Department of Energy
Washington, D.C. 20545
Docket No. 50-537
HQ:S:82:118

NOV 03 1982

Mr. Paul S. Check, Director
CRBR Program Office
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Check:

INSTRUMENTATION (CHAPTER 7) WORKING MEETING, SEPTEMBER 21 and 22, 1982 - ADDITIONAL INFORMATION

Reference: Longenecker to Check, Subject: Meeting Summary for Instrumentation (Chapter 7) Working Meeting, September 21 and 22, 1982, dated September 24, 1982

Enclosed is the additional information requested during the subject meeting for which response dates of November 1, 1982, were projected. Marked up Preliminary Safety Analysis Report (PSAR) pages will be incorporated into a future PSAR revision. Also included are responses for items 46 and 51 which originally had December 1, 1982, commitments.

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.

Sincerely,

John R. Longenecker

John R. Longenecker
Acting Director, Office of the
Clinch River Breeder Reactor
Plant Project
Office of Nuclear Energy

Enclosures

cc: Service List
Standard Distribution
Licensing Distribution



D001

Enclosure

CHAPTER 7 SEPTEMBER 21 AND 22, 1982 WORKING MEETING, ACTION ITEMS DUE TO NRC NOVEMBER 1, 1982

| Item | |
|---|---|
| 4 | |
| 17 | |
| 18 | |
| 42 | |
| 56 | |
| 62 | |
| 89 | |
| 90 | |
| 91 | |
| 92 | |
| 96 | Partial response; full response will be provided by 12/1/82 |
| 46 | This item originally scheduled for submittal December 1, 1982 |
| 51 | This item originally scheduled for submittal December 1, 1982 |

Item 4: I&C Design Criteria - tech. basis

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

Resolution: 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).

Within general plant areas (non-hazard areas), the primary RSS instrument channels are physically separated from the secondary RSS channels to meet the requirements of Regulatory Guide 1.75.

Within hazard areas, redundant channels of the primary RSS and secondary RSS are physically separated such that a common event within the defined area will not fail more than one channel of each RSS. Within the hazard area, physical separation is maintained to meet Regulatory 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.

- INSERT → 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.

- 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

The physical separation between conduits, penetrations, or racks containing redundant instrument channels shall meet the requirements of Regulatory Guide 1.75. Redundant instrument channels in the primary RSS shall be physically separated from one another in accordance with the requirements of Regulatory Guide 1.75. Redundant instrument channels in the secondary RSS shall be physically separated from one another in accordance with the requirements of Regulatory Guide 1.75. Functional capability is maintained in the event of single design basis events which might impact more than one sensor by alternate protective functions as described in Table 7-2-2.

Item 17: RSS - single failure criterion for PPS and channel independence

Comments: Discuss isolation techniques between primary and secondary systems - add this to the PSAR. Particularly address commonality at the inverter.

Resolution: The Primary and Secondary Reactor Shutdown Systems are isolated from each other, from the power supply inverter through to the control rod drives, by means of physical separation as discussed in Item 4 previously.

A new Section 7.2.1.2.4 is added to the PSAR which discusses Power Supplies to the Reactor Shutdown Systems. This discussion includes analysis that justifies no loss of reliability of shutdown as a consequence.

o Tornado

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

o Local Fires

All PPS 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.

o Local Explosions and Missiles

All PPS 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.

o Earthquakes

All PPS 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 PPS equipment is designed to remain functional under OBE and SSE conditions. The characteristics of the OBE and SSE used for the evaluation of the PPS are found in Section 3.7.

INSERT 7.2.1.2.4 IP

7.2.2 Analysis

The Plant Protection 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.

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.

INSERT

7.2.1.2.4 Protection System Power Supplies

The Primary and Secondary Shutdown Systems are connected to the same three vital supply distribution buses, i.e., channel A in each system is supplied from the same distribution panel. This commonality between the two systems is not considered to impact their separation because of the following design features:

- Loss of one common distribution bus will result in the tripping of one logic train in each RSS system. This will provide the correct indication for appropriate corrective action without prejudicing safety.
- Provision of isolation devices in the individual power supplies within the two protection systems will prevent any failure caused by a circuit failure in one system from affecting the proper safety function of the other system.
- These same isolation features will prevent a common electrical interference surge received in the cabling between the distribution panel and the two systems from impacting either system.

From this analysis of these features and the satisfactory experience with a system of this type in an extended operation test program, it is concluded that no reduction in system reliability arises from use of common power supplies for the Primary and Secondary Shutdown Systems.

Item 18 -- RRS -- single failure criterion for power supply (PS) and channel independence.

Comment: Provide a description of test results or test plans to demonstrate that faults within a PS or a trip channel will not propagate in such a way as to compromise trip channels associated with more than one vital bus.

Resolution: Section 7.2.2 has been revised to describe features of the power supplies to the PPS which prevent propagation of faults to Primary and Secondary trip channels which share the same Uninterruptible Power Supply.

Single Failure

No single failure within the Plant Protection System nor removal from service of any component or channel will prevent protective action when required.

57 Two independent, diverse reactor shutdown systems are provided, either of which is capable of terminating all excursions without allowing plant parameters to exceed specified limits. Each system uses three redundant instrument channels and logic trains. The Primary RSS is configured
57 using local coincidence logic while the Secondary RSS uses general coincidence logic. To provide further assurance against potential degradation of protection due to credible single events, functional and/or equipment diversity are included in the hardware design.

"INSERT 1"

Bypasses

Bypasses for normal operation require manual instating. Bypasses will be automatically removed whenever the subsystem is needed to provide protection. The equipment used to provide this action is part of the PPS. Administrative procedures are used to assure correct use of bypasses for infrequent operations such as two loop operation. If the protective action of some part of the system has been bypassed or deliberately rendered inoperative, this fact will be continuously indicated in the control room.

Multiple Setpoints

Where it is necessary to change to a more restrictive setpoint to provide adequate protection for a particular normal mode of operation or set of operating conditions, the PPS design will provide automatic means of assuring that the more restrictive setpoint is used. Administrative procedures assure proper setpoints for infrequent operations.

For CRBRP, power operation on two-loops will be an infrequent occurrence, and will only be initiated from a shutdown condition. While the reactor is shutdown, the PPS equipment will be aligned for two-loop operation which will include set down of the appropriate trip points. Sufficient trip point set down is being designed into the PPS equipment to adequately cover the possible range (conceptually from 2% to 100%) of trip point adjustment required. In addition, administrative procedures (specifically the pre-critical checkoff) will be invoked during startup to ensure that the proper PPS trip points have been set.

The analysis of plant performance during two-loop operation has not been completed to date. Therefore, the exact trip point settings for two-loop operation cannot be specified at this time. However, the range of trip point settings indicated above is adequate to ensure that trip points appropriate for the anticipated lowest two-loop operating power can be achieved.

In summary, the design of the PPS equipment trip point adjustments and other features for two-loop operation coupled with the anticipated two-loop operating power level and administrative procedures assure full compliance with Branch Technical Position EICSB 12 and satisfy Section 4.15 of IEEE std 279-1971. 16

Insert 1

The DC and AC Uninterruptible Power Supplies (UPS) to the redundant instrument channels and logic trains are provided from three respective redundant power divisions. The three divisions are physically and electrically independent such that loss of any one division will not prevent the other divisions from performing their safety function. The design of power supply equipment (inverters and battery chargers), which use solid state components, is such that it precludes the possibility of a fault in one power division to have any adverse affect on similar power supply of the other two divisions.

The inverters will be tested to demonstrate that a transient on the inverter output will have no affect on the input power supplies. Testing will be performed in accordance with ISA and ANSI C37.90.

Item 42: QR 421.45

Comments: Amend QR 421.45 to clarify there are no safety related sensor lines exposed to outside temperatures - (water and steamlines).

Resolution: Amended response to Q 421.45 attached.

Question CS 421.45

Describe features of the CRBRP environmental control system which insure that instrumentation sensing and sampling lines for systems important to safety are protected from freezing during extremely cold weather. Discuss the use of environmental monitoring and alarm systems to prevent loss of, or damage to, systems important to safety upon failure of the environmental control system. Discuss electrical independence of the environmental control system circuits, and the monitoring/alarm circuits.

Response

All safety related process, instrument and sampling lines are contained entirely within environmentally controlled buildings. Thus, there are no safety related instrumentation sensing or sampling lines located external to the building or near building access openings from the external environment, such as doors and equipment hatches, which could freeze as a result of exposure to cold weather.

The Nuclear Island Heating, Ventilating and Air Conditioning (NI HVAC) System will maintain a minimum temperature of $55^{o}F$ in all areas of the NI buildings which contain safety-related equipment. All HVAC units utilizing outside air for ventilation will alarm when the temperature of the air, measured upstream of the cooling coil, is below a fixed set point. Electrical independence of the NI HVAC System is described in Chapters 7.1 and 7.6 of the PSAR.

Item 56: Q421.26

Comments: Amend to clarify which items are safety related and include rationale why non-safety related items are classified as such.

Resolution: Amended response to Q421.26 attached.

Question CS 421.26

In the PSAR, Section 7.4.1.1.2 discusses the Protected Air-Cooled Condenser (PACC) and how air flows through it is controlled by a combination of fan blade pitch and inlet louver position. The staff requires a detailed discussion of this instrumentation and in particular the method used for fan blade pitch indications.

Response

The outlet louvers have discrete open and closed position sensors. These provide indication at both the local control panel and main control panel in the control room.

The inlet louvers have both discrete open and closed position sensors and a continuous position sensor. The continuous position sensor provides feedback to the louver control. Both types provide indication at the local control panel and the main control panel in the control room.

The fan blade pitch ~~uses~~ is sensed by continuous position sensors for both control and indication. The indication is provided at the local control panel and the main control panel in the control room.

Both the discrete and continuous sensors are integral to the actuator. The discrete sensors are roller switches activated by a cam and the continuous is a potentiometer.

This instrumentation discussed above is Class 1E with the exception of the indicating lights.

Item 62: Discuss (other than RSS) Safety Related System Display Information

Comments: Provide a summary description of the alarms and indicators for the PPS and ESF's.

Resolution: Summary descriptions of alarms and indicators are provided in the PSAR:

| | |
|---|---|
| PPS | Section 7.2.2 (amended) |
| CIS | Section 7.3.2.2 (amended) |
| DHRS & EVS | Section 7.6.3.1.2 |
| SGAHRS | Section 7.4.1.1.9 |

DHRS alarms are provided as follows:

1. Pri. Na make-up pump A coolant flow low
2. Pri. Na make-up pump B coolant flow low
3. EVST NaK pump A coolant flow low
4. EVST NaK pump B coolant flow low
5. Pri. Na make-up pump A PWR or phase loss
6. Pri. Na make-up pump B PWR or phase loss
7. EVST NaK pump A PWR or phase loss
8. EVST NaK pump B PWR or phase loss
9. Sequencer A failure
10. Sequencer B failure
11. ABHX A interlocks tripped
12. ABHX B interlocks tripped

- Tornado

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

- Local Fires

All PPS 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 PPS 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 PPS 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 PPS equipment is designed to remain functional under OBE and SSE conditions. The characteristics of the OBE and SSE used for the evaluation of the PPS are found in Section 3.7.

INSERT -A

7.2.2 Analysis

The Plant Protection 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.

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.

- INSERT-A

Information Read-Out

Indicators and alarms are provided as an operating aid and to keep the plant operator informed of the status of the RSS. Except for the IHX primary outlet temperature analog indicators which are part of the accident monitoring system, all indicators and alarms are not safety related. The following items are located on the Main Control Panel for operator information:

Analog Indication

A. Secondary Wide Range Log MSV Power Level
B. Secondary Wide Range Linear Power Level
C. Primary Power Range Power Level
D. Reactor Vessel Level
E. HTS Pump Speeds
F. HTS Loop Flows
G. Reactor Inlet Pressure
H. IHX Primary Outlet Temperature
I. Evaporator Outlet Temperature
J. Steam Flows
K. Feedwater Flows
L. Steam Drum Level

Indicating Lights

A. Instrument Channel Bypass Permissive Status
B. Instrument Channel Bypass Status
C. Logic Train Trip/Reset Status
D. HTS Loop Trip/Reset Status
E. HTS Loop Test Status

Annunciators

A. Instrument Channel Trip/Reset information is provided for each function listed in Table 7.2-1.
B. Logic Train Power Supply Failure
~~C. Two Loop Bypasses Instated~~

Information is also available to the operator via the Plant Data Handling and Display System.

There are three categories of CIS cabling: cables between the radiation monitoring sensors and logic panels; cabling between the logic panels and the power breakers; and cabling from the breakers to the valve actuators.

Wiring for the three CIS instrument channels will be routed exclusively with the three Secondary PPS instrument channels.

CIS logic train actuation wiring will be routed through two separated and independent conduits. A conduit will contain only wiring from a single CIS logic train. No intermixing of CIS logic trains within a conduit will be permitted. CIS logic train 1 wiring will be routed from CIS logic panel 1 to CIS breaker 1. CIS logic train 2 wiring will be routed from CIS logic panel 2 to CIS breaker 2.

All of the inside containment isolation valve actuation wiring (both manual and automatic) will be routed through at least one separated and independent conduit from CIS breaker 1 through a separate and independent containment isolation valve actuation containment penetration. Inside containment isolation valve actuation wiring will be routed through separate and independent conduits from the inside of the containment isolation valve actuation containment penetration to the individual containment isolation valves. No other wiring will be routed through the conduit and containment penetration containing inside containment isolation valve actuation wiring.

All of the outside containment isolation valve actuation wiring (both manual and automatic) will be routed through at least one separated and independent conduit from CIS breaker 2 to the individual outside containment isolation valves. No other wiring will be routed through the conduit containing outside containment isolation valve actuation wiring.

—INSERT— B

- INSERT - B

Information Read-Out

Indicators and alarms are provided as an operating aid and to keep the plant operator informed of the CIS status. All indicators and alarms are not safety related. The following items are located on the Main Control Panel for operator information.

Analog Indication

A. Head Access Area Radioactivity
B. Containment Exhaust Radioactivity

Indicating Lights

A. CIS Breaker Trip/Reset Status
B. CIS Isolation Valve Position

Annunciators

A. Head Access Area High Radiation
B. Containment Exhaust High Radiation

Item 89: SGB Flood Protection System

Comments: Provide summary of I&C system functional design, redundancy, and safety classification of non-safety I&C.

Resolution: Amended Sections 7.6.5.3.1 and 7.6.5.3.2 provide discussion of the instrumentation and controls provided for the Steam Generator Building flooding protection, the safety function to be performed, and the consequent safety classification and design requirements for I&C equipment.

7.6.5.3.1 Instrumentation

Instrumentation provided for this subsystem consists of Class 1E temperature, and moisture transducers. In addition, non-Class 1E level transducers are provided. The transducers and associated control logic are located in the SGB cells containing main feedwater or recirculation piping. Three independent moisture and temperature measurements in each cell are utilized for identifying a major water/steam line rupture. Water level measurements in each cell confirm a flooding condition and are annunciated in the main control room.

7.6.5.3.2 Controls

Each heat removal loop isolates the main feedwater supply upon detection of a major pipe rupture. The start-up and main feedwater control valves close upon activation by a two-out-of-three logic using measurements of moisture and temperature in each cell. The main feedwater isolation valve is independently closed upon activation by a two-out-of-three logic using the same three moisture and temperature measurements from each cell. Separation and isolation is maintained between the control valve and isolation valve activation logic.

Small water/steam leaks are identified in each SGB cell by measuring water level. Manual corrective control of flooding is initiated by the operator upon annunciation in the main control room. 45

Replace with insert A'



(Amend. 45 July 1978)

Insert A'

7.6.5.3.1 Instrumentation

The SGB flooding protection instrumentation consist of temperature, moisture and water level instrument channels. The temperature and moisture instrument channels are class 1E and the level channel is non-class 1E.

For each cell in the SGB which contains steam and water piping three independent and redundant temperature and moisture instrumentation channels are provided. These signals are buffered and provided to two independent logic trains.

In addition, two water level instrumentation channels are provided in each cell.

7.6.5.3.2 Controls

The flooding protection subsystem has a safety function and a non-safety function. The safety function is to detect a major pipe rupture and to isolate the feed water supply system and the affected loop. The non-safety function is to detect a small leak and annunciate in the main control room.

Upon detection of a major pipe rupture the startup and main feedwater control valves and the feedwater isolation valves are closed by two independent and separate class 1E logic trains. One logic train closes the startup and main feedwater control valves, the other the feedwater isolation valve.

Actuation of each logic train requires concurrent two-out-of-three signals from both temperature and moisture from the same cell of any one of the four cells in each heat transport loop.

Small leaks are detected in each cell by measuring water level and by alarms on water level, temperature and moisture. Operator action is initiated upon annunciation in the main control room.

Item 90: Inert Gas Blanketing System

Comments: Provide summary of I&C system functional design, redundancy and rationale for safety classification of I&C.

Resolution: PSAR Section 7.7.1.10 identifies those I&C systems that do not perform a safety related function and whose failure would not cause the failure of a safety related system to perform its safety related function. Included is the Inert Gas Receiving and Processing System (IGRP), which is further discussed in Section 9.5. Section 9.5.5 discusses Instrumentation requirements for the IGRP, none of which identify a safety related function for it.

Accordingly, the IGRP I&C system is not discussed in Section 7.6 which discusses I&C Systems required for safety.

Item 91: Auxiliary Liquid Metal System

Comments: Provide summary of I&C system functional design, redundancy and rationale for safety classification of I&C.

Resolution: PSAR Section 7.7.1.10 identifies those I&C systems that do not perform a safety related function and whose failure would not cause the failure of a safety related system to perform its safety related function. Included are portions of the Auxiliary Liquid Metal System. Other portions of this System are used by the Direct Heat Removal Service and the Spent Fuel Storage System which perform safety-related functions; instrumentation and controls for these portions of the Auxiliary Liquid Metal System are classified as safety related and are accordingly designed to requirements for safety related systems. The safety related portions of the instrumentation and controls for the Auxiliary Metal System are discussed in the amended Section 7.6.3 "Direct Heat Removal Service (DHRS) and Ex-Vessel Storage Tank (EVST) Cooling System Instrumentation and Control."

23

component movement prior to initiation. The type of core component is checked for compatibility with the intended destination. The destination for the core component is checked for occupancy and readiness to receive a particular core component. Core components can be identified by the IVTM to verify the type of core component prior to any movement into the reactor core or removal from the Reactor Vessel. The Central Computer monitors the operation of the other refueling machines and incorporates a software operational alarm system to add further depth to the design for operation without errors. The use of setpoint generation rather than direct digital control permits the IVTM and EVTM computer commands to be passed through a permissive hard-wired interlock system only if proper preconditions are met. In addition, the Central Computer monitors annunciator status and alarm failures. An alarm log can be displayed at all local computer CRT terminals.

Finally, a complete manual control capability is provided which also must work through the refueling interlock logic.

The analysis of the consequences of specific fuel handling events given in Section 15.5 has not identified a requirement for any specific safety interlocks.

Some interlocks are included in the design to preclude the possibility of major machine damage.

Typical interlocks are given below and in Table 7.7-1.

IVTM grapple/fuel element
EVTM grapple/fuel element
Rotating Plug drive system/IVTM grapple position
Rotating plug drive system/IVTM hold down sleeve
Rotating plug drive system/EVTM position
EVST drive motors/EVTM grapple position

Postulated Reactor Refueling System (RRS) accidents with potentially severe consequences were analyzed in detail to determine requirements for safety interlocks. The techniques employed included safety assurance diagrams, fault trees, mechanical and thermal analyses, and radiological release calculations. None of the analysis results showed off-site doses exceeding those presented in Section 15.5 or 15.7. The off-site doses in Section 15.5 and 15.7 resulting from postulated RRS accidents are all well below the 10 CFR 100 guideline exposures without taking credit for interlocks. It was therefore concluded that the RRS interlocks should not be designated as safety interlocks. 59

7.7.1.10 Nuclear Island Auxiliary Instrumentation and Control Systems

A number of Instrumentation and Control Systems, not discussed in Section 7.0, are provided in the plant to support various auxiliary systems. These systems do not perform a safety-related function, nor would their failure prevent the functioning of a safety-related system. These instrumentation systems, discussed in other sections of this report are:

| System | Section |
|---|---|
| Recirculating Gas | 3.A.1, 3.A.2 |
| Auxiliary Cooling Fluid | 9.7.5 |
| Inert Gas Receiving and Processing | 9.5 |
| Impurity Monitoring and Analysis | 9.8.5 |

7.7.1.11 Balance of Plant Instrumentation and Control Systems

A number of Instrumentation and Control Systems are provided to support various Balance of Plant Systems. These systems do not perform a safety-related function, nor would their failure prevent the functioning of safety-related systems.

7.7.1.11.1 Treated Water Instrumentation and Control System

The Treated Water System includes the Portable Water System, the Normal Plant Service Water System, the Secondary Service Closed Cooling Water System, The Emergency Plan Service Water System, the Normal and Emergency Plant Chilled Water Systems, and the Makeup Water Treatment System.

Auxiliary Liquid Metal

(This includes only those portions of the Auxiliary Liquid Metal System that are not associated with the Direct Heat Removal Service (DHRS) or the Spent Fuel Storage System (ex-vessel storage). The DHRS and the Spent Fuel Storage System are required for safety and their associated instrumentation and controls are discussed in Sections 7.6.3, 9.1.3 and 9.3.3).

and Ex-Vessel Storage Tank (EVST) Cooling System

7.6.3 Direct Heat Removal Service (DHRS) Instrumentation and Control System

7.6.3.1 Design Description

7.6.3.1.1 Function

The DHRS (fluid system and mechanical components as described in Section 5.6, and electrical components as described below) provides a supplementary means of removing long term decay heat from the reactor for the remote case in which none of the steam generator decay heat removal paths are available.

(– INSERT –)

The DHRS and EVST Cooling System instrumentation and controls are safety related and are provided to permit the monitoring of system conditions and to provide alarm indication of off-normal conditions. These are the same instrumentation and controls that are provided for EVST cooling (Section 9.1.3.1.5) and the reactor primary sodium overflow circuits (Section 9.3.2.5) with the addition of a few temperature monitoring instruments located on the NaK lines connecting the overflow heat exchanger with the EVST NaK cooling loops (see Figures 9.3-2 and 9.3-3).

7.6.3.1.2 Design Criteria

Design criteria that are applicable to DHRS and EVST Cooling System electrical equipment are as follows:

A. No single failure of an instrument, interconnecting cable or panel shall prevent a key process variable from being monitored.

B. DHRS valves shall be remotely operated and DHRS electrical equipment shall be controlled (see 5.6.2) from a panel in the Control Room to provide 1/2 hour start up capability.

C. Physical and electrical separation of redundant portions of DHRS (EVS cooling system, primary makeup pumps, instrumentation, and controls) shall be provided.

D. Electrical power supplied to electrical equipment shall be independent of off-site power.

E. Control instrumentation and electrical equipment shall function during and after an SSE.

F. Capability for periodic calibration and testing of electrical equipment shall be provided.

DHRS is separate in function and equipment location from the Steam Generator Auxiliary Heat Removal System (SGAHRS), and there is no common sharing of instrumentation or controls between them.

INSERT - C

The EVS Cooling System (described in Section 9.1.3) removes decay heat from fuel stored in the Ex-vessel Storage Tank. The redundant liquid metal cooling circuits using forced convection heat rejection and one liquid metal cooling circuit using natural draft heat rejection provide this function.

7.6.3.1.3 Equipment Design

As shown on Figure 5.1-1, the DHRS is part of the primary sodium processing, and the EVS Sodium Processing System. Description of the functioning of these systems for reactor decay heat removal is provided in Sections 9.1.3 and 9.3.2. The P&I diagrams are given in Figures 9.3-2 and 9.3-3.

DHRS electrical equipment and EVST cooling system meets the design criteria listed in Section 7.6.3.1.2 above in the following manner:

A. Control Systems

The following DHRS control functions and EVST cooling system are provided from separate, redundant control panels (local and main control room):

(1) Remote manual control of voltage to all NaK and sodium pumps.

(2) Remote manual control of ABHX dampers and fan speed.

(3) Remote manual override of pump and ABHX interlock circuits.

(4) Remote manual control of all valves required to provide DHRS and EVST cooling

B. Monitoring Instrumentation

Some instrumentation required to monitor the functional performance of the decay heat removal process loops is redundant from the sensor out to and including the readout panel, so that a single failure of an instrument, interconnecting cable or panel does not prevent the process loop from being monitored. In those cases where a redundant sensor is not provided, separate indicators on separate panels are provided. Where redundant sensors are not provided, loss of the sensor does not prevent the acquisition of equivalent diagnostic information from other sensors on the process loop.

The following EVST cooling and DHRS process variables are monitored with completely redundant instrumentation (sensors, cabling and panels):

*(1) EVST outlet sodium temperatures

* Required for post accident monitoring.

The EVST cooling system is described in Section 9.1.3 and the P&I diagram for the system is given in Figure 9.3-3.

The flow in the primary sodium overflow makeup loop and EVST NaK loops, and the EVST airblast heat exchanger fan speed is set at maximum design rates.

The only interlocks remaining active in DHRS during this mode of operation are those associated with protection of the NaK and sodium pumps against high temperature in the pump stators. Manual override of this interlock can also be performed with the knowledge that pump damage and early failure could result.

7.6.3.2 Design Analysis

When DHRS is activated, all automatic controls are bypassed, the pumps and valves are remotely set to provide maximum flow through the DHRS loops, and the airblast heat exchangers are remotely set to provide maximum cooling capability. Control of the pumps and the airblast heat exchanger is provided from three separate locations: a field panel adjacent to or in a cell adjacent to the equipment, a local panel in same building as the equipment, and the control panel in the main Control Room. The capability to provide power directly to the pumps, by bypassing all panel voltage and interlock control functions, is also provided so that no control function failure can keep DHRS electrical equipment from operating.

The EVST cooling system is normally controlled from a local panel located in the Reactor Service Building. In the event of the loss of this local control, the EVST cooling system equipment control is transferred to the Auxiliary Liquid Metal System panel located in the Main Control Room. All electrical equipment required for the functioning of the systems is classified as safety related and is qualified to IE requirements, and is provided with Class IE power supply, backed up by diesel generators to provide power during off-normal conditions.

Item 92: Sodium Purification System

Comments: Provide summary of I&C system functional design, redundance and rationale for safety classification of I&C.

Resolution: PSAR Section 7.7.1.10 identifies those I&C systems that do not perform a safety related function and whose failure would not cause the failure of a safety related system to perform its safety related function. Included is the Impurity Monitoring and Analysis System which is further discussed in Section 9.8. Section 9.8.5 discusses the Instrumentation Requirements for the Impurity Monitoring and Analysis System none of which identify a safety related function for it. Accordingly, the Impurity Monitoring and Analysis System is not discussed in Section 7.6 which discusses I&C Systems required for safety.

Item 96: Q421.19 (Control System Failures)

Comments: Obtain copy of Westinghouse response to this concern on SNUPPS. Amend response.

Resolution: The response provided by SNUPPS to this concern was reviewed. An amended CRBRP response (attached) includes an evaluation of the effects of control system failures, similar to that provided by SNUPPS. This evaluation demonstrates that design criteria applied to the Plant Protection System and the Plant Control System adequately ensure their capability to maintain the plant in a safe condition, including events where one or more control systems sustain failures or malfunctions.

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

~~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:~~

—REPLACE WITH INSERT—D



~~Amend. 69 July 1982~~

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.

INSERT - ▷

Response

The design criteria for the Plant Protection System require that 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 sensory 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 sensory instrument
2) loss of a single sensory 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) Steam Drum Level Control
E) Turbine Control

Analysis of such events have been conducted for typical control systems, i.e., A) thru part of C) above. PHTS Sodium Flow was included since the IHTS analysis gives similar but less severe results. 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 analysis 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.

## Loss of Any Single Instrument

Median select circuits are used by the control systems itemized above to provide the median of three sensors as the control feedback signal. Failure of one sensor, therefore, will not result in loss of control. The analysis in this section goes beyond a sensor failure 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 listed above 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.

## Loss of Power to a Protection Separation Group

This section analyzes the effects on the control systems caused by the loss of an inverter powering a protection channel. If the bus to protection channel A, B or C fails low, then the following PPS buffered signals used by the control systems will drop to zero: Channel A, B or C corresponding to failed bus for reactor flux, primary sodium flow, and superheater steam 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.

## Loss of Power to Control Systems

This section examines the effects on the control systems caused by loss of the power bus feeding the control systems. The supervisory, reactor and primary sodium flow control systems are powered from Non 1E System B Bus 12NIFB025B, and loss of this bus will affect all three systems. The primary rod controller is powered from Non 1E UPS System A Bus 12NJB301A. Table 2 provides the effects on these systems and on the plant upon loss of these buses.

Loss of Power to Control Systems (cont'd)

The table shows that loss of the control function results; however, no plant disturbance results and no reactor scram occurs.

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 1.

Conclusions

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

Table 1. Loss of Any Controller Feedback Signal

| Feedback Signal | System | Assumed Failure Direction | Effect | Bounding Event |
|---|---|---|---|---|
| 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 over time. Hence, bounding event is Spurious Primary Pump Trip (PSAR 15.3.1.2). |
| 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. |

Table 1 (cont'd):

| Feedback Signal | System | Assumed Failure Direction | Effect | Bounding Event |
|---|---|---|---|---|
| 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. |
| 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). |

Table 1 (cont'd):

| Feedback Signal | System | Assumed Failure Direction | Effect | Bounding Event |
|---|---|---|---|---|
| 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). |

Table 2. Loss of Power to Control Systems

| System | Effect on System | Effect on Plant | Bounding Event |
|---|---|---|---|
| Primary Flow Control | Loss of primary flow control function. Controller output (pump speed demand) drops to zero. Speed controller transfers to manual maintaining pump speed constant upon sudden drop in setpoint. | No plant disturbance. | Not applicable. |
| Reactor Control | Loss of reactor control function (core exit temperature and flux control). Rod rate signal drops to zero and direction signals in open contact state indicating no rod movement. | No plant disturbance. | Not applicable. |
| | Rod block signal in open contact state indicating rod block. | Rods blocked. | |
| Primary Rod Control | For loss of 120 VAC bus, rod control function (Group Rod or Single Rod Control) is lost. All primary rod position display information is lost. Movement of rods is inhibited. | No plant disturbance. Rod position indication lost. Rods stationary. | Not applicable. |
| | For loss of 480 VAC bus, no loss of control if other MG Set is running. | No effect on plant if redundant MG Set is running; otherwise plant scram. | |
| Supervisory Control | Loss of supervisory control function. Turbine load increase/decrease signals in open contact state indicating no change in turbine load. Bypass control logic signal in pressure mode. | No plant disturbance. NSSS under control as discussed above. Steam dump under pressure control. Turbine load constant. | Not applicable. |

Item 46: Address relationship of PHTS, IHTS and SGS with SHRS

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

Resolution: A discussion of DHRS instrumentation and controls including design criteria is provided in amended Section 7.6.3. There it is stated that DHRS and SGAHRS do not share or have any common instrumentation or controls, including sensors, control circuits, or control panels. Also, it is stated that the control and instrumentation for DHRS is classified as safety related. Accordingly the controls and instrumentation have been designed to 1E Safety Related requirements.

Item 51: DHRS Instrumentation

Comments: Determine if there are any interlocks which are process dependent and are used to place the Direct Heat Removal Service into service.

Resolution: The Direct Heat Removal Service (DHRS) is as described in PSAR Section 5.6.2.3.9. Sections 5.6.9.1 and 9.3 provide design, component, and operational aspects of the DHRS and 7.6.3 discusses DHRS instrumentation. No interlocks, which are process dependent and which would be required for puting DHRS into service, and no inhibit logic which would prevent DHRS from starting up on operating, are provided.