NORTHEAST UTILITIES

THE CONNECTICUT LIGHT AND POWER COMPANY
WESTERN MASSACHUSETTS ELECTRIC COMPANY
HOLYOKE WATER POWER COMPANY
NORTHEAST UTILITIES SERVICE COMPANY
NORTHEAST NUCLEAR ENERGY COMPANY

General Offices • Selden Street, Berlin, Connecticut

P.O. BOX 270
HARTFORD, CONNECTICUT 06141-0270
(203) 666-6911

April 2, 1984

Docket No. 50-423
B11091

Director of Nuclear Reactor Regulation
Mr. B. J. Youngblood, Chief
Licensing Branch No. 1
Division of Licensing
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Reference: (1) B. J. Youngblood to W. G. Counsil, Draft SER for Millstone Nuclear Power Station, Unit 3, dated December 20, 1983.

Dear Mr. Youngblood:

Millstone Nuclear Power Station, Unit 3
NRC - Instrumentation and Control Systems Branch (ICSB)
Review Meeting, March 13, 1984

A meeting was held between the NRC ICSB and Northeast Nuclear Energy Company (NNECO) in Bethesda, Maryland on March 13, 1984 to discuss nineteen (19) Draft SER open items contained in Reference (1). During the meeting each of the nineteen items was discussed. A status of each open item was noted as defined by one of the following three categories:

Closed - No further NNECO input or action is needed to resolve the NRC concern.

Confirmatory - NNECO must provide the requested information on the Millstone 3 docket, either by a letter or FSAR amendment.

Open - No resolution possible at this time, NNECO to address.

Attachment I provides the status of those Draft SER Open Items. It was agreed that NNECO will transmit a letter to the NRC providing a written response on each of those Draft SER open items by April 4, 1984. NNECO also agreed to provide all additional information as committed to in confirmatory items as the information becomes available. The attached responses to the open items (Attachment II) formalize the above commitment given orally at the meeting. The responses will be incorporated into the FSAR in a future amendment.

B001
1/35

If you have any concerns related to the information contained herein or any questions related to our responses, please contact our Licensing representative directly.

Very truly yours,

NORTHEAST NUCLEAR ENERGY COMPANY ET AL

By Northeast Nuclear Energy Company, their Agent

W. G. Counsil

W. G. Counsil
Senior Vice President

STATE OF CONNECTICUT)
) ss. Berlin
COUNTY OF HARTFORD)

Then personally appeared before me W. G. Counsil, who being duly sworn, did state that he is Senior Vice President of Northeast Nuclear Energy Company, Applicant herein, that he is authorized to execute and file the foregoing information in the name and on behalf of the Applicants herein and that the statements contained in said information are true and correct to the best of his knowledge and belief.

Lorraine J. D'Amico

Notary Public

My Commission Expires March 31, 1988

ATTACHMENT I

Status of the NRC-ICSB Draft SER Open Items
Discussed at the Meeting with the NRC-ICSB March 13, 1984

Item No.	Description	Status
ICSB-1	Design Modification for Automatic Reactor Trip using Shunt Trip Coil Attachment.	Open
ICSB-2	Conformance with Branch Technical Position ICSB-26	Closed
ICSB-4	Containment Isolation for the Main Steam Lines to the Turbine of the AFW Pump.	Closed
ICSB-5	Letdown Line Relief Valve	Closed
ICSB-6	Non-Class 1E Control Signals to Class 1E Control Circuits	Open
ICSB-8 and 23	Feedwater Isolation and Control Valves	Closed
ICSB-9	BOP Instrumentation and Control System Testing Capability	Confirmatory
ICSB-10	Remote Shutdown Capability	Closed
ICSB-11	IE Bulletin 79-27 Concerns	Confirmatory
ICSB-12	Bypass and Inoperable Status Panel	Closed
ICSB-13	NUREG-0737 Item II.F.1 Accident Monitoring Instrumentation Position (4), (5), and (6).	Closed
ICSB-16	RHR System Isolation Valve Interlocks	Closed
ICSB-17	Isolation of Low-pressure Systems from the High Pressure	Closed
ICSB-18	RCS Over-pressure Protection	Closed
ICSB-19	Reactor Coolant System Loop Isolation Valve Interlocks	Open
ICSB-21	Control System Failure caused by High-energy Line Breaks.	Open

Item No.	Description	Status
ICSB-22	Freeze Protection for Instrument Sensing Lines.	Closed
ICSB-24	Hydrogen Recombiner System	Closed

Summary - Closed - 13
Confirmatory - 2
Open - 4

ATTACHMENT II

Responses to the DRAFT SER Open Items

Item No.

ICSB-1
ICSB-2
ICSB-4
ICSB-5
ICSB-6
ICSB-8 and 23
ICSB-9
ICSB-10
ICSB-11
ICSB-12
ICSB-13
ICSB-16
ICSB-17
ICSB-18
ICSB-19
ICSB-21
ICSB-22
ICSB-24

Open Items

Instrumentation and Control Systems Branch

ICSB-1 Design Modification for Automatic Reactor Trip Using Shunt Coil Trip Attachment (Draft SER Section 7.2.2.4)

The Westinghouse Owners Group (WOG) has submitted a generic design modification to provide automatic reactor trip system (RTS) actuation of the breaker shunt trip attachments in response to Salem ATWS events. The staff has reviewed and accepted the generic design modification and has identified additional information required on a plant specific basis. The applicant has not however, provided a response to Generic Letter 83-28 which established the requirements for this modification. The resolution of this matter will be addressed in a supplement to this report. This is an open item.

Response (3/84)

On August 10, 1983, the NRC issued the Final Safety Evaluation Report (SER) on the Westinghouse Owners' Group (WOG) generic design modification to provide automatic reactor trip system actuation of the breaker shunt trip attachments. The SER endorsed the generic design, but listed thirteen items that must be addressed on a utility-specific basis prior to implementation of the shunt trip modification. The generic design has been evaluated to determine the applicability to Millstone 3 plant. The WOG generic modification for the automatic shunt trip actuation of the reactor trip system breakers will be incorporated to Millstone 3 design. The NRC Staff requested that NNECO to provide the specific information package to close this item.

Status (3/84)

Open.

Open Items

Instrumentation and Control Systems Branch

ICSB-2 Conformance With Branch Technical Position ICSB-26 (Draft SER Section 7.2.2.7)

Branch Technical Position ICSB-26, "Requirements for reactor protection system anticipatory trip", applies to the entire reactor protection system (RPS) from the sensors to the final actuated device. For sensors located in nonseismic areas the installation (including circuit routing) and design should be such that the effects of credible faults (i.e., grounding, shorting, application of high voltage, or electromagnetic interference) or failures in these areas could not be propagated back to the RPS and degrade the RPS performance or reliability. There are three groups of RPS related cables which are routed in the turbine building:

1. Turbine trip cause reactor trip input cables
2. Reactor trip to trip the turbine output cables
3. Turbine first stage pressure input to RPS interlock circuits.

The staff requested the applicant to demonstrate that his design is in conformance with BTP ICSB-26 or that exceptions are suitably justified. This is an open item.

Response (3/84)

A discussion of the reactor trip on turbine trip and the turbine trip on reactor trip was provided at the ICSB meeting. Included in the discussion was a description of the routing and separation for these trip circuits including the routing within the turbine building (a non-seismic structure). Layout drawings showing the rating and separation for the following three groups of RPS related cables which are routed in the turbine building were provided:

1. Reactor trip on turbine trip (input cables).

2. Turbine trip on reactor trip (output cables).

3. Turbine first stange pressure input to RPS interlock circuits.

FSAR Section 7.2 will be revised to indicate the conformance with the BTP ICSB-26.

Status (3/84)

Closed.

Open Items

Instrumentation and Control Systems Branch

ICSB-4 Containment Isolation For the Main Steam Lines to the Turbine of the AFW Pump (Draft SER Section 7.3.3.6

General Design Criteria 57 requires that each line that penetrates primary reactor containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall have at least one containment isolation valve which shall be either automatic, or locked closed, or capable of remote manual operation. The main steam lines to the turbine of the AFW pump have a motor operated check stop valve in parallel with an air-operated bypass valve, both of which are remote manually operated. The staff is concerned that the bypass valves (AOV84A, B, & D) are not supplied power from a Class 1E power source. Therefore, isolation of the bypass valves cannot be assured. This is an open item.

Response (3/84)

The 1/4 - inch bypass line and bypass valves (AOV 64 A, B, D) around the stop check valves will be eliminated. Pre-warming the three-inch turbine steam supply piping during scheduled (monthly) pump/turbine testing is not required. FSAR Section 6.2•4 will be revised to state that a class 1E power source is supplied to containment isolation valves (where applicable) to assure proper isolation of these valves.

Status (3/84)

Closed.

Open Items

Instrumentation and Control Systems Branch

ICSB-5 Letdown Line Relief Valve (Draft SER Section 7.3.3.7)

The staff raised a concern that the relief valve located on the letdown line would relieve primary coolant to the reactor drain tank in the event the isolation valve inside containment did not close on a containment isolation signal or if the outside containment isolation valve failed closed. The applicant has not responded to this concern. This is an open item.

Response (3/84)

The failure of inside containment isolation valve 3CHS*CV8160 to close upon demand of a safety signal presupposes a single random failure which may result in reactor coolant discharging to the pressurizer relief tank (PRT) via relief valve 3CHS*RV8117. Such discharge would be dependent upon the upstream isolation valves failing to close (3RCS*LCB459 and 460, and 3CHS*SV8149A, B and C and 3CHS*CV8160). Containment isolation is accomplished by the automatic closure of outside containment isolation valve 3CHS*CV8152 which receives the same safety signal as 3CHS*CV8160.

The upstream isolation valves close automatically upon pressurizer low level (level transmitters 3RCS*LT459, 460 and 461). Additionally, as the valves are air-operated, fail closed, the letdown line would be isolated upon loss of instrument air.

In the very unlikely event that the upstream letdown isolation valves should not be isolated, however, the letdown flow rate via the relief valve to the PRT would be limited by the letdown orifices, and would not exceed the normal letdown flow rate. Following closure of isolation valve 3CHS*CV8152, the pressure in the letdown line upstream of valve 3CHS*CV8152 would increase to that of the relief valve setpoint (600 psi nominal). This increase in pressure results in decreased letdown flow. This assumes no corresponding increase in RCS pressure. Should the initiating event result in increased RCS pressure, say, to the pressurizer safety valve setpoint, the inlet pressure to the orifice(s) would increase. In any event, the combined effect of increasing the pressure upstream and downstream of the orifice(s) would result in a letdown flow rate only approaching that of the normal letdown flow rate.

Flow into the Pressurizer Relief Tank via relief valve 3CHS*RV81 can be detected by:

(a) High temperature alarm from TI-125 located in the relief valve discharger piping.

(b) Tank level indicator LI-470 and high alarm.

(c) Tank temperature indicator TI-468 and high alarm.

The loss of coolant through the unisolated, letdown line does not affect the reactor coolant system heat removal capability, nor would it significantly affect

the amount of coolant within the system (even if safety injection had not been initiated). Consequently, core integrity is maintained and 10CFR50, Appendix K limits are not exceeded. The radiological effects external to the containment for letdown routed to the PRT would be trivial and bounded by effects analyzed for a break in the letdown line outside containment. The radiological effects external to the containment have been calculated for letdown spilling outside the containment (see Section 15.6.2). The analyses show that for 30 minutes of unisolated letdown flow, the resulting doses are only a small fraction of 10CFR100 limits.

Status (3/84)

Closed.

Open Items

Instrumentation and Control Systems Branch

ICSB-6 Non-Class IE Control Signals to
Class IE Control Circuits (Draft SER Section 7.3.3.11)

The staff requested the applicant to provide a list of non-Class IE control signals that are used as inputs to Class IE control circuits and justification that these non-Class IE signals are either bypassed by the ESF actuation signal, or that the non-Class IE signal can only act to the safe direction and therefore would not degrade safety systems. This is an open item.

Response (3/84)

The justification of the use of non-class 1E signals as input to class 1E control circuits will be provided at a later date.

Status (3/84)

Open.

Open Items

Instrumentation and Control Systems Branch

ICSB-8 Feedwater Isolation and Control Valves (Draft SER Section 7.3.3.13)

The staff requested detailed schematic drawings for feedwater isolation valves and feedwater control valves. The applicant stated that detailed drawings will not be available until March 1984. This is an open item.

Response (3/84)

A discussion of the feedwater isolation valves and feedwater control valves was provided using schematics during the ICSB meeting.

Status (3/84)

Closed.

Open Items

Instrumentation and Control Systems Branch

ICSB-9 BOP Instrumentation and Control System Testing Capability (Draft SER Section 7.3.3.15)

The FSAR Sections 7.2.2.2.3 and 7.3.2.2.5 describe the capability for testing the reactor trip system and the engineered safety feature system. Most of the descriptions are based on NSSS scope of supply equipment. It is not clear whether all the BOP instrumentation and control systems satisfy the same criteria. The staff cited an example on the refueling water storage tank (RWST) level measurement which is a BOP design. The low-low loop signal from one-out-of-two level switches will automatically stop the residual heat removal pump. The empty tank signal from one-out-of-two level switches will automatically stop the quench spray pumps. The testing of these actuation logic circuits are not discussed in the FSAR and they are not tested by the same method as NSSS ESF instrument systems. The staff requested that the applicant performs a thorough evaluation on the BOP safety related instrumentation and control systems with respect to testing capabilities, identify any instrument channels which cannot be tested as described in Sections 7.2.2.2.3 and 7.3.2.2.5, and to justify that the design is in conformance with the testing requirements of GDC-21. This is an open item.

Response (3/84)

See revised FSAR Section 7.3

Status (3/84)

Confirmatory.

7.3 ENGINEERED SAFETY FEATURES SYSTEM

In addition to the requirements for a reactor trip for anticipated abnormal transients, the facility is provided with adequate instrumentation and controls to sense accident situations and initiate the operation of necessary engineered safety features. The occurrence of a limiting fault, such as a loss-of-coolant accident or a steam line break, requires a reactor trip plus actuation of one or more of the engineered safety features in order to prevent or mitigate damage to the core and reactor coolant system component and ensure containment integrity.

In order to accomplish these design objectives, the engineered safety features system has proper and timely initiating signals which are to be supplied by the sensors, transmitters, and logic components making up the various instrumentation channels of the engineered safety features actuation system.

7.3.1 Description

The engineered safety features actuation system (ESFAS) uses selected plant parameters, determines whether or not predetermined safety limits are being exceeded and, if they are, combines the signals into logic matrices sensitive to combinations indicative of primary or secondary system boundary ruptures (Class III or IV faults). Once the required logic combination is completed, the system sends actuation signals to the appropriate engineered safety features components. The ESFAS meets the requirements of Criteria 13, 20, 27, 28, and 38 of the 1971 General Design Criteria (GDC).

7.3.1.1 System Description

The ESFAS is a functionally defined system described in this section. The equipment which provides the actuation functions identified in Section 7.3.1.1.1 is listed and discussed in this section (WCAP-7013, 1973; WCAP-7488-L, 1971; WCAP-7705, 1976):

1. Process Instrumentation and Control System (WCAP-7013, 1973).

2. Solid State Logic Protection System (WCAP-7488-L, 1971).

3. Engineered Safety Features Test Cabinet (WCAP-7705, 1976).

4. Manual Actuation Circuits.

5. Emergency Generator Load Sequence Control Logic Description 24-9.4 (NUSCo., 25212-28723) (Section 1.7 - Logic Diagram Package).

The ESFAS consists of two discrete portions of circuitry: (1) an analog portion consisting of three to four redundant channels per parameter or variable to monitor various plant parameters such as the reactor coolant system and steam system pressures, temperatures and

flows and containment pressures; and (2) a digital portion consisting of two redundant logic trains which receive inputs from the analog protection channels and perform the logic needed to actuate the engineered safety features. Each digital train is capable of actuating the engineered safety features (ESF) equipment required. Two channels of pressure switches are provided on the refueling water storage tank (RWST) to perform ESF functions. The intent is that any single failure within the ESFAS shall not prevent system action when required.

The redundant concept is applied to both the analog and logic portions of the system. Separation of redundant analog channels begins at the process sensors and is maintained in the field wiring, containment vessel penetrations and analog protection racks terminating at the redundant safeguards logic racks. The design meets the requirements of Criteria 20, 21, 22, 23, and 24 of the 1971 GDC.

The variables are sensed by the analog circuitry as discussed in WCAP-7013 (1973) and in Section 7.2. The outputs from the analog channels are combined into actuation logic as shown on Figure 7.2-1, Sheets 5, 6, 7, and 8. Tables 7.3-1 and 7.3-2 give additional information pertaining to logic and function.

The interlocks associated with the ESFAS are outlined in Table 7.3-3. These interlocks satisfy the functional requirements discussed in Section 7.1.2.

Manual actuation from the control board of containment isolation Phase A is provided by operation of either one of the redundant momentary containment isolation Phase A controls. The separate trains are thereby linked by mechanical means in a fashion similar to that shown on Figure 7.1-3. Also on the control board is a manual actuation of safety injection by one of the redundant controls and a manual actuation of containment isolation Phase B by either of the two sets of controls.

Manual controls are also provided to switch from the injection to the recirculation phase after a loss-of-coolant accident.

7.3.1.1.1 Function Initiation

The specific functions which rely on the ESFAS for initiation are:

1. A reactor trip, provided one has not already been generated by the reactor trip system.

2. Charging pumps, safety injection pumps, residual heat removal pumps, and associated valving which provide emergency makeup water to the cold legs of the reactor coolant system following a loss-of-coolant accident (Table 7.3-4 and NUSCo. Logic Description 24-9.4 provided in Logic Description Package, Section 1.7).

3. Those pumps which serve as part of the heat sink for containment cooling (e.g., service water and component cooling water pumps) (NUSCo. Logic Description 24-9.4).

4. Motor-driven and steam-driven auxiliary feedwater pumps (NUSCo. Logic Description 24-9.4).

5. Phase A containment isolation, whose function is to prevent fission product release. (Isolation of all lines not essential to reactor protection.) (Table 7.3-5).

6. Steam line isolation to prevent the continuous, uncontrolled blowdown of more than one steam generator and thereby uncontrolled reactor coolant system cooldown (Table 7.3-6).

7. Main feedwater line isolation, as required, to prevent or mitigate the effect of excessive cooldown (Table 7.3-7).

8. Start the emergency generators to assure backup supply of power to emergency and supporting systems components.

9. Isolate the control room intake ducts and pressurize the control room to meet control room occupancy requirements. (Table 7.3-8).

10. Containment depressurization actuation (CDA) which performs the following functions:

    a. Initiates containment spray to reduce containment pressure and temperature following a loss-of-coolant or main steam line break accident inside of containment (Table 7.3-9).

    b. Initiates Phase B containment isolation which isolates the containment following a loss of reactor coolant accident, or a main steam or feedwater line break within containment to limit radioactive releases. (Phase B isolation, together with Phase A isolation, results in isolation of all but safety injection and spray lines penetrating the containment.) (Table 7.3-10).

11. Emergency generator load sequencing is initiated when an LOP signal exists (NUSCo. Logic Description 24-9.4). The emergency generator performs its sequencing function when an LOP signal exists.

7.3.1.1.2 Analog Circuitry

The process analog sensors and racks for the ESFAS are covered in WCAP-7013 (1973). Discussed in this report are the parameters to be measured, including pressures, flows, tank and vessel water levels, and temperatures, as well as the measurement and signal transmission considerations. These latter considerations include the

transmitters, orifices and flow elements, resistance temperature detectors, as well as automatic calculations, signal conditioning, and location and mounting of the devices.

The sensors monitoring the primary system are located as shown on the piping flow diagrams in Chapter 5, reactor coolant system. The secondary system sensor locations are shown on the steam system flow diagrams given in Chapter 10.

7.3.1.1.3 Digital Circuitry

The ESF logic racks are discussed in detail in WCAP-7488-L (1971). The description includes the considerations and provisions for physical and electrical separation, as well as details of the circuitry. WCAP-7488-L (1971) also covers certain aspects of online test provisions, provisions for test points, considerations for the instrument power source, considerations for accomplishing physical separations. The outputs from the analog channels are combined into actuation logic as shown on Sheets 5 (T), 6 (Pressurizer Pressure), 7 (Steam Flow Pressure and Differential Pressure), 8 (Engineered Safety Features Actuation), and 14 (Auxiliary Feedwater) on Figure 7.2-1.

To facilitate engineered safety features actuation testing, four cabinets (two per train) are provided which enable operation, to the maximum practical extent, of safety features loads on a group-by-group basis until actuation of all devices has been checked. Final actuation testing is discussed in detail in Section 7.3.2.

7.3.1.1.4 Final Actuation Circuitry

The outputs of the solid state logic protection system (the slave relays) are energized to actuate, as are most final actuators and actuated devices. These devices are listed as follows:

1. Safety injection system pump and valve actuators. See Chapter 6 for flow diagrams and additional information.

2. Containment isolation (Phase A - "T" signal isolates all nonessential process lines on receipt of safety injection signal; Phase B - "P" signal isolates remaining process lines (which do not include safety injection lines) on receipt of 2/4 hi-3 containment pressure signal). For further information, see Section 6.2.4.

3. Service water pump and valve actuations (Chapter 9).

4. Auxiliary feed pumps start (Chapter 10).

5. Diesel start (Chapter 8).

6. Feedwater isolation (Chapter 10).

7. Ventilation isolation valve and damper actuators (Chapter 6). 3.25

8. Steam line isolation valve actuators (Chapter 10). 3.26

9. Quench spray and recirculation containment pumps and valve actuators (Chapter 6). 3.27

7.3.1.1.5 ESF and Essential Auxiliary Support Systems 3.30

Engineered Safety Features System 3.32

Systems that comprise the ESF for Millstone 3 are listed in Table 7.3-11. Their function and operation following ESFAS initiation are summarized in this section. Additional information on these systems can be found in the referenced sections. 3.34 3.36 3.37

Emergency Core Cooling System 3.40

The emergency core cooling system (ECCS) is described in Section 6.3 and is shown on Figure 6.3-1. Development of the SIS and CDA is shown on Figure 7.2-1 (Sheet 8 of 19). 3.42 3.44

The low pressure safety injection system, high pressure safety injection system, charging pumps in the chemical and volume control system, containment recirculation system, and residual heat removal system perform the function of core cooling for both normal plant cooldown and emergency core cooling. 3.45 3.46 3.47

When a safety injection signal (SIS) occurs, the injection mode of operation is automatically initiated. The charging pumps are started and lined up to take suction from the RWST and discharge to the reactor coolant cold leg. 3.48 3.49 3.50

The component interlocks used in different modes of system operation follow. 3.51

1. The SIS is interlocked with the following components and initiates the indicated action: 3.53

   a. Charging pumps start on SIS. 3.55

   b. RWST suction valves to charging pumps open on SIS. 3.56

   c. Charging pumps to RCS cold leg injection headers parallel isolation valves open on SIS. 3.57

   d. Normal charging path valves close on SIS. 3.58

   e. Charging pump miniflow valves close on SIS. 3.59

   f. Safety injection pumps start on SIS. 3.60

   g. The RHS pumps start on SIS. 4.1

h. Any closed accumulator isolation valves open. 4.2

i. Volume control tank (VCT) outlet isolation valves close on SIS. 4.3

2. Switchover from injection mode to recirculation involves the following interlocks: 4.6

a. The residual heat removal system (RHS) pumps are stopped automatically when one of the two low-low level switches sense a low-low level in the RWST. 4.8 4.9

b. Interlocks are provided to assure isolation of the RHS and proper alignment of the containment recirculation system for core cooling. 4.11 4.12

c. The safety injection pump and charging pump recirculation suction isolation valves can be opened provided that the safety injection pump miniflow lines have been isolated. 4.13 4.14

d. After approximately 15 hours, cold leg recirculation is terminated and hot leg recirculation is initiated. This is done to terminate any boiling in the core should the break be in one of the RCS cold legs, and to prevent boron precipitation. 4.15 4.16 4.17

A. RHS Pump Interlock from Injection to Recirculation 4.20

The details of achieving cold leg recirculation following safety injection are given in Section 6.3.2 and in Table 6.3-7. Figure 7.6-3 shows the logic which is used to automatically control RHS pumps. 4.22 4.23 4.25

B. Sequenced Safeguard Signals 4.28

A sequenced safeguard signal is generated by the emergency generator LOAD SEQUENCE for the safety injection pump, RHS pump, or charging pump whenever the signals listed with the associated pumps exist. 4.30 4.31

1. Safety Injection Pump 4.35

- SIS or SIS and LOP 4.37
- CDA or CDA and LOP 4.38
- SIS recirculation mode then LOP 4.40
- CDA recirculation mode then LOP 4.41

2. Residual Heat Removal Pumps 4.44

- SIS or SIS and LOP 4.46
- CDA or CDA and LOP 4.47

3. Charging Pumps 4.51

- SIS or SIS and LOP 4.53
- CDA or CDA and LOP 4.54
- SIS recirculation mode and then LOP 4.55
- CDA recirculation mode and then LOP 4.57

C. Component Controls 4.60

1. Residual Heat Removal System Pumps 5.2

The RHS pumps have manual controls on the main control board and at the switchgear. An annunciator is alarmed in the control room when LOCAL control is selected. The pumps are started automatically on receipt of a sequenced safeguard signal. When a safety injection signal exists, the pumps are stopped automatically on low-low RWST level, and low-low level is alarmed in the control room. Ammeters and indicator lights are located on the main control board and at the switchgear for the RHS pumps. ESF status lights on the main control board indicate when the RHS pumps are running. RHS pump AUTO trip and overcurrent is alarmed in the control room. 5.4 5.6 5.7 5.8 5.10 5.11 5.12

Bypass and inoperable alarms are provided in accordance with Regulatory Guide 1.47. 5.13

Analysis 5.15

A. IEEE Standard 279-1971, Paragraph 4.2: 5.17

There are two residual heat removal pumps powered from separate emergency buses. No single failure at the system level will prevent operation of at least one residual heat removal system train. 5.19 5.21

B. IEEE Standard 279-1971, Paragraph 4.4: 5.24

Equipment qualifications are discussed in Sections 3.10 and 3.11. 5.26

C. IEEE Standard 279-1971, Paragraphs 4.9 and 4.10:

One train of the residual heat removal system at a time is taken out of service and periodically tested in accordance with the Technical Specifications in Chapter 16.

This testing will consist of manually starting the pump during normal surveillance of the system or the breaker for the pump will be racked out. Once the pump is running or the breaker is racked out, the AUTO start and tripping is verified using the emergency generator load sequencer with safety signals generated internally or externally to the sequencer.

During the instrument functional test, the instrumentation setpoints and their operability are checked. The test to verify the automatic response of the system is performed during each refueling period. Correct settings of temperature and flow instrumentation are verified by applying a simulated signal.

D. IEEE Standard 279-1971, Paragraph 4.13:

A RHR pump low pressure safety injection system Train A bypass annunciator is alarmed in the control room when any of the following conditions exist for Train A or B:

- Residual heat removal pump control switch in pull to lock.
- Loss of control power.
- Circuit breaker racked out.

E. IEEE Standard 279-1971, Paragraph 4.16:

Once a safety signal is received, the residual heat removal system will go to completion. Deliberate operator action is required to stop the RHR pumps. The safety signal must be reset and manual controls used.

F. IEEE Standard 279-1971, Paragraph 4.17:

The residual heat removal pumps have manual controls on the main control board and at the switchgear. A REMOTE/LOCAL control transfer switch at the switchgear is alarmed in the control room when LOCAL is selected.

2. Safety Injection Pumps 6.13

The safety injection pumps have manual controls on the main control board and at the switchgear. An annunciator is alarmed in the control room when LOCAL control is selected. The pumps are started automatically on receipt of a sequenced safeguard signal. Ammeters and indicator lights are located on the main control board and at the switchgear for the safety injection pumps. ESF status lights on the main control board indicate when a safety injection pump is running. Safety injection pump AUTO Trip or overcurrent is alarmed in the control room. Bypass and inoperable alarms are provided in accordance with Regulatory Guide 1.47. Indicators on the main control board monitor safety injection pump discharge flow. 6.15 6.17 6.18 6.19 6.21 6.22 6.23 6.24

Analysis 6.26

A. IEEE Standard 279-1971, Paragraph 4.2: 6.28

There are two safety injection pumps powered from separate emergency buses. No single failure at the system level will prevent safety injection. 6.30 6.31

B. IEEE Standard 279-1971, Paragraph 4.4: 6.35

Equipment qualifications are dicussed in Sections 3.10 and 3.11. 6.37

C. IEEE Standard 279-1971, Paragraph 4.13: 6.41

A bypass and inoperable annunciator in the control room is alarmed when any of the following conditions exists for Train A or B: 6.43 6.44

- Safety injection pump control switch in pull to lock. 6.47
- Loss of control power or breaker racked out. 6.48
- Bypass pushbutton depressed. 6.49

D. IEEE Standard 279-1971, Paragraph 4.17: 6.52

The safety injection pumps have manual controls on the main control board and at the switchgear. A REMOTE/LOCAL control transfer switch at the switchgear is alarmed in the control room when LOCAL is selected. 6.54 6.55

E. IEEE Standard 279-1971, Pargaraphs 4.9 and 4.10: 6.59

One train at a time is taken out of service and periodically tested in accordance with the Technical Specifications in Chapter 16. 7.1 7.2

This testing will consist of manually starting the pump during normal surveillance of the system or the breaker for the pump will be racked out. Once the pump is running or the breaker is racked out, the AUTO start and tripping is verified using the emergency generator load sequencer with safety signals generated internally or externally to the sequencer.

During the instrument functional test, the instrumentation setpoints and their operability are checked. The test to verify the automatic response of the system is performed during each refueling period. Correct settings of temperature and flow instrumentation are verified by applying a simulated signal.

3. Charging Pumps

Normally, one charging pump is running. During a loss-of-coolant accident (LOCA), two charging pumps operate as part of the safety injection system. The third pump is a swing pump with a breaker cubicle on each emergency bus that is normally empty. The swing pump uses the breaker of the pump which is not in service. Mechanical and keylock switches prevent the pump from being placed on Train A and Train B emergency buses at the same time.

On a loss-of-power (LOP) signal the charging pump that is running is not stripped from the emergency bus; therefore, the pump starts immediately when power is restored. The pumps are started automatically on receipt of a sequenced safeguard signal.

Manual controls are provided on the main control board and at the switchgear for the charging pumps. An annunciator is alarmed on the main control board when local control is selected. ESF status lights indicate when a charging pump is running.

Ammeter and indicator lights are located at the switchgear and on the main control board.

Bypass and inoperable alarms are provided in accordance with Regulatory Guide 1.47.

Each charging pump has an auxiliary lube-oil pump with a local STOP-AUTO control switch. An annunciator is alarmed on the main control board when STOP is selected. The auxiliary lube-oil pumps will start automatically when AUTO is selected on low lube oil pressure, or when the associated charging pump is stopped. The auxiliary lube-oil pump will

stop automatically when AUTO is selected and lube-oil pressure is above a predetermined pressure and the associated charging pump is started. 7.38

Analysis 7.40

A. IEEE Standard 279-1971, Paragraph 4.2: 7.42

There are three charging pumps, 3CHS*P3A, B, and C. The C pump is a swing pump. Normally, two charging pumps (3CHS*P3A and B) have their breakers racked in and one of the two is running. In the event that the A or B pump fails, its breaker is racked out and racked into the C pump cubicle (Train A or B). Mechanical and electrical interlocks prevent the C pump from being connected to two buses at the same time. 7.44 7.47 7.48 7.49

Power is supplied to the charging pumps from two separate emergency buses. No single failure at the system level will prevent charging pump safety injection. 7.50 7.51

B. IEEE Standard 279-1971, Paragraph 4.4: 7.54

Equipment qualifications are dicussed in Sections 3.10 and 3.11. 7.56

C. IEEE Standard 279-1971, Paragraph 4.13: 7.60

A bypass and inoperable annunciator in the control room is alarmed when any of the following conditions exists for Train A or B: 8.2 8.3

- Charging pump A, B, or C control switch in pull to lock or loss of control power or breaker racked out. 8.6
- Charging pump cubicle ventilation system bypassed. 8.7
- Auxiliary building filter system fan control switch in pull to lock. 8.8
- Auxiliary building filter system fan loss of control power or breaker racked out. 8.9
- Bypassed pushbutton depressed for charging pumps safety injection. 8.10

D. IEEE Standard 279-1971, Paragraph 4.16: 8.13

Once a safety signal is initiated, the charging pumps go to completion. Deliberate operator action is required to stop a charging pump. The safety signal must be reset and the pump stopped by manual controls. 8.15 8.16 8.17

E. IEEE Standard 279-1971, Paragraph 4.17: 8.21

The charging pumps have manual controls on the main control board and at the switchgear. A REMOTE/LOCAL control transfer switch at the switchgear is alarmed in the control room when LOCAL is selected. 8.23 8.24

F. IEEE Standard 279-1971, Paragraph 4.10: 8.28

One charging pump at a time can be taken out of service and periodically tested in accordance with the Technical Specifications in Chapter 16. 8.30 8.31

This testing will consist of manually starting the pump during normal surveillance of the system or the breaker for the pump will be racked out. Once the pump is running or the breaker is racked out, the AUTO start and tripping is verified using the emergency generator load sequencer with safety signals generated internally or externally to the sequencer. 8.33 8.35 8.36 8.37

8.38

During the instrument functional test, the instrumentation setpoints and their operability are checked. The test to verify the automatic response of the system is performed during each refueling period. Correct settings of temperature and flow instrumentation are verified by applying a simulated signal. 8.39 8.40 8.41

4. Refueling Water Storage Tank to Charging Pump Valve 8.44

Redundant RWST to charging pump valves have manual controls and indicator lights on the main control board and at the auxiliary shutdown panel. REMOTE/LOCAL transfer switches are on the transfer switch panels. An annunciator is alarmed in the control room when LOCAL control is selected. ESF status lights indicate when the valves are open. Open and closed valve positions are monitored by the plant computer. The valves open automatically on receipt of an SIS or when the volume control tank level is low-low. 8.46 8.49 8.50 8.52 8.53

Analysis 8.55

A. IEEE Standard 279-1971, Paragraph 4.2: 8.57

The RWST to charging pump valves are redundant and powered from separate emergency buses. No single failure at the system level will prevent charging pump safety injection. 8.59 9.1

B. IEEE Standard 279-1971, Paragraph 4.4:

Equipment qualifications are discussed in Sections 3.10 and 3.11.

C. IEEE Standard 279-1971, Paragraph 4.13:

The charging pump high pressure safety injection bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B):

- Circuit breaker for valve open.
- Loss of control power to valve.
- Valve motor thermal overload.

D. IEEE Standard 279-1971, Paragraph 4.16:

Once an SIS is initiated, the RWST to charging pump valves go to the fully open position. Deliberate operator action is required to close the valves. The SIS must be reset and the valves closed by manual controls.

E. IEEE Standard 279-1971, Paragraph 4.17:

The RWST to charging pump valves have manual controls on the main control board and at the auxiliary shutdown panel. The REMOTE/LOCAL control transfer switches on the transfer switch panels are alarmed in the control room whenever LOCAL is selected.

F. IEEE Standard 279-1971, Paragraph 4.10:

The RWST valves are periodically tested in accordance with the Technical Specifications in Chapter 16. Refer to Sections 7.3.1.2 and 7.3.2 for testing of engineered safety actuation system.

5. Volume Control Tank Outlet Isolation Valves

Redundant volume control tank (VCT) outlet isolation valves have manual controls and indicator lights on the main control board and on the auxiliary shutdown panel. REMOTE/LOCAL transfer switches are on the transfer switch panel. An annunciator is alarmed in the control room when LOCAL control is selected. ESF status lights indicate when the valves are closed. An annunciator is alarmed in the control room when a VCT outlet isolation valve is closed. Open and close valve positions are monitored by the plant computer. The valves close automatically on receipt of an SIS or VCT low-low level signal, provided the associated RWST to the charging pump valve is open.

Analysis 9.57

A. IEEE Standard 279-1971, Paragraph 4.2: 9.59

The VCT outlet isolation valves are redundant and powered from separate emergency buses. No single failure at the system level will prevent VCT outlet isolation. 10.1 10.3

B. IEEE Standard 279-1971, Paragraph 4.4: 10.6

Equipment qualifications are discussed in Sections 3.10 and 3.11. 10.8

C. IEEE Standard 279-1971, Paragraph 4.13: 10.12

A charging pump high pressure safety injection bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B): 10.14 10.15

- Circuit breaker for valve open. 10.18
- Loss of control power to valve. 10.19
- Valve motor thermal overload. 10.20

D. IEEE Standard 279-1971, Paragraph 4.16: 10.23

Once an SIS or VCT low-low level signal is received, the VCT outlet isolation valves go fully closed. The SIS must be reset and the VCT low-low level signal cleared and the valves opened by manual controls. 10.25 10.27

E. IEEE Standard 279-1971, Paragraph 4.17: 10.30

The VCT outlet isolation valves have manual controls on the main control board and at the auxiliary shutdown panel. The REMOTE/LOCAL control transfer switches on the transfer switch panels are alarmed in the control room whenever LOCAL is selected. 10.32 10.34 10.35

F. IEEE Standard 279-1971, Paragraph 4.10: 10.38

The VCT isolation valves are periodically tested in accordance with the Technical Specifications in Chapter 16. Refer to Sections 7.3.1.2 and 7.3.2 for testing of engineered safety actuation system. 10.40 10.42

6. Charging Pump to Reactor Cold Leg Isolation Valves 10.45

Redundant charging pump to reactor cold leg isolation valves have manual controls and indicator lights on the main control board. Open and closed valve positions are monitored by the plant computer. ESF status lights indicate 10.47 10.50 10.51

when the valves are open. An annunciator is alarmed in the control room when an isolation valve is open. The valves open automatically on receipt of an SIS.

Analysis

A. IEEE Standard 279-1971, Paragraph 4.2:

The charging pump to reactor cold leg isolation valves are redundant and powered from separate emergency buses. No single failure at the system level will prevent charging pump safety injection.

B. IEEE Standard 279-1971, Paragraph 4.4:

Equipment qualifications are discussed in Sections 3.10 and 3.11.

C. IEEE Standard 279-1971, Paragraph 4.13:

The charging pump high pressure safety injection bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B):

- Circuit breaker for valve open.
- Loss of control power to valve.
- Valve motor thermal overload.

D. IEEE Standard 279-1971, Paragraph 4.16:

Once an SIS is initiated, the charging pump to cold leg isolation valves go to fully open. Deliberate operator action is required to close the valves. The SIS must be reset and the valves closed by manual controls.

E. IEEE Standard 279-1971, Paragraph 4.17:

The charging pump to cold leg isolation valves have manual controls on the main control board.

F. IEEE Standard 279-1971, Paragraph 4.10:

The charging pumps to reactor cold leg isolation valves are periodically tested in accordance with the Technical Specifications in Chapter 16. Refer to Sections 7.3.1.2 and 7.3.2 for testing of engineered safety actuation system.

7. Charging Pump to Reactor Coolant System Isolation Valves

Redundant charging pump to reactor coolant system isolation valves (normal charging flow path) have manual controls and

indicator lights on the main control board. Open and close valve positions are monitored by the plant computer. ESF status lights indicate when the valves are closed. The valves close automatically on receipt of an SIS.

Analysis

A. IEEE Standard 279-1971, Paragraph 4.2:

The charging pump to reactor coolant system isolation valves are redundant and powered from separate emergency buses. No single failure at the system level will prevent isolation of normal charging to reactor coolant system.

B. IEEE Standard 279-1971, Paragraph 4.4:

Equipment qualifications are discussed in Sections 3.10 and 3.11.

C. IEEE Standard 279-1971, Paragraph 4.13:

The charging pump high pressure safety injection bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B):

- Circuit breaker for valve open.
- Loss of control power to valve.
- Valve motor thermal overload.

D. IEEE Standard 279-1971, Paragraph 4.16:

Once an SIS is initiated, the charging pump to reactor coolant isolation valves go to the fully closed position. Deliberate operator action is required to open the valves. The SIS must be reset and the valves opened by manual controls.

E. IEEE Standard 279-1971, Paragraph 4.17:

The charging pump to reactor coolant isolation valves have manual controls on the main control board and at the auxiliary shutdown panel. The REMOTE/LOCAL control transfer switches on the transfer switch panels are alarmed in the control room whenever LOCAL is selected.

F. IEEE Standard 279-1971, Paragraph 4.10:

The RWST valves are periodically tested in accordance with the Technical Specifications in Chapter 16. Refer to Sections 7.3.1.2 and 7.3.2 for testing of engineered safety actuation system.

8. Charging Pump Miniflow Isolation Valves (Train B) 12.42

The miniflow isolation valve for each charging pump has manual controls and indicator lights on the main control board and at the auxiliary shutdown panel. REMOTE/LOCAL control transfer switches are on a transfer switch panel. An annunciator is alarmed in the control room when LOCAL control is selected. An annunciator is alarmed in the control room when a valve is closed. ESF status lights indicate when a valve is closed. Open and closed positions are monitored by the plant computer. The valves close automatically on receipt of an SIS. 12.44 12.47 12.48 12.49 12.50 12.51 12.52

9. Charging Pump Miniflow Isolation Valve (Train A) 12.55

The charging pump combined miniflow isolation valve has manual control and indicator lights on the main control board. An annunciator alarms in the control room when the valve is closed. An ESF status light indicates when the valve is closed. The valve is closed automatically on receipt of an SIS. 12.57 12.59 12.60 13.1

Analysis 13.3

A. IEEE Standard 279-1971, Paragraph 4.2: 13.5

There are three Train B minflow isolation valves and one combined Train A miniflow isolation valve. The Train A and Train B valves are powered from separate emergency buses. No single failure at the system level will prevent charging pump miniflow isolation. 13.7 13.9 13.10

B. IEEE Standard 279-1971, Paragraph 4.4: 13.13

Equipment qualifications are discussed in Sections 3.10 and 3.11. 13.15

C. IEEE Standard 279-1971, Paragraph 4.13: 13.19

The charging pump high pressure safety injection bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B): 13.21 13.22

- Circuit breaker for valve open. 13.25
- Loss of control power to valve. 13.26
- Valve motor thermal overload. 13.27

D. IEEE Standard 279-1971, Paragraph 4.16: 13.30

Once an SIS is initiated, the charging pump to miniflow isolation valves go to the fully closed position. Deliberate operator action is required to open the 13.32 13.34

valves. The SIS must be reset and the valves closed by manual controls.

E. IEEE Standard 279-1971, Paragraph 4.17:

The Train B charging pump miniflow isolation valves have manual controls on the main control board and at the auxiliary shutdown panel. The REMOTE/LOCAL control transfer switches on the transfer switch panels are alarmed in the control room whenever LOCAL is selected.

F. IEEE Standard 279-1971, Paragraph 4.10:

The charging pump miniflow isolation valves are periodically tested in accordance with the Technical Specifications in Chapter 16. Refer to Sections 7.3.1.2 and 7.3.2 for testing of engineered safety actuation system.

10. Accumulator Isolation Valves

Two accumulator isolation valves are powered from the Train A emergency bus; the other two are powered from the Train B emergency bus. Each valve has manual controls and indicator lights on the main control board and at the auxiliary shutdown panel. An annunciator is alarmed in the control room when LOCAL control is selected. ESF status lights indicate when a valve is closed. An annunciator is alarmed in the control room when a valve is closed. Open and close positions are monitored by the plant computer. The valves open automatically on receipt of an SIS and will open automatically on a high pressurizer pressure signal provided the associated control switch is in the AUTO position.

Analysis

A. IEEE Standard 279-1971, Paragraph 4.2:

The Train A and B accumulator isolation valves are powered from separate emergency buses. No single failure at the system level will prevent charging pump miniflow isolation.

B. IEEE Standard 279-1971, Paragraph 4.4:

Equipment qualifications are discussed in Sections 3.10 and 3.11.

C. IEEE Standard 279-1971, Paragraph 4.13:

The accumulator tank low pressure safety injection bypass annunciator is alarmed in the control room whenever an accumulator isolation valve is not fully open.

D. IEEE Standard 279-1971, Paragraph 4.16:

Once an SIS is initiated, the accumulator isolation valves go to the fully open position. Deliberate operator action is required to close a valve. The SIS must be reset and the valves closed by manual controls.

E. IEEE Standard 279-1971, Paragraph 4.17:

The accumulator isolation valves have manual controls on the main control board and at the auxiliary shutdown panel. The REMOTE/LOCAL control transfer switches on the transfer switch panels are alarmed in the control room whenever LOCAL is selected.

F. IEEE Standard 279-1971, Paragraph 4.10:

The accumulator isolation valves are periodically tested in accordance with the Technical Specifications in Chapter 16. Refer to Sections 7.3.1.2 and 7.3.2 for testing of engineered safety actuation system.

Containment Depressurization System

The containment depressurization systems' design is described in Section 6.2.2 and the flow diagrams are shown on Figures 6.2-37 and 6.2-38. The containment depressurization systems consist of the quench spray system and the containment recirculation spray system.

The containment depressurization systems operate only subsequent to a design basis accident (DBA). During normal unit operation, the motor-operated valves in the containment recirculation pump suction lines and discharge headers are open. To ensure proper position of these valves, the CDA signal actuates the valves to open and to override a possible close-test position. The motor-operated isolation valves in the quench spray system are closed during normal unit operation. The isolation valves in the quench spray discharge headers and in the outlet line of the refueling water chemical addition tank open upon receipt of a CDA signal. The solenoid pilot air-operated valves in the suction line from the RWST to the refueling water recirculation pumps close on a safety injection signal (SIS), thus isolating the nonsafety related portion of the suction piping downsteam of the second isolation valve.

The quench spray pumps are started automatically on receipt of a CDA signal. On receipt of a CDA signal combined with a LOP signal, the quench spray pumps are sequenced on by the emergency generator load

sequencer. The quench spray pumps are stopped automatically on receipt of a RWST empty signal. 15.15

The containment recirculation pumps are sequenced on automatically by the emergency generator load sequencer following receipt of a CDA signal or a CDA combined with a LOP signal. 15.16 15.18

A. Containment Recirculation System Instrumentation 15.21

The following instrumentation is provided in the control room to monitor the system performance. 15.23

1. Redundant level indicators for the containment sump. One level channel is recorded. 15.27

2. Containment recirculation pump discharge pressure indicators. 15.28

3. Containment recirculation pump seal head tank low level alarm which detects seal water leakage or seal failure. 15.29

4. Containment recirculation cooler shell outlet temperature. 15.30

5. Redundant containment sump temperature indicators. 15.31

6. Containment recirculation cooler outlet flow indicators. 15.32

7. Containment recirculation pump flow indicators. 15.33

8. Containment recirculation pump low discharge pressure annunciators interlocked with pump running signal. 15.34

A pressure transmitter in the common test line from the RWST and a pressure transmitter in the discharge line of each containment recirculation pump are utilized by the plant computer to monitor pump differential pressure and verify performance of the containment recirculation pumps. 15.36 15.37 15.38

Analysis 15.41

A. IEEE Standard 279-1971, Paragraph 4.2: 15.42

The containment recirculation system is divided into two separate, redundant mechanical and electrical trains. This provides redundancy to prevent a failure of a an active or passive component from impairing the system capability to supply water for the containment depressurization system. 15.44 15.46 15.47

B. IEEE Standard 279-1971, Paragraph 4.4: 15.50

Equipment qualifications are discussed in Sections 3.10 and 3.11. 15.52

C. IEEE Standard 279-1971, Paragraph 4.13: 15.56

The containment recirculation system bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A and B): 15.58 15.59

- Containment isolation recirculation pump loss of control power or breaker racked out. 16.2
- Containment recirculation pump control switch in pull to lock. 16.3
- Service water system bypassed. 16.4
- Containment recirculation pump area air conditioning unit - loss of control power or circuit breaker open. 16.5
- Service water valve to reactor plant component cooling water heat exchanger not fully closed and circuit breaker open or loss of control power. 16.6 16.7
- Service water valve to containment recirculation coolers not fully open and loss of control power or circuit breaker open. 16.8 16.9
- Service water outlet valve for containment recirculation coolers not fully open. 16.10
- Service water valve to turbine plant component cooling heat exchangers not fully closed and loss of power or circuit breaker open. 16.11 16.12
- Service water valves to reactor plant component cooling heat exchangers in TEST (No-No Equip). 16.13
- Service water inlet valves for containment recirculation coolers in TEST (No-No Equip). 16.14
- Service water valves to turbine plant component cooling water heat exchangers in TEST (No-No Equip). 16.15
- Recirculation spray header isolation valve fully open and loss of power or circuit breaker open. 16.16
- Cross-connect valve to low pressure safety injection system not fully closed. 16.17
- Recirculation spray pump suction valve not fully open and loss of power or circuit breaker open. 16.18
- Manual bypass pushbutton depressed. 16.19

D. IEEE Standard 279-1971, Paragraph 4.16: 16.22

Once a CDA signal is received, the containment recirculation pumps are started automatically. Deliberate operator action is required to stop the pumps. 16.24 16.25

E. IEEE Standard 279-1971, Paragraph 4.10: 16.29

The containment recirculation system is periodically tested in accordance with the Technical Specifications in Chapter 16. 16.31 16.32

The operability of the containment recirculation system controls and indications is verified during the instrument functional test. Also, during this test the instrumentation setpoints and their operability are checked. The test to verify the automatic response of the system is performed during each refueling period. Correct settings of temperature, flow, and level instrumentation are verified by applying a simulated signal. 16.34 16.36 16.37 16.38

F. IEEE Standard 279-1971, Paragraph 4.17: 16.41

Controls and indicators are provided in the control room for manual operation of the containment recirculation system. REMOTE/LOCAL control selector switches are provided for the containment recirculation pumps outside the control room at the switchgear. An annunciator is alarmed in the control room when LOCAL control is selected. 16.43 16.45 16.46 16.47

Switchover from the injection to recirculation phase for the recirculation system is described in Section 6.3. Logic for the RWST signals is found in Section 6.3.5.4. 16.49 16.50

B. Quench Spray System Instrumentation 16.53

The following instrumentation is provided in the control room to monitor the quench spray system. 16.55

1. Quench spray pump discharge flow indicators and low flow annunciators. 16.58

2. RWST (level indication and level alarms). 16.59

3. Temperature indicators are provided on the main control board for the RWST, the refueling water recirculation pump suction, and the refueling water coolers outlet. High and low RWST temperature is alarmed on the main control board. 16.60 17.2

4. The refueling water recirculation pumps and the associated coolers operate only during normal unit operation. One refueling water recirculation pump is normally running with the other in standby. The standby pump is started on a predetermined RWST high temperature signal. Both pumps are 17.3 17.4 17.5 17.6

stopped by a low temperature signal - RWST temperature or refueling water recirculation pump suction line temperature. 17.7
The objective of the instrumentation associated with the refueling water recirculation pumps is to maintain the temperature of the refueling water within design limits. 17.8 17.9

5. The refueling water chemical addition tank is provided with level and temperature indicators on the main control board. Low level and low temperature are alarmed on the main control board. 17.10 17.11 17.12

Analysis 17.15

A. IEEE Standard 279-1971, Paragraph 4.2: 17.16

The quench spray system is divided into two separate, redundant mechanical and electrical trains. This dual concept provides redundancy to prevent a failure of an active component or a passive component at the system level to supply water for the containment depressurization system. 17.18 17.20 17.21

B. IEEE Standard 279-1971, Paragraph 4.4: 17.24

Equipment qualifications are discussed in Sections 3.10 and 3.11. 17.26

C. IEEE Standard 279-1971, Paragraph 4.13: 17.30

The quench spray pump bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A and B): 17.32 17.33

- Quench spray pump in pull to lock. 17.36
- Chemical addition tank outlet valve loss of control power or circuit breaker open. 17.37
- Quench spray header isolation valve loss of control power or circuit breaker open. 17.38
- Quench spray pump loss of control power or breaker racked out. 17.39
- Quench spray pump area air conditioning unit loss of control power or circuit breaker open. 17.40
- Manual bypass pushbutton depressed. 17.41

D. IEEE Standard 279-1971, Paragraph 4.17: 17.44

The quench spray pumps have manual controls on the main control board and at the auxiliary shutdown panel. The REMOTE/LOCAL control transfer swtiches on the transfer 17.46 17.48

switch panel are alarmed in the control room whenever LOCAL is selected. 17.49

E. IEEE Standard 279-1971, Paragraph 4.10: 17.52

The quench spray pumps are periodically tested in accordance with the Technical Specifications in Chapter 16. 17.54

The operability of the quench spray system controls and indications is verified during the instrument functional test. Also, during this test the instrumentation setpoints and their operability are checked. The test to verify the automatic response of the system is performed during each refueling period. Correct settings of temperature, flow, and level instrumentation are verified by applying a simulated signal. 17.57 17.58 17.59 17.60

The testing and calibration of the level switches used for the detection of the RWST level is accomplished by taking one logic Train (A or B) out of service for a short duration. The testing of the RWST level used for tripping of the quench spray pumps will be used as an example. The circuit breakers are first put in the trip position and racked out one train at a time, or the quench spray pumps will be started manually. The level switches for the train under test are then isolated at the manifold valve in the safeguard building. A simulated pressure signal is then injected into the transmitter which will simulate level in the RWST. This signal will energize an output relay located in the quench spray pump switchgear. Contacts from this output relay, which are used to trip the pump breaker, will be monitored for closing and opening. If the quench spray pumps are started manually, the output relay will automatically stop the quench spray pumps at the proper setpoint. Contacts which open and close valves will also be monitored by position lights associated with these particular valves. Verification that the test pressure connections have been removed and manifold valves have been reopened is accomplished by the use of alarms, valve position lights, and adminstrative procedures. 18.1 18.2 18.3 18.4 18.6 18.7 18.8 18.9 18.10 18.11 18.13 18.14 18.15

Testing and inspections of the containment heat removal and depressurization systems are described in Section 6.2.2.4. 18.17 18.18

Containment Isolation System 18.21

The initiation signals for the containment isolation system are a part of the engineered safety features actuation system. Penetration types and containment isolation valve arrangements are described in detail in Section 6.2.4. 18.23 18.26

The safety function of the containment isolation system is to isolate automatically appropriate lines penetrating the containment structure 18.27 18.28

in order to limit the uncontrolled release of radioactive materials to the environment, following an accident. 18.29

Analysis 18.32

A. IEEE Standard 279-1971, Paragraph 4.2: 18.33

Containment isolation valves are located inside and outside of the containment structure, ensuring containment integrity. The containment isolation system provides two barriers between the atmosphere outside the containment structure and 1) the atmosphere inside the containment structure, 2)the reactor coolant system, and 3) the systems connected to Items 1 or 2 as a result of or subsequent to a DBA signal provided by safety injection, containment isolation Phase A (CDA), containment isolation Phase B (CIB), feedwater isolation (FWI), or steam link isolation (SLI). 18.35 18.38 18.39 18.40 18.41 18.42

These signals will open or close containment structure penetrations for ESF systems which function to mitigate the consequences of an accident. 18.43 18.44

Containment isolation valves are actuated by solenoid-operated air pilot valves or by motor-operators. Valves controlled by solenoid-operated air pilot valves are designed to fail in the closed position upon loss of power or instrument air. Operators for motor-operated valves are designed for fast closure so as to ensure containment isolation in shortest possible time. Motor-operated valves fail "as is" position. Torque and limit switches set for proper valve setting. 18.45 18.46 18.48 18.50 18.51

B. IEEE Standard 279-1971, Paragraph 4.4: 18.54

Equipment qualifications are discussed in Sections 3.10 and 3.11. 18.56

C. IEEE Standard 279-1971, Paragraph 4.13: 18.60

A containment isolation Phase A bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B): 19.2 19.3

- Reactor coolant pump seal water return valve - loss of power or circuit breaker open or motor thermal overload. 19.6
- Reactor coolant pump seal water return valve in TEST (No-No Equip). 19.7
- Manual bypass pushbutton depressed. 19.8

A containment isolation Phase B bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B):

- Reactor plant component cooling isolation valve - loss of power or circuit breaker open or motor thermal overload.
- Manual bypass pushbutton depressed.

D. IEEE Standard 279-1971, Paragraph 4.16:

Any automatic containment isolation action, once initiated, will go to completion. The return to normal operating conditions requires deliberate operator action.

E. IEEE Standard 279-1971, Paragraph 4.17:

The operator has the means for manual initiation of the containment isolation system independent of automatic actuation. Manual controls and visual indication for the containment isolation valves are described in Section 7.5.

F. IEEE Standard 279-1971, Paragraph 4.10:

Containment isolation valves are tested to ensure they are capable of closing by operating manual switches in the control room and by observing the position lights. Periodic testing during normal operation is performed on all containment isolation valves except those where the test would interrupt or upset normal operation. Testing of these valves is performed during refueling shutdowns (Table 7.3-12).

Refer to Section 6.2.4.4 for testing and inspection procedures of containment isolation valves in various systems. Table 6.2-66 lists design, operating, and functional parameters of all containment isolation valves.

The design bases for the controls of the containment isolation system are:

1. Physical and electrical separation between controls of the redundant containment isolation valves is provided to prevent electrical faults or physical damage to one of the containment isolation valve controls from affecting the controls of the redundant valve.

2. The controls of the containment isolation system are designed to withstand seismic loads and to operate in adverse environmental conditions in accordance with requirements described in Sections 3.10 and 3.11, respectively.

Status lights monitoring the status of containment isolation valves enable the operator, during emergency conditions, to make sure all isolation valves are in the required position, or to take corrective action if necessary.

Combustible Gas Control System in Containment (HCS)

The combustible gas control system is described in Section 6.2.5 and its flow diagram is shown on Figure 6.2-48.

The hydrogen recombiner system is utilized in the long term following a DBA and, therefore, is safety related (QA Category I). Each of the redundant trains in the hydrogen recombiner system is completely instrumented to ensure the system performs its safety function following any single failure.

A hydrogen analyzer is permanently installed in each train to provide the capability of analyzing the hydrogen content in the gas being drawn from the containment atmosphere or in the gas being returned to the containment atmosphere.

A temperature controller senses the electric preheater discharge gas temperature and controls the heating element to maintain the 350°F gas temperature required to minimize the possibility of halogen gas inhibiting the recombiner. Flow, temperature, and pressure indication is provided at each hydrogen recombiner blower discharge. Temperature indication is provided at the discharge of each electric preheater, recirculator, and inside a pressure indicator and is provided at discharge of each hydrogen recombiner.

Each set of instrumentation and controls requiring electric power is supplied from an independent source. 120V ac power is supplied from the 120V ac vital buses and 125V dc power from the 125V dc buses.

Analysis

A. IEEE Standard 279-1971, Paragraph 4.2:

Combustible gas control is maintained by the DBA hydrogen recombiner system which monitors the hydrogen concentration within the containment and maintains this concentration at a safe level in the long term following a design basis LOCA.

The DBA hydrogen recombiner system has two redundant 100 percent capacity trains to maintain the hydrogen in the containment atmosphere at a safe concentration following a DBA. Each of the redundant trains is fully instrumented and electric power is supplied from independent Class 1E emergency buses to ensure the system performs its safety function.

No single failure at the system level will prevent the hydrogen recombiner system to process and maintain the hydrogen concentration in the containment atmosphere below

the limits specified in Regulatory Guide 1.7 following a DBA.

B. IEEE Standard 279-1971, Paragraph 4.4: 20.31

Equipment qualifications are discussed in Section 3.10 and 3.11. 20.33

C. IEEE Standard 279-1971, Paragraph 4.13: 20.37

A DBA hydrogen recombiner system bypassed annunciator is alarmed in the control room whenever any of the following conditions exists (Train A or B): 20.39 20.40

- Recombiner building inlet and outlet ventilation damper loss of power. 20.43

- Manual bypass pushbutton depressed. 20.44

D. IEEE Standard 279-1971, Paragraph 4.16: 20.47

The DBA hydrogen recombiner system is manually initiated and monitored locally in the hydrogen recombiner building. 20.49
After the initial heatup of the system, the system operates automatically with common alarms located in the control room to alert the operator of a malfunction. 20.51 20.52

E. IEEE Standard 279-1971, Paragraph 4.17: 20.55

The DBA hydrogen recombiner system operating parameters are monitored, indicated, and controlled locally. In addition, recombiner bypassed and common trouble alarms are annunciated in the control room. Indicators and a recorder (Channel A only) for hydrogen gas concentration are located on the main control boards. The system bypass pushbutton and loss of control power to the system cubicle ventilation dampers are monitored by the plant computer. 20.57 20.59 20.60 21.1 21.2

F. IEEE Standard 279-1971, Paragraphs 4.9 and 4.10: 21.5

One recombiner train at a time can be taken out of service and periodically tested in accordance with the Technical Specifications in Chapter 16. Testing of the system is accomplished by placing each subsystem into normal operation. Temperature, flow, pressure indicators, and the temperature controller are tested at the same time as the system as described in Section 6.2.5.4. The hydrogen analyzer is tested, by injecting sample gases, to verify zero and span calibration. 21.7 21.10 21.11 21.13

Supplementary Leak Collection and Release System 21.16

The supplementary leak collection and release system (SLCRS) is described in Section 6.2.3; its flow diagram is shown on Figure 6.2-46. 21.18 21.19

The SLCRS consist of two exhaust fans, each supplied from a separate emergency bus, two filter banks, and the associated ductwork and dampers. 21.21 21.22

The SLCRS exhausts, creates, and maintains a partial vacuum of 1/4-inch water gage in the enclosure building and contiguous buildings upon receipt of an SIS signal or when manually started. 21.23 21.24

Following a LOCA, the SIS signal 1) opens the SLCRS Train A and B filter bank inlet and 2) starts the SLCRS Train A and B exhaust fans 21.25 21.26

High differential pressure across the roughing filter, high efficiency particulate air (HEPA) filter, carbon adsorber, and HEPA filter of each filter bank is alarmed in the control room. 21.27 21.28

The filtered exhaust is monitored for radiation (Section 11.5) prior to discharge to atmosphere via the Millstone 1 stack. 21.29 21.30

Analysis 21.33

A. IEEE Standard 279-1971, Paragraph 4.2: 21.34

The supplementary leak collection and release system is divided into two separate, redundant mechanical and electrical trains. This dual train concept provides sufficient redundancy to prevent a single failure from impairing the system capability to maintain a negative pressure of 0.25 inches in the enclosure building. 21.36 21.39 21.40

B. IEEE Standard 279-1971, Paragraph 4.4: 21.43

Equipment qualifications are discussed in Section 3.10 and 3.11. 21.45

C. IEEE Standard 279-1971, Paragraph 4.13: 21.49

The supplementary leak collection and release bypassed annunciator is alarmed in control room whenever any of the following conditions exists (Train A or B): 21.51 21.52

- SLCRS fan control switch in pull to lock position. 21.55
- SLCRS fan loss of power or circuit breaker open. 21.56
- Manual bypass pushbutton depressed. 21.57

D. IEEE Standard 279-1971, Paragraph 4.16: 21.60

Once an SIS is received, the SLCRS exhausts, creates, and maintains a partial vacuum of 0.25 inches. Deliberate operator action is required to release the SLCRS from maintaining this vacuum. 22.2 22.4

E. IEEE Standard 279-1971, Paragraph 4.10: 22.7

The SLCRS is periodically tested in accordance with the Technical Specifications in Chapter 16. 22.9

Fans, air operated dampers, and controls for the supplementary leak collection system are tested by automatically starting on a simulated SIS signal and allowing them to reach rated speed with all dampers in the operating position before being shut down. During the test, the instrumentation setpoints and their operability are checked. 22.11 22.12 22.14

Auxiliary Feedwater System 22.17

The auxiliary feedwater system which, except for some SSPS initiation signals, is in the balance-of-plant and is described in Section 10.4.9. The safety related portions of the auxiliary feedwater system are shown on Figure 10.4-9. The auxiliary feedwater system meets all the requirements of IEEE Standard 279-1971. 22.19 22.20 22.22 22.23

One turbine-driven auxiliary feedwater pump and two motor-driven pumps are provided. Each motor-driven pump has half the capacity of the turbine-driven pump. Power is supplied to the motor-driven pumps from separate emergency buses. Steam supply to the turbine-driven pump is shown on Figure 10.3-1. A branch line from three main steam lines (A,B,D) is connected into a common header to supply steam to the turbine. A normally closed air-operated valve is installed in each branch line (A,B,D). Each air-operated valve is controlled by two solenoid-operated valves connected in series in the air supply line. The solenoid-operated valves are supplied power from separate emergency buses. Loss of power to either solenoid-operated valve will vent air to open the associated air-operated valve. A motor-operated stop check valve is installed in each line. These valves are normally in the open position. Power for each of the motor-operated stop check valves is supplied from an emergency bus. 22.24 22.25 22.26 22.27 22.28 22.29 22.30 22.31 22.32 22.33 22.34 22.35

During normal operation, the operability of all valves in the auxiliary feedwater system is verified by remote manual action. The three air-operated valves are exercised similarly by isolating the steam supply to the turbine-driven auxiliary feedwater pump by closing the motor-operated stop check valves in the steam lines. 22.36 22.38 22.39

In the auxiliary feedwater system, the motor-driven pumps are initiated automatically by the following signals: (These signals also close the blowdown isolation and sample line valves for all steam generators.) 22.40 22.41

- Safety injection or containment depressurization (from solid state protection system). 22.43

- Two out of four (2/4) low-low level in any steam generator (from solid state protection system). 22.44

- Emergency bus loss of power 22.45

The motor-driven pumps are also started manually. 22.47

Starting the turbine-driven pump as well as closing the blowdown isolation and sample valves is initiated automatically by a loss of power or a 2/4 Low-Low level signal in 2/4 steam generators (from solid state protection system). 22.48 22.49 22.50

The turbine-driven pump is also started manually. 22.51

Indication and controls required for the auxiliary feedwater system in the event of inaccessibility of the control room are provided on the auxiliary shutdown panel described in Section 7.4. Table 7.5-1 is a list of indications provided on the main control board. The solenoid-operated modulating valves in the auxiliary feedwater supply line to each steam generator are manually-operated from the main control board or from the auxiliary shutdown panel. 22.52 22.53 22.54 22.55 22.56

The motor-operated valves in the auxiliary feedwater lines from the motor-driven auxiliary feedwater pumps discharge are manually-operated from the main control board or from the auxiliary shutdown panel. The valves associated with any one auxiliary feedwater line are powered from different emergency buses. The valves are normally open so that loss of power to one emergency bus does not prevent the isolation or control of auxiliary feedwater to a steam generator. An air-operated valve is provided between each steam generator auxiliary feedwater pump suction and the condensate storage tank to allow pump suction to be taken from tank. The condensate storage tank suction valves for the motor-driven pumps can be operated from the main control board or from the auxiliary shutdown panel. The condensate storage tank suction valve for the turbine-driven auxiliary feedwater pump can be operated from the main control board only. These valves are normally closed and fail closed on loss of control air or electric power. 22.57 22.58 22.59 22.60 23.2 23.3 23.4 23.6 23.8

Steam generator auxiliary feedwater pump suction and discharge pressure is indicated in the control room and monitored by the plant computer. Flow in each steam generator auxiliary feedwater supply line is indicated by flow indicators in the control room and on the auxiliary shutdown panel. The correct operation of a pressure loop is verified in conjunction with the steam generator auxiliary feedwater pump test described in Section 10.4.9.4. The steam generator auxiliary feedwater pumps are operated during this test. 23.9 23.10 23.11 23.12 23.13 23.15

Redundant demineralized water storage tank (DWST) level transmitters with redundant level indicators are provided on the main control board and on the auxiliary shutdown panel. Level is recorded for one 23.16 23.17 23.18

channel and the other channel provides high, low, and low-low level annunciation on the main control board. 23.19

The DWST temperature is maintained above a minimum temperature 23.20
automatically by a demineralized water storage tank electric heater 23.21
and circulating pump. Low temperature is alarmed on the main control 23.22
board.

Power for each train is supplied from a separate emergency bus. 23.23
Failure of any train does not degrade system capability to supply 23.24
sufficient feedwater to the steam generators.

Testing of actuated devices and associated control is performed 23.25
periodically to ensure reliability and performance. Bypass 23.26
indication is provided in the control room and is isolated such that
it does not degrade the protection function of the auxiliary 23.27
feedwater system.

Analysis 23.30

A. IEEE Standard 279-1971, Paragraph 4.2: 23.31

There are two motor-driven auxiliary feedwater pumps with 23.33
power supplied from separate emergency buses. The motor- 23.35
driven pumps each supply auxiliary feedwater to two steam
generators.

A turbine-driven auxiliary feedwater pump supplies auxiliary 23.36
feedwater to all four steam generators. The turbine is 23.37
supplied steam from three separate steam generators
(3RCS*SG1A, B, or D). Each steam supply line to the 23.38
auxiliary feedpump turbine has an air-operated valve
normally closed and a motor-operated valve normally open. 23.39
Each air-operated valve has two solenoid valves, each 23.40
supplied power from separate emergency dc buses. Loss of 23.41
power to either solenoid valve will vent air from the
associated air-operated valve and cause it to open. Two of 23.42
the normally open motor-operated valves are powered from the
Train A emergency bus and the other is powered from the 23.43
Train B emergency bus. No single failure at the system 23.44
level will prevent the auxiliary feedwater pumps from
supplying auxiliary feedwater to the steam generators. 23.45

Each auxiliary feedwater line from a motor-driven pump has a 23.46
normally open solenoid valve that fails open and a motor- 23.47
operated valve normally open that fails as is on loss of
power. The valves are powered from separate emergency 23.48
buses; the motor-operated valve is powered from the same
electrical train as the motor-driven pump. No single 23.50
failure prevents the control of auxiliary feedwater flow
from a motor-operated driven pump to a steam generator. 23.51

Each auxiliary feedwater line from the turbine-driven pump 23.52
has two normally open solenoid valves that fail open. The 23.53

valves are powered from separate emergency buses. No single failure will prevent the control of auxiliary feedwater flow to a steam generator. 23.54

Each auxiliary feedwater line to a steam generator has a Train A and Train B feedwater flow transmitter and indicator powered from separate power supplies. Two Train A and two Train B auxiliary feedwater flow indicators, one for each steam generator, are on the main control board and on the auxiliary shutdown panel. No single failure will prevent at least two auxiliary feedwater flow indicators from indicating at the main control board and at the auxiliary shutdown panels. There is a Train A and Train B steam generator level indicator for each steam generator on the main control board and at the auxiliary shutdown panel that can be used as backup indication for the flow indicators. 23.55 23.56 23.57 23.58 23.59 23.60 24.1 24.2

There are two trains of DWST level indicators on the main control board and at the auxiliary shutdown panel. The Train A level is recorded on the main control board. The trains are powered from separate buses. No single failure will prevent DWST level indication on the main control board or at the auxiliary shutdown panel. 24.3 24.4 24.5 24.6

No single failure at the system level will prevent auxiliary feedwater from being supplied to the steam generators. 24.7

B. IEEE Standard 279-1971, Paragraph 4.4: 24.10

Equipment qualifications are discussed in Sections 3.10 and 3.11. 24.12

C. IEEE Standard 279-1971, Paragraph 4.13: 24.16

The motor-driven auxiliary feedwater system bypass (Train A) annunciator is alarmed in the control room whenever any of the following conditions exist: 24.18 24.19

- Any auxiliary feedwater control and isolation valve for motor-driven pumps not fully open. 24.22
- Auxiliary feedwater pump ventilation system bypassed. 24.23
- Either feedpump motor loss of control power or breaker racked out. 24.24
- Motor control switch in pull to lock position. 24.25
- Manual bypass pushbutton depressed. 24.26

The auxiliary turbine-driven feedpump bypass (Train B) annunciator is alarmed in the control room whenever any of the following conditions exist: 24.28 24.29

- Any auxiliary feedwater control and isolation valve for turbine-driven pump not fully open. 24.31

- 3MSS*MOV17A, B, or D not fully open. 24.32

- Auxiliary feedwater pump ventilation system bypassed. 24.33

- Turbine-driven auxiliary feedwater pump manually tripped. 24.34

- Manual bypass pushbutton depressed. 24.35

D. IEEE Standard 279-1971, Paragraph 4.16: 24.38

Once an auxiliary feedwater pump start signal is received, the auxiliary feedwater pumps go to completion and run. Deliberate operator action must be taken to stop an auxiliary feedwater pump. The AUTO start signal must be cleared and the pumps stopped by manual controls. An exception is that the motor-driven pumps are stopped automatically by low suction pressure, low lube oil pressure, and are stopped automatically by electrical protection trips. The turbine-driven auxiliary feedwater pump is stopped automatically by low suction pressure, low lube oil pressure, and overspeed. 24.40 24.42 24.43 24.44 24.45 24.46 24.47

E. IEEE Standard 279-1971, Paragraph 4.17: 24.50

The motor-driven auxiliary feedwater pumps have manual controls on the main control board and at the switchgear. REMOTE/LOCAL control transfer switches at the switchgear are alarmed in the control room when LOCAL is selected. 24.52 24.54 24.55

The turbine-driven auxiliary feedwater pump steam supply valves have manual controls on the main control board and at the auxiliary shutdown panel. REMOTE/LOCAL control transfer switches on the transfer switch panels are alarmed in the control room when LOCAL is selected. 24.56 24.58 24.59

The turbine-driven auxiliary feedwater pump speed changer has manual controls on the main control board. REMOTE/LOCAL control transfer switches on the transfer switch panels are alarmed in the control room when LOCAL is selected. 24.60 25.1 25.2

The auxiliary feedwater control and isolation valves have manual controls on the main control board and at the shutdown panels. REMOTE/LOCAL control transfer switches on the transfer switch panels are alarmed in the control room when LOCAL is selected. 25.3 25.5 25.6

F. IEEE Standard 279-1971, Paragraph 4.10: 25.8

During the instrument functional test, the instrumentation setponts and their operability are checked. The test to 25.10 25.12

verify the automatic response of the system is performed during each refueling period. Correct settings of temperature, flow, and level instrumentation are verified by applying a simulated signal.

One motor-driven feedwater pump at a time is taken out of service and periodically tested in accordance with the Technical Specifications in Chapter 16.

This testing will consist of manually starting the pump during normal surveillance of the system or the breaker for the pump will be racked out. Once the pump is running or the breaker is racked out, the AUTO start and tripping is verified using the emergency generator load sequencer with safety signals generated internally or externally to the sequencer.

Refer to Section 10.4.9.4 for testing of turbine-driven auxiliary feedwater pump.

The auxiliary feedwater control and isolation valves are periodically tested in accordance with the Technical Specifications in Chapter 16. The valves are operated manually with controls on the main control board and at the auxiliary shutdown panel.

The steam supply valves for the turbine-driven pump are periodically tested in accordance with the Technical Specifications in Chapter 16.

G. IEEE Standard 279-1971, Paragraphs 4.9 and 4.10:

The DWST level transmitters, auxiliary feedwater flow transmitters, and auxiliary feedpump suction pressure transmitters are periodically tested in accordance with the Technical Specifications in Chapter 16. The transmitters and pressure switches are tested by injecting a simulated signal into the instrumentation loop.

ESF Filtration System

The ESF filtration system consists of the auxiliary building filter system (ABFS) which is described in Section 9.4.3 and its flow diagram is shown on Figure 9.4-2.

The ABFS consists of two ABFS exhaust fans, each supplied from a separate emergency bus, two main filter banks, and the associated ductwork and dampers.

The following areas are exhausted by the ABFS:

- Waste disposal building

- Auxiliary building 25.50
- Containment purge air system 25.51
- Charging pump and component cooling water pump area 25.52

Exhaust from the areas can be directed through the auxiliary building 25.54
filters or bypassed to atmosphere. Both paths of exhaust are 25.55
provided with redundant air-operated dampers with solenoid pilot
valves. With the exception of the filter inlet from the charging 25.56
pump and component cooling water pump area, the redundant dampers are 25.57
in series and fail closed on loss of power or air.

The filter inlet dampers from the charging pump and component cooling 25.58
water area are in parallel and fail open on loss of power or air. 25.59
Normally, the exhaust from the areas is bypassed to the atmosphere. 25.60
However, the exhaust from any or all of the areas can be manually 26.1
directed through the filters. On receipt of a SIS or LOP signal, 26.2
filter inlet dampers from the charging pump and component cooling
water pump area are opened automatically. All other inlet dampers 26.4
and filter bypass to atmosphere dampers are closed on receipt of a
SIS, or by manual operation, the Train A filter inlet and exhaust fan 26.5
discharge dampers open and start the Train A filter exhaust fan.
Train B is then on standby. The safeguard signal is initiated by a 26.7
SIS or CDA signal. During LOP, the exhaust fans are sequenced in 26.8
accordance with the emergency generator load sequence. The standby 26.9
filter train is started automatically on a low air flow signal from
the operating train.

During refueling and in the event of high radiation from one of the 26.10
areas exhausted by the ABFS, the exhaust flows are manually diverted 26.11
to the auxiliary building filter bank.

The fuel building filter banks are normally bypassed by the 26.12
unfiltered exhaust fan. During refueling and in the event of high 26.13
radiation, the fuel building exhaust is manually diverted to the fuel
building filter bank. Either Train A or Train B is operated with the 26.15
other train in standby.

The auxiliary building and fuel building filter banks have manual 26.16
controls located on the main heating and ventilation panel in the 26.17
control room and at the switchgear. REMOTE/LOCAL control selector 26.18
switches are provided at the switchgear. An annunciator is alarmed 26.19
in the control room when LOCAL control is selected.

High differential pressure across the prefilter, carbon adsorber, 26.20
and/or HEPA filter of each filter bank is alarmed in the control 26.21
room.

Analysis 26.24

A. IEEE Standard 279-1971, Paragraph 4.2: 26.25

There are two redundant ESF filtration Trains (A and B). 26.27
The equipment in Train A is supplied from one emergency bus 26.29
and Train B equipment is supplied from a separate emergency 26.30
bus. No single failure at the system level will prevent the 26.31
ESF filtration system from filtering the air system during
an accident. 26.32

B. IEEE Standard 279-1971, Paragraph 4.4: 26.35

Equipment qualifications are discussed in Sections 3.10 and 26.37
3.11.

C. IEEE Standard 279-1971, Paragraph 4.13: 26.41

A charging pump high pressure safety injection system bypass 26.43
annunciator is alarmed in the control room whenever any of
the following conditions exist (Train A or B): 26.44

- Auxiliary building filter system fan in pull to lock 26.47
position.

- Auxiliary building filter system fan loss of control 26.48
power or breaker racked out.

- Auxiliary building filter system fan outlet damper loss 26.49
of power or circuit breaker open.

D. IEEE Standard 279-1971, Paragraph 4.16: 26.52

Once initiated by a safety signal, the ESF filtration system 26.54
will go to completion. Return to normal operation requres 26.56
deliberate operator action by resetting safety signals and
using manual controls.

E. IEEE Standard 279-1971, Paragraph 4.17: 26.59

The auxiliary building and fuel building filter banks have 27.1
manual controls located on the main heating and ventilation
panel in the control room and at the switchgear. 27.2
REMOTE/LOCAL control selector switches are provided at the 27.4
switchgear. An annunciator is alarmed in the control room 27.5
when LOCAL control is selected.

F. IEEE Standard 279-1971, Paragraph 4.10: 27.8

The ESF filtration system is periodically tested in 27.10
accordance with the Technical Specifications in Chapter 16.

During the instrument functional test, the instrumentation 27.12
setpoints are checked. The operability of the controls and 27.13

indication is verified when the system is in test. The test to verify the auxiliary response of the system is performed during each refueling period. Correct settings of temperature and flow instrumentation are verified by applying a simulated signal. AUTO start is verified using the emergency load sequencer with safety signals generated internally or externally to the sequencer.

Essential Auxiliary Support Systems

Auxiliary support systems that are required to function upon initiation of ESFAS are listed in Table 7.3-11. A summary description of these systems are provided in this section. Additional details can be found in the referenced sections.

Service Water System

The service water system is described in Section 9.2.1 and its flow diagram is shown on Figure 9.2-1. For the purpose of instrumentation and control application, a recapitulation of the system design follows.

Two service water headers, each supplied by two service water pumps, are provided. The power for the two-train design is supplied from two separate emergency buses as shown on Figure 8.1-1. Either of the two redundant service water system trains has the capability to supply sufficient quantities of cooling water to the required equipment for safe shutdown. For the emergency mode of operation, the supply lines to the nonsafety related equipment are isolated by automatic closure of isolation valves. A LOP, CDA, or service water low header pressure signal automatically closes isolation valves in the supply line to the turbine plant component cooling heat exchangers. A LOP or CDA signal also automatically closes isolation valves in the supply lines to the circulating water pumps' lube water and chemical feed chlorination system. In addition to those closed on a LOP or CDA signal, the CDA signal automatically closes the isolation valves in the supply lines to the reactor plant component cooling heat exchangers and automatically opens supply valves to the containment recirculation coolers. A LOP, SIS, or CDA signal causes automatic opening of the air-operated valves in the outlet lines from the diesel engine coolers. A LOP signal starts service water booster pumps that supply the MCC and rod control area air-conditioning units.

Continuous radiation monitoring is provided in the service water discharge headers (Section 11.5). Following a DBA, continuous radiation monitoring (Section 11.5) is provided in the discharge of each train of containment recirculation coolers. Each containment recirculation cooler has a remotely-operated valve in its supply and discharge line. On a high radiation alarm, the operator can isolate the affected containment recirculation cooler train.

Control switches and indicating lights for the service water pump motors are provided on the main control board and at the switchgear.

REMOTE/LOCAL control selector switches and LEAD/FOLLOW pump selector switches are located at the switchgear. An annunciator is alarmed in the control room when LOCAL control is selected. One service water pump in each train is started manually. The standby pump is started automatically by a pressure switch detecting low discharge pressure in the associated header. The action of these pressure switches is blocked by a LOP signal.

The service water pumps are operated in the following manner under the indicated accident conditions:

1. LOCA with offsite power available. All pumps that are operating prior to the accident continue to operate.

2. LOCA coincident with loss of offsite power. Two pumps, one on each emergency bus, start automatically in accordance with the emergency generator loading sequence. Should one of the two service water pumps fail to start, the redundant pump on the same emergency bus starts automatically after a time delay.

3. Loss-of-offsite power. Two pumps, one of each emergency bus, start automatically in accordance with the emergency generator loading sequence. Should one of the two service water pumps fail to start, the redundant pump on the same emergency bus starts automatically after a time delay.

The service water system is also a cooling source for the control building chilled water system. A three-way valve in the chiller condenser outlet line and a temperature controller in the booster pump discharge line provide temperature control for the chilled water system condenser by means of a controlled bypass from the three-way valve to the booster pump suction.

The control building chilled water system service water booster pumps are interlocked to start and stop with the associated control building chilled water pump. Pressure in the service water headers is indicated in the control room. For reliability purposes, correct operation of the pressure measuring loop in the service water header is verified during operation of the service water system by valving the pressure transmitter out of service and applying a simulated signal. Similarly, the header low pressure annunciation is also verified during normal operation. These tests verify correct operation of the loops and of the indications provided in the control room.

Service water discharge flow indicators and high/low flow annunciators are provided on the main control board for the containment recirculation coolers and reactor plant component cooling heat exchangers. High/low service water outlet flow annunciators are provided for the diesel engine jacket water coolers.

Correct operation of flow measuring loops is verified by valving the flow transmitter out of service and applying a simulated signal.

The operability of the service water system controls and indications common for both normal and emergency mode of operation is verified by their normal use. Instrumentation provided for the containment recirculation coolers is tested in conjection with the containment recirculation system test.

Bypass indication is provided in the control room for the service water system.

Analysis

A. IEEE Standard 279-1971, Paragraph 4.2:

There are two redundant service water trains (A and B) and there are two service water pumps in each train. Normally one pump in each train is running with the other in standby. The pumps in Train A are supplied from one emergency bus and Train B pumps are supplied from a separate emergency bus. No single failure at the system level will prevent the service water pumps from supplying service water.

B. IEEE Standard 279-1971, Paragraph 4.4:

Equipment qualifications are discussed in Sections 3.10 and 3.11.

C. IEEE Standard 279-1971, Paragraph 4.13:

A bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B):

- Service water pump loss of control power or breaker racked out or control switch in pull to lock and the other pump in the same train with loss of control power or breaker racked out or control switch in pull to lock.
- Service water pump area air conditioning unit circuit breaker open or loss of control power.
- Service water pump area air conditioning unit control switch in pull to lock.
- Manual bypass pushbutton depressed.

D. IEEE Standard 279-1971, Paragraph 4.16:

Once a safety signal is initiated, the lead service water pump in each Train (A and B) will start. In the event that the lead pump does not start, the follow pump will start one-half second later. To stop a running service water pump requires deliberate operator action; the safety signals must be reset and manual controls used to stop the pump.

E. IEEE Standard 279-1971, Paragraph 4.17:

The service water pumps have manual controls located on the main control board and at the switchgear. REMOTE/LOCAL control selector switches at the switchgear are alarmed in the control room when LOCAL control is selected.

F. IEEE Standard 279-1971, Paragraph 4.10:

One service water pump at a time can be taken out of service and periodically tested in accordance with the Technical Specifications in Chapter 16.

This testing will consist of manually starting the pump during normal surveillance of the system or the breaker for the pump will be racked out. Once the pump is running or the breaker is racked out, the AUTO start and tripping is verified using the emergency generator load sequencer with safety signals generated internally or externally to the sequencer.

During the instrument functional test, the instrumentation setpoints and their operability are checked. The operability of the controls and indications is verified when the system is in test. The test to verify the automatic response of the system is performed during each refueling period. Correct settings of temperature and flow instrumentation are verified by applying a simulated signal.

Reactor Plant Component Cooling Water System

The reactor plant component cooling water system design is described in Section 9.2.2.1 and the flow diagram is shown on Figure 9.2-2.

Manual controls and indicating lights for the reactor plant component cooling water pumps are provided in the control room and at the switchgear. REMOTE/LOCAL control selector switches are provided at the switchgear; an annunciator is alarmed in the control room when LOCAL control is selected. Normally, two pumps are operating with the third pump on stand-by in Train B. Three pump motor breakers are supplied for four breaker cubicles - two for each train. The pumps for Trains A and B are normally racked into their respective cubicles, with the third pump breaker racked into its Train B cubicle. The third pump may be operated on Train A by first racking its breaker out of Train B and then racking it into the Train A cubicle. An electrical interlock prevents simultaneous operation of two pumps on the same train. A keylock switch is provided which allows the third pump to operate on one train or the other, but not on both at once. Motor overcurrent and auto trip are alarmed in the control room. Status lights and bypass indication are provided in the control room. Power to Trains A and B reactor plant component cooling water pump motors is supplied from separate emergency buses.

The reactor plant component cooling pumps are started automatically by an SIS or LOP signal. The pumps are sequenced on by the emergency generator load sequencer when an LOP signal exists.

Redundant level switches located on the surge tank for the reactor plant component cooling water system are set to detect a sudden drop in reactor plant component cooling water system surge tank level, which would result from a rupture of nonsafety-related system piping. These level switches automatically close isolation valves, thus isolating the system's safety-related portions from the nonsafety-related.

All supply lines to reactor plant component cooling water users, both safety-related and nonsafety-related, are provided with flow indicators and high flow alarms in the control room. Flow is totalled by the plant computer. Remote temperature indicators and high temperature alarms are provided in the suction lines of each reactor plant component cooling pump. Each compartment of the reactor plant component cooling water surge tank is provided with a level sensing channel. The makeup to the surge tank is automatically controlled by level in the compartment. The level in each compartment is indicated, and low and high level extremes are alarmed in the control room.

A radiation monitor is utilized to monitor Train A or Train B outlet from the reactor plant component cooling water heat exchangers. Indication and alarm are provided locally; and indication, recording, and alarm are provided in the control room (Section 11.5).

The containment isolation valves in the reactor plant component cooling water lines serving the equipment inside the containment structure are closed automatically on receipt of a CIB signal. Trains A and B cross-connect valves inside the containment are closed automatically on receipt of an SIS or surge tank low-low-low level signal.

Following a LOP or CIA signal, the cooling water source for the nonsafety-related components inside the containment structure is automatically transferred from the chilled water system to the reactor plant component cooling water system.

ESF status lights are provided in the control room for the reactor plant component cooling water system valves that receive a safety signal. Reactor plant component cooling water system bypass alarms are provided on the main control board.

A. Analysis of Reactor Plant Component Cooling Water System 30.34

Analysis 30.36

A. IEEE Standard 279-1971, Paragraph 4.2: 30.38

The reactor plant component cooling water system is divided into two separate, redundant mechanical and electrical trains. The system is normally cross-connected; the cross-connect valves are closed automatically by an SIS supplied or surge tank low-low-low level signal. The cross-connect valves are air-operated and fail close on loss of air or loss of power to the associated solenoid valve. No single failure at the system level will prevent the system from supplying reactor plant component cooling water for at least one train. 30.40 30.43 30.45 30.47 30.48

B. IEEE Standard 279-1971, Paragraph 4.4: 30.51

Equipment qualifications are discussed in Sections 3.10 and 3.11. 30.53

C. IEEE Standard 279-1971, Paragraph 4.13: 30.57

A reactor plant component cooling system bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B): 30.59 30.60

- Reactor plant component cooling pump (A or B) control switch in pull to lock or circuit breaker racked out or loss of control power and reactor plant component cooling pump (C) control switch in pull to lock or circuit breaker racked out or loss of control power. 31.3 31.4 31.5
- Containment isolation valve not fully open. 31.6
- Service water system bypassed. 31.7
- Reactor plant component cooling heat exchanger service water supply valve not fully open. 31.8
- Manual bypass pushbutton depressed. 31.9

D. IEEE Standard 279-1971, Paragraph 4.16: 31.12

Once an SIS is received, the reactor plant component cooling pumps are started automatically. When a LOP exists, the pumps are automatically started by the emergency generator load sequencer. Deliberate operator action must be taken to stop a pump. The SIS and LOP must be reset and manual control used to stop a pump. 31.14 31.16 31.17 31.18

The containment air recirculation cooling coil supply and return valves are opened automatically by a LOP or CIA 31.19

signal. The LOP and CIA must be reset to close the valves manually. The valves close automatically on reactor plant component cooling water surge tank low-low-low level. The surge tank low-low-low level signal must be cleared and the CLOSE/AUTO pushbutton depressed before the valves can be opened automatically or manually. 31.21 31.22 31.23 31.24

The nonsafety header supply and return isolation valves close automatically on receipt of a CIA or reactor plant component cooling surge tank low-low-low level signal. The CIA must be reset and the surge tank low-low-low level signal cleared and manual controls used to open the valves. 31.25 31.27

The reactor plant component cooling cross-connect valves close automatically on receipt of a SIS or reactor plant component cooling surge tank low-low-low level signal. The SIS must be reset and the surge tank low-low-low level signal cleared and manual controls used to open the valves. 31.28 31.30

The containment isolation valves close automatically on receipt of a CIB signal. The CDA signal must be reset and manual controls used to open the valves. 31.31 31.32

The reactor plant component cooling heat exchanger service water supply valves close automatically on receipt of a CDA signal. The CDA signal must be reset and manual controls used to open the valves. 31.33 31.35

E. IEEE Standard 279-1971, Paragraph 4.10: 31.38

The reactor plant component cooling system is periodically tested in accordance with the Technical Specifications in Chapter 16. 31.40 31.41

The operability of the reactor plant component cooling water system controls and indications is verified during the instrument functional test. Also, during this test the instrumentation setpoints and their operability are checked. The test to verify the automatic response of the system is performed during each refueling period. Correct settings of temperature, flow, and level instrumentation are verified by applying a simulated signal. 31.43 31.45 31.46 31.47

F. IEEE Standard 279-1971, Paragraph 4.17: 31.50

Controls and indicators are provided in the control room for manual operation of the reactor plant component cooling water system. REMOTE/LOCAL control selector switches are provided for the reactor plant component cooling water pumps outside the control room at the switchgear. Annunciator is alarmed in the control room when LOCAL control is selected. 31.52 31.55 31.57

Chilled Water 31.59

Description of instrumentation and controls is provided in Section 9.4.1.5. 32.1

Electrical 32.5

Description of the onsite electrical system is found in FSAR Section 8.3. 32.7

Emergency Generator Load Sequencer 32.11

The emergency generator loading sequencer (EGLS) is a solid-state digital system which provides relay contact outputs to shed loads, block manual starts, and sequentially load the plant safety buses during emergency conditions. The primary purpose of the EGLS is to automatically control the loading of the safety buses when a loss of offsite power has occurred and the buses are being reenergized by the emergency diesel generator. 32.13 32.15 32.16 32.17

The EGLS accepts bus undervoltage (BUV), SIS, containment depressurization (CDA), recirculation (RECIRC), auxiliary reserve breaker (AR BKR) status, and diesel generator breaker (DG BKR) status input signals in the form of contact closures and will provide a predetermined sequence of outputs. 32.18 32.19 32.20

The overall sequencing system is comprised of two EGLS cabinets, which are identical except for markings. 32.21

The EGLS has seven operating modes. Five of these modes are for plant emergency conditions which involve a loss of offsite power. The other two are for plant emergency conditions which do not involve a loss of offsite power. The modes, in terms of which EGLS inputs are activated, are as follows. 32.23 32.24 32.25

1. SIS only 32.27
2. CDA only or SIS and CDA 32.28
3. LOP only 32.29
4. SIS and LOP 32.30
5. CDA and LOP or SIS and CDA and LOP 32.31
6. SIS, RECIRC, and LOP 32.32
7. CDA or SIS and CDA, RECIRC, and LOP 32.33

The modes are prioritized such that a CDA mode will always take precedence over a SIS mode when both inputs are present and such that a LOP mode will always take precedence over a non-LOP mode. 32.35 32.36

In each of the LOP operating modes, the EGLS first recognizes a loss of power on the plant safety buses and immediately generates LOP and manual start block (MSB) output signals to plant safety equipment. These signals effectively strip the bus and temporarily inhibit the operator from restarting any loads. This allows the diesel generator time to start, achieve proper voltage and frequency and, via the DG BKR, be connected to the plant safety bus without incurring adverse loading conditions. Upon receiving a signal confirming that the DG BKR has closed, the EGLS will begin generating time sequenced safeguard sequencer start (SSS) and manual trip block (MTB) signals to plant equipment. The SSS and MTB signals, once initiated, are maintained until the EGLS is reset or a change in operating mode occurs. The EGLS automatically terminates individual LOP signals associated with the loads being started and terminates the remaining LOP signals and MSB signals automatically, 40 seconds after the DG BKR has closed. Should a SIS or CDA input occur without a LOP, the appropriate SSS and MTB signals are generated immediately without time sequencing, and the LOP and MSB outputs remain reset. The MTB signal inhibits the operator from retripping loads once they have been automatically started.

LOP outputs also are generated for plant equipment which does not have an associated EGLS SSS output signal. In some cases, the LOP outputs are terminated at the end of the 40-second period. In other cases, the LOP outputs are not terminated until the EGLS is manually reset. In some of the cases, the LOP outputs are also generated by a SIS only or CDA only input.

The EGLS also provides trip outputs to the AR BKRs. The AR BKR trip output is generated by either a SIS or CDA input, but only if the AR BKRs are already open. The output response of the EGLS, except for the AR BKR trip signal and two specific loads, to a SIS or CDA input, is delayed approximately 5 seconds if the AR BKRs are open. The AR BKR trip signal remains reset and the EGLS response delay is bypassed if the AR BKRs are closed when a SIS or CDA input occurs.

Initiation of the RECIRC and LOP operating modes differs from the other LOP operating modes in as much as that during recirculation, the SIS or CDA input must have occurred and been reset prior to the loss of power. Otherwise, even though the RECIRC input is present, the EGLS will respond in a SIS and LOP or CDA and LOP operating mode. Internal memories, which must be manually reset, retain the information necessary to allow the EGLS to differentiate between RECIRC and non-RECIRC operating modes.

Station LOP and sequencer LOP memories, which also must be manually reset, are used to retain information concerning the initial loss of power and reenergization of the bus by the diesel generator. Two memories are employed to prevent the EGLS from responding to transient voltage dips appearing on the bus during loading. Normally, the EGLS would not respond to a second loss of power if both memories had not been reset, but circuitry in the EGLS provides a 3-second window between the sequencer LOP test and station LOP

reset during which the EGLS will respond to a second or subsequent LOP occurring during reset procedures. 33.12

Analysis 33.15

A. IEEE Standard 279-1971, Paragraph 4.2 33.16

The emergency generator load sequencers are divided into two separate, redundant mechanical and electrical trains. No signal failure at the system level will prevent the system from sequentially loading the plant safety buses during emergency conditions. 33.18 33.20 33.21

B. IEEE Standard 279-1971, Paragraph 4.4: 33.24

Equipment qualifications are discussed in Sections 3.10 and 3.11. 33.26

C. IEEE Standard 279-1971, Paragraph 4.13: 33.30

An emergency generator load sequencer bypass annunciator will alarm in the control room whenever any of the following conditions exist (Train A or B): 33.32 33.33

- System is in manual Test 2. 33.36
- Control power not available. 33.37
- Manual bypass pushbutton depressed. 33.38

D. IEEE Standard 279-1971, Paragraph 4.10: 33.41

The emergency generator load sequencer is tested periodically in accordance with the Technical Specifications in Chapter 16. 33.43 33.44

The following is a description of the various test modes that will be used to verify the operability of the EGLS. 33.47

Auto Test 33.49

The auto test circuit (ATC) is an EGLS subsystem that is contained within the sequencer panel. The ATC is designed to run continuously having 45 separate test states. Each test state is 10 m sec in duration with actual testing being performed during the last 1 m sec of each test state. An exception to this is three test states where the test state timer is interrupted long enough to verify the operability of the normal frequency clocks. 33.50 33.52 33.53 33.55 33.56

The ATC verifies two basic types of EGLS responses. First, that no outputs occur when no Auto Test Inputs (ATIs) are applied. Second, that the proper outputs occur when ATIs are applied. 33.58 33.59

Each odd numbered test state is used to verify that the proper output patterns occur when various combinations of ATIs are injected into the front end (input buffers) of the sequencer logic. Conversely, each even numbered test state verifies that no outputs occur when no ATIs are applied. The even test states also verify that the EGLS was reset following the last odd numbered test.

For each test, the ATC makes the assumption that the sequencer will fail. At the start of each test, a delayed EGLS fault signal is generated. This, in effect, leaves the sequencer with 990 μsec in which to properly respond in order to reset the fault delay timer. A successful fault delay reset will allow the ATC to begin the next test state. If a fault is detected, the ATC stops testing the EGLS and provides main board annunciation. The ATC display on the EGLS front panel indicates the specific test state where the fault occured.

The input and output relays are never actuated by the ATC and, hence, are not verified as operable by the ATC. The input relays will be tested for system operability during the EGLS integrated test. This test will be performed at each refueling cycle. The output relays will be tested quarterly by starting all the individual loads through the sequencer, utilizing the output relays. In addition, if a real plant input is received by the EGLS requiring action, the ATC is automatically faulted to prevent it from interfering with EGLS operation.

In summation, the ATC verifies, on a continuing basis, all critical electrical paths in which a failure would prevent the EGLS from performing its complete safety function. The ATC will be used to satisfy the monthly actuation logic surveillance requirement.

Auto Test Test

An auto test test panel is supplied with the EGLS system as test equipment that will be used on a quarterly basis to verify the operability of the ATC.

The auto test test panel has the ability to simulate an EGLS failure for ATC operational verification (the ability of the ATC to identify a failure). This is accomplished by creating auto test outputs (ATOs) when they should not occur or by inhibiting ATOs when they should occur. Every auto test fault circuit can be verified using the auto test test panel.

Manual Test Features

Mode 1

The manual test features provide a means to simulate EGLS inputs and verify response to those inputs. When initiated, Manual Test 1 inhibits all sequencer outputs except MSBs. Each individual load, however, may be selectively unblocked using its associated TEST/INHIBIT switch; i.e., placing the switch into the TEST position.

This allows the option of testing the EGLS logic including sequence times or additionally testing selected output relay(s) by actually starting the loads. The latter provides the means to satisfy the requirement of periodically testing safety-related loads.

The inputs to the EGLS are provided by front panel pushbuttons for LOP, SIS, CDA, and RECIRC. These inputs can be applied at any time and in any order during a test to obtain any mode of operation desired. A DG breaker pushbutton is not provided; rather, a simulated DG breaker closure is automatically generated 9 seconds after the LOP pushbutton is pressed.

Testing the EGLS using Manual Test 1 does not remove the sequencer from service. If at any time during testing a real input is received, the EGLS resets itself to normal operation responding to the input signal regardless of the TEST/INHIBIT switch positions.

Mode 2

Manual Test 2 is identical to Manual Test 1 except that the EGLS is not reset when a real input signal is received. Rather, the EGLS responds to the input-condition taking into account the individual load TEST/INHIBIT switches. Manual Test 2 provides the ability to perform integrated systems testing, inhibiting loads that are not desirable to operate.

EGLS Integrated Test

This is a factory duplicated test that will be performed each refueling to verify system operation by actuating the input relays and monitoring the output relays for proper response. One contact from each relay in the EGLS cabinet is monitored by a data logger that documents all inputs and outputs and the time that each relay operated relative to the beginning of the test. The tests that will be included within the EGLS integrated test are listed below.

LOP	CDA RECIRC only
SIS and LOP	SIS followed by CDA
CDA and LOP	LOP followed by CDA
SIS RECIRC and LOP	LOP followed by SIS
CDA RECIRC and LOP	LOP followed by SIS RECIRC
SIS only	LOP followed by CDA RECIRC
CDA only	SIS and DG breaker without LOP
SIS RECIRC only	SIS followed by LOP

Emergency Generator Fuel Oil System

The emergency generator fuel oil system design and description are given in Section 9.5.4 and the flow diagram is shown on Figure 9.5-2.

Each of the two emergency generator fuel oil storage tanks is provided with fuel oil level indication locally and on the emergency generator panel. A low fuel oil level is alarmed on the emergency

generator panel. Fuel oil moisture content will be tested as discussed in Section 9.5.4. 35.31

Each of the two emergency generator fuel oil day tanks is provided with level switches to automatically start and stop the associated emergency generator fuel oil transfer pumps in a LEAD-FOLLOW arrangement. The LEAD-FOLLOW emergency generator fuel oil transfer pumps for each tank are powered from the associated emergency bus. The selected "lead" emergency generator fuel oil transfer pump is started when its associated level switch in the emergency fuel oil day tank reaches a predetermined level. If the "lead" emergency generator fuel oil transfer pump fails to start and the oil level continues to decrease, the "follow" emergency generator fuel oil transfer pump is started when the fuel oil level reaches the predetermined low level switch setting. At this level, low level alarm is on the emergency generator panel to inform the operator of a malfunction. The emergency generator fuel oil transfer pumps stop automatically at a predetermined day tank high level. In addition to the level switches for pump control, remote manual pump controls provided on the emergency generator panel. 35.32 35.33 35.34 35.35 35.36 35.37 35.38 35.39 35.41 35.42 35.43 35.44

At a predetermined level, an emergency generator day tank level switch actuates a Low-Low level alarm on the emergency generator panel. A high level switch is actuated at a predetermined emergency generator fuel oil day tank level to alarm on the the emergency generator panel. 35.45 35.46 35.47 35.48

Fuel oil level in each emergency generator fuel oil day tank is indicated on the emergency generator panel and on the main control board. 35.49 35.50

To annunciate fouling on the in-line emergency generator fuel oil strainers, differential pressure alarms are provided on the emergency generator panel. 35.51 35.52

Fuel oil transfer pump discharge pressure fuel oil day tank, and storage tank levels are monitored by the plant computer. 35.53 35.54

An emergency generator panel trouble annunciator is alarmed in the control room when any alarm exists on the emergency generator panel. 35.55 35.56

Level controls and indicators are tested in conjunction with the diesel engine test described in Section 8.3. The frequency of this test is given in Chapter 16. 35.57 35.58

Emergency Diesel Engine Cooling Water System 36.1

The emergency diesel engine cooling water system is described in Section 9.5.5 and its flow diagram is shown on Figure 9.5-3. 36.3 36.4

The emergency diesel engine cooling water system has low pressure, high temperature, and low temperature alarm switches. A low level alarm switch is on the overhead expansion tank. 36.6 36.8

Annunciators on the emergency generator panels alarm when the following conditions exist:

- Emergency diesel generator jacket coolant pressure low.
- Emergency diesel generator jacket cooling temperature high.
- Emergency diesel generator jacket coolant temperature low.
- Emergency diesel generator fresh water expansion tank level low.

A trouble alarm for each emergency diesel generator panel on the main control board is alarmed whenever the associated panel has an alarm on it.

Temperature regulating valves controlled by temperature controllers maintain the engine cooling water at a preset temperature when the engine is running.

An electric heater controlled by a temperature controller has a local AUTO/OFF control switch. The heater is energized when the standby jacket cooling pump is running and jacket coolant temperature is less than a preset temperature and the control switch is in AUTO. The heater is deenergized automatically when the standby jacket coolant pump is stopped or the jacket coolant temperature is greater than a preset temperature. The heater is deenergized manually by placing control switch in the OFF position.

The standby jacket coolant pump has a local START/STOP/AUTO control switch. The pump is started automatically when engine speed is less than a preset speed and the control switch is AUTO or stopped when engine speed is above a preset speed. The pump can be stopped or started manually with the control switch.

Emergency Generator Starting Air System

The emergency generator starting air system is described in Section 9.5.6 and its flow diagram is shown on Figure 9.5-3.

There are two air compressors and separate air systems for each diesel generator. Each air compressor is equipped with a manual control switch and indicator lights, located on the motor control center. A pressure switch on the air receiver tank automatically starts and stops each compressor. The switch is set to start the compressor when the tank pressure drops below the low setpoint pressure of 375 psig and to stop the compressor when the pressure reaches the high setpoint pressure of 425 psig. Relief valves on the receiver tanks and at each compressor discharge are set at 450 psig to protect the system from overpressurization. The compressor motor is also protected against thermal overload.

If the receiver tank pressure drops to the low-low setpoint pressure of 350 psig, the condition actuates an alarm on the respective

emergency generator panel and the emergency generator trouble alarm on the main control board. Each receiver tank is also provided with a local pressure indicator. 36.47

A control air system is connected to the starting air system (Figure 9.5-3) to provide a source of air for operation of different components in the jacket coolant temperature control system and the shutdown control system. Refer to Section 9.5.6.5 for a discussion of components supplied by air. 36.48 36.49 36.50

Emergency Diesel Engine Lubrication System 36.53

The emergency diesel engine lubrication system is described in Section 9.5.7 and its flow diagram is shown on Figure 9.5-3. 36.55 36.56

A low lubricating oil level alarm is provided to alert personnel when the lubricating oil level in the sump falls below the manufacturer's recommended minimum level. 36.58 36.59

A high-pressure alarm is provided to alert personnel when the pressure in the crankcase exceeds the manufacturer's recommended high-pressure limit. 36.60 37.1

A high-level alarm switch is provided to alert personnel when the oil level in the separate rocker arm lubricating oil tank exceeds the manufacturer's recommended maximum. 37.2 37.3

A low-pressure alarm is provided to alert personnel when the rocker arm lubricating oil pressure falls below the manufacturer's recommended minimum. 37.4 37.5

Actuation of the low lube oil pressure switch will energize an annunciator and give an alarm that the lubricating oil pressure has reached a dangerously low level. Actuation of any two of these low lube oil pressure switches will shut down the engine. 37.6 37.7 37.8

High- and low-temperature alarms are provided to alert personnel when the oil temperature rises above or falls below the operating range recommended by the manufacturer. 37.9 37.10

The following annunciators are on each emergency generator level panel: 37.11

- Moisture detector circulating pump motor thermal overload or loss of control power. 37.13
- Lube oil moisture content high. 37.14
- Rocker arm lube oil pressure low. 37.15
- Crankcase pressure high. 37.16
- Lube oil sump temperature low. 37.17

- Lube oil sump level low. 37.18
- Lube oil temperature high. 37.19
- Rocker arm reservoir level high. 37.20
- Lube oil pressure low. 37.21

An emergency generator local panel trouble annunciator for each panel is located on the main control board and is alarmed whenever a respective local panel annunciator is alarmed. 37.23 37.24

The prelube oil filter pump has a local STOP/START control switch and the motor has thermal overload protection. The rocker arm prelube oil pump has a local STOP/START control switch and a remote STOP/START control switch on the main control board. The motor has thermal overload protection. 37.25 37.27 37.29

The emergency generator prelube oil heater has a local OFF/AUTO control switch. When in AUTO, the heater is automatically energized when the following conditions exist: 37.30 37.31

- Emergency generator speed below a preset setpoint. 37.33
- Lube oil temperature below a preset temperature. 37.34
- Prelube oil filter pump running. 37.35

The emergency generator prelube oil heater is deenergized when any of the above conditions is not met or when the control switch is in OFF. 37.37 37.38

Emergency Generator Combustion Air Intake and Exhaust System 37.41

The emergency generator combustion air intake and exhaust system is described in Section 9.5.8 and its flow diagram is shown on Figure 9.5-3. 37.43 37.44

The combustion air intake and exhaust sytem is available when the diesel engine is started. 37.46

When air is drawn in through the filter and silencer, a manometer measures pressure drop. 37.47

Green (running) and red (stopped) status lights are provided in the main control room for the diesel engine. 37.48

Annunciation is provided in the local and main control board for high pressure drop across the filter. 37.49

A recorder is provided for high opacity in exhaust gases. 37.50

A pressure indicator is provided locally for inlet pressure to the diesel. 37.51

An exhaust pyrometer is provided, complete with multi-circuit selector switch and thermocouples for each exhaust, turbocharger nozzle, and common exhaust.

Analysis

A. IEEE Standard 279-1971, Paragraph 4.2:

The emergency generator fuel oil system is divided into two separate, redundant mechanical and electrical trains. This dual train concept provides sufficient redundancy to prevent a single failure from impairing the systems capability to supply fuel oil to at least one of the diesel engines.

Each emergency generator has the following associated systems: emergency diesel generator engine cooling water system, starting air system, engine lubrication system, and combustion air intake and exhaust system. The electrical equipment for these associated systems is supplied from separate emergency buses. The electrical equipment is not safety grade and is disconnected from the emergency buses automatically by a SIS, CDA, or LOP signal to prevent degrading the emergency buses. The equipment is not required for emergency generator operation. Each emergency generator and its associated system are completely independent and separate from each other. No single failure at the system level can prevent the emergency generators from providing power to at least one emergency bus.

B. IEEE Standard 279-1971, Paragraph 4.4:

Equipment qualifications are discussed in Sections 3.10 and 3.11. Exceptions to equipment qualifications are:

- Emergency generator air compressors.
- Emergency generator standby jacket coolant pump and heater.
- Prelube oil filter pump and heater.
- Rocker arm prelube oil pump.

C. IEEE Standard 279-1971, Paragraph 4.13:

An emergency diesel generator system bypass annunciator is alarmed in the control room whenever any of the following conditions exist:

- Emergency generator breaker racked out or loss of control power.
- Emergency generator air compressor loss of control power or motor thermal overload.

- Emergency generator crankcase vacuum pump loss of control power or motor thermal overload. 38.34

- Emergency generator auxiliary fuel oil pump loss of control power or motor thermal overload. 38.35

- Remote voltage switch in MANUAL. 38.36

- Local voltage mode switch in MANUAL. 38.37

- Manual bypass pushbutton depressed. 38.38

D. IEEE Standard 279-1971, Paragraph 4.16: 38.41

Once a LOP, SIS, or CDA signal is received, the emergency generator will attempt to start. If not started in 10 seconds, the start signal is blocked and a "diesel not ready for AUTO start" annunciator will alarm in the control room and at the emergency generator local panel. An emergency diesel reset pushbutton in the control room or at the emergency generator panel must be depressed and the engine will attempt to start again. Once started, deliberate operator action must be taken to stop the emergency generator. 38.43 38.45 38.47 38.48 38.50

E. IEEE Standard 279-1971, Paragraph 4.10: 38.53

The emergency generator is periodically tested in accordance with the Technical Specifications in Chapter 16. 38.55

The operability of the emergency generator system controls and indications is verified during the instrument functional test. Also, during this test the instrumentation setpoints and their operability are checked. Correct settings of temperature, pressure, and level instrumentation are verified by applying a simulated signal. The operability of the prelube oil filter pump, rocker arm prelube oil pumps, standby jacket coolant pump, and air compressors is verified by normal operation when the emergency generator is not running. 38.57 38.59 38.60 39.1 39.2

F. IEEE Standard 279-1971, Paragraph 4.17: 39.5

Manual controls and indication are on the main control baord and at the emergency generator panels for manual operation of the emergency generators. 39.7 39.8

Air-Conditioning, Heating, Cooling, and Ventilation Systems 39.12

The safety-related (QA Category I) air-conditioning, heating, cooling, and ventilation systems are listed in Table 3.2-1. 39.14 39.15

The system designs, flow diagrams, and instrumentation applications are given in Section 9.4. The design bases for the control and 39.17 39.18

instrumentation of the safety-related air-conditioning, heating, cooling, and ventilation systems adhere to the following: 39.19

1. Automatic operation during normal and accident conditions. 39.21

2. Manual controls and indication of the status of all components in the control room. 39.22

3. Automatic controls as well as manual controls of redundant components are independent and electrically and physically separated. 39.23 39.24

4. Failure of an operating component and/or start of the redundant component is annunciated in the control room. 39.25

5. Redundant motors and motor-operated dampers have power supplied from separate emergency buses. Each redundant air-operated damper, with solenoid pilot valve, has power supplied from the separate dc bus. The dampers are designed to fail in the position of greater safety on loss of air and/or power supply. 39.26 39.27 39.28

The safety objective of the instrumentation and control for safety-related air-conditioning, heating, cooling, and ventilation systems is to maintain the temperatures within the specific areas they serve, within the design limits required, during normal and accident conditions. The control room and instrument rack and computer rooms are automatically isolated from the outside atmosphere on receiving a control building isolation (CBI) signal. A CBI signal is generated whenever any one of the following conditions exist: 39.30 39.31 39.32 39.33 39.34 39.35

- Outside atmosphere radiation hi-hi. 39.37
- Containment pressure hi-1, 2 out of 3 (2/3) hi. 39.38
- Outside atmosphere chlorine hi. 39.39
- Manual SIS. 39.40
- Manual CBI. 39.41

A differential pressure indicator with a scale division from zero to 0.25 in wg is provided in the control room to enable the operator to determine that the pressure in the control room is being maintained slightly above the atmospheric pressure following an accident. 39.43 39.44 39.45

Where high efficiency particulate air (HEPA) filters or carbon adsorbers are provided in the system, differential pressure alarms are provided to alert the operator to excessive differential pressure across the filter or adsorber and to indicate that changeover to the standby train should be made. 39.46 39.47 39.48

39.51

Control Building Isolation

The control building isolation (CBI) logic receives automatic 39.53
isolation signals from one chlorine monitor per train and one 39.55
radiation monitor per train located in the intake ventilation to the
control building. A containment hi-1 pressure signal (2/3 logic) is 39.56
also utilized as an input to the CBI logic.

A CBI signal (Train A or B) can be manually initiated from CBI 39.57
pushbuttons on the main control board or from the main heating and 39.58
ventilation panel in the control room. A CBI is also initiated by a 39.59
manual SIS initiation.

A control room pressurization signal is automatically initiated 39.60
60 seconds after a CBI signal is received.

The CBI logic relays are located in auxiliary relay panels AR4 40.1
(Train A) and AR5 (Train B). The panels are in the instrument rack 40.2
room. The output relays have test pushbuttons in the auxiliary relay 40.3
panels. The CBI K1 relays are interlocked with the controls for the 40.4
ventilation isolation valves and the chilled water pump. The CBI K2 40.5
relays are interlocked with the air storage tanks' outlet valves.
This arrangement allows for testing the ventilation isolation valves 40.6
and chilled water pumps for each Train (A or B), and for testing the 40.7
air storage tanks' outlet valves of each Train (A or B) separately.
The logic relays are energized to isolate and pressurize the control 40.8
room. CBI RESET pushbuttons (Train A and B) are on the main control 40.9
board.

40.12

Analysis

40.13

A. IEEE Standard 279-1971, Paragraph 4.1:

40.15

A CBI signal is automatically initiated on receipt of a high 40.16
radiation, high chlorine, or containment hi-1 pressure high.

An exception is the chlorine monitors which are not safety 40.18
grade qualified (see Item C, Equipment Qualification).

40.21

B. IEEE Standard 279-1971, Paragraph 4.2:

The CBI has redundant and separate trains supplied from 40.23
separate safety-related 120 V ac and separate 125 V dc
buses. An exception is that the chlorine monitors are not 40.26
supplied from safety-related buses. However, a CBI signal 40.27
is initiated on loss of power to the chlorine monitors. No 40.28
single failure will prevent a CBI at the system level.

40.31

C. IEEE Standard 279-1971, Paragraph 4.3:

Equipment qualifications are discussed in Sections 3.10 and 40.33
3.11.

An exception to equipment qualifications is that the chlorine monitors for CBI are not safety grade qualified. A safety grade isolator in the output of the monitors prevents degrading the safety grade CBI circuits. Upon the occurrence of a seismic event, the control room ventilation will be put into the recirculation mode manually. An evaluation will be made to determine if chlorine leakage is present. If chlorine leakage exists, control room pressurization will be manually initiated.

D. IEEE Standard 279-1971, Paragraph 4.8:

The radiation monitors, chlorine monitors, and containment pressure transmitters all derive signals that are direct measures of the variable being monitored.

E. IEEE Standard 279-1971, Paragraphs 4.9 and 4.10:

Testing of the automatic CBI signals from the chlorine monitor, radiation monitor, and containment hi-1 pressure signal (2/3 logic) will be performed by testing each signal for each train.

The test for the chlorine monitors will consist of verifying, every 12 hours, that power is available and no trouble alarms exist at each unit.

Every 90 days each probe of the monitor will be checked and calibrated with a sample gas. The alarm setpoint and trip function will be verified with a probe simulator and a step change function check by inserting each probe with a chlorine concentration.

At each refueling, a CBI actuation will be tested including a test of the pressurization system using a known chlorine sample.

The inlet ventilation radiation monitors will be calibrated on a refueling basis using solid point calibration sources and a fixed geometry.

On a monthly basis, an analog channel operational test verifies the alarm setpoint will be performed.

The individual signals shall automatically close the CBI valves and activate the pressurization system with a 60-second time delay.

Once it has been verified that the CBI signal performed its function, and before pressurization of the control room, the operator will reset the system with the manual CBI reset pushbuttons.

Testing the containment hi-1 pressure (2/3 logic) will be accomplished in accordance with Section 7.3.2.2.5. 41.8

F. IEEE Standard 279-1971, Paragraph 4.13: 41.11

Bypass and inoperative alarms on the main control board for CBI Train A and B are in accordance with Regulatory Guide 1.47. A CBI bypass annunciator is alarmed on the main control board whenever any of the following conditions exist: 41.13 41.16

- CBI bypass pushbutton depressed. 41.18
- Loss of control power to CBI logic relays. 41.19

G. IEEE Standard 279-1971, Paragraph 4.16: 41.22

A CBI initiated on the system level will go to completion with the following exception: control room pressurization is delayed 60 seconds after a CBI signal is initiated. The CBI signal can be reset manually on the main control board and prevent control room pressurization before the time delay expires. 41.24 41.26 41.27

After a CBI has gone to completion, deliberate operator action is required to return to operation. The CBI signal must be manually reset. The ventilation isolation valves must be manually opened and the air storage tank outlet valves are manually closed. 41.28 41.29 41.30

H. IEEE Standard 279-1971, Paragraph 4.17: 41.33

A CBI signal can be initiated manually with pushbuttons on the main heating and ventilation panel and on the main control board. A manual SIS signal also initiates a CBI signal. No single failure within the manual, automatic, or common portions of the CBI system will prevent a CBI initiation. 41.35 41.38 41.39

I. IEEE Standard 279-1971, Paragraph 4.18: 41.42

The CBI radiation monitor setpoints are administratively controlled. The setpoint cannot be changed at the monitor until a permissive has been granted by a key at the radiation monitoring panel in the control room. The permissive key is administratively controlled. 41.44 41.46 41.48

The chlorine monitor setpoint ajdustments are in a local control unit that is adminstratively controlled. 41.49

J. IEEE Standard 279-1971, Paragraph 4.19: 41.52

High chlorine is alarmed on the main heating and ventilation panel in the control room. High radiation is alarmed on the 41.54 41.56

main control board and on the radiation monitoring system console in the control room. An ESF status light indicates on the main control board when a CBI signal exists. Hi-1 containment pressure high is alarmed on the main control board by any channel. Indicator lights on the main control board indicate each channel that is alarmed and each is monitored for high pressure by the plant computer.

Charging Pumps Cooling System

The charging pumps cooling system is a supporting system for the charging pumps and is required to operate during normal unit operation and following a LOCA and/or loss-of-power. The system design and description are given in Section 9.2.2.4 and its flow diagram is shown on Figure 9.2-5.

Control switches and indicator lights for the charging pump cooling pumps are provided on the main control board and on the auxiliary shutdown panel. REMOTE/LOCAL control selector switches are located on the transfer switch panels in the vicinity of the auxiliary shutdown panel. An annunciator is alarmed in the control room when local control is selected. For normal unit operation, one of the two pumps is required to operate. This pump is started manually and the other pump is placed on standby. The pump in standby is automatically started on low pressure by a pressure switch in the pump's discharge header.

Following a loss-of-power and/or on receipt of an SIS signal, the redundant isolation valves in the charging pumps cooling pumps discharge header crossover, and in the charging pumps coolers outlet crossover automatically close, thus providing the two independent flow paths required during these modes of operation. Each charging pump's cooling pump motor's power supply is from a separate emergency bus, and the motors start automatically on loss-of-power and/or on an SIS. The air-solenoid, pilot-operated isolation valves are supplied from separate dc buses and on loss of air and/or loss-of-power fail closed.

The charging pumps cooling surge tank is divided into two compartments with each compartment serving one charging pump's cooling pump, thus providing redundancy in the fluid system design. Instrumentation is provided to monitor and control water level in each compartment of the surge tank at all times. The reactor plant component cooling water system automatically provides normal makeup to each surge tank compartment.

During the operational system test, the instrumentation setpoints and their operability are checked and adjusted. The operability of the charging pumps cooling system controls and indications is verified by their normal use. The test to verify the automatic response of the system is performed during each refueling period. Correct settings of temperature, flow, and level instrumentation are verified by applying a simulated signal. Pressure transmitters in the suction

and discharge of each cooling pump are monitored by the plant computer to determine pump performance. 42.33

ESF status lights are provided on the main control board to indicate charging pumps cooling pump and crossover valve status. 42.34 42.35

Analysis 42.38

A. IEEE Standard 279-1971, Paragraph 4.2: 42.39

The charging pumps cooling system is normally cross-connected at the discharge and suction of the cooling pumps. On receipt of a SIS or LOP signal, the cross-connect valves are closed automatically to separate Train A from Train B. There are four normally open, air-operated, cross-connected valves that fail closed on loss of air or loss of power to the solenoid valves. Solenoid valves control air to the cross-connect valves; two are powered from the Train A emergency dc bus and two are powered from the Train B emergency dc bus. 42.41 42.43 42.44 42.45 42.47 42.48

A temperature control valve for each charging pump cooler is controlled by a temperature indicating controller and a safety-related solenoid valve powered from an emergency dc bus. The temperature control valve opens to the heat exchanger on loss of air, loss of power to the solenoid valve, or when the charging pump cooler outlet temperature is greater than a predetermined setpoint. The solenoid valves are powered from separate buses. 42.49 42.50 42.51 42.52 42.53

The charging pumps cooling pumps are powered from separate emergency buses. Normally, one pump is running and the other on standby. On receipt of an SIS or LOP signal, both pumps are started automatically. 42.54 42.55 42.56

No single failure at the system level can prevent cooling water from being supplied to at least one charging pump. 42.57

B. IEEE Standard 279-1971, Paragraph 4.4: 42.60

Equipment qualifications are discussed in Sections 3.10 and 3.11. 43.2

C. IEEE Standard 279-1971, Paragraph 4.13: 43.6

A charging pump high pressure safety injection bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B): 43.8 43.9

- Charging pumps cooling control switch in pull to lock position. 43.12
- Charging pumps cooling pump loss of control power. 43.13

- Charging pumps cooling pump motor thermal overload. 43.14

D. IEEE Standard 279-1971, Paragraph 4.16: 43.17

Once an SIS or LOP signal is received, the charging pumps cooling pumps are started and the cross-connect valves are closed. Deliberate operator action must be taken to open the valves or stop a pump. The SIS and LOP signals must be reset and manual control used by the operator. 43.19 43.22 43.23

E. IEEE Standard 279-1971, Paragraphs 4.9 and 4.10: 43.26

The charging pumps cooling system is periodically tested in accordance with the Technical Specifications in Chapter 16. 43.28 43.29

The operability of the charging pumps cooling system controls and indicators is verified during the instrument functional test. Also, during this test the instrumentation setpoints and their operability are checked. The test to verify the automatic response of the system is peformed during each refueling period. Correct settings of temperature, flow, and level instrumentation are verified by applying a simulated signal. 43.31 43.33 43.34 43.35

F. IEEE Standard 279-1971, Paragraph 4.17: 43.38

Controls and indicators are provided in the control room for manual operation of the charging pumps cooling system. REMOTE/LOCAL control selector switches are provided at the transfer switch panels outside the control room, and manual controls and indication are on the auxiliary shutdown panels. An annunciator is alarmed in the control room when local control is selected. 43.40 43.42 43.43 43.44

Safety Injection Pumps Cooling System 43.47

The safety injection pumps cooling system is a supporting system for the safety injection pumps and is required to operate only following a LOCA. 43.49 43.50

The system design and description are given in Section 9.2.2.5, and the flow diagram is shown on Figure 9.2-4. The power supply for each train of the two-train system is from a separate emergency bus. 43.52 43.54

The starting of the safety injection pumps cooling pumps is interlocked with the starting of the safety injection pumps; i.e., when a safety injection pump is started for testing purposes or due to a SIS, its associated cooling pump is started automatically. The safety injection cooling pumps surge tank is divided into two compartments, with each compartment serving a separate pump, thus providing redundancy in the fluid system design. Instrumentation is provided to monitor and maintain water level in each compartment of the surge tank. The component cooling water system automatically provides normal makeup to each surge tank compartment. 43.55 43.56 43.58 43.59 43.60 44.1

During the operational system test, the instrumentation setpoints and their operability are checked and adjusted. 44.2

The operability of the safety injection pumps cooling system controls and indications are verified during the safety injection system test Section 6.3.4. Correct settings of temperature, pressure, and level instrumentation are verified by applying a simulated signal. Pressure transmitters in the suction and discharge of each cooling pump are monitored by the plant computer to determine pump performance. 44.3 44.4 44.5 44.6 44.7

ESF status lights are provided on the main control board to indicate status of the safety injection pumps cooling pumps. 44.8 44.9

Analysis 44.12

A. IEEE Standard 279-1971, Paragraph 4.2: 44.13

The safety injection pumps cooling system is divided into two mechanical and electrical trains. The safety injection pumps cooling pumps are powered from separate emergency buses. No single failure at the system level can prevent the safety injection pumps cooling system from supplying cooling water to at least one safety injection pump. 44.15 44.17 44.18 44.19

B. IEEE Standard 279-1971, Paragraph 4.4: 44.22

Equipment qualifications are discussed in Sections 3.10 and 3.11. 44.24

C. IEEE Standard 279-1971, Paragraph 4.13: 44.28

A safety injection pump high pressure safety injection bypass annunciator is alarmed in the control room whenever any of the following conditions exist (Train A or B): 44.30 44.31

- Safety injection pump cooling pump circuit breaker open. 44.34
- Safety injection pump cooling pump loss of control power. 44.35
- Safety injection pump cooling pump motor thermal overload. 44.36

D. IEEE Standard 279-1971, Paragraph 4.16: 44.39

Once a safety injection pump is started, the cooling pump starts automatically. Deliberate operator action must be taken to stop a cooling pump. The associated safety injection pumps must be stopped and manual controls used to stop the cooling pump. 44.41 44.43 44.44

E. IEEE Standard 279-1971, Paragraphs 4.9 and 4.10: 44.47

The safety injection pumps cooling system is periodically tested in accordance with the Technical Specifications in Chapter 16. 44.49 44.50

The operability of the safety injection pumps cooling system controls and indicators is verified during the instrument functional test. Also, during this test the instrumentation setpoints and their operability are checked. The test to verify the automatic response of the system is peformed during each refueling period. Correct settings of temperature, flow, and level instrumentation are verified by applying a simulated signal. 44.52 44.54 44.55 44.56

F. IEEE Standard 279-1971, Paragraph 4.17: 44.59

Controls and indicators are provided in the control room for manual operation of the safety injection pumps cooling system. 45.1 45.2

7.3.1.2 Design Bases Information 45.6

The functional diagrams presented on Figure 7.2-1, Sheets 5, 6, 7, and 8, provide a graphic outline of the functional logic associated with requirements for the ESFAS. Requirements for the ESF system are given in Chapter 6. Given below is the design bases information required in IEEE Standard 279-1971. 45.7 45.9 45.10 45.11

7.3.1.2.1 Generating Station Conditions 45.13

The following is a summary of those generating station conditions requiring protective action. 45.14

1. Primary System: 45.18

   a. Rupture in small pipes or cracks in large pipes. 45.20

   b. Rupture of a reactor coolant pipe (LOCA). 45.21

   c. Steam generator tube rupture. 45.23

2. Secondary System: 45.26

   a. Minor secondary system pipe breaks resulting in steam release rates equivalent to a single dump, relief, or safety valve. 45.28 45.29

   b. Rupture of a major steam pipe. 45.31

3. Control Building Isolation: 45.34

a. Outside atomosphere chlorine high 45.36

b. Intake radiation high-high. 45.37

c. Containment Pressure high (hi-1). 45.38

7.3.1.2.2 Generating Station Variables 45.42

The following list summarizes the generating station variables required to be monitored for the automatic initiation of safety injection during each accident identified in the preceding section. Post-accident monitoring requirements are given in Table 7.5-1. 45.43 45.46 45.47

1. Primary System Accidents: 45.50

a. Pressurizer pressure. 45.52

b. Containment pressure (not required for steam generator tube rupture). 45.53

2. Secondary System Accidents: 45.57

a. Pressurizer pressure. 45.59

b. Steam line pressures and pressure rate. 45.60

c. Containment pressure. 46.2

3. Control Building: 46.5

a. Chlorine high. 46.7

b. Radiation high-high. 46.8

c. Containment pressure hi-1. 46.9

7.3.1.2.3 Spatially Dependent Variables 46.13

The only variable sensed by the ESFAS which has spatial dependence is reactor coolant temperature. The effect on the measurement is negated by taking multiple samples from the reactor coolant hot leg and averaging these samples by mixing the resistance temperature detector bypass loop. 46.14 46.16 46.17

7.3.1.2.4 Limits, Margins, and Setpoints 46.19

Prudent operational limits, available margins, and setpoints before onset of unsafe conditions requiring protective action are discussed in Chapters 15 and 16. 46.20 46.21

7.3.1.2.5 Abnormal Events 46.24

The malfunctions, accidents, or other unusual events which could physically damage protection system components or could cause environmental changes are as follows. 46.25 46.27

1. Loss-of-coolant accident (Chapter 15) 46.29
2. Secondary system accidents (Chapter 15) 46.30
3. Earthquakes (Chapters 2 and 3) 46.31
4. Fire (Section 9.5.1) 46.32
5. Explosion (Hydrogen buildup inside containment) (Section 15.4) 46.33
6. Missiles (Section 3.5) 46.34
7. Flood (Chapters 2 and 3) 46.35
8. LOP (Chapter 8) 46.36
9. Chlorine (Control room habitability) (Section 2.2.3.1) 46.37

7.3.1.2.6 Minimum Performance Requirements 46.40

Minimum performance requirements are as follows. 46.41

1. System Response Times 46.45

   The ESFAS response time is defined as the interval required for the ESF sequence to the point in time that the appropriate variable(s) exceed setpoints. The response time includes sensor/process (analog) and logic (digital) delay plus the time delay associated with tripping open the reactor trip breakers and control and latching mechanisms, although the ESF actuation signal occurs before or simultaneously with ESF sequence initiation (Figure 7.2-1, Sheet 8). The values listed herein are maximum allowable times consistent with the safety analyses and are systematically verified during plant preoperational startup tests. These maximum delay times thus include all compensation and therefore require that any such network be aligned and operating during verification testing. 46.47 46.50 46.51 46.52 46.53 46.54 46.55 46.56

   The ESFAS is always capable of having response time tests performed using the same methods as those tests performed during the preoperational test program or following significant component changes. Maximum allowable time delays in generating the actuation signal for loss-of-coolant protection are: 46.57 46.58

   a. Pressurizer pressure 2.0 seconds 46.60

Maximum allowable time delays in generating the actuation signal for steam line break protection are: 47.3

a.	Steam line pressure	2.0 seconds	47.5
b.	Steam line pressure rate	2.0 seconds	47.7
c.	High containment pressure for closing main steam line stop valves	1.5 seconds	47.10 47.11 47.12
d.	Actuation signals for auxiliary feed pumps	2.0 seconds	47.16 47.17

Maximum allowable time delays in generating the actuation signal for CBI: 47.21

a.	Chlorine	4 seconds	47.23
b.	Radiation	(later) seconds	47.25
c.	Containment pressure	Assumed to be instantaneous	47.28 47.29

2. System accuracies: 47.34

Accuracies required for generating the required actuation signals for loss-of-coolant protection are: 47.36

a.	Pressurizer pressure (uncompensated)	±14 psi	47.41 47.42

Accuracies required in generating the required action signals for a steam break protection are given: 47.46

a.	Steam line pressure	±4 percent of span	47.49 47.50
b.	Steam line pressure rate	±5 percent psi/sec	47.54 47.55
c.	Containment pressure signal	±1.8 percent of full scale	47.59 47.60

Accuracies required for generating the required actuation for CBI: 48.4

a.	Chlorine	±3 percent of full scale	48.7 48.8
b.	Radiation	±10 percent at center scale	48.12 48.13

c.	Containment pressure	±1.8 percent of full scale	48.17 48.18

3. Ranges of sensed variables to be accommodated until conclusion of protective action is assured. 48.22

Ranges required in generating the required actuation signals for loss-of-coolant protection are given: 48.24

a.	Pressurizer pressure	1,700 to 2,500 psig	48.27 48.28
b.	Containment pressure	0 to 60 psig	48.31

Ranges required in generating the required actuation signals for steam line break protection are given: 48.34

a.	T	530 to 630°F	48.36
b.	Steam line pressure (from which steam line pressure rate is derived)	0 to 1,200 psig	48.39 48.40 48.41
c.	Containment pressure	0 to 60 psia	48.44

Ranges required in generating the required signals for CBI: 48.47

a.	Chlorine	0-10 ppm	48.49
b.	Radiation	10^{-6} μci/cc- 10^{-1} μci/cc	
c.	Containment pressure	0-60 psia	48.56

7.3.1.3 Final System Drawings 48.60

The schematic diagrams for the systems discussed in this section are listed in Section 1.7 and are submitted in support of this application. 49.1 49.3

7.3.2 Analysis 49.6

Failure mode and effects analyses have been performed on ESF systems equipment within the Westinghouse scope of supply (WCAP-8584). The Millstone ESF systems, although not identical, have been designed to equivalent safety design criteria. 49.7 49.10

Analyses of the instrumentation and control systems used to initiate the operation of the ESF systems and their essential auxiliary supporting systems have been made. For balance-of-plant safety systems, the assurance that safety-related instrumentation and control fulfill their functions (assuming a single failure) is achieved by the use of redundant channels, trains, components, and power supplies with the appropriate separation provided between them. 49.11 49.12 49.13 49.14 49.15

Detailed documentation in the form of the failure modes and effects analysis or fault tree analyses (based on actual wiring diagrams and components of the plant) are presented in a separate report described in Section 7.3.2.1. The analyses were made to assure that each system satisfies the applicable design criteria and will perform as intended during all plant operations and accident conditions for which its function is required.

The ESF and essential supporting systems are designed so that a loss of plant instrument air, the loss of cooling water to vital equipment, a plant load rejection, or a turbine trip will not prevent the completion of the safety function under postulated accidents and failures. Evaluation of the individual and combined capabilities of the ESF and supporting systems can be found in Chapters 6 and 15.

7.3.2.1 Failure Modes and Effects Analysis

The systematic, organized, analytical procedure for identifying the possible modes of failure and evaluating their consequences is called a failure modes and effects analysis (FMEA). Its purpose is to demonstrate and verify how the General Design Criteria (GDC) and IEEE Standard 279-1971 requirements are satisfied. FMEAs that are performed on the Class 1E electric power and instrumentation and control portions of the safety-related auxiliary supporting systems also determine if they will meet the single failure criteria.

The FMEA is produced in the form of a computerized tabulation that identifies the component, its failure mode, the method of failure detection, and its effect on the safety-related system. This tabulation is derived from the fault tree analysis (FTA). Figure 7.3-1 shows a typical page from a FMEA.

The FTA is a technique by which failures that can contribute to an undesired event are systematically and deductively organized from a top event down to subordinate events. It is pictorially represented by rectangular blocks connected via flow lines to logic gates, all placed together in a tree-shaped configuration.

The FTA identifies all failure modes that are significant to the failure of the safety-related system, the failure paths from the failed items up through the fault tree to a single top failure event, and any single failures that may result in the failure of the system to perform its intended safety function. It also provides a visual display of how the system can malfunction. See Figure 7.3-2 for an example of a computer-plotted fault tree diagram.

When the event blocks and logic gates have been assigned unique computer readable codes, the FTA can be processed and printed out as a standard format, auditable permanent record tabulation called the FMEA. The FMEAs for the systems listed in Table 7.3-11 are in a report titled Failure Modes and Effects Analysis, submitted as part of the documentation provided in Section 1.7.4.

7.3.2.2 Compliance with Standards and Design Criteria 49.54

Discussion of the GDC is provided in various sections of Chapter 7 where a particular GDC is applicable. Applicable GDCs include Criteria 13, 20, 21, 22, 23, 24, 25, 27, 28, 35, 37, 38, 40, 43, and 46 of the 1971 GDC. compliance with certain IEEE Standards is presented in Sections 7.1.2.7, 7.1.2.9, 7.1.2.10, and 7.1.2.11. Compliance with Regulatory Guide 1.22 is discussed in Section 7.1.2.5. The discussion given below shows that the ESFAS complies with IEEE Standard 279-1971 (Institute of Electrical and Electronics Engineers, Inc. 1971). 49.55 49.57 49.58 49.59 49.60 50.1

7.3.2.2.1 Single Failure Criteria 50.3

The discussion presented in Section 7.2.2.2.3 is applicable to the ESFAS with the following exception. 50.4

In the ESF, a loss of instrument power will call for actuation of ESF equipment controlled by the specific bistable that lost power (containment spray excepted). The actuated equipment must have power to comply. The power supply for the protection systems is discussed in Section 7.6 and in Chapter 8. For containment spray, the final bistables are energized to trip to avoid spurious actuation. In addition, manual containment spray requires a simultaneous actuation of two manual controls. This is considered acceptable because spray actuation on hi-3 containment pressure signal provides automatic initiation of the system via protection channels. Moreover, two sets (two switches per set) of containment spray manual initiation switches are provided to meet the requirements of IEEE Standard 279-1971. Also, it is possible for all ESF equipment (valves, pumps, etc) to be individually manually actuated from the control board. Hence, a third mode of containment spray initiation is available. The design meets the requirements of Criteria 21 and 23 of the 1971 GDC. 50.6 50.7 50.8 50.9 50.10 50.11 50.12 50.14 50.15 50.16 50.17 50.18 50.19

7.3.2.2.2 Equipment Qualification 50.21

Equipment qualifications are discussed in Sections 3.10 and 3.11. 50.22

7.3.2.2.3 Channel Independence 50.25

The discussion presented in Section 7.2.2.2.3 is applicable. The ESF slave relay outputs from the solid state logic protection cabinets are redundant, and the actuation signals associated with each train are energized up to and including the final actuators by the separate ac power supplies which power the logic trains. 50.27 50.29 50.30

7.3.2.2.4 Control and Protection System Interaction 50.32

The discussions presented in Section 7.2.2.2.3 are applicable. 50.33

7.3.2.2.5 Capability for Sensor Checks and Equipment Test Calibration 50.38

The discussions of system testability in Section 7.2.2.2.3 are applicable to the sensor, analog circuitry, and logic trains of the ESFAS. 50.41 50.42

The following discussions cover those areas in which the testing provisions differ from those for the reactor trip system. 50.44 50.45

Testing of Engineered Safety Features Actuation Systems 50.48

The ESFASs are tested to provide assurance that the systems will operate as designed and will be available to function properly in the unlikely event of an accident. The testing program meets the requirements of Criteria 21, 37, 40, and 43 of the 1971 GDC and Regulatory Guide 1.22 as discussed in Section 7.1.2.8. The tests described in Section 7.3.2.2.3 and further discussed in Section 6.3.4 meet the requirements on testing of the ECCS as stated in GDC 37, except for the operation of those components that will cause an actual safety injection. The test, as described, demonstrates the performance of the full operational sequence that brings the system into operation, the tranfer between normal and emergency power sources, and the operation of associated cooling water systems. The safety injection and residual heat removal pumps are started and operated and their performance verified in a separate test discussed in Section 6.3.4. When the pump tests are considered in conjunction with the ECCS test, the requirements of GDC 37 on testing of the ECCS are met as closely as possible without causing an actual safety injection. 50.50 50.51 50.53 50.55 50.56 50.58 50.59 51.1 51.2 51.3 51.4

The system design, as described in Sections 6.3.4, 7.2.2.2.3, and 7.3.2.3.3, provides complete periodic testability during reactor operation of all logic and components associated with the ECCS. This design meets the requirements of Regulatory Guide 1.22 as discussed in the above sections. The program is as follows: 51.5 51.6 51.7 51.8

1. Prior to initial plant operations, ESF system tests are conducted. 51.10

2. Subsequent to initial startup, ESF system tests are conducted during each regularly scheduled refueling outage. 51.11

3. During online operation of the reactor, all of the ESF analog and logic circuitry can be fully tested. In addition, essentially all of the ESF final actuators can be fully tested. The remaining few final actuators, whose operation is not compatible with online plant operation, can be checked by means of continuity testing. 51.12 51.13 51.14 51.15

4. During normal operation, the operability of testable final actuation devices of the ESF systemscan be tested by manual initiation from the control room or, as indicated in 3 51.16 51.17

above, by actuation of the solid state protection system slave relays from the ESF test cabinets. 51.18

Performance Test Acceptability Standard for the Safety Injection Signal and For the Automatic Signal for Containment Depressurization Actuation Generation 51.20 51.21

During reactor operation the basis for ESFAS acceptability will be the successful completion of the overlapping tests performed on the initiating system and the ESFAS (Figure 7.3-3). Checks of process indications verify operability of the sensors. Analog checks and tests verify the operability of the analog circuitry from the input of these circuits through to and including the logic input relays except for the input relays associated with the containment spray function which are tested during the solid state logic testing. Solid state logic testing also checks the digital signal path from and including logic input relay contacts through the logic matrices and master relays and perform continuity tests on the coils of the output slave relays; final actuator testing operates the output slave relays and verifies operability of those devices which require safeguards actuation and which can be tested without causing plant upset. A continuity check is performed on the actuators of the untestable devices. Operation of the final devices is confirmed by control board indication and visual observation that the appropriate pump breakers close and automatic valves shall have completed their travel. 51.23 51.24 51.26 51.27 51.28 51.29 51.30 51.31 51.32 51.33 51.34 51.35 51.36

The basis for acceptability for the ESF interlocks will be control board indication of proper receipt of the signal upon introducing the required input at the appropriate setpoint. 51.37 51.38

Maintenance checks (performed during regularly scheduled refueling outages), such as resistance to ground of signal cables in radiation environments are based on qualification test data which identifies what constitutes acceptable radiation, thermal, etc, degradation. 51.39 51.40 51.41

Frequency of Performance of Engineered Safety Features Actuation Tests 51.44

During reactor operation, complete system testing (excluding sensors or those devices whose operation would cause plant upset) is performed periodically as specified in the Technical Specifications. Testing, including the sensors, is also performed during scheduled plant shutdown for refueling. 51.46 51.48 51.49

Engineered Safety Features Actuation Test Description 51.52

The following sections describe the testing circuitry and procedures for the online portion of the testing program. The guidelines used in developing the circuitry and procedures are: 51.54 51.56

1. The test procedures must not involve the potential for damage to any plant equipment. 51.58

2. The test procedures must minimize the potential for accidental tripping. 51.59

3. The provisions for online testing must minimize complication of engineered safety features actuation circuits so that their reliability is not degraded. 51.60 52.1

Description of Initiation Circuitry 52.4

Several systems, as listed in 7.3.1.1.1, comprise the total engineered safety features system, the majority of which may be initiated by different process conditions and be reset independently of each other. 52.6 52.7

The remaining functions are initiated by a common signal (safety injection) which in turn may be generated by different process conditions. 52.9 52.10

In addition, operation of all other vital auxiliary support systems, such as auxiliary feedwater, component cooling, and service water, is initiated by the safety injection signal. 52.11 52.12

The output of each of the initiation circuits consists of a master relay which drives slave relays for contact multiplication as required. The logic, master, and slave relays are mounted in the solid state logic protection cabinets designated Train A and Train B, respectively, for the redundant counterparts. The master and slave relay circuits operate various pump and fan circuit breakers or starters, motor-operated valve contactors, solenoid-operated valves, emergency generator starting, etc. 52.13 52.14 52.15 52.16 52.17 52.18

Analog Testing 52.21

Analog testing is identical to that used for reactor trip circuitry and is described in Section 7.2.2.2.3. 52.23

An exception to this is containment spray, which is energized to actuate 2/4 and reverts to 2/3 when one channel is in test. 52.25 52.26

Solid State Logic Testing 52.29

Except for containment spray channels, solid state logic testing is the same as that discussed in Section 7.2.2.2.3. During logic testing of one train, the other train can initiate the required engineered safety features function. For additional details, see WCAP-7488-L (1971). 52.31 52.33 52.34

Actuator Testing 52.37

At this point, testing of the initiation circuits through operation of the master relay and its contacts to the coils of the slave relays has been accomplished. The ESFAS logic slave relays in the SSPS output cabinets are subjected to coil continuity tests by the output relay tester in the SSPS cabinets. Slave relays (K601, K602, etc.) 52.39 52.40 52.42 52.44

do not operate because of reduced voltage applied to their coils by the mode selector switch (TEST/OPERATE). A multiple position master relay selector switch chooses different master relays and corresponding slave relays to which the coil continuity is applied. The master relay selector switch is returned to "OFF" before the mode selector switch is placed back in the "OPERATE" mode. However, failure to do so will not result in defeat of the protective function. The ESFAS slave relays are activated during testing by the online test cabinet so that overlap testing is maintained.

The ESFAS final actuation device or actuated equipment testing is performed from the engineered safeguards test cabinets. These cabinets are located near the solid state logic protection system equipment. There is one test cabinet provided for each of the two protection Trains A and B. Each cabinet contains individual test switches necessary to actuate the slave relays. To prevent accidental actuation, test switches are of the type that must be rotated and then depressed to operate the slave relays. Assignments of contacts of the slave relays for actuation of various final devices or actuators has been made such that groups of devices or actuated equipment can be operated individually during plant operation without causing plant upset or equipment damage. In the unlikely event that an SIS is initiated during the test of the final device that is actuated by this test, the device will already be in its safeguards position.

During this last procedure, close communication between the main control room operator and the operator at the test panel is maintained. Prior to the energizing of a slave relay, the operator in the main control room assures that plant conditions will permit operation of the equipment that will be actuated by the relay. After the tester has energized the slave relay, the main control room operator observes that all equipment has operated as indicated by appropriate indicating lamps, monitor lamps and annunciators on the control board, and records all operations. He then resets all devices and prepares for operation of the next slave relay actuated equipment.

By means of the procedure outlined above, all ESF devices actuated by ESFAS initiation circuits, with the exceptions noted in Section 7.1.2.5 under a discussion of Regulatory Guide 1.22 are operated by the automatic circuitry.

Actuator Blocking and Continuity Test Circuits

These few final actuation devices that cannot be designed to be actuated during plant operation (discussed in Section 7.1.2.5) have been assigned to slave relays for which additional test circuitry has been provided to individually block actuation to a final device upon operation of the associated slave relay during testing. Operation of these slave relays, including contact operations, and continuity of the electrical circuits associated with the final devices' control are checked in lieu of actuation operation. The circuits provide for monitoring of the slave relay contacts, the devices' control circuit

cabling, control voltage, and the devices' actuation solenoids. Interlocking prevents blocking the output from more than one output relay in a protection train at a time. Interlocking between trains is also provided to prevent continuity testing the both trains simultaneously, therefore the redundant device associated with the protection train not under test will be available if event protection action is required. If an accident occurs during testing, the automatic actuation circuitry will override testing as noted above. One exception to this is that if the accident occurs while testing a slave relay whose output must be blocked, those few final actuation devices associated with this slave relay will not be overridden; however, the redundant devices in the other train would be operational and would perform the required safety function. Actuation devices to be blocked are identified in Section 7.1.2.5.

The continuity test circuits for these components that cannot be actuated online are verified by test lights on the safeguards test cabinets.

The typical schemes for blocking operation of selected protection function actuator circuits are shown on Figure 7.3-4 as details A and B. The schemes operate as explained below and are duplicated for each safeguards train.

Detail A shows the circuit for contact closure for protection function actuation. Under normal plant operation and equipment not under test, the test lamps "DS*" for the various circuits will be energized. Typical circuit path will be through the normally closed test relay contact "K8*" and through test lamp connections 1 to 3. Coils "X1" and "X2" will be capable of being energized for protection function actuation upon closure of solid state logic output relay contacts "K*." Coil "X1" or "X2" is typical for a breaker closing auxiliary coil, motor starter master coil, coil of a solenoid valve, auxiliary relay, etc. When the contacts "K8*" are opened to block energizing of coil "X1" and "X2," the white lamp is deenergized, and the slave relay "K*" may be energized to perform continuity testing. To verify operability of the blocking in both blocking and restoring normal service, open the blocking relay contact in series with lamp connections - the test lamp should be deenergized; close the block relay contact in series with the lamp connections - the test lamp should now be energized, which verifies that the circuit is not in its normal, i.e., operable condition.

Detail B shows the circuit for contact opening for protection function actuation. Under normal plant operation and equipment not under test, the white test lamps "DS*" for the various circuits will be energized, and the green test lamp "DS*" will be deenergized. Typical circuit path for white lamp "DS*" will be through the normally closed solid state logic output relay contact "K*" and through test lamp connections 1 to 3. Coils "Y1" and "Y2" will be capable of being deenergized for protection function actuation upon opening of solid state logic output relay contacts "K*." Coil "Y2" is typical for a solenoid valve coil, auxiliary relay, etc. When the contacts "K8*" are closed to block deenergizing of coils "Y1" and

"Y2," the green test lamp is energized and the slave relay "K*" may be energized to verify operation (opening of its contacts). To verify operability of the blocking relay in both blocking and restoring normal service, close the blocking relay contact to the green lamp - the green test lamp should now be energized also; open this blocking relay contact - the green test lamp should be deenergized, which verifies that the circuit is now in its normal, i.e., operable position. 54.5 54.6 54.7 54.8 54.9

Time Required for Testing 54.12

It is estimated that analog testing can be performed at a rate of several channels per hour. Logic testing of both Trains A and B can be performed in less than 30 minutes. Testing of actuated components (including those which can only be partially tested) will be a function of control room operator availability. It is expected to require several shifts to accomplish these tests. During this procedure, automatic actuation circuitry will override testing, except for those few devices associated with a single slave relay whose outputs must be blocked and then only while blocked. It is anticipated that continuity testing associated with a blocked slave relay could take several minutes. During this time, the redundant devices in the other train would be functional. 54.14 54.16 54.17 54.19 54.20 54.21 54.22 54.23

Summary of Online Testing Capabilities 54.26

The procedures described provide capability for checking completely from the process signal to the logic cabinets and from there to the individual pump and fan circuit breakers or starters, valve contactors, pilot solenoid valves, etc, including all field cabling actually used in the circuitry called upon to operate for an accident condition. For those few devices whose operation could adversely affect plant or equipment operation, the same procedure provides for checking from the process signal to the logic rack. To check the fianl actuation device, a continuity test of the individual control circuits is performed. 54.28 54.29 54.31 54.32 54.33 54.34 54.35

The procedures require testing at various locations: 54.36

1. Analog testing and verification of bistable setpoint are accomplished at process analog racks. Verification of bistable relay operation is done at the main control room status lights. 54.38 54.39

2. Logic testing through operation of the master relays and low voltage application to slave relays is done at the logic rack test panel. 54.40 54.41

3. Testing of pumps, fans, and valves is done at a test panel located in the vicinity of the logic racks in combination with the control room operator. 54.42 54.43

4. Continuity testing for those circuits that cannot be operated is done at the same test panel mentioned in 3 above. 54.44

The reactor coolant pump essential service isolation valves consist of the isolation valves for the component cooling water return and the seal water return header. 54.46 54.47

The main reason for not testing these valves periodically is that the reactor coolant pumps may be damaged. Although pump damage from this type of test would not result in a situation which endangers the health and safety of the public, it could result in unnecessary shutdown of the reactor for an extended period of time while the reactor coolant pump or certain of its parts could be replaced. 54.48 54.49 54.50 54.51

Testing During Shutdown 54.54

ECCS tests will be performed periodically in accordance with the Technical Specifications with the reactor coolant system isolated from the ECCS by closing the appropriate valve. A test SIS will then be applied to initiate operation of active components (pumps and valves) of the ECCS. This is in compliance with Criterion 37 of the 1971 GDC. 54.56 54.57 54.58 54.59

Containment spray system tests will be performed periodically. The pump tests will be performed with the isolation valves in the spray supply lines at the containment and spray additive tank blocked closed and the valves will be tested periodically with the pumps shutdown. 55.1 55.2

Periodic Maintenance Inspections 55.5

The maintenance procedures which follow will be accomplished in accordance with applicable plant procedures. The frequency will depend on the operating conditions and requirements of the reactor power plant. If any degradation of equipment operation is noted, either mechanically or electrically, remedial action is taken to repair, replace, or readjust the equipment. Optimum operating performance must be achieved at all times. 55.7 55.9 55.10 55.12

Typical maintenance procedures include the following. 55.13

1. Check cleanliness of all exterior and interior surfaces. 55.15

2. Check all fuses for corrosion. 55.16

3. Inspect for loose or broken control knobs and burned out indicator lamps. 55.17

4. Inspect for moisture and condition of cables and wiring. 55.18

5. Mechanically check all connectors and terminal boards for looseness, poor connection, or corrosion. 55.19

6. Inspect the components of each assembly for signs of overheating or component deterioration. 55.20

7. Perform complete system operating check. 55.21

The balance of the requirments listed in Institutue of Electrical and Electronic Engineers, Inc. (1976) (Paragraphs 4.11 through 4.22) are discussed in Section 7.2.2.2.1. Paragraph 4.20 receives special attention in Section 7.5. 55.23 55.24 55.25

7.3.2.2.6 Manual Resets and Blocking Features 55.27

The manual reset feature associated with containment spray actuation is provided in the design of the solid state protection system design for two basic purposes First, the feature permits the operator to start an interruption procedure of automatic containment spray in the event of false initiation of an actuate signal. Second, although spray system performance is automatic, the reset feature enables the operator to start a manual takeover of the system to handle unexpected events which can be better dealt with by operator appraisal of changing conditions following an accident. 55.28 55.30 55.31 55.32 55.33 55.34

It is most important to note that manual control of the spray system does not occur, once actuation has begun, by just resetting the associated logic devices alone. Components will seal in (latch) so that removal of the actuate signal, in itself, will neither cancel or prevent completion of protective action or provide the operator with manual override of the automatic system by this single action. In order to take complete control of the system to interrupt its automatic performance, the operator must deliberately unlatch relays which have "sealed in" the initial actuate signals in the associated motor control center, in addition to tripping the pump motor circuit breakers, if stopping the pumps is desirable or necessary. 55.35 55.36 55.37 55.38 55.40 55.41 55.42

The manual reset feature associated with containment spray, therefore, does not perform a bypass function. It is merely the first of several manual operations required to take control from the automatic system or interrupt its completion should such an action be considered necessary. 55.43 55.44 55.45

In the event that the operator anticipates system actuation and erroneously concludes that it is undesirable or unnecessary and imposes a standing reset condition in one train (by operating and holding the corresponding reset switch at the time the initiate signal is transmitted) the other train will automatically carry the protective action to completion. In the event that the reset condition is imposed simultaneously in both trains at the time the initiate signals are generated, the automatic sequential completion of system action is interrupted and control has been taken by the operator. Manual takeover will be maintained, even though the reset switches are released, if the original initiate signal exists. Should the initiate signal then clear and return again, automatic system actuation will repeat. 55.46 55.47 55.48 55.50 55.51 55.53 55.54 55.55

Note also that any time delays imposed on the system action are to be applied after the initiating signals are latched. Delay of actuate signals for fluid systems lineup, load sequencing, etc, do not provide the operator time to interrupt automatic completion, with manual reset alone, as would be the case if time delay was imposed prior to sealing of the initial actuate signal.

The manual block features associated with pressurizer and steam line SISs provide the operator with the means to block initiation of safety injection during plant startup. These block features meet the requirements of Paragraph 4.12 of IEEE Standard 279-1971 in that automatic removal of the block occurs when plant conditions require the protection system to be functional.

7.3.2.2.7 Manual Initiation of Protection Actions (Regulatory Guide 1.62)

There are four individual main steam stop valve momentary control switches (one per loop) mounted on the control board. Each switch when actuated, will isolate one of the main steam lines. In addition, there will be two system level switches. Operating either switch will actuate all four main steam line isolation and bypass valves at the system level.

Manual initiation of switchover to recirculation is in compliance with Section 4.17 of IEEE Standard 279-1971 with the following comment.

Manual initiation of either one of two redundant safety injection actuation main control board mounted switches provides for actuation of the components required for reactor protection and mitigation of adverse consequences of the postulated accident, including delayed actuation of sequenced started emergency electrical loads as well as components providing switchover from the safety injection mode to the cold leg recirculation mode following a loss of primary coolant accident. Therefore, once safety injection is initiated, those components of the ECCS (Section 6.3) which are realigned as part of the semi-automatic switchover go to completion on low refueling storage tank water level without any manual action. Manual operation of other components or manual verification of proper position as part of emergency procedures is not precluded nor otherwise in conflict with the above described compliance to paragraph 4.17 of IEEE Standard 279-1971 of the semi-automatic switchover circuits.

No exception to the requirements of IEEE Standard 279-1971 has been taken in the manual initiation circuit of safety injection. Although Paragraph 4.17 of IEEE Standard 279-1971 requires that a single failure within common portions of the protective system shall not defeat the protective action by manual or automatic means, the standard does not specifically preclude the sharing of initiated circuitry logic between automatic and manual functions. It is true that the manual safety injection initiation functions associated with one actuation train (e.g., Train A) shares portions of the automatic initiation circuitry logic of the same logic train; however, a single

failure in shared functions does not defeat the protective action of the redundant actuation train (e.g., Train B). A single failure in shared functions does not defeat the protective action of the safety function. It is further noted that the sharing of the logic by manual and automatic initiation is consistent with the system level action requirements of the IEEE Standard 279-1971, Paragraph 4.17 and consistent with the minimization of complexity.

7.3.2.3 Further Considerations

7.3.2.3.1 Instrument Air and Component Cooling

In addition to the considerations given above, a loss of instrument air or loss of component cooling water to vital equipment has been considered. Neither the loss of instrument air nor the loss of cooling water (assuming no other accident conditions) can cause safety limits as given in Chapter 16 to be exceeded. Likewise, loss of either one of the two will not adversely affect the core or the reactor coolant system nor will it prevent an orderly shutdown if this is necessary. Furthermore, all pneumatically-operated valves and controls will assume a preferred operating position upon loss of instrument air. It is also noted that for conservatism during the accident analysis (Chapter 15), credit is not taken for the instrument air systems nor for any control system benefit.

The design does not provide any circuitry which will directly trip the reactor coolant pumps on a loss of component cooling water. Normally, indication in the control room is provided whenever component cooling water is lost. The reactor coolant pumps can run about 10 minutes after a loss of component cooling water. This provides adequate time for the operator to correct the problem or trip the plant if necessary.

7.3.2.4 Summary

The effectiveness of the ESFAS is evaluated in Chapter 15, based on the ability of the system to contain the effects of Condition III and IV faults, including loss-of-coolant and steam break accidents. The ESFAS parameters are based upon the component performance specifications which are given by the manufacturer or verified by test for each component. Appropriate factors to account for uncertainties in the data are factored into the constants characterizing the system.

The ESFAS must detect Condition III and IV faults and generate signals which actuate the ESF. The system must sense the accident condition and generate the signal actuating the protection function reliably and within a time determined by, and consistent with, the accident analyses in Chapter 15.

Much longer times are associated with the actuation of the mechanical and fluid system equipment associated with engineered safety features. This includes the time required for switching, bringing

pumps and other equipment to speed and the time required for them to take load. 57.14

Operating procedures require that the complete ESFAS normally be operable. However, redundance of system components is such that the system operability assumed for the safety analyses can still be met with certain instrumentation channels out of service. Channels that are out of service are to be placed in the tripped mode or bypass mode in the case of containment spray. 57.15 57.16 57.17 57.18

7.3.2.4.1 Loss-of-Coolant Protection 57.20

By analysis of LOCAs and in system tests, it has been verified that except for very small coolant system breaks which can be protected against by the charging pumps followed by an orderly shutdown, the effects of various LOCAs are reliably detected by low pressurizer pressure signal; the ECCS is actuated in time to prevent or limit core damage. 57.21 57.23 57.24

For large coolant system breaks, the passive accumulators inject first because of the rapid pressure drop. This protects the reactor during the unavoidable delay associated with actuating the active ECCS phase. 57.25 57.26

High containment pressure also actuates the ECCS. Therefore, emergency core cooling actuation can be brought about by sensing this other direct consequence of a primary system break; that is, the ESFAS detects the leakage of the coolant into the containment. The generation time of the actuation signal of about 1.5 second, after detection of the consequences of the accident, is adequate. 57.28 57.29 57.30 57.31

Containment spray will provide additional emergency cooling of containmemt and also limit fission product release upon sensing elevated containment pressure (hi-3) to mitigate the effects of a LOCA. 57.32 57.33

The delay time between detection of the accident condition and the generation of the actuation signal for these systems is assumed to be about 1.0 second, well within the capability of the protection system equipment. However, this time is short compared to that required for startup of the fluid systems. 57.34 57.35 57.36

The analyses in Chapter 15 show that the diverse methods of detecting the accident condition and the time for generation of the signals by the protection systems are adequate to provide reliable and timely protection against the effects of loss-of-coolant. 57.37 57.38 57.39

7.3.2.4.2 Steam Line Break Protection 57.41

The ECCS is also actuated in order to protect against a steam line break. About 2.0 seconds elapses between sensing low steam line pressure and generation of the actuation signal. Analysis of steam break accidents assuming this delay for signal generation shows that the ECCS is actuated for a steam line break in time to limit or 57.42 57.44 57.45 57.46

prevent further core damage for steam line break cases. There is a reactor trip but the core reactivity is further reduced by the highly borated water injected by the ECCS.

Additional protection against the effects of steam line break is provided by feedwater isolation which occurs upon actuation of the emergency core cooling system. Feedwater line isolation is initiated in order to prevent excessive cooldown of the reactor vessel and thus protect the reactor coolant system boundary.

Additional protection against a steam break accident is provided by closure of all steam line isolation valves in order to prevent uncontrolled blowdown of all steam generators. The generation of the protection system signal (about 2.0 seconds) is again short compared to the time to trip the fast acting steam line isolation valves which are designed to close in less than approximately 5 seconds.

In addition to actuation of the ESF, the effect of a steam line break accident also generates a signal resulting in a reactor trip on overpower or following ECCS actuation. However, the core reactivity is further reduced by the highly borated water injected by the ECCS.

The analyses in Chapter 15 of the steam break accidents and an evaluation of the protection system instrumentation and channel design shows that the ESFAS are effective in preventing or mitigating the effects of a steam break accident.

7.3.3 References for Section 7.3

IEEE Standard 279-1971. The Institute of Electrical and Electronics Engineers, Inc. IEEE Standard: Criteria for Protection System for Nuclear Power Generating Stations.

NUSCo. No. 25212-28723. Emergency Generator Load Sequence Control Logic Description 24-9.4. Northeast Utilities Service Company, Millstone Nuclear Power Station - Unit 3.

WCAP-7013, 1973. Reid, J. B. Process Instrumentation for Westinghouse Nuclear Steam Supply System (4 Loop Plant using WCID 7300 Series Process Instrumentation).

WCAP-7488-L (Proprietary) and WCAP-7672, 1971 (Non-Proprietary) 1971.

WCAP-7705, Revision 2. (Information only; i.e., not a generic topical WCAP) 1976. Swogger, J. W. Testing of Engineered Safety Features Actuation System.

Open Items

Instrumentation and Control Systems Branch

ICSB-10 Remote Shutdown Capability (Draft SER Section 7.4.2.3)

In the FSAR Section 7.4.1.3, the applicant states that the design basis for control room evacuation does not consider a single failure. The staff finds the applicant's design basis for remote shutdown capability unacceptable. The FSAR Table 7.4-1, "Instruments and Controls Outside Control Room For Cold Shutdown" has not identified the transfer switches whether from train A equipment or from train B equipment. The staff requested the applicant to clarify the design criteria for remote shutdown station, and provide detailed layout drawings for transfer switch panels and the auxiliary shutdown panel. The applicant should also address the isolation, separation, qualification, and transfer/override provisions of the remote shutdown station in Section 7.4 of the FSAR. Detailed schematics related to remote shutdown operation should be provided for staff review. This is an open item.

Response (3/84)

See revised FSAR Section 7.4.

Status (3/84)

Closed.

7.4.1.5 Other Considerations 1.10

1. Additional shutdown air compressors are powered from Class IE buses and are provided to increase availability of normal controls and minimize operator actions. 1.12 1.13

2. Other equipment supplied from Class IE buses to minimize impact on nonsafety equipment in containment include: 1.14

   a. Containment recirculation coolers 1.16

   b. CRDM air cooling fans 1.17

3. Loss of instrument air does not prevent the operation of the minimum systems necessary for hot standby or cold shutdown described in Section 7.4.1. 1.19 1.20

7.4.2 Analysis 1.23

Hot shutdown is a stable plant condition, automatically reached following a reactor trip from power. The plant design features also permit the achievement of cold shutdown as referred to in Section 7.4.1.2 and described in Section 5.4.7. In the unlikely event that access to the control room is restricted, the plant can be safely kept at a hot standby by the use of the monitoring indicators and the controls listed in Sections 7.4.1.1 and 7.4.1.2, and described in Section 7.4.1.3, until the control room can be re-entered. 1.24 1.26 1.28 1.29 1.30

Cold shutdown conditions can be achieved from outside the control room through the use of suitable procedures and by virtue of local control of the equipment listed in Section 7.4.1.2, in conjunction with the instrumentation and controls provided on the auxiliary shutdown panel (ASP) (Table 7.4-1). The layout of the ASP is provided in the ESK series drawings, listed in Section 1.7. 1.31 1.32 1.33 1.34

The design basis for the ASP is as follows: 1.36

1. The design of the system to provide redundant safety grade capability to achieve and maintain a safe shutdown condition from location(s) remote from the control room is as follows: 1.39 1.40

   Panels and associated equipment used in control room evacuation are located at elevation 4 feet-6 inches in the control building. Also located at elevation 4 feet-6 inches is the emergency switchgear for each train, along with two transfer switch panels (TSP) and the ASP. 1.43 1.46 1.47

   Controls which are located on the TSP and ASP are listed in Table 7.4-1. Most pumps have their controls located at their respective emergency switchgear. 1.48 1.49

   Two rooms are provided to separate the redundant emergency switchgear and the transfer switch panels. The ASP panel is located in the purple switchgear room (Train B) and the two 1.50 1.51

Trains (A and B) of the ASP are separated by a non-train panel. 1.52 1.53

2. All controls and instrumentation required for the reactor hot and cold shutdown from ASP are decoupled from those normally used in the main control room in order to ensure that the control room evacuation event does not defeat the operation of equipment and controls necessary for remote shutdown in case of failure of equipment in the main control room. 1.55 1.57 1.58 1.59

3. The ASP is provided with a communication network to important plant locations which include locations of equipment required for reactor shutdown. The control room and cable spreading room can be isolated from the system by controls at the ASP. 1.60 2.2

4. The following design criteria are applicable to the instrumentation and control devices located on the ASP: 2.3

ANSI C37.90	1978	2.5
IEEE 279	1971	2.6
IEEE 308	1974	2.7
IEEE 323	1974	2.8
IEEE 344	1975	2.9
IEEE 338	1971	2.10
IEEE 379	1972	2.11
IEEE 384	1974	2.12
IEEE 420	1974	2.13
NUREG-0588	Dec. 1979	2.14
RG 1.75	Feb. 1974	2.15

5. Redundant instrumentation and controls (Train A and B) are provided on the auxiliary shutdown panel and are listed in Table 7.4-1. 2.18 2.19

6. There are no cases in which transfer from the main control room to the auxiliary shutdown panel requires a jumper or equipment to be received. 2.20 2.21

7. The design is such that transfer of equipment from the main control room to the alternate shutdown area will not change the status of the equipment. 2.22 2.23

8. Loss of offsite power will not negate shutdown capability from the remote shutdown area. 2.24 2.25

9. The design is such that access to the remote shutdown stations at the ASP, the TSPs and the 4 kV switchgear requires keys for operation of equipment. Access to these areas is under administrative control. 2.26 2.27 2.28

Each cabinet located at the remote shutdown area (TSPs, ASP) has door limit switches mounted on the front and rear doors 2.30 2.31

which annunciate in the main control room whenever personnel gain access to the equipment. Also, each transfer switch mounted on the TSPs is annunciated in the main control room whenever local control of assigned equipment has been taken over.

10. The ASP is located such that it can be safely occupied during a remote shutdown event. Ventilation temperature control and radiation protection are provided to allow continuous occupancy.

11. The design requirements for compliance with Appendix R, 10CFR50, are explained in the Millstone 3 Fire Protection Evaluation Report.

The controls available on the ASP provide the capabilities of achieving and maintaining a safe shutdown when the main control room is inaccessible. The controls necessary for immediate operator action to establish a stable plant condition are available on the ASP or in adjacent emergency switchgear rooms. The controls provide a means of sustaining the capability for boration, letdown, residual heat removal, natural circulation, continuing reactor coolant pump seal injection and for thermal barrier cooling water flow, and depressurization

The instrumentation and control functions which are required to be aligned for maintaining safe shutdown of the reactor that are discussed above are the minimum number of instrumentation and control functions.

Proper operation of other nonsafety related systems will allow a more normal shutdown to be made and maintained by preventing a transient (Section 7.7).

In considering more restrictive conditions than those discussed in Section 7.4, certain accidents and transients are postulated in the Chapter 15.0 safety analyses which take credit for safe shutdown when the protection systems reactor trip terminates the transients and the engineered safety features system mitigates the consequences of the accident. In these transients, in general, no credit is taken for the control system operation should such operation mitigate the consequences of a transient. Should such operation not mitigate the consequences of a transient, no penalties are taken in the analyses for incorrect control system actions over and above the incorrect action of the control system, whose equipment failure was assumed to have initiated the transient. These analyses in Chapter 15.0 show that safety is not adversely affected when such transients include the following:

1. Inadvertent boron dilution

2. Loss of normal feedwater

3. Loss of external electrical load and/or turbine trip

4. Loss of ac power to the station auxiliaries (station blackout) 3.7

The results of the analysis which determined the applicability of the nuclear steam supply system safe shutdown systems to the NRC General Design Criteria, IEEE Standard 279-1971, applicable NRC Regulatory Guides and other industry standards are presented in Table 7.1-1. The functions considered and listed below include both safety-related and nonsafety-related equipment. 3.9 3.10 3.11 3.12

1. Reactor trip system 3.14
2. Engineered safety features actuation system 3.15
3. Safety-related display instrumentation for post-accident monitoring 3.16
4. Main control board 3.17
5. Auxiliary shutdown station 3.18
6. Residual heat removal 3.20
7. Instrument power supply 3.21
8. Control systems 3.22

TABLE 7.4-1 1.9

INSTRUMENTS AND CONTROLS OUTSIDE CONTROL ROOM FOR COLD SHUTDOWN 1.12

Safety-Related Instruments on ASP		ASP Section 1 Electrical Train A (Orange)	ASP Section 3 Electrical Train B (Purple)	1.15 1.16 1.17 1.18
Description				
RHR Heat Exchanger Outlet Cooling Flow	(0-800 gpm)	3CCP*F167A2	3CCP*FI67B2	1.20 1.21
Boric Acid Tank 5A Level	(0-100%)	3CHS*LI102A	3CHS*LI104A	1.23
Boric Acid Tank 5B Level	(0-100%)	3CHS*LI105A	3CHS*LI106A	1.25
Stm Gen 1 Level	(0-100%)	3FWS*LI501A	3FWS*LI519A	1.27
Stm Gen 2 Level	(0-100%)	3FWS*LI529A	3FWS*LI502A	1.29
Stm Gen 3 Level	(0-100%)	3FWS*LI503A	3FWS*LI537A	1.31
Stm Gen 4 Level	(0-100%)	3FWS*LI548A	3FWS*LI504A	1.33
RCS Pressure	(0-3000 psig)	3RCS*PI405B	3RCS*PI403B	1.35
Demin Water Storage Tank Level	(0-100%)	3FWA*LI20A2	3FWA*LI20B2	1.50 1.51
Stm Gen 1 Aux Fdwtr Flow	(0-350 gpm)	3FWA*FI51A2	Note 1	1.53
Stm Gen 2 Aux Fdwtr Flow	(0-350 gpm)	Note 1	3FWA*FI33B2	1.55
Stm Gen 3 Aux Fdwtr Flow	(0-350 gpm)	Note 1	3FWA*FI33C2	1.57
Stm Gen 4 Aux Fdwtr Flow	(0-350 gpm)	3FWA*FI51D2	Note 1	1.59
Refueling Water Storage Tank Level	(0-100%)	3QSS*LI930A	3QSS*LI931A	2.1 2.2
RC Loop 1 Hot Leg Temp	(0-700°F)	3RCS*TI413C	Note 2	2.4
RC Loop 2 Hot Leg Temp	(0-700°F)	3RCS*TI423C	Note 2	2.6
RC Loop 3 Hot Leg Temp	(0-700°F)	3RCS*TI433C	Note 2	2.8
RC Loop 4 Hot Leg Temp	(0-700°F)	3RCS*TI443C	Note 2	2.10
RC Loop 1 Cold Leg Temp	(0-700°F)	Note 2	3RCS*TI413D	2.12
RC Loop 2 Cold Leg Temp	(0-700°F)	Note 2	3RCS*TI423D	2.14
RC Loop 3 Cold Leg Temp	(0-700°F)	Note 2	3RCS*TI433D	2.16

7-34

TABLE 7.4-1 (Cont)

Description		ASP Section 1 Electrical Train A (Orange)	ASP Section 3 Electrical Train B (Purple)	
RC Loop 4 Cold Leg Temp	(0-700°F)	Note 2	3RCS*TI443D	2.18
Pressurizer Level	(0-100%)	3RCS*LI459C	RCS*LI460C	2.20
Pressurizer Pressure	(1700-2500 psig)	3RCS*PI455B	3RCS*PI456B	2.22 2.23
Stm Gen 1 Pressure	(0-1300 psig)	3MSS*PI514B	3MSS*PI515B	2.25
Stm Gen 2 Pressure	(0-1300 psig)	3MSS*PI524B	3MSS*PI525B	2.27
Stm Gen 3 Pressure	(0-1300 psig)	3MSS*PI534B	3MSS*PI535B	2.29
Stm Gen 4 Pressure	(0-1300 psig)	3MSS*PI544B	3MSS*PI545B	2.31
Emer 4.16 kV Bus 34C Train A	(0-5250V)	VM2-3ENS*SWG-A	Note 3	2.33 2.34
Emer 4.16 kV Bus 34D Train B	(0-5250V)	Note 3	VM2-3ENS*SWG-B	2.36 2.37
Containment Pressure	(0-60 psia)	3LMS*PI937A	3LMS*PI936A	2.39
Safety-Related Equipment with Control Switches on ASP				2.41 2.42
Description				2.44
Aux Fdwtr Control Valve (Throttling)		3FWA*HV31A	3FWA*HV31B	2.46
Aux Fdwtr Control Valve (Throttling)		3FWA*HV31D	3FWA*HV31C	2.48
Aux Fdwtr Control Valve (Throttling)		3FWA*HV32A	3FWA*HV32B	2.50
Aux Fdwtr Control Valve (Throttling)		3FWA*HV32D	3FWA*HV32C	2.52
Aux Fdwtr Control Valve (Throttling)		3FWA*HV36B	3FWA*HV36A	2.54
Aux Fdwtr Control Valve (Throttling)		3FWA*HV36C	3FWA*HV36D	2.56
Aux Fdwtr Isolation Valve		3FWA*MOV35B	3FWA*MOV35A	2.58
Aux Fdwtr Isolation Valve		3FWA*MOV35C	3FWA*MOV35D	2.60
Aux Fdwtr Pump Alt Suction Valve		3FWA*AOV23A	3FWA*AOV23B	3.3

7-24

TABLE 7.4-1 (Cont)

Description	ASP Section 1 Electrical Train A (Orange)	ASP Section 3 Electrical Train B (Purple)	
Turbine Driven Aux Fdwtr Pump Stm Supply Valve	3MSS*AOV31A	3MSS*AOV31B	3.6 3.7
Turbine Driven Aux Fdwtr Pump Stm Supply Valve	Note 4	3MSS*AOV31D	3.9 3.10
Main Stm Pressure Relieving Valve Isol Valve	3MSS*MOV18A	3MSS*MOV18B	3.12 3.13
Main Stm Pressure Relieving Valve Isol Valve	3MSS*MOV18C	3MSS*MOV18D	3.15 3.16
Main Stm Pressure Relieving Valve Bypass Valve	3MSS*MOV74B	3MSS*MOV74A	3.18 3.19
Main Stm Pressure Relieving Valve Bypass Valve	3MSS*MOV74D	3MSS*MOV74C	3.21 3.22
Pressurizer Power Relief Valve	3RCS*PCV455A	3RCS*PCV456	3.24
Pressurizer Relief Isol Valve	3RCS*MV8000B	3RCS*MV8000A	3.26
Pressurizer Aux Spray Valve	3RCS*AV8145	Note 5	3.28
Reactor Vessel Head Vent Isol Valve	3RCS*SV8095A	3RCS*SV8095B	3.30
Reactor Vessel Head Vent Isol Valve	3RCS*SV8096A	3RCS*SV8096B	3.32
Reactor Vessel to Excess Letdown Valve	3RCS*MV8098	Note 6	3.34
Reactor Vessel to Pressurizer Relief Tank Letdown Valve	3RCS*HCV442A	3RCS*HCV442B	3.36 3.37
Pressurizer Level Control Valve	3RCS*LCV459	Note 7	3.39
Pressurizer Level Control Valve	3RCS*LCV46[illegible]	Note 7	3.41
Letdown Orifice Isol Valve	3CHS*[illegible]	Note 8	3.43
Letdown Orifice Isol Valve	3CHS*AV8149B	Note 8	3.45
Letdown Orifice Isol Valve	3CHS*AV8149C	Note 8	3.47
Letdown to CVT/GWS Divert Valve	3CHS*LCV112A	Note 9	3.49
Vol Control Tank Outlet Isol	3CHS*LCV112B	3CHS*LCV112C	3.51

7-24

TABLE 7.4-1 (Cont)

Description	ASP Section 1 Electrical Train A (Orange)	ASP Section 3 Electrical Train B (Purple)	
Valve			3.52
RWST to Charging Pump Suction Valve	3CHS*LCV112D	3CHS*LCV112E	3.54 3.55
Charging System to RCS Isol Valve	3CHS*AV8147	3CHS*AV8146	3.57
Boric Acid Gravity Feed Valve	3CHS*MV8507A	3CHS*MV8507B	3.59
Charging Header Isol Valve	3CHS*MV8438A	3CHS*MV8438B	4.1
Charging Header Isol Valve	3CHS*MV8438C	Note 10	4.3
Charging Pump A Recirc Valve	Note 11	3CHS*MV8111A	4.5
Charging Pump B Recirc Valve	Note 11	3CHS*MV8111B	4.7
Charging Pump C Recirc Valve	Note 11	3CHS*MV8111C	4.9
LPSI to Charging Pumps Suction Valve	3CHS*MV8468A	3CHS*MV8468B	4.11
Charging Header Flow Control Valve	3CHS*HVC190A	3CHS*HCV190B	4.13
Charging Header Isol Bypass Valve	3CHS*MV8116	Note 12	4.15
Charging Pump to RCS Isol Valve	3CHS*MV8105	3CHS*MV8106	4.17
Charging Pump Miniflow Control Valve	3CHS*MV8511A	3CHS*MV8511B	4.19
RHS Heat Exchanger Component Cooling Water Outlet Valve	3CCP*FV66A	3CCP*FV66B	4.21 4.22
RHS to Cold Leg Isol Valve	3SIL*MV8809A	3SIL*MV8809B	4.24
RWST to RHR Pump Suction Valve	3SIL*MV8812A	3SIL*MV8812B	4.26
Safety Injection Accumulator Tank Isol Valve	3SIL*MV8808A	3SIL*MOV8808B	4.28 4.29
Safety Injection Accumulator Tank Isol Valve	3SIL*MV8808C	3SIL*MOV8808D	4.31 4.32
Safety Injection Accumulator Tank 1 Nitrogen Supply	3SIL*SV8875A	3SIL*SV8875E	4.35 4.36
Safety Injection Accumulator Tank 2	3SIL*SV8875B	3SIL*SV8875F	4.39

7-22

TABLE 7.4-1 (Cont)

Description	ASP Section 1 Electrical Train A (Orange)	ASP Section 3 Electrical Train B (Purple)	
Nitrogen Supply			4.40
Safety Injection Accumulator Tank 3 Nitrogen Supply	3SIL*SV8875C	3SIL*SV8875G	4.42 4.43
Safety Injection Accumulator Tank 4 Nitrogen Supply	3SIL*SV8875D	3SIL*SV8875H	4.45 4.46
Safety Injection Accumulator Vent Control	3SIL*HCV943A	3SIL*HCV943B	4.48 4.49
RHS Inlet Isol Valve	3RHS*MV8701A	3RHS*MV8701B	4.51
RHS Inlet Isol Valve	3RHS*MV8701C	3RHS*MV8702B	4.53
RHS Inlet Isol Valve	3RHS*MV8702A	3RHS*MV8702C	4.55
Charging Pump Cooling Pump	3CCE*P1A	3CCE*P1B	4.57
Pressurizer Heater Backup	3RCS*H1A (Group A)	3RCS*H1B (Group B)	4.59 4.60
Cold Shutdown Air Compressor	3IAS-C2A	3IAS-C2B	5.2
Air Conditioning Unit for SI, QS, and RHR Pump Area	3HVQ*ACUS1A	3HVQ*ACUS1B	5.5 5.6
Safety-Related Miscellaneous Controls			5.9
Main Stm Line Safety Injection Block/Reset	Train A	Train B	5.11 5.12
Pressurizer Pressure Safety Injection Block/Reset	Train A	Train B	5.14 5.15
Sequencer LOP Reset	Train A	Train B	5.17
Sequencer LOP Reset Light	Train A	Train B	5.19
RCS Cold Overpressure Mitigating Arm/Block	Train A	Train B	5.22 5.23

7-24

TABLE 7.4-1 (Cont)

Nonsafety-Related Instruments on ASP Section 2/Non-Train			
Description		Mark No.	
Reserve Instrument Air Header Pressure	(0-150 psig)	3IAS-PI73B	5.40
NIS-Source Range Count Rate		3NMS-NI31C	5.43
NIS-Source Range Count Rate		3NMS-NI32C	5.45
RHR Heat Exchanger A Outlet Temp	(50-400°F)	3RHS-TI604	5.47
NIS-Intermediate Range Count Rate		3NMI-NI35C	5.50
NIS-Intermediate Range Count Rate		3NMI-NI36C	5.53
Condensate Storage Tank Level	(0-100%)	3CNS-LI15A	6.7
Volume Control Tank Level	(0-100%)	3CHS-LI112A	6.10
Letdown Flow	(0-200 gpm)	3CHS-FI132A	6.12
Regenerative Heat Exchanger Outlet Temp	(100-600°F)	3CHS-TI126A	6.14
RHR Loop B Outlet Temp	(50-400°F)	3RHS-TI605	6.17
RCP 1 Seal Water Flow	(0-15 gpm)	3CHS-FI145C	6.19
RCP 2 Seal Water Flow	(0-15 gpm)	3CHS-FI144C	6.21
RCP 3 Seal Water Flow	(0-15 gpm)	3CHS-FI143C	6.23
RCP 4 Seal Water Flow	(0-15 gpm)	3CHS-FI142C	6.25

Equipment with Nonsafety-Related Controls ASP Section 2/Non-Train			
Description			6.27
Excess Letdown Flow Control Valve		3CHS*HCV123	6.32
RHR Letdown Flow Control Valve		3CHS*HCV128	6.34

7-21

TABLE 7.4-1 (Cont)

Description	Mark No.	
Charging Flow Control Valve	3CHS*FCV121	6.36
Low Pressure Letdown Control Valve	3CHS*PCV131	6.38
RCP Seal Water Supply Control Valve	3CHS*HCV182	6.40
RHR Heat Exchanger A Outlet Flow Control	3RHS*HCV606	6.42 6.43
RHR Heat Exchanger A Bypass Control	3RHS*FCV618	6.45 6.46
RHR Heat Exchanger A Component Cooling Flow Control	3CCP*FV66A	6.48 6.49
RHR Heat Exchanger B Component Cooling Flow Control	3CCP*FV66B	6.51 6.52
RHR Heat Exchanger B Outlet Flow Control	3RHS*HCV607	6.54 6.55
RHR Heat Exchanger B Bypass Flow Control	3RHS*FCV619	6.57 6.58
Main Stm Pressure Relieving Valve	3MSS*PV20A	6.60
Main Stm Pressure Relieving Valve	3MSS*PV20B	7.2
Main Stm Pressure Relieving Valve	3MSS*PV20C	7.4
Main Stm Pressure Relieving Valve	3MSS*PV20D	7.6
Miscellaneous Controls ASP Section 2/Non-Train		7.8
White Indicator Light (Steam Line Safety Injection Blocked, Train A)		7.10
White Indicator Light (Steam Line Safety Injection Blocked, Train B)		7.12
White Indicator Light (Pressurizer Safety Injection Blocked, Train A)		7.14
White Indicator Light (Pressurizer Safety Injection Blocked, Train B)		7.16

7-21

TABLE 7.4-1 (Cont)

Safety-Related Controls on 4160V Emergency Switchgear		7.25 7.26
Motor-Driven Aux Fdwtr Pumps	3FWA*P1A, Train A	7.28
	3FWA*P1B, Train B	7.29
Charging Pumps	3CHS*P3A, Train A	7.31
	3CHS*P3B, Train B	7.32
	3CHS*P3C, Swing Pump	7.33
Service Water Pumps	3SWP*P1A, Train A	7.35
	3SWP*P1C, Train A	7.36
	3SWP*P1B, Train B	7.37
	3SWP*P1D, Train B	7.38
Reactor Plant Component Cooling Pumps	3CCP*P1A, Train A	7.40
	3CCP*P1B, Train B	7.41
	3CCP*P1C, Swing Pump	7.42
Control Building Chilled Water Pumps	3HVK*P1A, Train A	7.44
	3HVK*P1B, Train B	7.45
RHR Pumps	3RHS*P1A, Train A	7.47
	3RHS*P1B, Train B	7.48

7.2-1

TABLE 7.4-1 (Cont)

NOTES: 7.52

1. There is one auxiliary feedwater flow indicator per steam generator on the ASP - two are Train A and two are Train B. 7.54 7.55

2. The RC loop hot leg temperature indicators are Train A; the cold leg temperature indicators are Train B. 7.56

3. There is one emergency bus volt meter for each emergency bus (Trains A and B) on the ASP. 7.57

4. There are three steam supply valves for the turbine-driven auxiliary feedwater pump - one is Train A and two are Train B 7.58 7.59

5. The pressurizer auxiliary spray valve is Train A only. 7.60

6. There is no Train B reactor vessel to the excess letdown valve. 8.1

7. 3RCS*LCV459 and 460 are in series; both are Train A letdown valves. 8.2

8. The three letdown orifice isolation valves are all Train A. 8.3

9. 3CHS*LCV112A is Train A; 3CHS*AOV71 up stream of 3CHS*LCV112A is non-train and can be controlled from the main board or gaseous waste panel. 8.4 8.5

10. 3CHS*MV8438C is Train A only; it is the charging header cross connect valve. 8.6

11. 3CHS*MV8111A, B, and C - charging pump recirculation valves are all Train B. 8.7

    3CHS*MV8110 is the Train A common recirculation valve and can be operated from the main control board; it is normally OPEN. 8.9 8.10

12. The charging header isolation bypass valve is Train A only. 8.12

Open Items

Instrumentation and Control Systems Branch

ICSB-11 IE Bulletin 79-27 Concerns (Draft SER Section 7.5.2.1)

The staff requested that the applicant review the adequacy of emergency operating procedures to be used by control room operators to attain safe shutdown on loss of any Class IE or non-Class IE bus supplying power to safety-or non safety-related instrument and control systems. This issue was addressed for operating reactors through IE Bulletin 79-27. In FSAR Amendment No. 5, the applicant responded that Millstone Unit 3 can achieve a cold shutdown condition without the use of any non-class IE power. All the equipment required to achieve a cold shutdown is redundant and is powered from redundant Class IE buses, which satisfies the single failure criterion. However, the staff pointed out that loss of a single instrument bus could affect the interlock circuits to isolate both trains of Residual Heat Removal system, therefore, the applicant's response did not adequately address the concerns identified in IE Bulletin 79-27. The staff requested that the applicant re-evaluate his response to resolve this concern. Additional information is required to address items requested in IE Bulletin 79-27. This is an open item.

Response (3/84)

Refer to the revised response to Question 420.1. The NRC Staff requested to provide additional information on the testing procedure for RHR isolation valves.

Status (3/84)

Confirmatory.

NRC Letter: May 31, 1983

Question Q420.1 (Section 7.5)

Provide response to IE Bulletin 79-27 concerns. (An event requiring operator action concurrent with failure of important instrumentation upon which these operator actions should be based.)

Response:

~~The Applicant~~ has reviewed the Class 1E and non-Class 1E bus power supply to safety and nonsafety related instrumentation and control systems which could affect the ability to achieve a cold shutdown condition.

Millstone Unit 3 can achieve a cold shutdown condition without the use of any non-Class 1E power. The station is designed in compliance with Regulatory Guides 1.139 and 1.53. Since all the equipment required to achieve a cold shutdown is redundant and is powered from redundant Class 1E buses, the single failure criteria is satisfied. Loss of power on Class 1E or loss of power on non-Class 1E buses is annunciated on the main control board. Plant procedures will be developed to meet the operational concerns of IE Bulletin 79-27.

~~See Rev~~ INSERT 'A'

INSERT 'A'

Response

The applicant has reviewed the class 1E and non-class 1E bus power supply to safety and non-safety related instrumentation and control systems which could affect the ability to achieve a cold shutdown condition.

Millstone Unit 3 can achieve a cold shutdown condition without the use of any non-class 1E power. The station is designed in compliance with Regulatory Guides 1.139 and 1.53. Since all the equipment required to achieve a cold shutdown is redundant and is powered from redundant class 1E buses, the single failure criteria is satisfied.

An exception to the above single failure criteria on redundant buses are the Residual Heat Removal (RHR) isolation valves.

An event that could be postulated to occur in the system that could render the system inoperable is that a loss of offsite power coincident with a loss of a diesel generator which powers one of the suction valves in each RHR trains. This loss of power could prevent system operation even though that system is available from the train that has not experienced a diesel failure. The system is designed with three valves in series on the suction side of each pump. Two of these valves are powered from the same diesel that powers the pump, and are located inside the containment structure. The third valve is located outside of the containment in the ESF building, and is powered from the diesel of the opposite train.

The system as designed complies to all the requirements for isolating the Reactor Coolant System (RCS) from the RHR system during normal plant operation when the RCS pressure is greater than 750 psig. However, if we impose the criteria that we must consider a loss of power, then we must consider the loss of the suction valve in the active train.

If the event as described above were to occur, the following operator action would have to be taken to put the RHR into service after the RCS pressure has been reduced to 425 psig. The valve in the ESF building must be manually opened. To accomplish this, the key which opens the padlock on the handwheel of the valve without power must be obtained from the shift supervisor in the main control room. After obtaining the key, the breaker for the affected valve should be racked open and the padlock removed from the handwheel. The valve can now be opened by using the handwheel. After this is accomplished the control room operator can open the valves located inside containment from the main control board and start the RHR pump on the active train. If the system pressure subsequently increases to above a 750 psig the valve inside the containment would automatically close and isolate the system.

In addition, plant procedures will be developed to meet these operational concerns.

Open Items

Instrumentation and Control Systems Branch

ICSB-12 Bypass and Inoperable Status Panel (Draft SER Section 7.5.2.2)

The FSAR Section 1.8 states that Millstone 3 design is in conformance with R. G. 1.47, Bypassed and inoperable status indication for nuclear power plant safety systems. During the review, the staff reviewed design drawings which contain information of the bypass and inoperable status panel. However, there is no information in the FSAR to describe the system. The staff requested that the applicant provides the descriptive information in Section 7.5 of the FSAR to demonstrate conformance with R. G. 1.47. This is an open item.

Response (3/84)

See revised FSAR Section 7.5.

Status (3/84)

Closed.

7.5.2 Analysis

Analyses for compliance with the requirements of this section are addressed in Table 7.5-1. Further information is provided in the Millstone 3 Design Basis Response to Regulatory Guide 1.97, Revision 2, as referenced in Section 1.7.

7.5.3 Compliance with other Regulatory Requirements

1. Compliance with Regulatory Guide 1.47 for bypassed and inoperable status design philosophy is described below.

   a. An indicator of bypass is provided for each protection system. "Bypass" includes any deliberate action which renders a protection system inoperable.

   b. The indicator is at the system level, not the channel or component level. (Quench spray is a system. A quench spray pump is a component.) There is a separate indicator for each train.

   c. The indicator is operated automatically only by actions which meet all these criteria:

      - The action is deliberate. (Component failure may be indicated by component failure indicators but should not operate the system bypass indicator. It is not the intent of the indicator to show operator errors or component failures.)

      - The action is expected to occur more often than once a year. This "more often than once a year" criterion should be interpreted liberally. If an accessible, permanently installed electrical control device will bypass a safety system, assume that it will be used more than once a year.

        Devices within the containment are not accessible.

      - The action is expected when the protection system must be operable. (Bypass of source range flux trip during normal power operation should not, for example, be indicated on the system bypass indicator. It may be indicated on a channel or component status indicator.)

      - The action renders the system inoperable, not merely potentially inoperable. (If, for example, redundant, parallel, 100 percent valves are provided for the discharge line of a spray pump, the system bypass indicator should not be actuated by the closing of only one of those valves. Valve closing may be indicated on a component status indicator. If both valves have been deliberately moved from the "Open"

8-8

position, the system bypass indicator should be operated. If, on the other hand, each valve carried only 50 percent flow, the system would be inoperable if either was not open. That inoperability should be indicated at the system level. Also, if a system is put in the "Trip" mode during test, there should be no operation of the system bypass indicator. Such a test may be indicated on a channel status indicator. If a channel is put into bypass mode for test and sufficient redundant channels remain capable of operating the protection system and not more than one channel at a time is expected to be tested, the channel bypass should not be indicated at the system level. If an actuation signal will override the bypass, the system bypass indicator should not be operated.

- Some deliberate action has been taken place in the protection system or a necessary supporting system. (For example, if the cooling water inlet valve for a recirculation spray heat exchanger is deliberately closed, the system bypass indicator for the recirculation spray system should be operated.)

c. The bypass indicators are separate from other plant indicators and grouped in a logical fashion.

d. A capability is provided to operate each bypass indicator manually. This lets the operator provide bypass indication for an event that renders a safety system inoperable but does not automatically operate the system bypass indicator.

e. There is not any capability to defeat an automatic operation of a bypass indicator. (Audible alarms may be silenced.)

f. The bypass indicators are accompanied by audible alarm.

g. No immediate operator action is required as a result of any system bypass indication.

h. The indication system is mechanically and electrically isolated from the safety system to avoid degradation of the safety system. No fault in the indicator system can impair the ability of the safety system to perform its safety-related function. The bypass indicators are not considered safety-related; i.e., they need not be designed to safety system criteria such as IEEE-279.

i. In accordance with IEE-279, Paragraph 4.20, the operator must be able to determine why a system level bypass is indicated. This information is provided by the plant computer.

8-7

j. Service water system inoperative and diesel generator inoperative indicators are provided. These support systems are unique. They are important enough to warrant bypass indicators, but these indicators are differentiated from saftey system bypass indicators by color. 2.18 2.19 2.20 2.21

k. System design meets the recommendations of ICBS-21 as follows: 2.22

- Each safety system has a Train A (orange) and Train B (purple) bypass indicator. The indicators are grouped together by train on the main contol board. Support systems have white bypass indicators and are arranged together with the associated train of bypass indicators. 2.24 2.25 2.26

- Millstone 3 has no shared safety systems. 2.27 8-8

- Means by which the operator can cancel erroneous bypassed indications are not provided. 2.28

- The bypass indication systems does not perform functions essential to safety. No operator action is required based solely on the bypass indication. 2.29 2.30

- The indication system has no effect on plant safety systems. 2.31

- The bypass indicating and annunciating function can be tested during normal plant operation. 2.32

2. Compliance with Regulatory Guide 1.75 for separation criteria is described in Section 1.8 and the separate report on Regulatory Guide 1.97. 2.34 2.35

3. Compliance with Regulatory Guide 1.105 for instrument spans and setpoints is described in Sections 1.8, 7.1 and the separate report on Regulatory Guide 1.97. 2.36 2.37

4. The safety parameter display system (SPDS) and the emergency response facilities (ERF) requirements are currently being finalized. This information will be provided in a future amendment. 2.38 2.39 2.40

Open Items

Instrumentation and Control Systems Branch

ICSB-13 NUREG-0737 Item II.F.1 Accident Monitoring
Instrumentation Position (4), (5), and (6) (Draft SER Section 7.5.2.4)

Position (4), (5), and (6) of this action plan item require installation of the extended range containment pressure monitors, containment water level monitors, and containment hydrogen concentration monitors. Table 7.5-1 of the FSAR indicated that information on these parameters will be provided later. This is an open item.

Response (3/84)

Refer to the revised FSAR Table 7.5-1.

Status (3/84)

Closed.

TABLE 7.5-1 (Cont)

Variable	Range/Status	Type/ Category	Qualification Environmental	Qualification Seismic	Number of Channels	Indicator Device	Implementation Data
Containment hydrogen concentration	0-10%	A1, B1, C1	~~Later~~ Yes	~~Later~~ Yes	~~Later~~ 2	~~Later~~ 2 meters 1 recorder	Core load
Neutron flux	10^{-9} - 125%	B1	Yes	Yes	2 per reactor	2 meter displays	Core load
Containment water level (wide range)	~~Later~~ 0 - 1,500,000 GAL	A1, B2, C2	Yes	Yes	2 per plant	2 meters 1 recorder	Core load
Main steamline isolation valve	Open/closed	B2, D2	Yes	Yes	1 per valve	1 pair of lights per valve	Complete
Main steamline bypass valve	Open/closed	D2	Yes	Yes	1 per valve	1 pair of lights per valve	Complete
Control rod position	0-228 steps	B3	No	No	1/rod	1 position light/rod	Complete
RCS pressure (extended range)	0-3500 psig	A1, C1	Yes	Yes	2 per plant	2 meters 1 recorder	Core load
Containment pressure (extended range)	0-200 psia	C1	Yes	Yes	2 per plant	2 meters 1 dual recorder	Core load
Containment isolation valve status	Open/closed	C2	Yes	Yes	1 per valve	1 pair of lights per valve	Complete
Hydrogen recombiner cubicle ventilation radiation	7.1×10^{-4} µCi/cc - 7.1 µCi/cc	C2, E2	Yes	Yes	2 per plant	2 recorders, CRT, digital display meter	Complete
Turbine driven auxiliary feedwater pump steam exhaust radiation	10_3^{-1} µCi/cc - $10^{}$ µCi/cc	C2, E2	Yes	Yes	1 per plant	CRT	Complete
Ventilation vent (extended range)	10_5^{-7} µCi/cc - 10^{5} µCi/cc	C2, E2	Yes	Yes	1 per plant	1 recorder, CRT, digital display meter	Complete
Supplementary leak collection (extended range)	10_5^{-7} µCi/cc - 10^{5} µCi/cc	C2, E2	Yes	Yes	1 per plant	1 recorder	Complete

Open Items

Instrumentation and Control Systems Branch

ICSB-16 RHR System Isolation Valve Interlock (Draft SER Section 7.6.2.1)

There are several inconsistencies in the FSAR description of the RHR valve interlocks. Section 7.6.2.1 states that the pressure limit is 700 psig, but in Section 5.4.7.2.4 states that the limit is 750 psig. Figure 7.6-1 shows additional interlocks on valve open circuits that is neither mentioned in Section 7.6.2.1 nor in Section 5.4.7.2.4. The applicant has not addressed the requirements of Branch Technical Position ICSB-3 for using diverse pressure transmitters. This is an open item.

Response (3/84)

Refer to revised FSAR Sections 7.6.2.1, 7.3, 6.3.2.1, 6.3.2.8 and Figure 6.3-36 (1 of 1).

Status (3/84)

Closed.

a. Charging pumps start on SIS

b. RWST suction valves to charging pumps open on SIS

c. Charging pumps to RCS cold leg injection headers parallel isolation valves open on SIS

d. Normal charging path valves close on SIS

e. Charging pump miniflow valves close on SIS

f. Safety injection pumps start on SIS

g. The RHS pumps start on SIS

h. Any closed accumulator isolation valves open

i. Volume control tank (VCT) outlet isolation valves close on SIS

2. Switchover from injection mode to recirculation involves the following interlocks:

a. The residual heat removal system (RHS) pumps are stopped automatically when one of the two low-low level transmitters indicates a Low-Low level in the RWST.

Switches → detect

b. Interlocks are provided to assure isolation of the RHS and proper alignment of the containment recirculation system for core cooling.

c. The safety injection pump and charging pump recirculation suction isolation valves can be opened provided that the safety injection pump miniflow lines have been isolated.

d. After approximately 15 hours, cold leg recirculation is terminated and hot leg recirculation is initiated. This is done to terminate any boiling in the core should the break be in one of the RCS cold legs, and to prevent boron precipitation.

A. RHS Pump Interlock from Injection to Recirculation

The details of achieving cold leg recirculation following safety injection are given in Section 6.3.2 and in Table 6.3-7. Figure 7.6-3 shows the logic which is used to automatically control RHS pumps.

B. Sequenced Safeguard Signals

A sequenced safeguard signal is generated by the emergency generator LOAD SEQUENCE for the safety injection pump, RHS pump, or charging pump whenever the signals listed with the associated pumps exist.

Also for 930, 932

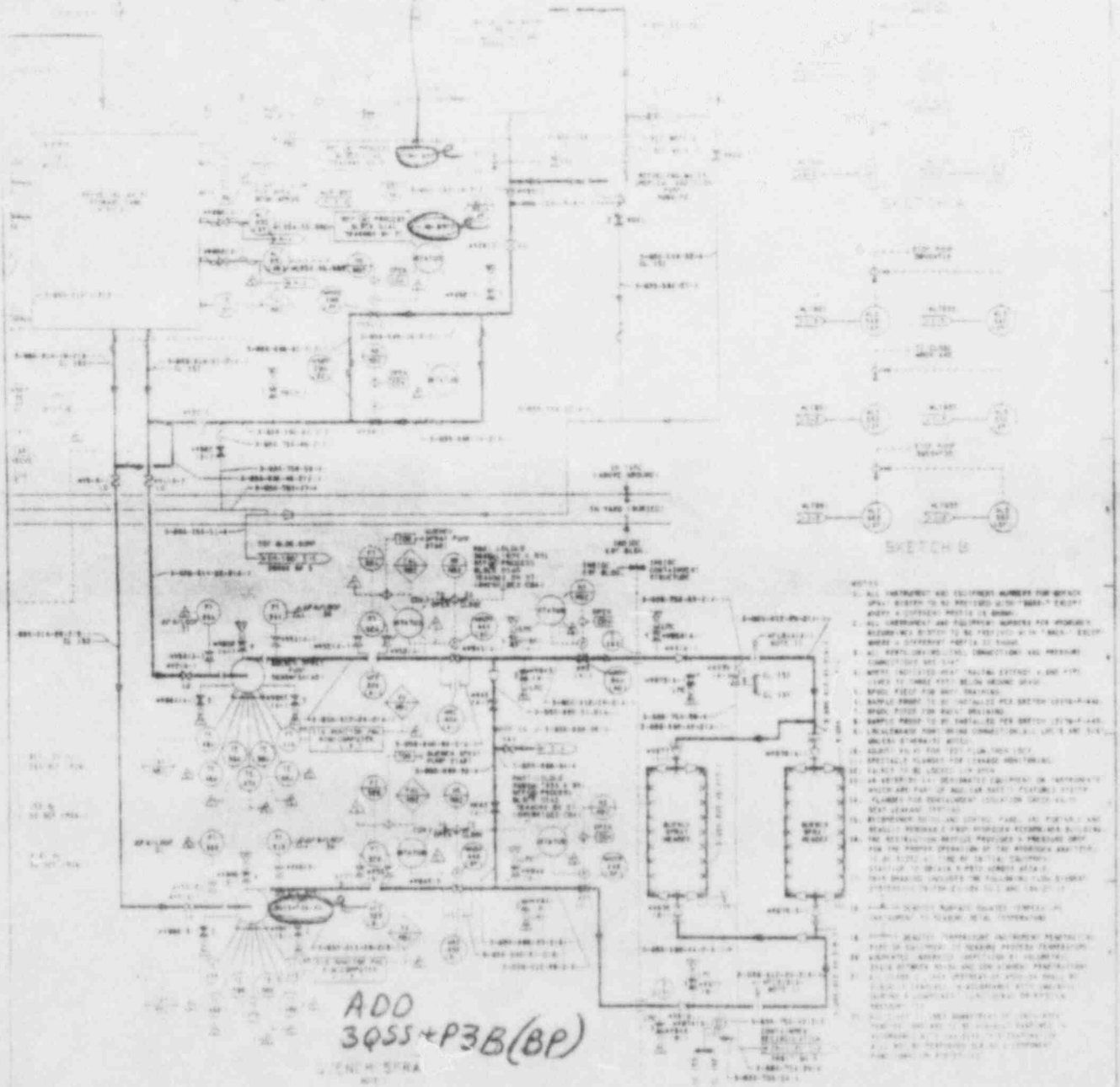


FIGURE 6.2-36 (1 OF 1)
QUENCH SPRAY & HYDROGEN RECOMBINER SYSTEM
MILLSTONE NUCLEAR POWER STATION UNIT 3
FINAL SAFETY ANALYSIS REPORT

Do not Type

LOCA even assuming a single failure in the emergency power system such as the failure of one diesel to start.

6.3.2.2 Piping and Instrumentation Diagrams

The process flow diagrams of the ECCS are shown on Figure 6.3-1. The piping and instrumentation diagrams associated with the ECCS are shown on Figures 6.2-37 and 6.3-2. Pertinent design and operating parameters for the components of the ECCS are given in Table 6.3-1. The codes and standards to which the individual components of the ECCS are designed are listed in Table 3.2-1.

The component interlocks used in different modes of system operation are listed below:

1. The safety injection signal (SIS) is interlocked with the following components and initiates the indicated action:

   a. Charging pumps start on SIS

   b. RWST suction valves to charging pumps open on SIS

   c. Charging pumps to RCS cold leg injection headers parallel isolation valves open on SIS

   d. Normal charging path valves close on SIS

   e. Charging pump miniflow valves close on SIS

   f. Safety injection pumps start on SIS

   g. The RHR pumps start on SIS

   h. Any closed accumulator isolation valves open

   i. Volume control tank (VCT) outlet isolation valves close on SIS

2. Switchover from injection mode to recirculation involves the following interlocks:

   a. The RHS pumps are stopped automatically when ~~two~~ ONE (two) of the ~~low~~ low level ~~transmitters~~ switches ~~indicate~~ detect a low-low level in the RWST. X X

   b. Interlocks are provided to assure isolation of the RHS and proper alignment of the containment recirculation system for core cooling.

   c. The safety injection pump and charging pump recirculation suction isolation valves can be opened provided that the safety injection pump miniflow lines have been isolated.

Do not Type

6.3.2.2.8 Manual Actions

Manual actions are the key to the success for proper operation of the ECCS during the changeover of operation. The changeover from the injection mode to recirculation mode is initiated automatically and completed locally by operator action from the main control room. These actions are delineated in Table 6.3-7. ~~Interlock~~ logic is provided to automatically stop the ~~two~~ pumps when ~~one~~ of ~~four~~ refueling water storage tank level ~~channels~~ indicate a RWST level less than a low-low level setpoint in conjunction with the initiation of the SIS.

The two charging pumps and the two safety injection pumps would continue to take suction from the refueling water storage tank following the above automatic action until manual operator action is taken to align these pumps in series with the containment recirculation pumps.

~~The RWST low level protection logic consists of four level channels with each level channel assigned to a separate process control protection set. Four RWST level transmitters provide level signals to corresponding normally deenergized level channel bistables. Each level channel bistable would be energized on receipt of a RWST level signal less than the low level setpoint.~~

Four RWST level transmitters provide level indication. The ~~Four~~ level switches are used to sense low-low level.

~~Two~~ One out of ~~four~~ two ~~redundant~~ logic ~~is~~ are utilized ~~in both protection cabinets A and B~~ in both trains to ensure a trip signal, ~~in the event that two of the four level channel bistables are energized~~. This trip signal, in conjunction with the SIS, provides the actuation signal to stop the corresponding RHR pump.

The low-low RWST level signal is also alarmed to inform the operator to initiate the manual action required to realign the charging, safety injection, and containment recirculation pumps for the recirculation mode. The manual switchover sequence that must be performed by the operator is delineated in Table 6.3-7. Following the automatic and manual switchover sequence, the containment recirculation pumps would take suction from the containment sump and deliver borated water directly to the RCS cold legs. A portion of the recirculation pump discharge flow would be used to provide suction to the two safety injection pumps which would also deliver directly to the RCS cold legs. As part of the manual switchover procedure (Table 6.3-7, Step 4-C), the suctions of the safety injection and charging pumps are cross-connected in the event of the failure of either recirculation pump.

Section 7.5 gives process information available to the operator in the control room following an accident.

The remaining inventory in the RWST below the low-low level is large enough to allow sufficient time for manual realignment of the charging and safety injection pumps.

7.6 ALL OTHER SYSTEMS REQUIRED FOR SAFETY

7.6.1 Instrumentation and Control Power Supply System

The instrumentation and control power supply system is described in Section 8.3.

7.6.2 Residual Heat Removal Isolation Valves

7.6.2.1 Description

The residual heat removal system (RHS) isolation valves are normally closed and are only opened for residual heat removal after system pressure is reduced to approximately 425 psig.

The RHS valves are provided with red (OPEN) and green (CLOSED) position indicating lights located at the keylock control switch for each valve. These lights are powered by valve control power and actuated by valve motor operator limit switches.

There are three motor-operated valves in series in each of the two RHS pump suction lines from the reactor coolant system (RCS) hot legs. Two valves in series located close to the containment walls, one inside containment and one outside containment, are provided with interlocks. The interlock features provided for the isolation valves are identical for both trains and are shown on Figure 7.6-1.

Each of the two valves is interlocked so that it cannot be opened unless the RCS pressure is below approximately 425 psig. This interlock prevents the valve from being opened when the RCS pressure plus the RHS pump pressure would be above the RHS system design pressure. A second pressure interlock is provided to close the valve automatically if the RCS pressure subsequently increases to above (750) psig. These interlocks for each train are independent and diverse, derived from signals generated by transmitters manufactured by two different vendors.

The third valve in each train is located inside the containment and is operated by a keylock control switch. No interlocks are provided.

7.6.2.2 Analysis

Based on the scope definitions presented in IEEE Standard 279-1971 and 338-1971, these criteria do not apply to the RHS isolation valve interlocks; however, in order to meet NRC requirements and because of the possible severity of the consequences of loss of function, the requirements of IEEE Standard 279-1971 will be applied with the following comments:

1. For the purpose of applying IEEE Standard 279-1971, to this circuit, the following definitions will be used.

   a. Protection System

      The two valves in series in each line and all components of their interlocking and closure circuits

Open Items

Instrumentation and Control Systems Branch

ICSB-17 Isolation of Low Pressure Systems
From the High Pressure RCS (Draft SER Section 7.6.2.2)

General Design Criteria 15 requires that reactor coolant system and associated auxiliary, control and protection system shall be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation including anticipated operational occurrences. The staff requested that the applicant identify all points of interface between the Reactor Coolant System (RCS) and systems whose design pressure is less than that of the RCS and for each interface to discuss the degree of conformance to the requirements of Branch Technical Position ICSB No. 3 and how the associated interlock circuits conform to the requirements of IEEE 279. This is an open item.

Response (3/84)

A review was conducted to identify low-pressure system interfaces with the RCS. Interface points which consist of passive pressure boundary barriers (reactor coolant pump thermal barriers and seals, manually operated normally closed valves), or lines designed to be exposed to the RCS at full pressure (PORV discharge lines) were not considered; such boundaries are designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation. The remaining interface points, and a description of their isolation provisions are provided below:

a) Residual Heat Removal System Suction Lines - The isolation valve arrangement for these two lines is shown in Figure 5.4-5. Each line has three motor-operated isolation valves in series. The valves are interlocked to prevent opening and to automatically close at RCS pressures which are high enough to damage the RHR system. These interlocks are described in Sections 5.4.7.2.4 and 7.6.2 of the FSAR. The outermost isolation valve in each suction line is on a different safety-related power train, than the two innermost isolation valves. Valve position indication for all six valves is provided at the main control board.

   The RCS pressure boundary is located at the second valve from the RCS (MV8701A, 8702B) during normal operation. The two valves just outside containment (MV8701B, 8702A) provide additional assurance of containment isolation during power operation.

   During shutdown cooling, overpressure protection of the RHR system is provided by relief valves on the suction lines (RV870A, B) and administrative controls. The relief valves are designed to protect the RHR system from the inadvertent start of two charging pumps, on two high pressure safety injection pumps. Should RCS pressure increase above RHR design pressure, despite the relief valves, the RHR suction valves will automatically close.

b) Reactor Coolant System Letdown Line - The letdown line isolation valve arrangement consists of two series valves (LCV-459, 460) at the RCS (Figure 5.1-1, Sheet 2) two series valves at the containment penetration (CV-8152, 8160) and three parallel valves at the letdown orifices (SV-8149A, B, C) (Figure 9.3-8, Sheet 1).

All of these valves are air-operated and are designed to fail-closed on loss of air or loss of electrical signal. Valve position indication is provided in the control room. The two containment isolation valve control circuits are on separate emergency power trains.

Although the piping between the two containment isolation valves is of a lower design pressure than RCS pressure, a relief valve, which discharges to the pressurizer relief tank (RV-8117), protects this section of piping from overpressure, should the downstream isolation valve (CV-8152) close while the upstream valves remain open. The CVCS letdown orifices restrict letdown line flow so that relief valve capacity is not exceeded.

c) Excess Letdown Lines - These lines contain two different types of isolation valve arrangements, as shown on Figures 5.1-1, Sheet 3 and Figure 9.3-7, Sheet 1:

1) One line is connected to the reactor vessel head vent system, downstream of valves SV-8095A,B and SV-8096A,B. These valves provide the primary means of isolating the RCS from downstream piping. Additional isolation capability is provided by downstream series valves MV-8098 and HCV-123. As can be seen from Figures 5.1-1, Sheet 3 and 9.3-7, Sheet 1, four series normally closed valves must be opened to allow communication of fluid pressure between the RCS, and the low pressure portion of the excess letdown line. These consist of two fail-closed solenoid valves which are operated by emergency power on the head vent system, a motor-operated valve actuated by emergency power (MV-8098), and a fail-closed, air-operated valve actuated by a nonsafety grade control circuit. All of these valves have handswitches and position indication in the control room.

2) There are four drain line connections for excess letdown on the RCS cold legs (Figure 5.1-1, Sheet 3). Each of these has a normally closed, fail-closed isolation valve (AV-8037 A, B, C, D). These are headered together, and further isolated from the low pressure portion of excess letdown piping by normally closed, fail-closed, series valves AV-8153 and HCV-123. AV-8153 is controlled by a safety grade control circuit, and HCV-123 by a nonsafety grade control circuit. All of the isolation valves have position indication and hand switches in the control room.

d) Sample System - The sample system is connected to the RCS at the hot legs, the cold legs, and the pressurizer liquid and vapor spaces (Figure 9.3-2, Sheet 2). The low pressure portion of the sampling system is normally

isolated from RCS pressure by a normally closed, fail-closed solenoid valve, and a back pressure actuated pressure regulating valve. The solenoid valve is actuated by a non-safety grade power source, and is controlled at the sample panel.

Additional overpressure protection is provided by a flow restricting orifice upstream of the pressure regulating valve, and a relief valve downstream of the pressure regulating valve. Finally, additional isolation capability is provided for each sample line by two series, normally open, fail-closed, solenoid valves. These valves are powered by diverse safety-related power supplies and have handswitches and position indication in the control room. They are located between the normally closed solenoid valve and the pressure regulating valve.

e) Charging Line Connection - The CVCS charging line connects to the RCS at the loop 1 and loop 4 cold legs, and at the auxiliary spray line at the pressurizer (Figure 9.3-8, Sheet 1). The charging line downstream of the charging pumps is designed to the same pressure as the RCS, and normally operates at a slightly greater pressure than the RCS.

The boundary between the RCS cold legs and the CVCS charging lines consists of two series check valves on each line (V-31, 32 on loop 1; V-147, 148 on loop 4). The boundary between the CVCS and the pressurizer consists of a check valve (V-175) in series with a normally closed, fail closed air operated valve (AV-8145). AV-8145 has main control board indication, and control, and its control circuit is connected to a safety-related train.

Additional motor operated, air operated, and check valves are available in the charging line, to provide further assurance of isolation when required.

f) ECCS Discharge Line Connections - The ECCS discharge lines connect to RCS at the following locations:

a) Interface between the LPSI/HPSI systems and the RCS cold legs (four points).

b) Interface between the charging pumps and the RCS cold legs (four points).

c) Interface between HPSI/LPSI systems and the RCS hot legs (four points).

These interface points are shown on Figure 5.1-1, Sheets 1 and 2. At least two series check valves separate the RCS from the ECCS at the above points. A leakage detection line is connected between the check valves to allow periodic monitoring of any leakage past the check valve closest to the RCS. The leakage detection lines are headered together and discharge to the Reactor Plant Gaseous Drains System (Figure 6.3-2, Sheet 1).

Open Items

Instrumentation and Control Systems Branch

Isolation between the high and low pressure portions of the leakage detection line is achieved by two series, normally closed, fail closed air operated valves (CV8871, 8964). These valves have hand switches and position indication in the control room. The control signal for each valve comes from a separate safety related train, and both valves close automatically on a CIA.

We consider the isolation provisions between the RCS and connected lower pressure systems discussed in this response to meet or exceed the intent of BTP ICSB 3.

Status (3/84)

Closed

Open Items

Instrumentation and Control Systems Branch

ICSB-18 RCS Overpressure Protection (Draft SER Section 7.6.2.3)

The reactor coolant system overpressure protection during low temperature operation is provided by the automatic opening of two pressurizer power operated relief valves (PORV). The actuation logic for PORV continuously monitors RCS temperature and pressure conditions. When pressure exceeds the programmed limit, an alarm will alert the operator to manually arm the system by a switch located on the main control board. During the design review, the staff raised a concern that a single failure could preclude the automatic actuation for all modes of operation including low temperature operation. The applicant noted that the design has not been finalized. This is an open item.

Response (3/84)

The design of pressurizer PORV control and block valves was discussed at the ICSB meeting. The discussion focused on the possibility that a single failure could preclude the automatic actuation logic for all modes of operation including low temperature operation. The electrical schematics for Pressurizer PORV control and the block valves control were provided to the NRC Staff review and the Staff accepted the schematic used to preclude the above concern.

Status (3/84)

Closed.

Open Items

Instrumentation and Control Systems Branch

ICSB-19 Reactor Coolant System Loop Isolation Valve Interlocks (Draft SER Section 7.6.2.5)

The FSAR Section 7.6.5 describes the reactor coolant system loop isolation valve interlocks. The description is incomplete and additional information is required to clarify that the design is in conformance with IEEE-279 requirements. This is an open item.

Response (3/84)

A discussion of the reactor coolant loop isolation valve interlocks was provided during the ICSB meeting. The applicant has determined to use the option of N-1 loop operation for Millstone 3 and appropriate changes to the FSAR will be submitted to the NRC for review when finalized.

Status (3/84)

Open.

Open Items

Instrumentation and Control Systems Branch

ICSB-21 Control System Failure Caused By High-Energy Line Breaks (Draft SER Section 7.2.2.2)

Operating reactor licensees were informed by IE Information Notice 79-22, that if certain non safety-grade control equipment were subjected to the adverse environment of a high energy line break, it may impact the safety analyses and the adequacy of the protection functions performed by the safety-grade equipment. The staff has requested a review to determine whether the harsh environment associated with high-energy line breaks might cause control system malfunction and result in a consequence more severe than those of the FSAR Chapter 15 analyses or beyond the capability of operators or safety systems.

The applicant has not provided a response to this open item.

Response (3/84)

The attached response to Question 420.3 was provided and discussed at the ICSB meeting. The staff requested to revise and modify the response to consider effects of harsh environment associated with high-energy line breaks on PORV control system.

Status (3/84)

Open.

NRC Letter: May 31, 1983

Question Q420.3 (Section 7.7)

Provide response to IE Information Notice 79-22 concerns. (Control system malfunction due to a high energy break inside or outside of containment.)

Response:

Steam Generator Power Operated Relief Valve Control System

During normal plant operation, steam generator relief is accomplished by 3MSS*PV20. This valve is controlled by nonsafety-related instrumentation which will automatically modulate the valve. Should these nonsafety-related controls malfunction, resulting in high steam generator pressure, the main steam safety valves will relieve the pressure. Safety-related analog indication is available in the control room to alert the operator to take manual control of the main steam pressure relief bypass valve (3MSS*MOV74), which is safety-related. Should a malfunction result in low steam generator pressure, there is safety-related analog indication in the control room to alert the operator to manually close the main steam pressure relief isolation valve (3MSS*MOV18), which is safety-related. In addition, excessive low steam line pressure will result in main steam isolation and SIS.

Pressurizer Power Operated Relief Valve Control System

Should a malfunction of the nonsafety-related elements in the automatic control circuit of the pressurizer PORVs result in high or low pressurizer pressure, there is safety-related instrumentation in the control room to alert the operator of the condition so that the operator can then manually control the PORVs using the safety-related control switch on the main control board.

Main Feedwater Control System

As discussed in FSAR Section 10.4.7.3, a malfunction in the nonsafety-related portion of the feedwater system could lead to one of two possible events: high water level inventory within a steam generator or low water level within a steam generator. For either case, level is monitored by fully qualified safety-related instrumentation which initiates protective action to fully qualified safety-related equipment. Therefore, no nonsafety-related failure could impact the protective functions performed by the safety-related equipment.

Automatic Rod Control System

Westinghouse WCAP-8976 provides a failure modes and effects analysis of the solid state, full length rod control system (FLRCS). Attachment Q420.3-1 is an abstract which summarizes the WCAP, concluding that the design of the FLRCS will perform its intended

DELETE AND ADD INSERT A'

reactivity control function accounting for failure of single active components.

ATTACHMENT Q420.3-1

The full length rod control system (FLRCS) controls the power to the rod drive mechanisms for rod movement in response to signals received from the reactor control system, or from signals generated through reactor operator action. Rod movement is used to control reactivity of the reactor during plant operation. The FLRCS is designed to perform its reactivity control function in conjunction with the reactor control and protection system to maintain the reactor core with design safety limits.

By the use of a failure mode and effects analysis, it is shown that the FLRCS will perform its reactivity control functions considering the loss of single active components. That is, sufficient fault limiting control circuits are provided which block control rod movement and/or indicate presence of a fault condition at the control board. Reactor operator action or automatic reactor trip will thus mitigate the consequences of potential failure of the FLRCS. The analysis also qualitatively demonstrates the reliability of the FLCRS to perform its intended function.

INSERT 'A'

STEAMLINE BREAK COINCIDENT WITH CONTROL ROD WITHDRAWAL

INTRODUCTION

During a high energy line break (such as a steamline rupture), certain sensors used in control systems could be exposed to an adverse environment. If the equipment is not qualified for the adverse environment, a control system malfunction may occur.

The automatic rod control system is one of the control systems that could malfunction. The rod control system relies on measurements of T_{avg}, nuclear power, and turbine impulse pressure to determine if control rod motion is required. A small steamline rupture may occur outside of containment in the vicinity of the turbine impulse pressure transmitters, or inside containment in the vicinity of the excore detectors, thus exposing equipment used in rod control to an adverse environment. If the associated cabling and connections are not properly qualified, then the potential for steam impinging on this equipment and causing a control system malfunction must be addressed. One type of resultant malfunction may initiate the withdrawal of the control rods coincident with the steamline break.

An analysis was made of steamline break with coincident withdrawal of the control rods to address the rod control system malfunction due to an adverse environment.

AVAILABLE PROTECTION

The following functions provide protection during this rod withdrawal type of transient:

Reactor Trip

- Power range neutron flux instrumentation actuates a reactor trip if two out of four channels exceed an overpower setpoint.

- A reactor trip is actuated if any two out of four ΔT channels exceed the overpower ΔT setpoint.

- A high pressurizer pressure reactor trip is actuated from any two out of four pressure channels which are set at a fixed point. This set pressure is less than the set pressure for the pressurizer safety valves.

- A high ~~pressure~~ pressurizer water level reactor trip is actuated from any two out of three level channels when the reactor power is above approximately 10 percent (Permissive 7).

- A reactor trip is actuated subsequent to SIS actuation. SI may be actuated as a result of the steam line break.

RCCA Withdrawal Blocks

- High neutron flux (one out of four power range)

- Overpower ΔT (two out of four)

- Overtemperature ΔT (two out of four)

The following functions provide protection for the steam line break:

Safety Injection

- Two out of four low pressurizer pressure signals

- Two out of three low steamline pressure signals in any one loop

Feedwater Isolation

Sustained high feedwater flow would cause additional cooldown. Therefore, in addition to the normal control action, which will close the main feedwater valves following a reactor trip, an SI signal will rapidly close all feedwater control valves and backup feedwater isolation valves, trip the main feedwater pumps, and close the feedwater pump discharge valves.

Steam Line Isolation

- Safety injection system actuation derived from two out of three low steamline pressure signal in any one loop (above Permissive-11)

- Two out of three high negative steam pressure rate in any one loop (below Permissive-11)

All of the above functions may be actuated by a SLB/RCCA withdrawal transient.

ANALYSIS OF EFFECTS AND CONSEQUENCES

Method of Analysis

This transient is analyzed by the LOFTRAN code[1]. This code simulates the neutron kinetics, RCS, pressurizer, pressurizer relief and safety valves, pressurizer spray, steam generator, and steam generator safety valves. The code computes pertinent plant variables, including temperatures, pressures, and power level.

---

1. Burnett, T. W. T., et al., "LOFTRAN Code Description," WCAP-7907, June 1972. Also supplementary information in letter from T. M. Anderson, NS-TMA-1802, May 26, 1978 and NS-TMA-1824, June 16, 1978.

A detailed thermal and hydraulic digital-computer code, THINC, has been used to determine if DNB occurs for the core conditions computed by the LOFTRAN code.

The following assumptions were made for this transient.

a. Initial conditions of maximum core power and reactor coolant average temperature and minimum reactor coolant pressure, resulting in the minimum initial margin to DNB are used.

b. End-of-life shutdown margin and equilibrium xenon conditions. The most reactive RCCA stuck in its fully withdrawn position is assumed for conditions following reactor trip.

c. A negative moderator coefficient corresponding to the end-of-life unrodded core is used. This maximizes the reactivity insertion caused by the cooldown during the steam line break.

d. Minimum capability for injection of boron (2,000 ppm) solution corresponding to the most restrictive single failure in the safety injection system. The emergency core cooling system consists of three systems: 1) the passive accumulators, 2) the residual heat removal system, and 3) the safety injection system. Only the safety injection system is modeled for this analysis.

e. The reactor trip on overpower ΔT and overtemperature ΔT are assumed to be actuated at a conservative value. The ΔT trips include all adverse instrumentation and setpoint errors; the delays for trip actuation are assumed to be the maximum values.

f. The RCCA trip insertion characteristic is based on the assumption that the highest worth assembly is stuck in its fully withdrawn position.

g. The break size assumed for this transient is 1.72 feet^2 (.43 ft^2 per S.G.). This is the largest break size for which a low steamline pressure signal will not occur prior to the reactor trip on OPΔT. Prior to the

eventual steamline isolation on low steamline pressure, this break is fed by all four steam generators. Following steamline isolation the break will be fed from one steam generator causing an assymetric transient.

h. In computing the steam flow during a steamline break, the Moody Curve for fL/D=0 is used.

Results

The calculated sequence of events for the SLB/RCCA withdrawal transient is shown on Table 1.

Figures 1 and 2 show the RCS transient and core heat flux following the steamline rupture with coincident RCCA withdrawal.

The steamline break affects the turbine impulse transmitters and causes the control rods to withdraw at the initiation of the transient. This causes an increase in reactor power and core heat flux to the point at which the overpower delta-T trip setpoint is reached. This increase in core power generates a reactor trip which terminates the most adverse part of the transient. The steamline break causes an increased heat removal and consequent decrease in primary pressure simultaneous with the increase in reactor power. Secondary pressure also decreases until the low steamline pressure setpoint is reached initiating steamline and feedwater isolation.

Because of the lower RCS pressure coincident with the increase in reactor power, the minimum DNBR may be more adverse than the Rod Withdrawal at Power transient analyzed in the FSAR. Thus, the steamline break with coincident RCCA withdrawal is analyzed to ensure that the FSAR is limiting. The most limiting part of this transient pertinent to this study is immediately prior to reactor trip; for this reason the analysis is terminated at 50 seconds. The modeling of Engineered Safeguards Features (SI, SLI, FWI) is not needed since they will not be generated prior to reactor trip. The return to power following reactor trip and steamline isolation is bounded by the transient for

the larger break presented in the FSAR. The FSAR analysis assumed a larger break size and initial conditions corresponding to no-load temperatures (i.e., less stored energy in the RCS and reactor fuel).

Margin to Critical Heat Flux

A DNB analysis was performed for this transient. The DNBR was found to be greater than the limit value at all times.

CONCLUSIONS

The analysis demonstrates that the DNBR does not decrease below the limit value and no fuel or clad damage is predicted. Additionally, no system overpressurization is expected, thus all applicable safety criteria are met. Furthermore, the results are bounded by the accident analyses currently presented in the FSAR. Prior to reactor trip, this transient is bounded by the uncontrolled Rod Withdrawal at Power event. As stated in the results, this transient is bounded by the large steamline break analysis in the FSAR after reactor trip. There is therefore adequate protection on the Millstone 3 plant to ensure plant safety for this transient.

TABLE 1

TIME SEQUENCE OF EVENTS OF THE
STEAM LINE BREAK WITH A COINCIDENT CONTROL ROD WITHDRAWAL

Event	Time (sec)
Steam line ruptures	0.
Overpower delta-T reactor trip setpoint reached	8.6
Rods begin to fall	10.6
Low steam line pressure setpoint reached	23.5
Steam line isolation occurs	30.5
Feedwater isolation occurs	30.5

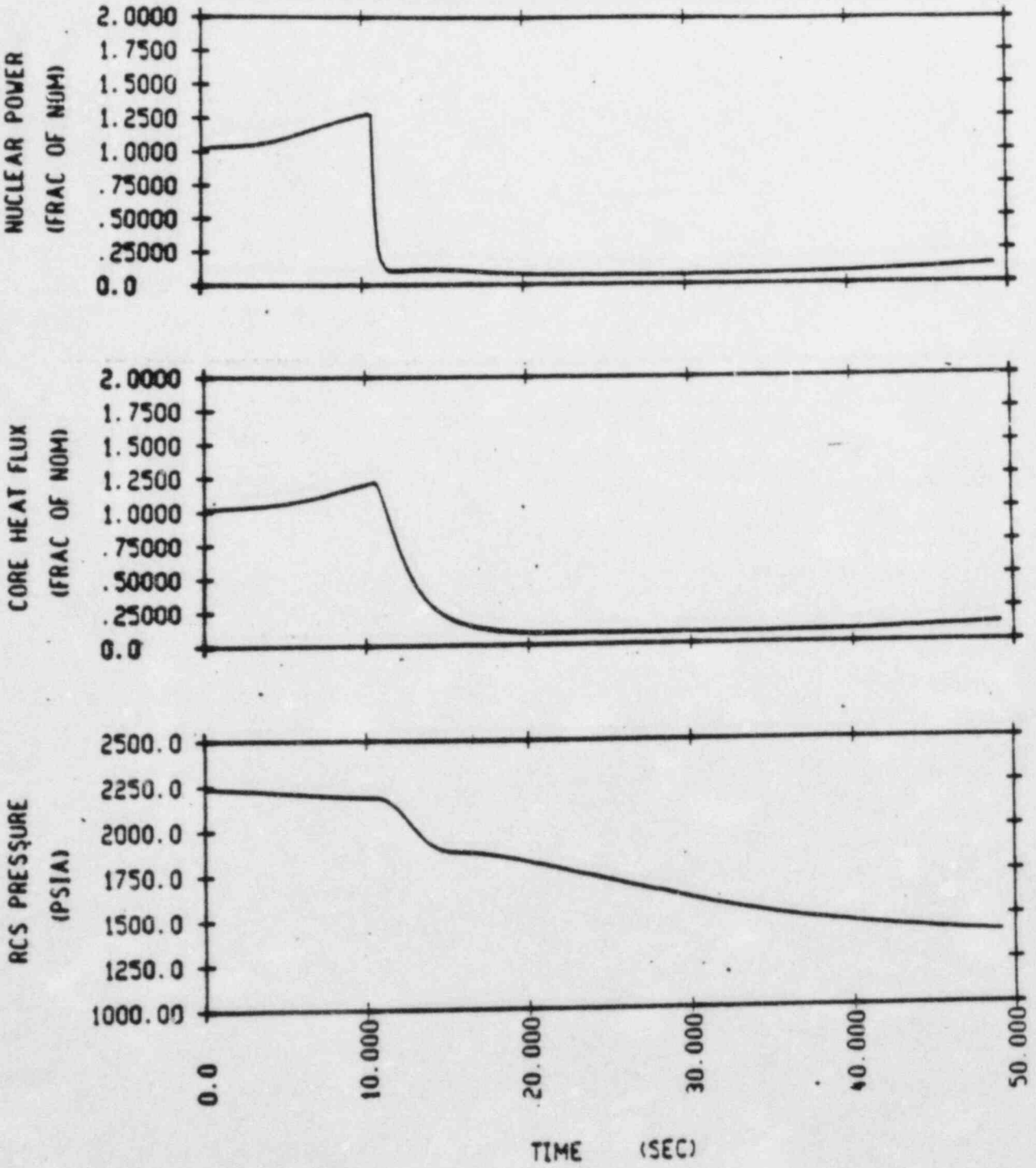


FIGURE 1

NUCLEAR POWER, CORE HEAT FLUX, AND RCS PRESSURE
FOR THE MILLSTONE 3 SLB/RCCA WITHDRAWAL TRANSIENT

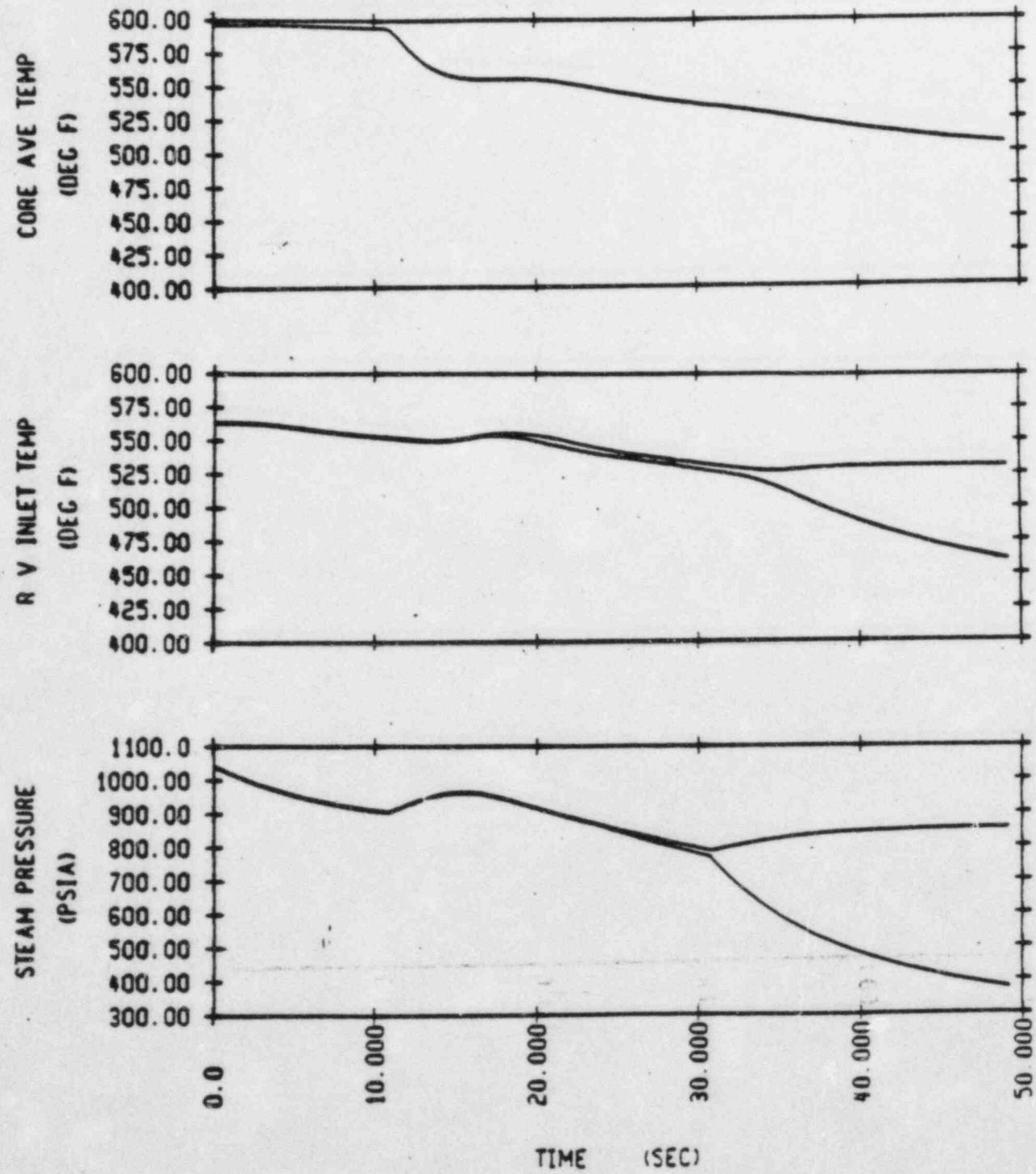


FIGURE 2

CORE T_{avg}, REACTOR VESSEL INLET TEMPERATURE, AND SG PRESSURE FOR THE MILLSTONE 3 SLB/RCCA WITHDRAWAL TRANSIENT

Open Items

Instrumentation and Control Systems Branch

ICSB-22 Freeze Protection for Instrument Sensing Lines (Draft SER Section 7.7.2.3)

The instrument sensing lines that can be exposed to freezing temperature only provided an environmental control systems (heating and ventilation or heat tracing) to protect the lines from freezing during extremely cold weather. The environment associated with safety related sensing lines should be monitored and alarmed so that appropriate corrective action can be taken to prevent loss of or damage to the lines from freezing in the event of loss of the environmental control system. The staff requested the applicant to document the freeze protection system design in Section 7.7 of the FSAR. This is an open item.

Response (3/84)

For Millstone 3 the environmental control system as it applies to instrument sensing lines is the freeze protection (electrical heat tracing) system. Refer to FSAR section 7.6.9 for the description of the heat tracing of safety related system. The Millstone 3 freeze protection system meets the requirements of Regulatory Guide 1.151 as listed in Position C.5.a, C.5.b, C.5.c and C.5.d.

5a) "Instrument sensing lines that can be exposed to freezing temperatures and that contain or can be expected to contain a condensable mixture or fluid that can freeze should be provided an environmental control system (heating and ventilation or heat tracing) to protect the lines from freezing during extremely cold weather."

This requirement is met for Millstone 3 instrument sensing lines.

5b) "The environment associated with those instrument sensing lines in a. that are safety related should be monitored and alarmed so that appropriate corrective action can be taken to prevent loss of or damage to the lines from freezing in the event of loss of the environment control system."

All safety-related instrument sensing lines with freeze protection are temperature monitored and alarmed.

5c) "The environment control system recommended in a., and for which b. applies, should be electrically independent of the monitoring and alarm system so that a single failure in either system, including their power sources, does not affect the capability of the other system."

Because two separate heat tracing and monitoring systems each with an independent power source are employed for each safety-related instrument sensing line with freeze protection, a single failure in any of the two systems will not affect the capability of the other system.

5d) "The environment control and monitoring systems of a. and b. should be designed to standards commensurate with their importance to safety and with administrative controls that are implemented to address events or conditions that could render the systems inoperable."

Open Items

Instrumentation and Control Systems Branch

The design of the freeze protection system is such that safety-related instrument sensing lines requiring freeze protection are provided with two independent heat tracing systems. Each heat tracing system has its own temperature monitoring system. Administrative controls include periodic surveillance to insure that the heat tracing systems are properly operating.

Status (3/84)

Closed.

Open Items

Instrumentation and Control Systems Branch

ICSB-23 Feedwater Isolation Valve Schematic (Draft SER Section 7.3.2.3)

Refer to ICSB-8.

Open Items

Instrumentation and Control Systems Branch

ICSB-24 Hydrogen Recombiner System (Draft SER Section 7.3.2.4)

The DBA hydrogen recombiner system controls the building of hydrogen gas inside the containment. The DBA hydrogen recombiner system consists of hydrogen monitors and hydrogen recombiners. The applicant has not completed the design on this system. The staff will review this design later.

Response (3/84)

The DBA hydrogen recombiner system is described in the FSAR Sections 6.2.5 and 7.3.1.1.5. Millstone Unit 3 Containment Hydrogen Monitoring System is designed as Category 1 (class 1E) with dual redundant trains (train A & train B). This system addresses the requirements set forth in NUREG-0737, Item II F.1 (6).

Each train contains stand alone analyzer and control cabinets which analyzes, monitors, alarms and trends containment hydrogen concentration.

The Containment Hydrogen Monitoring System will sample Hydrogen sources on an automatic/manual basis selectable from the control cabinet located in Hydrogen Recombiner Building Control Area.

Withdrawal of the samples from existing hydrogen recombiner lines, measurement of hydrogen concentration and return of the total sample to the containment are the basic functional assignments of the hydrogen analyzer cabinet.

Periodic calibration of the hydrogen monitoring system is automatically performed upon command from the hydrogen analyzer control cabinet. The mixture of hydrogen and nitrogen gases is used for the calibration.

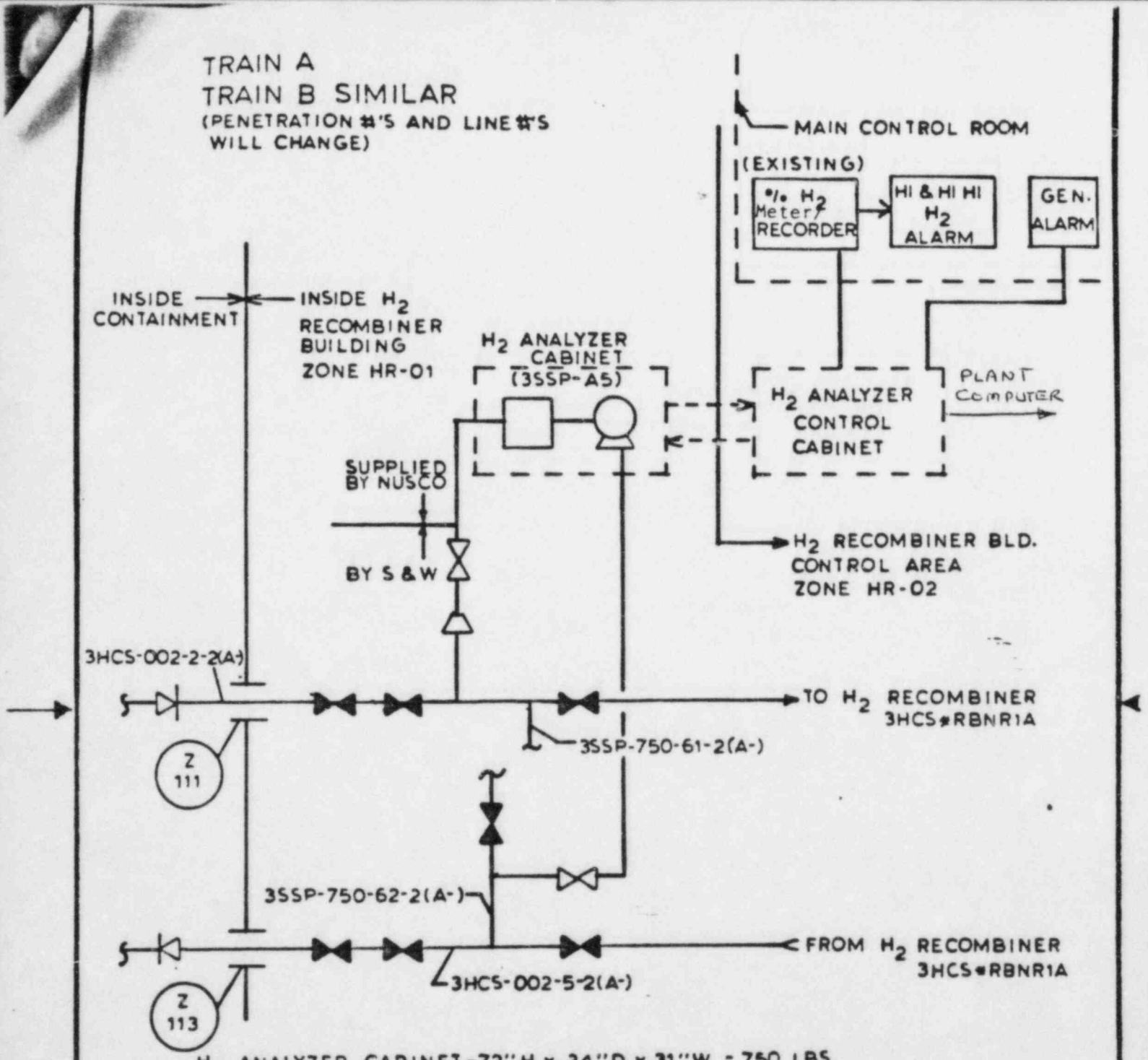
Hydrogen Analyzer control concentration will be measured and converted to an analog signal (0-10% H_2) for display on the digital panel meter, mounted on the control cabinet.

The system will have analog output for display (2 meters), recording (train A only) and alarming in the Main Control Board. Input is also provided to the plant computer.

Attached sketch shows the location and general arrangements for Hydrogen Monitoring System.

Status (3/84)

Closed.



NUSCO SPEC. NO: SP-EE-141 REV. 0

MF	P A #	NO	DATE	REVISIONS	BY	CHK	APP	APP	P A #		

NORTHEAST UTILITIES SERVICE CO.

FOR MILLSTONE UNIT 3

TITLE CONTAINMENT HYDROGEN MONITORING SYSTEM

BY KKB	CHKD	APP	APP
DATE 10-24-83	DATE	DATE	DATE
SCALE FSK		DWG NO SK-NRB-102583	