diversity

The SGAHRS (fluid system and mechanical components) is designed with suitable redundancy and diversity so that it can perform its safety functions following a single failure of an active component for anticipated, unlikely and extremely unlikely plant conditions. The design of SGAHRS relating to these objectives is discussed in Section 5.6.1.

Redundancy and diversity are also provided within the initiating circuitry of the SGAHRS control system. As shown in Figure 7.4-1, the system is actuated 54 on two-out-of-three trip signals from either low steam drum level, or high steam-to-feedwater flow ratio.

7.4.1.1.6 Actuated Devices

All automatic valves and motors in the SGAHRS are provided with remote manual control capability, so that the entire system can be operated from the control 54 room or the remote shutdown panels.

All isolation valves within the SGAHRS utilize an electrohydraulic actuator. 54 All isolation valves are designed to fail to the position of greater safety upon loss of electrical power.

All required components of the SGAHRS instrumentation and control system operate on a vital electrical bus.

7.4.1.1.7 Testability

Instrumentation and controls for the SGAHRS are designed and arranged to allow for complete testability during reactor power operation. Bypassing of the actuated components (i.e., isolation valves and motors) is not required during testing as operation of these components during power operation poses no penalty on plant operation.

7.4.1.1.8 Separation

54 The SGAHRS instrumentation and control system, as part of the Decay Heat Removal System, is designed to maintain required isolation and separation between redundant channels (see Section 7.1.2.2).

The separation of SGAHRS equipment and cables from those of DHRS is described in section 7.6.3.

(3) Low EVST sodium, EVST NaK and primary makeup flowrate (each pump loop)

(4) High and low EVST sodium inlet temperature (each loop)

(5) High and low EVST NaK expansion tank level (each loop)

(6) High and low EVST sodium level

(7) High and low EVST sodium temperature

(8) Low sodium valve temperatures

(9) High and low DHRS expansion tank level

Key process variables that are connected to annunciators are also connected to the plant data handling and display system.

D. Other Features

Remotely operated valves in EVST cooling and DHRS circuits incorporate either "fail safe" or "fail in place" features and are provided with direct manual (reach rods on sodium valves) override capability in event of I&C or gas supply failures. DHRS valves are provided with accumulators to provide 1/2 hour startup capability for a period of 10 hours after the gas supply is lost.

Type 1E power is supplied to the equipment and instrumentation required to provide the safety related functions of EVST cooling and DHRS as shown in Figure 7.6-11. This assures independence of off-site power.

Functional testing of all portion of DHRS that are not used during the course of normal operations will be tested on an annual basis during reactor refueling.

Equipment required to provide power to EVST and DHRS pumps, airblast heat exchangers and the monitoring instrumentation in the control panels shall be designed and tested to Seismic Category I requirements.

The DHRS control panel is configured to hi-light the DHRS coolant flow circuits with visual aids to assist the operator during DHRS initiation and operation.

INSERT 1

7.6.3.1.4 Initiating Circuits

Reactor decay heat removal through DHRS is initiated from the Control Room panel as described in Sections 9.1.3 and 9.3.2.

7.6.3.1.5 Bypass and Interlocks

When the DHRS is activated, automatic control of the EVST airblast heat exchangers is bypassed. All valves in this circuit are also operated on a direct or remote manual basis.

September Item 84, November Item (9) -- Delayed Neutron Detection

NRC Concern:

DND redundancy, seismic classification and test requirements.

Resolution:

Section 7.5.4.1.2 has been revised to address the above subjects.

The cover gas monitoring system line in containment has redundant Category 1 Accident Monitoring Instrumentation (gamma monitors) to measure cover gas activity that will provide a quantitative measure of gross fuel failures. Since the cover gas monitors are IE, there is no necessity to make the Delayed Neutron Detectors IE.

order to increase the signal to background ratio. Monitoring is done with a planar germanium (Ge) gamma detector which continuously monitors specific fission gas radioisotopes. An alarm in the main control room (plant annunciator) will be activated in the event of an abnormal activity level increase for any of these radioisotopes. A multichannel analyzer, including a minicomputer, analyzes the signal from the detector to display the entire gamma ray spectrum. The minicomputer with additional input of the reactor power provides basic characteristics of the failure, i.e., magnitude and burnup, which may be used to supplement the Failed Fuel Location Subsystem through correlation with core and blanket history.

Failure of the minicomputer does not affect the failure detection capability of the CGMS. In this case, the multichannel analyzer memory will still be functional; however, the characterization capability will be lost. During normal operation when there are no failures, the minicomputer is not used. However, if there is a fuel failure, which requires characterization, data from the multichannel analyzer can be recorded and analyzed manually. In addition, a gas grab sample could be obtained, and then analyzed in the Plant Service building Laboratory which has equipment equivalent to the CGMS multichannel analyzer and minicomputer. By using this equipment one can characterize the fuel failure and provide the desired information.

7.5.4.1.2 Reactor Delayed Neutron Monitoring Subsystem

~~The Reactor Delayed Neutron Monitoring Subsystem includes a Delayed Neutron Monitor consisting of an assembly of three BF$_3$ filled gas proportional neutron detectors, mounted in a shielded moderator assembly adjacent to each of the three Primary Heat Transport System hot leg pipes.~~

REPLACE WITH INSERT 7.5-16

Coolant sodium transported past the detector assembly, is continuously monitored for delayed neutrons emitted by decay of radioactive precursors in the sodium. The system sensitivity is dependent on the signal-to-background ratio of the system. Signal is defined as detected delayed neutrons produced by recoil of precursors from fuel exposed by cladding failure, or from fission of fuel washed out into the sodium through a failure. Background is defined as detected neutrons from known sources which are not initially related to failed fuel (fuel pin contamination, fissionable impurities in core structural materials, fissionable materials in the sodium, and neutrons from the reactor).

The shielding and moderator assembly provides 1) reduction of gamma interference from Na-24, 2) moderation of neutrons, 3) capability for remote insertion of a calibrated neutron source, 4) capability for insertion and removal of the detector assemblies from the reactor containment building operating floor without deinerting the PHTS cells.

INSERT 7.5-16

The reactor delayed neutron monitoring subsystem consists of three monitoring channels, one channel for each of the three primary loops. Each channel contains signal conditioners, readout equipment, and an assembly containing multiple neutron detectors. Each detector assembly is mounted in a shield/moderator block adjacent to one of the three primary heat transport system hot leg pipes. The multiple detectors in each assembly provide sufficient countrate for detection as well as redundancy in case of a single detector failure. The delayed neutron monitoring subsystem is required to be in service at all times during plant operation. In certain situations, continued plant operation is permitted for short periods of time following the failure of a channel monitoring a single loop. In order to allow such operation, a number of prerequisite conditions must exist. These include requirements that the CGMS system is operational and shows no changes during the outage, and that the other two DND channels are also operational and provide steady output with no indication of change during the outage. The system design provides high availability since detector repair or replacement can be accomplished during operation and multiple detectors are in each source/moderator block. Also, the preamplifiers and signal conditioning equipment are accessible for maintenance, checkout, and repair or replacement at all times during reactor operation. This subsystem is seismically qualified for an operational basis earthquake.

September Items 17,18

November Item (12) -- Primary and Secondary RSS Sharing of Power Supplies

NRC Concern:

Commit to providing a description prior to the OL of the test program and acceptance criteria for demonstrating fault isolation between the primary and secondary RSS power supplies. Refer to St. Lucie unit 2 for an example.

Resolution:

Section 7.2 has been revised to indicate that an analysis will be performed to identify any transients which could originate from within one of the reactor shutdown systems and be coupled through the AC vital distribution bus to the other shutdown system. If significant transients are identified by this analysis, then a test program will be defined to confirm the continued operation of the remaining reactor shutdown equipment connected to the same vital power source. A description of any such test program will be provided prior to the application for an Operating License.

- Tornado

The RSS is protected from the effects of the design basis tornado by locating the equipment within tornado hardened structures.

- Local Fires

All RSS equipment, including sensors, actuators, signal conditioning equipment, wiring, scram breakers, and cabinets housing this equipment is redundant and separated. These characteristics make any credible fire of no consequence to the safety of the plant. The separation of the redundant components increases the time required for fire to cause extensive damage and also allows time for the fire to be brought to the attention of the operator such that corrective action may be initiated. Fire protection systems are also provided as discussed in Section 9.13.

- Local Explosions and Missiles

All RSS equipment essential for reactor trip is redundant. Physical separation (distance or mechanical barriers) and electrical isolation exists between redundant components. This physical separation of redundant components minimized the possibility of a local explosion or missile damaging more than one redundant component. The remaining redundant components are still capable of performing the required protective functions.

- Earthquakes

All RSS equipment, including sensors, actuators, signal conditioning equipment, wiring, scram breakers and structures (e.g., cabinets) housing such equipment, is classed as Seismic Category I. As such, all RSS equipment is designed to remain functional under OBE and SSE conditions. The characteristics of the OBE and SSE used for the evaluation of the RSS are found in Section 3.7.

INSERT 7.2-13

7.2.2 Analysis

The Reactor Shutdown System meets the safety related channel performance and reliability requirements of the NRC General Design Criteria, IEEE Standard 279-1971, applicable NRC Regulatory Guides and other appropriate criteria and standards.

The RSS Logic is designed to conform to the IEEE Standards listed in Table 7.2-4.

General Functional Requirement

The Plant Protection System is designed to automatically initiate appropriate protective action to prevent unacceptable plant or component damage or the release or spread of radioactive materials.

Supersedes version transmitted by WLB20576

INSERT 7.2-13

7.2.1.2.4 REACTOR SHUTDOWN SYSTEM POWER SUPPLIES

The Primary and Secondary reactor shutdown systems are powered from the three Class 1E 120/208 volt Vital (Uninterruptable) AC Power Systems. Redundant channels within each shutdown system are powered from separate independent load groups with one channel/logic train from each system connected to the same vital AC power system. This commonality between one set of redundant channels/logic trains is not considered to impact their independence because of the following design features:

- The design of the Vital AC Power System assures independence between the three redundant power divisions such that failures within a power division load group will not propagate to a redundant load group.
- Loss of one vital power division will result in tripping one logic train in each reactor shutdown system.
- Provision of isolation devices in the individual power supplies within the two reactor shutdown systems will prevent any circuit failure in one redundant channel/logic train of one system from affecting the proper safety function of the other system.
- Features will be provided within the Primary and Secondary systems to accommodate electrical surges from the AC vital power source without loss of safety function in either system.

An analysis will be performed to identify any transients which could originate from within one of the reactor shutdown systems and be coupled through the AC vital distribution bus to the other shutdown system. If significant transients are identified by this analysis, then a test program will be defined to confirm the continued operation of the remaining reactor shutdown equipment connected to the same vital power source. A description of any such test program will be provided prior to the application for an Operating License.

September Items 4,7,8: I&C Design Criteria - Tech. Basis
November Item (13)

NRC Concern:

PSAR, page 7.1-3, clarify PPS primary/secondary separation requirements in terms of Reg. Guide 1.75 among redundant channels by primary and secondary systems and between primary and secondary systems.

Position:

Section 7.1.2.2 has been amended (attached) to clarify the application of Reg. Guide 1.75 in the design of the Reactor Shutdown Systems (RSS).

The RSS (Primary and Secondary) equipment and cables of safety divisions 1, 2 and 3 (channels A, B and C) are physically and electrically separated as per IEEE 384 and Reg. Guide 1.75, such that a common event within the defined area will not fail more than one channel of each RSS.

All RSS cables are run in conduits except in the reactor head access area where the cables are run in enclosed wireways. Separate conduits are used for primary RSS and secondary RSS cables.

Physical separation of primary and secondary RSS of the same division (channel) meets the requirements of IEEE 384 and Reg. Guide 1.75 in non-hazard areas (control room and cable spreading rooms). In other areas of the plant primary and secondary RSS equipment and cables of the same division may be located in the same hazard zone.

Most of the conduit runs of Primary and Secondary RSS of Division 3 (Channel C) are embedded in floors and walls and meet the separation requirements of IEEE 384 and Reg. Guide 1.75.

7.1.2.2 Independence of Redundant Safety Related Systems

To assure that independence of redundant safety related equipment is preserved, the following specific physical separation criteria are imposed for safety related instrumentation.

- All interrack PPS wiring shall be run in conduits (or equivalent) with wiring for redundant channels run in separate conduits. Only PPS wiring shall be included in these conduits. Primary RSS wiring shall not be run in the same conduit as secondary RSS wiring. Wiring for the CIS may be run in conduits containing either primary RSS wiring or conduits containing secondary shutdown system wiring, but never intermixed. Expanded criteria for physical separation of the CIS are given in Section 7.3.2.2.

- Wiring for other safety related systems may be run in conduits containing either primary RSS wiring or conduits containing secondary RSS wiring, but never intermixed, provided that no degradation of the separation between primary and secondary RSS results.

- Wiring for redundant channels shall be brought through separate containment penetrations with only PPS wiring brought through these penetrations. Primary RSS wiring shall not be brought through the same penetration as secondary RSS wiring. Wiring for the CIS and other safety related systems will be brought through the same penetration as the RSS wiring with which it is routed.

- Instrumentation equipment associated with redundant channels shall be mounted in separate racks (or completely, metallically enclosed compartments). Only PPS channel instrumentation shall be mounted in these racks. Primary RSS equipment shall not be located in the same rack as Secondary RSS equipment.

- ~~The physical separation between conduits, penetrations, or racks containing redundant instrument channels shall be specified on an individual case basis to meet the requirements of Regulatory Guide 1.75. This separation shall provide assurance that credible single events do not simultaneously degrade redundant channels or redundant shutdown systems.~~ INSERT "2"

- The wiring from a PPS buffered output which is used for a non-PPS purpose may be included in the same rack as PPS equipment. The PPS wiring shall be physically separated from the non-PPS wiring. The amount of separation shall meet the requirements of IEEE 384-1974.

- Electrical power for redundant PPS equipment shall be supplied from separate sources such that failure of a single power source

INSERT 2

The physical and electrical separation between DC and AC uninterruptible power supplies, conduits, equipment or racks of instrument channels of safety divisions 1, 2 and 3 shall meet the requirements of IEEE 384 and Reg. Guide 1.75. Redundant instrument channels in the primary RSS shall be physically separated from one another in accordance with the requirements of IEEE 384 and Reg. Guide 1.75. Redundant instrument channels in the secondary RSS shall be physically separated from one another in accordance with the requirements of IEEE 384 and Reg. Guide 1.75.

Physical separation of Primary and Secondary RSS of the same division (channel) shall meet the requirements of IEEE 384 and Reg. Guide 1.75 in non-hazard areas. In other areas of the plant primary and secondary RSS equipment and cables of the same division may be located in the same hazard zone.

Functional capability is maintained in the event of single design basis events which might impact more than one sensor by alternate protective functions as indicated in Table 7-2-2.

September Items 69,70; November Item (18)-- Start-up Trips

NRC Concern:

Provide a discussion of the diversity of the primary and secondary flux trips during start-up.

Resolution:

Additional information about the Start-up Flux trip subsystem has been added to section 7.2.

REPLACE WITH INSERT 7.2-10

Startup Nuclear

The Startup Nuclear Subsystem (Figure 7.2-8) obtains a wide range log channel measurement of nuclear power from the fission counters and compares it to a fixed-set point. If nuclear power is greater than the set point, a reactor trip is initiated. A permissive module is provided which allows manual bypass of this subsystem upon the verification of the operation of the wide range linear channel. This subsystem provides protection against positive reactivity disturbances occurring during startup.

Primary to Intermediate Flow Ratio

The Primary to Intermediate Flow Ratio subsystems (Figure 7.2-8) protect against an imbalance in the heat removal capability of the primary and intermediate loops. The heat removal capability of a particular loop is determined by measurement of the sodium flow within the loop. The Secondary RSS includes two of these subsystems, Primary Flow High and Primary Flow Low. In the Primary Flow High subsystem, the output of the high primary flow auctioneer is compared to the summation of the outputs from the low intermediate flow auctioneer and a signal proportional to the total primary flow. When the high primary flow auctioneer signal exceeds the low intermediate flow auctioneer signal by an amount proportional to the total primary flow, a reactor trip is initiated.

Similarly in the Primary Flow Low subsystem, a comparison is made between low primary flow and high intermediate flow. When the high intermediate flow auctioneer signal exceeds the low primary flow auctioneer signal by an amount proportional to the total primary flow, a reactor trip is initiated. These subsystems are manually bypassed during plant startup. The permissive signal used is based on reactor power. If reactor power is less than 10%, the subsystems can be manually bypassed.

Steam Drum Level

The Steam Drum Level Subsystems (Figure 7.2-9) measure steam drum water level and compare it to two individual fixed set points. A reactor tripp is initiated whenever the drum water level decreases below this fixed setpoint. There are three of these subsystems, one per HTS loop. Analysis of these subsystems are based upon worst case parameter values. For two loop operation, a manual bypass is instated under administrative control by changing the hardware configuation. Two loop bypasses are also under permissive control. Nuclear flux must be less than 10% of full power flux at the time of instating and the primary flow in the shutdown loop must be less than 15% of full flow or the two loop bypass is automatically removed.

HTS Pump Voltage

The HTS Pump Voltage Subsystem (Figure 7.2-9) provides protection for loss of pumping power for two or three HTS loops. Three undervoltage relays, one on each HTS pump bus, are used as redundant channels. If two of the three redundant channels are tripped, reactor trip ensues. A time delay is included to allow the plant to continue operation through momentary power outages.

3

INSERT 7.2-10

Startup Nuclear

The Startup Nuclear Subsystem (Figure 7.2-8) compares the output of wide range log mean square voltage measurements of nuclear power from the secondary fission chambers with a fixed setpoint. If nuclear power is greater than the setpoint, a reactor trip is initiated. This system provides protection against any positive reactivity disturbances, which may take place during startup. This trip function is located in the Secondary Shutdown System, as withdrawal of the Secondary Control Rods is interlocked so as to take place prior to criticality. The Secondary System therefore provides the major protection against reactivity transients during startup. Availability of this trip function prior to startup is ensured by the following design and procedural features. First, the Startup Nuclear Subsystem utilizes a wide range fission chamber, which provides a measurable output signal when the reactor is shutdown. Second, the wide range log counting electronics, the wide range mean square voltage electronics, and the wide range linear power electronics will be tested prior to startup to ensure calibrated and compatible signal outputs.

It should be noted that these features will also confirm the availability of other trip functions supplied from the secondary fission chambers; in particular, the modified positive flux rate subsystems and the flux to flow subsystems described previously.

A permissive module is provided, which allows manual bypass of the Startup Nuclear Subsystem. The permissive signal for this bypass is taken from the linear power electronics, also supplied from the secondary fission chambers.

The Startup Nuclear Subsystem also provides a means to confirm that the primary power range DC linear channels are functioning prior to reaching significant power levels. At approximately 5% reactor power, a check of the primary power range DC linear channels will be performed to ensure that they are on scale. Administrative procedures will prohibit bypassing of the Startup Nuclear subsystem if the primary power range DC linear channels are not functioning and indicating values consistent with the wide range linear power channels.

September Item 67
November ITEM (19), NRC QUESTION 421.15

NRC CONCERN

Reponse to Q421.15 needs to be expanded to cover manual initiation capability in safety-related systems utilizing microprocessors.

RESPONSE

The Solid State Programmable Logic System controls and actuates safety-related, Class 1E equipment. It contains the control logic, signal conditioners, isolation devices, and auxiliary circuits. The SSPLS can potentially use microprocessor based circuitry. The SSPLS will be qualified to IEEE 323, 344 and 383 as required for all Class 1E devices in order to preclude common mode failures. In addition, the SSPLS is comprised of three(3) separate and redundant safety related systems so that a failure in a system will not affect any component or device in the other system.

Also, all motor operated or pneumatically actuated valves controlled by the SSPLS can also be operated or actuated manually. Pumps, fans, and dampers, however, require the SSPLS in order to operate.

PSAR paragraph 8.3.1.1.2 describes the SSPLS.

Response to Q421.15 will be revised as attached, to include the above description.

Question CS421.15

Identify and document where microprocessors, multiplexers, or computer systems may be used in or interface with safety-related systems.

Response

Many microprocessors, multiplexers, and computers are used in CRBRP systems; however, in general, they are used in non-Class 1E applications. Whenever a microprocessor, multiplexer or computer acquires a Class 1E signal, that signal is isolated by a qualified Class 1E isolator before being utilized by a non-Class 1E system.

The two systems which use microprocessors, multiplexers or computers for Class 1E applications are the Solid State Programmable Logic System (SSPLS) and the Radiation Monitoring System. Information about these systems is provided below. The Plant Data Handling and Display System (PDH&DS) is the largest computer system used in the plant. Information about this system is also provided below.

The Radiation Monitoring System has Remote Processor Stations which are microporcessor based, radiation monitoring electronic and communication assemblies. PSAR Paragraph 11.4.2.1 describes the Remote Process Stations. The microprocessor receives raw count rate and process system data, and manipulates the data into the desired form. Data exchange and monitor control is via channel dedicated multiplexed signal paths. Non-Class 1E equipment can exercise control over a Class 1E radiation monitor. Any data extracted from the Class 1E monitors for use in non-Class 1E equipment is via Class 1E grade buffers.

The Solid State Programmable Logic System controls and actuates Safety-Related, Class 1E equipment. It contains the control logic, signal conditioners, isolation devices, and auxiliary circuits. The SSPLS can potentially use microprocessor based circuitry. PSAR Paragraph 8.3.1.1.2 describes the SSPLS.

INSERT 1

The CRBRP Plant Data Handling and Display System (PDH&DS) is a non-safety-related microprocessor based system that interfaces with safety-related systems and non-safety-related systems as well for the purpose of retrieving data for operator information. The system provides for information display and data handling, inoperable status monitoring of safety systems and emergency response facility data display. In all cases, Class 1E grade buffers are used for isolation between the PDH&DS and safety-related systems. The PDH&DS is described in PSAR paragraph 7.8.

INSERT 1

The SSPLS will be qualified to IEEE 323, 344 and 383 as required for all Class 1E devices in order to preclude common mode failures. In addition, the SSPLS is comprised of three (3) separate and redundant safety related systems so that a failure in a system will not affect any component or device in the other system. Also, all motor operated or pneumatically actuated valves controlled by the SSPLS can also be operated or actuated manually. Pumps, fans, and dampers, however, require the SSPLS in order to operate.