

Docket No.: 50-354

APPLICANT: PUBLIC SERVICE ELECTRIC AND GAS COMPANY (PSE&G)

FACILITY: HOPE CREEK GENERATING STATION

SUBJECT: SUMMARY OF INSTRUMENTATION AND CONTROL SYSTEMS BRANCH (ICSB)
MEETING

On June 26, 27 and 28, 1984, a meeting was held in the San Francisco, California, offices of the Bechtel Power Corporation to discuss ICSB open items not resolved since the January 1984 meeting.

Enclosure 1 lists the current status of each agenda item. Agenda items are identified pursuant to Enclosure 6 of the November 21, 1983, letter from A. Schwencer, NRC, to R. L. Mittl, PSE&G. The status of these agenda items is further discussed in Enclosures 2 and 3. Enclosure 2 documents the results of the meeting held with the applicant. The meeting notes provide background information regarding the status of each open item and identify the documentation required from the applicant in order to resolve them.

Certain items considered to be resolved based on the ICSB review of draft information will be listed as open in the SER if the required supporting documentation is not submitted on the docket.

Dave Wagner, Project Manager
Licensing Branch No. 2
Division of Licensing

Enclosures:
As stated

cc: See next page

JM
DSEC:ICSB
JMauk
8/11/84

for Dave Wagner
DL:LB#
DWagner:pob
8/11/84

AS
DL:LB#
ASchwencer
8/12/84

8408200463 840813
PDR ADDCK 05000354
A PDR



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

AUG 13 1984

Docket No.: 50-354

APPLICANT: PUBLIC SERVICE ELECTRIC AND GAS COMPANY (PSE&G)

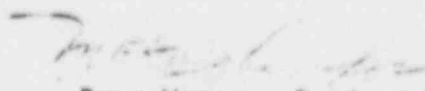
FACILITY: HOPE CREEK GENERATING STATION

SUBJECT: SUMMARY OF INSTRUMENTATION AND CONTROL SYSTEMS BRANCH (ICSB)
MEETING

On June 26, 27 and 28, 1984, a meeting was held in the San Francisco, California, offices of the Bechtel Power Corporation to discuss ICSB open items not resolved since the January 1984 meeting.

Enclosure 1 lists the current status of each agenda item. Agenda items are identified pursuant to Enclosure 6 of the November 21, 1983, letter from A. Schwencer, NRC, to R. L. Mittl, PSE&G. The status of these agenda items is further discussed in Enclosures 2 and 3. Enclosure 2 documents the results of the meeting held with the applicant. The meeting notes provide background information regarding the status of each open item and identify the documentation required from the applicant in order to resolve them.

Certain items considered to be resolved based on the ICSB review of draft information will be listed as open in the SER if the required supporting documentation is not submitted on the docket.


Dave Wagner, Project Manager
Licensing Branch No. 2
Division of Licensing

Enclosures:
As stated

cc: See next page

SUMMARY OF
HOPE CREEK OL REVIEW STATUS FOR CHAPTER 7
(INSTRUMENTATION & CONTROLS)
AGENDA ITEMS

<u>Agenda Item Number</u>	<u>STATUS</u>
421.1	resolved
2	resolved
3	resolved
4	resolved
5	resolved
6	resolved
7	resolved
8	resolved
9	resolved
10	open
11	resolved
12	resolved
13	confirmatory
14	resolved
15	resolved
16	resolved
17	resolved
18	confirmatory
19	resolved
20	resolved
21	confirmatory
22	confirmatory
23	confirmatory
24	resolved
25	resolved
26	confirmatory
27	resolved
28	resolved
29	resolved
30	confirmatory
31	resolved
32	resolved

Agenda Item Number

STATUS

33	resolved
34	resolved
35	open
36	resolved
37	resolved
38	resolved
39	resolved
40	resolved
41	license condition
42	confirmatory
43	resolved
44	resolved
45	confirmatory
46	resolved
47	resolved
48	resolved
49	resolved
50	resolved
51	open
52	open
53	resolved
54	resolved
55	resolved
56	resolved
57	resolved

Date: June 26, 1984
Location: Bechtel Offices, 8th Floor, 221 Main St., S.F.
Subject: Hope Creek Project (Docket No. 50-354)
• NRC ICSB Questions
Attendees: See attached sheet

Review of Questions

421.49 GETARS - Acceptable

Copy of the multiplexer I/O list by specific signal assignment was given to the NRC for review. Based on the NRC confirming signal assignment, Question 421.49 and DSER 210 will be acceptable.

421.2 GDC Conformance - Acceptable

DSER 194 - Acceptable.

Add note 12 to Table 7.1-3 as follows:

The SSEAVS consists of the RSP Room HVAC System and the RBEACS. The RBEACS is also part of the ESF Equipment Area Cooling System and satisfies the design requirements of that system.

421.7 Regulatory Guide 1.47 - Acceptable

421.10 Regulatory Guide 1.75 - Open

1. NRC ICSB will check with PSB on acceptability of Chapter 8 (FSAR) references to IEEE 384-81.
2. Bechtel to add sentence identifying isolation devices are used for computer and annunciator inputs.
3. GE-NPSD will furnish a description of the analysis, methodology and date for analysis completion justifying exemptions to Regulatory Guide 1.75. GE will revise FSAR page 7.1-16.

421.13 Isolation Devices - Confirmatory (DSER 189)

1. Bechtel to define maximum credible "hot short" failure. The test report should show that the surge testing, when completed, is in excess of the maximum postulated credible "hot short" condition as indicated in the response to this question.

421.13 (Cont'd)

2. GE-NPSD to furnish testing write-up on NSSS isolator by 6/27/84.

GE will verify the applicability of their test results to Hope Creek plant including the maximum postulated credible "hot short" condition used to test similar isolators in the BOP, if applicable.

- 421.17 RPS Sensors in Turbine Building - Acceptable

DSER 185 - Acceptable

- 421.19 Common Instrument Taps - Acceptable

DSER 196 - Acceptable

- 421.26 Mode Switch Misoperations - Confirmatory

Confirmatory until new write-up is reviewed by the NRC - 6/26/84.
7/15/84

- 421.30 IE Bulletin 80-06, ESF Reset Controls - Confirmatory

Change last paragraph in Amendment 5 response to read as follows:

"Compliance of the remaining valves identified above, with the exception of the SRVs, with IE Bulletin 80-06 will be incorporated with the design modifications dictated by the resolution of TMI Item II.E.4.2. Modifications will be completed prior to fuel load."

Will remain confirmatory until the NRC review of GE mods for TMI items (Containment iso.) is completed and will be verified by the NRC during preoperational testing.

- 421.30A HPCI Seal-in - Open

PSE&G will verify design and advise by 6/28/84.

- 421.32 FSAR Table 7.3-15 - Acceptable

421.38 Remote Shutdown System - Acceptable

DSER 200 - Acceptable

The fourth paragraph of 7.4.1.4.3.5, page 7.4-12,
will be replaced by the following:

"In the event that the RSP is lost, the design provides
for separate equipment independent of that in the RSP.
This equipment is presented in Table 7.4-3 and all is
designed in accordance with Class 1E requirements."

NRC

PSE&G

GE

Bechtel

ATTENDEES

6/26/84

NAME

ORGANIZATION

- ... List
- G. N. KAPANDRITIS
- George A. Chiluvu
- Jerry L. Mancula
- W. GAILEY
- B. A. PEARSON
- J. B. JAMES
- Arnold Koslow
- George Darmohray
- ROBERT SKWAREK
- J. J. WROBLEWSKI
- RW ROSKO
- T. McGuire
- * LE FLORES
- * G. H. Stoltz
- * P. DiDomenico
- * K. Cooke
- * R. Henderson
- * J. Klee
- * J. Schott
- * S. Fahrachi
- * S. Yin

- Bechtel - Control Systems
- Bechtel - APE
- NRC/NER
- NRC/MAR
- PSE & G - Const. Proj. ENGR
- PSE & G - LIC. MGR
- GENERAL ELECTRIC Hope Creek Light
- GE - C+I
- GE - Licensing ^{SITE ENGINEER}
- PSE & G Control & Electrical
- PSE & G - PRINCIPAL ENGR. I&C
- " " " "
- " SENIOR ENGR - I&C
- EIGEN ENGINEERING - PRINC. ENGR.
- B. Control Syst
- BECHTEL - CS EGS
- Bechtel - Electrical (EGS)
- Bechtel - Mechanical (EGS)
- Bechtel - Mechanical
- Bechtel - Control Systems
- Bechtel - Control Systems
- Bechtel - Mechanical

Meeting

Date: June 27, 1984
Location: Bechtel Offices, 8th Floor, 221 Main St., S.F.
Subject: Hope Creek Project (Docket No. 50-354)
NRC ICSB Questions
Attendees: See attached sheet

Review of Questions

421.39 Heat Tracing in CST Level Sensing Line - Acceptable

DSER 195 - Acceptable


In the event normal indication is unavailable, administrative plant procedures will confirm availability of the condensate storage tank. The following statements will be added:

In the unlikely event that the analog output of the installed RTD becomes unavailable, administrative procedures will provide for verification that the sensing line is not in danger of freezing.

The technical specifications will include surveillance requirements for testing the environmental control and monitoring systems at least once per year prior to the onset of freezing weather.

Heaters are not used in any HCGS safety-related panel to control humidity and/or temperature.

421.40 Standby Liquid Control System - Acceptable

Deleted footnote  in drawing 791E409AC, Sheet 3. Power supply configuration is acceptable.

Bailey 862 discussion will be part of Question 421.35.

421.54 Credit for Nonsafety-Related Instrumentation in Chapter 15 Analysis - Acceptable

DSER 209 - Acceptable

The following response will be added:

The recirculation-runback feature of the HCGS is primarily an operation device to increase plant availability. It reduces the incidence of scrams from low vessel water level due to misoperations of the feedwater system. Although the recirculation-runback feature is simulated in the analyses of a complete loss of feedwater

421.54 (Cont'd)

flow, as described in Section 15.2.7 of the FSAR, the analyses show it does not make a significant contribution to the mitigation of this event.

The analysis confirms that the reactor power would begin decreasing at the initiation of the feedwater loss because the reduced inlet subcooling would increase the voids. This would tend to increase the MCPR and to decrease reactor pressure. Therefore, in the absence of recirculation-runback there would be no challenge to the core thermal margin or vessel pressure boundary before scram, and it would be inappropriate to prescribe surveillance of the recirculation-runback feature in the technical specifications.

421.18 Setpoint Methodology - Confirmatory

DSER 188 - Confirmatory

Remain confirmatory until final methodology is reviewed and approved by the NRC.

421.21 High Drywell Temperature Effects on RPV Level Sensing Line Reference Legs - Confirmatory

The draft response to this question describing the re-routing of the RPV level sensing lines requires review by NRC and will be discussed with Reactor Systems Branch and Instrumentation and Controls Systems Branch on July 11, 1984 meeting.

421.23 Failures in Reactor Vessel Level Sensing Lines - Confirmatory

DSER 184 - Confirmatory

The response to this question requires review by NRC and will be discussed with Reactor Systems Branch and Instrumentation and Control Systems Branch on July 11, 1984. The following underlined item will be added on page 421.23-2 Amendment 5:

Failure Combination 1 would be the failure of the division 1 instrument reference line connected to condensing chamber B21-D004A combined with a failure such that level transmitter B21-N080C indicates high water level. In the analysis of this combination, it was assumed that the manual selection switch for feedwater control is on the failed instrument line (division 1) and that the operator does not switch the control to the other instrument line (division 2) as would be expected. This would cause the feedwater controller to respond to the erroneous high-level signal by reducing the feedwater flow.

421.51 Control System Failure Analysis - Open

DSER 208 - Open

Question 421.51 sets forth the following design requirement:

In the analysis of control systems failures, the failure of control systems is considered the initiating event. The consequences of such an initiating event should be acceptably mitigated (bounded by existing FSAR Analysis 15) by the protection systems assuming a single active failure (in any one of the protection systems). This question will be discussed further on 6/28/84.

421.6 First-of-a-Kind Instruments

DSER 197

For SLCS, discuss the design using:

1. Bailey design schematic
2. Bechtel functional logic drawings
3. GE wiring diagrams

Determine separation between manual and automatic functions using Bailey design schematics for all Non-NSSS systems.

Discussion of various design features for 862 logic will be continued 6/28/84.

Frank T. Wank 6/28/84
Robert A. Calvo 6/28/84
William J. Bailey 6/28/84

NRC PSE&G

Al Barnes 6/28/84
G. N. Kapanditis 6/28/84

GE BECHTEL

A Henders

6/27/84

<u>NAME</u>	<u>ORGANIZATION</u>
R. A. LINT	Bechtel - Control System
GN KAPANDRITIS	Bechtel - APE
W. GAILEY	PSE+G - Civil Prof. Engr
Jose A. Calvo	NRC/NRR/ICSB
Jerry L. Mauch	NRC/NRR/ICSB
BRUCE A. PRESTON	PSE+G - WC. MGR.
DEAN JAMES	GE HOPE CREEK LICENSING ENGINEER
Arnold Koslow	GE C+I
George Darmohray	GE Licensing
J. J. WROBLEWSKI	PSE+G - PRINCIPAL ENGR
R. W. Rosko	PSE+G - PRINCIPAL ENGR
T. R. MCGUIRE	PSE+G - SENIOR ENGR (CONTROLS)
* K Cooke	Bechtel - Elect Group Super
* P. Schragger	Bechtel - Control Systems
ROBERT SKWAREK	PSE+G - SITE ENGINEERING - ISC
* ROBERT K. SCHROEDER	GE C+I
* DAVE J. WRUBLEWSKI	BAILEY CONTROLS
* RALPH R. DUNBAR	" "
* Douglas J. Dura	" "

* PART TIME

Meeting

Date: June 28, 1984

Location: Bechtel Offices, 8th Floor, 221 Main St., S.F.

Subject: Hope Creek Project (Docket No. 50-354)
NRC ICSB Questions

Attendees: See attached sheet

Review of Questions

421.6 First-of-a-Kind Instrumentation - Acceptable
DSER 197 - Acceptable

Additional information was discussed in detail. Insert A to the response of Question 421.6, which is attached, will be used to revise the FSAR.

421.35 Regulatory Guide 1.62 - Open
DSER 193 - Open

The response to this item remains open for NRC internal review of the HCGS design.

--- 421.51 Control System Failure Analysis - Open
DSER 208 - Open

A clarification of the methodology to resolve this issue is included in the attached pages of the FSAR.

421.42 IE Bulletin 79-27 - Confirmatory
DSER 199

Discussed a change in the analysis methodology. The methodology will be similar to that used on the Limerick project. A revised response containing this methodology was reviewed during the meeting and is attached to these meeting notes.

421.52 IE 79-22-HELB - Open
DSER 207

A plant walkdown has been completed. This item remains open pending submittal and staff review of this analysis. Staff will advise whether this item can be considered confirmatory in lieu of "open".

421.22 AT Power Testing - Confirmatory

DSER 186 - Confirmatory

The NSSS portion of this response is considered acceptable. The BOP portion of the response is considered confirmatory until the final results of the survey is submitted and reviewed by the NRC.

421.4 Removal of Fuses for Testing - Acceptable

DSER 187 - Acceptable

GE has reviewed the NSSS systems and determined that no fuses need to be removed and no jumpers are used during testing. NRC considers this response acceptable.

421.10 Regulatory Guide 1.75 - Separation - Open

The NMS (APRMs, IRMs) and GE process radiation monitoring system, located in the NMS panels and participating as inputs to protection systems, will be analyzed to assure that for the worst-case postulated single event, adequate redundancy will remain to assure that the protective functions provided by these devices are not lost. An amendment will be made to FSAR page 7.1-16.

421.10a PSE&G to advise the NRC within two weeks on the proposed course of action concerning the NMS power supply.

421.30a IE Bulletin 80-06 - Confirmatory

ESF Reset Controls

The seal-in features for the HPCI and RCIC pump discharge valves were reviewed. This response is considered confirmatory based on review and acceptance of the final design for the HPCI pump discharge valve.

421.9 Acceptable

421.12 Acceptable

421.14 Acceptable

421.37 Acceptable

421.46 Acceptable

421.55 Acceptable

421.41 Regulatory Guide 1.97. This would be considered a license condition.

José A. Calvo 6/26/84

James L. March 6/28/84

NRC

William J. Jilly 6/28/84

PSEG

Al Barnes 6/24/84

GE

Dr. Kapanidze 6/28/84

BECHTEL

Attendees

6/28/84

Name

Organization

R. A. Lint

Bechtel - control/system

P. DiDOMENICO

BECHTEL - CG EGS

R. W. ROSKO

P.S. EEG - CONT. I

T. McGUIRE

"

J. WROBLEWSKI

"

R. SKWALEC

" STE. CONTROL

D JAMES

GE HOPE CREEK LICENSING ENV.

G. Darmohray

GE LICENSING

A. Koslow

GE C+I

BA PRESTON

PSE+G - LIC. MGR.

D. J. WROBLEWSKI

BAILEY CONTROLS

R. R. Dumba

"

"

DOUG DURA

"

"

Jerry L. Mauch

NRC / NAR / ICSB

JOSE A. CALVO

NRC / NRP / ICSB

G. N. KAPANDRITIS

BECHTEL - APE

* K. COOKE

Bechtel

* J. Schott

Bechtel

* T. Johnston

Bechtel

W. GAILLEY

PSE+G - Co. Procs Gen

alarm panel also provides indication of fuse module fuse failure, cooling fan failure, and in which bay (of the 12 bay assembly) the failure occurred.

A digital logic assembly trouble summary alarm is annunciated in the main control room whenever any of the following conditions exist in a Class 1E logic assembly:

- 1) Door open
- 2) Fuse module fuse failure
- 3) Fuse module interlock (fuse module withdrawn)
- 4) Power bus failure
- 5) Power supply failure
- 6) Cooling fan failure
- 7) Optic link failure (optical isolation system trouble).

High system reliability is achieved by segregating control of field devices (e.g., switchgear, MCC, etc.) into different circuits within a logic assembly. Each circuit is composed of a single fuse module and as many logic modules and output driver relays as required to control a field device. Several related field devices may be controlled from the same circuit. The fuse module protects the logic assembly power supplies from individual circuit faults.

Testing of a system circuit from its control switch through the output(s) of the associated logic modules is made possible by a switch on the fuse module which, when operated, disables the output driver relays. This disabling is continuously indicated in the main control room. Light emitting diodes on the face of the logic module indicate the presence or lack of input signals from the associated control switch and the presence or lack of signals to the output driver relays.

* INSERT ^(A) TO 421.6 *NOT POWER*
The Bailey 862 equipment is functionally described in the logic diagrams provided to the NRC and listed in Table 1.7-3.

Equipment qualification reports are referenced in Sections 3.10 and 3.11.

INSERT (A) ~~NOTES~~

TO 42.6 RESPONSE

The reliability of the 862 Logic Module may also be evaluated by reviewing three facets of the design and manufacturing process. The first facet deals with the application of proven design methods which have been used in other Bailey products or within the I&C industry. Part of this first phase is the evaluation of the design via methods prescribed in Mil Std. 217C. The second area concerns the verification of the 862 Logic Modules ability to perform under various environmental stresses via qualification testing. The third facet deals with the in-plant maintenance of the Logic Modules ability to perform by use of surveillance.

An → Bailey has employed conservative methods in the design of the 862 Logic Module via the use of proven circuitry schemes. Example of this is found in the voltage regulator circuitry which provides power for the module. Another example ~~would be~~ is the input buffer circuitry. The most prominent feature with regards to the reliability of the module can be found in the analysis performed on the component items of the module which insure the components are not overstressed. This analysis is accomplished by using Bailey derating factors in conjunction with the Mil Std. 217C. This analysis results in conservative stress ratio calculations demonstrating that each component is not overstressed. All calculations are maintained in auditable files at the Bailey Controls Company in Wickliffe, Ohio. This analysis also provides MTBF values. In the case of the 862 Logic Module, the MTBF is analyzed to be 11.6 years. This value takes into consideration all components including those which are not essential to the LE function such as test switches and capacitors. It is expected that disabling failures would occur less frequently.

The second area which establishes confidence in the 862 Logic Modules design is the testing performed during the qualification program. The results of these tests demonstrate the designs capability to perform under abnormal and normal environments including seismic events, the effects of RFI/EMI, and voltage spikes. All data is documented in accordance with Appendix B to 10CRF50 and is available for audit at the Bailey Controls Test Lab in Wickliffe, Ohio. Buffers driving the control output relays are usually only momentarily energized, thus resulting in less stress on these components.

The third area for consideration includes the testability or the recognition of failure. Although there is no in-service testing of the module, some failures are self-evident. As an example, the failure of an output buffer in indicating applications would result in the loss of the indication at the main control console. ~~Also, the indicating modules are equipped with an LED indicator to alert the operator to a loss of the 9V or 24V power supplies.~~ In addition, during operation logic module LEDs can be observed to check module functionability and memory status.

421.6

One area not previously mentioned is the operating experience of this module in similar applications. This module is presently being used at three facilities. As a result, the 862 Logic Module has five years of operating experience without significant failures.

In summary, these points show the concise and deliberate actions the Bailey 862 Logic Module (and system) employ to obtain and maintain high reliability in its operating capability as is evidenced by its successful operating history to date. The use of existing design tailored to replace relay logic simplifies and enhances the motor control system. The result is a testable, secure system of proven design performing its task in a sound and reliable manner.

A. Common Power Source Failure

An outline of the methodology for the common power source failure analysis follows:

1. Identify all nonsafety-grade control systems that have the potential of affecting the critical reactor parameters of water level, pressure, or power.
2. Review these control systems at the component level; identifying the effects of the loss of power to each system component and the subsequent interactions with other components and systems.
3. Generate bus trees denoting the bus hierarchy and cascading configuration of all power busses that supply components of control systems under study.
4. Perform a combined effects analysis. Evaluate the failure of each power bus (load center, motor control center, etc.) starting with the lowest-level source common to multiple control systems and working up each bus tree to the highest common power level. At each level examine the effects of the single bus failure and the consequences of cascading bus failures on all control systems' components.
5. Postulate the limiting transient events as a result of the combined effects analysis and compare these events to those analyzed in Chapter 15. *that the worst case limiting event*
6. Perform ~~any~~ additional transient calculations or analyses necessary to ensure ~~the postulated limiting events are~~ bounded by those analyzed in Chapter 15 *with the assumption there is a single event failure in a safety system required to mitigate effects of the event.*
7. Document the results of the analyses of common power source failure, providing recommendations as appropriate.

B. Common Sensor or Sensing Line Failure

An outline of the methodology for the common sensor or sensing line failure analysis follows:

1. Identify the nonsafety-grade control systems that have the potential of affecting the critical reactor parameters of water level, pressure, or power.
2. Identify all instrument sensing lines and sensors utilized by two or more of these control systems.

X
 (5) INSERT A

Insert (A) to 421.51 response

HCGS FSAR

4/84

3. Analyze the effects of failure of a common sensor of a complete plug or a guillotine break in each of these common instrument lines. Examine the effects of erroneous signals on each instrument and on each function (scrams, trips, permissive signals, etc.) that could be actuated or rendered inoperative.
4. Examine the interactive effects among all systems affected by the common sensing line or sensor failure and the consequential combined effects on the critical reactor parameters.
5. Compare the consequences of these postulated events with those analyzed in Chapter 15 to ensure the consequences of the postulated events are bounded by the results of the Chapter 15 events and to ensure the postulated events would not require actions or responses beyond the capabilities of the operators or the safety systems. Perform ~~any~~ additional transient calculations or analyses necessary to ensure ~~the~~ that the worst ~~postulated~~ limiting events are³ bounded⁴ by those analyzed in Chapter 15^x with the assumption there is a single active failure in a safety system required to mitigate effects of the event.
6. Document the results of the analyses of common sensing line or sensor failures and provide recommendations as appropriate.

The programs described in the responses to this question and to questions 421.42 and 421.52 will be conducted as a combined effort that will be completed by December, 1984.

* SEE INSERT A

(1)

INSERT A

FOR QUESTION 421.51-2

*As it is used in item 6, "bounded" means within the consequence limits for abnormal operational transients given in Section 15.0.3.1.2 of the FSAR or, if the combined probability of occurrence of both the initiating event and the single active failure is similar to the occurrence probabilities of limiting faults (see Section 15.0.3.1), "bounded" means within the consequence limits for limiting the faults given in Section 15.0.3.1.3.

QUESTION 421.42 (SECTION 7.5)

If reactor controls and vital instruments derive power from common electrical distribution systems, the failure of such electrical distribution systems may result in an event requiring operator action concurrent with failure of important instrumentation upon which these operator actions should be based. IE Bulletin 79-27 addresses several concerns related to the above subject. You are requested to provide information and a discussion based on each IE Bulletin 79-27 concern. Also, you are to:

- 1) Confirm that all a.c. and d.c. instrument buses that could affect the ability to achieve a cold shutdown condition were reviewed. Identify these buses.
- 2) Confirm that all instrumentation and controls required by emergency shutdown procedures were considered in review. Identify these instruments and controls at the system level of detail.
- 3) Confirm that clear, simple unambiguous annunciation of loss of power is provided in the control room for each bus addressed in item 1 above. Identify any exceptions.
- 4) Confirm that the effect of loss of power to each load on each bus identified in item 1 above including ability to reach cold shutdown, was considered in the review.
- 5) Confirm that the re-review of IE Circular No. 79-02 which is required by Action Item 3 of Bulletin 79-27 was extended to include both Class 1E and non-Class 1E inverter supplied instrument or control buses. Identify these buses or confirm that they are included in the listing required by Item 1 above.

RESPONSE

An analysis will be conducted based on the ~~General Electric~~ ^{Limerick} methodology for answering the concerns raised in IE Bulletin 79-27. This methodology has been reviewed ~~and approved~~ ^{Limerick Generating Station approach} by the NRC via a report written for the ~~WNP-2~~ project. The methodology provides for a systematic and comprehensive analysis to ensure that, in the event of a single power bus failure, sufficient control room indicators, instruments, and controls exist to achieve a cold shutdown.

An outline of the methodology follows:

1. Review the Class 1E and non-Class 1E busses including inverters supplying power to instrumentation and controls in

Use plant emergency operating procedures to

under emergency

systems used in attaining the cold shutdown condition?
Identify busses that could affect the ability to achieve cold shutdown. ~~Use plant operating procedures and procedures developed for certain power bus failures to ensure the identification of all critical power busses.~~

2. Identify the instrumentation ^{of these} and control devices connected to each identified power bus. Evaluate the effects of a loss of power to each load, including the limiting effects on the ability to achieve cold shutdown.
- ~~3. Create bus trees denoting the bus hierarchy and the cascading bus configuration of all busses that power instrumentation and controls the operator would manipulate in going to cold shutdown.~~
- ~~4. Determine the annunciators and alarms that would alert the operator to a failure of any of the identified busses.~~
- ~~4.5. Determine the effects of any single power bus loss on the ability to continue in each particular shutdown path being used at the time the bus loss occurs. Include the cascading effects of any bus loss, and consider alternate indications and controls powered by unaffected busses that may aid the operator in the event of a bus loss. Identify alternative shutdown paths available and existing procedures for restoration of the affected bus.~~
- 5.8. Document the results of the analysis, providing recommendations of hardware or procedural changes as appropriate.

The programs described in the responses to this question and to Questions 421.51 and 421.52 will be conducted as a combined effort that will be completed by December, 1984.

insert

The Emergency Operating Procedures will be reviewed to verify that sufficient instrumentation and controls exist to achieve cold shutdown by identifying alternative shutdown paths and instrumentation.

QUESTION 421.2 (SECTION 7.1)*Revise table 7.1-3*

Section 7.1.2.2 and 7.1.2.3 of the FSAR indicate the applicability of the conformance statements provided for each system is included in Table 7.1-3 for GDCs, RGs and other standards. Table 7.1-3 is inconsistent with Table 7-1 of the SRP (e.g., the table does not include GDC-1 or RG 1.62, remote shutdown systems do not include RG.1.22). Identify and provide the rationale for all deviations between FSAR Table 7.1-3 and SRP Table 7.1.

RESPONSE

Table 7.1-3 has been revised to resolve inconsistencies with SRP Table 7-1.

Several systems identified on Table 7.1-3 differ from SRP Table 7-1. These differences and justifications for the differences are identified below on a system by system basis.

- a. Primary containment isolation system (PCIS) -
 1. Difference - The applicability of Regulatory Guide 1.47. to the PCIS.
 2. Justification - The PCIS does not fall under the guidelines established in Regulatory Guide 1.47, Section B, for which automatic bypassed and inoperable status indication on a system level basis must be provided.

The PCIS, described in Section 7.3.1.1.5, is not capable of being manually bypassed or placed out of service at the system level. Further, there are no operational bypasses associated with the PCIS.

Certain valves actuated by the PCIS are provided with isolation override capabilities which allows for reopening of these valves after they have traveled to their isolated position. This override condition is specifically indicated in the main control room on a component (valve) level. It is automatically removed when the PCIS initiating signal clears. See Section 7.3.1.1.5, part f.

- b. Engineered safety features (ESF) equipment area cooling system -

1. Difference - The applicability of Regulatory Guide 1.47 to the ESF equipment area cooling system.
2. Justification - The ESF equipment area cooling system consists of the following subsystems:
 - (a) reactor building equipment area cooling system (See Section 9.4.2)
 - (b) auxiliary building diesel area heating, ventilation, and air conditioning (ABDA-HVAC) system (See Section 9.4.6)
 - (1) diesel generator room recirculation
 - (2) switchgear room cooling
 - (3) diesel area battery room exhaust
 - (4) diesel area IE panel room supply
 - (c) auxiliary building control area HVAC (ABCA-HVAC) (See Section 9.4.1)
 - (1) control area battery exhaust
 - (2) control equipment room supply
 - (d) service water intake structure HVAC (See Section 9.4.7).

*-100% systems
 in state at 110°
 at 115°
 H. temp alarm
 in the
 control room
 in which these
 systems
 100% systems
 in total
 under control*

The design of the ESF equipment area cooling subsystems precludes the necessity for strict compliance with Regulatory Guide 1.47 since the criteria of Position 3 of the regulatory guide are not satisfied in any case. However, the ESF equipment area cooling systems do satisfy the intent of Regulatory Guide 1.47 as described in the following paragraphs:

- (a) reactor building equipment area cooling system:
 - (1) remote control panel trouble alarm - a summary alarm in the main control room that alarms whenever the control switches (on the remote control panel) for an ECCS or SACS pump room cooler pair are in other than the normal configuration of "AUTO LEAD" and "AUTO." Individual alarms are provided on the remote control panel annunciator.

- (2) manual out-of-service indication - manual out-of-service switches and indicators are provided as an administrative control for use whenever an ECCS or SACS pump room cooler or pair of coolers must be placed out of service. This indication is provided on a per 1E channel basis and is also illuminated automatically whenever the associated standby diesel generator manual out-of-service switch is actuated. Actuation of a manual out-of-service switch also causes actuation of a "BOP Safety System Out-Of-Service" annunciator in the main control room.
 - (3) computer monitoring:
 - i) low flow on an operating unit cooler (digital)
 - ii) ECCS and SACS pump rooms temperature (analog)
- b) (ABDA-HVAC) diesel generator room recirculation
- (1) remote control panel trouble alarm - a summary alarm in the main control room that alarms whenever a low flow condition is sensed on a running recirculation unit. This alarm condition does not occur when the recirculation unit control switch (at the remote control panel) is in the "STOP" position. This condition is individually alarmed on the remote control panel annunciator.
 - (2) manual out-of-service indication - manual out-of-service switches and indicators are provided in the main control room as an administrative control for use whenever a recirculation unit must be placed out of service. This indication is provided on a per 1E channel basis and is also illuminated automatically whenever the associated standby diesel generator manual out-of-service switch is actuated. Actuation of a manual out-of-service switch also causes actuation of a "BOP System Out-

Of-Service" annunciator in the main control room.

- (3) computer monitoring:
 - i) diesel generator room temperature (analog).

(c) (ABDA-HVAC) switchgear room cooling

- (1) remote control panel trouble alarm - a summary alarm in the main control room that alarms whenever either of the following conditions exist on an operating switchgear room unit cooler:
 - i) low flow - does not occur when the switchgear room unit cooler control switch (at the remote control panel) is in the "STOP" position.
 - ii) unit cooler filter differential pressure high

These alarms are individually indicated on the remote control panel annunciator.

- (2) main control room alarm/status lights - the following status lights are provided in the main control room for each switchgear room unit cooler:
 - i) running (status)
 - ii) stopped (status)
 - ii) low flow (alarm)
- (3) manual out-of-service indication - manual out-of-service switches and indicators are provided in the main control room as an administrative control for use whenever a switchgear room unit cooler must be placed out of service. This indication is provided on a per 1E channel basis and is also illuminated automatically whenever the associated standby diesel generator manual out-of-service switch is actuated. Actuation of a manual out-of-service switch also causes actuation of

a "BOP Safety System Out-Of-Service" annunciator in the main control room.

(4) computer monitoring:

i) switchgear room exhaust temperature (analog).

(d) (ABDA-HVAC) diesel area battery room exhaust (el. 148 ft.)

(1) remote control panel trouble alarm - a summary alarm in the main control room that alarms whenever either of the following conditions exist:

i) low flow - this alarm does not occur when the exhaust fan control switch (at the remote control panel) is in the "STOP" position.

ii) exhaust fan not running

These alarms are individually indicated at the remote control panel annunciator.

(2) computer monitoring:

i) exhaust fan low flow (digital)

ii) battery room exhaust temperature (analog).

(e) (ABDA-HVAC) diesel area battery room exhaust (el. 163 ft-6 in.)

(1) remote control panel trouble alarm - a summary alarm in the main control room that alarms whenever a low flow condition exists on the running battery exhaust fan. This alarm does not occur if the exhaust fan control switch (at the remote control panel) is in the "STOP" position. The low flow alarms are individually indicated on the remote control panel annunciator.

(2) computer monitoring:

i) exhaust fan low flow (digital).

(f) (ABDA-HVAC) diesel area IE panel room supply

(1) remote control panel trouble alarm - a summary alarm in the main control room that alarms whenever any of the following conditions exist:

- i) low flow - this alarm does not occur if the unit cooler control switch (at the remote control panel) is in the "STOP" position.
- ii) unit cooler discharge temperature high or low
- iii) unit cooler filter differential pressure high

These alarms are individually indicated on the remote control panel annunciator.

(2) computer monitoring:

- i) unit cooler suction temperature (digital) - combined exhaust from the IE panel rooms.

(g) (ABCA-HVAC) control area battery exhaust

(1) remote control panel trouble alarm - a summary alarm in the main control room that alarms whenever any of the following conditions exist:

- i) exhaust fan discharge low flow - this alarm does not occur if the battery exhaust fan control switch (at the remote control panel) is in the "STOP" position.
- ii) battery room exhaust flow low - for each control area battery room.

These alarms are individually indicated on the remote control panel annunciator.

(h) (ABCA-HVAC) control equipment room supply

(1) control area HVAC trouble alarm - an annunciator in the main control room that is actuated whenever any of the following conditions exist on the control equipment room supply system:

- i) cooler unit motor malfunction
 - ii) cooler unit circuit breaker malfunction
 - iii) control equipment room supply temperature high or low.
- (2) main control room status lights - the following status/alarm lights are provided in the main control room for each control equipment room supply cooler unit:
- i) overload/power failure (alarm)
 - ii) inoperative (status)
 - iii) low flow (alarm)
 - iv) high filter differential pressure (alarm)
 - v) high/low supply air temperature (alarm)
 - vi) lockout (status)
 - vii) auto (status)
 - viii) start (status)
 - ix) stop (status)
- (3) out-of-service indication - the following conditions will actuate an auxiliary building control area HVAC out-of-service status light in the main control room:
- i) manual out-of-service
 - ii) associated standby diesel generator manual out-of-service
 - iii) associated channel of control area chilled water system out-of-service
 - iv) control equipment room supply unit cooler locked out.

Actuation of this out-of-service indication also causes actuation of a "BOP Safety System Out-Of-Service" annunciator in the main control room.

- (i) service water intake structure
 - (1) remote control panel trouble alarm - a summary alarm is provided in the main control room that alarms whenever any of the following conditions exist:
 - i) service water pump room supply fan low flow - this alarm will not occur if the supply fan control switch (at the remote control panel) is in the "STOP" position.
 - ii) service water pump room exhaust fan low flow - this alarm will not occur if the exhaust fan control switch (at the remote control panel) is in the "STOP" position.
 - iii) traveling screen motor room supply fan low flow - this alarm will not occur if the supply fan control switch (at the remote control panel) is in the "STOP" position.
 - iv) service water pump room temperature high or low
 - v) traveling screen motor room temperature high or low.

These alarms are all individually indicated on the remote control panel annunciator.

- (2) manual out-of-service indication - manual out-of-service switches and indicators are provided in the main control room as an administrative control for use whenever a service water pump room supply or exhaust fan or a traveling screen motor room supply fan is placed out of service. This indication is provided on a per 1E channel basis and is also illuminated automatically whenever the associated standby diesel generator manual out-of-

service switch is actuated. Actuation of a manual out-of-service switch also causes actuation of a "BOP" Safety System Out-Of-Service" annunciator in the main control room.

- c. Safe shutdown equipment area ventilation system (SSEAVS).

The SSEAVS consists of two subsystems:

1. The reactor building equipment area cooling system (described in Section 9.4.2) which is also part of the ESF equipment area cooling system and is designed to the criteria applicable to that system. See part (b) of this response.
2. The remote shutdown panel (RSP) room HVAC system (described in Section 9.4.2).

(a) Differences - the applicability of the following NRC regulatory positions to the RSP room HVAC system:

- (1) GDC 19
- (2) IEEE Standard 279-1971
- (3) Regulatory Guide 1.22
- (4) Regulatory Guide 1.47
- (5) Regulatory Guide 1.53
- (6) Regulatory Guide 1.62
- (7) Regulatory Guide 1.75
- (8) Regulatory Guide 1.105
- (9) Regulatory Guide 1.118

(b) Justification - The RSP room HVAC system, as described in Section 9.4.3, is not safety-related. The system design bases are specifically identified in Section 9.4.3.1.3.

The above listed regulatory positions are applicable to safety systems. Since the instrumentation and controls of the RSP room HVAC system are not safety-related, strict

*36 hours
torus
104
72 hours
torus
108*

compliance with these regulatory positions is not required for this system.

d. Plant Computer Systems

1. Differences - The applicability of the following NRC regulatory positions to the plant computer systems:
 - (a) GDC 1
 - (b) GDC 2
 - (c) GDC 4
 - (d) IEEE Standard 279-1971
 - (e) Regulatory Guide 1.22
 - (f) Regulatory Guide 1.47
 - (g) Regulatory Guide 1.53
 - (h) Regulatory Guide 1.75
 - (i) Regulatory Guide 1.105
 - (j) Regulatory Guide 1.118
2. Justification - The plant computer systems, as identified in Section 7.5.1.3.3, are nonsafety-related systems that provide information to operating personnel in the form of graphic displays and alarming functions.

The listed NRC regulatory positions are applicable to protection systems and other systems important to safety. The plant computer systems do not fall under either of these categories and therefore do not fall under the applicability of these regulatory positions.

QUESTION 421.4 (SECTION 7.1)

FSAR Section 7.1.2.4 provides a discussion of design conformance to Regulatory Guide 1.118, Periodic Testing of Electrical Power and Protection Systems, June 1976 as an endorsement of IEEE-338-1977 and provides clarifications to two positions of this RG. The version of R.G. 1.118 cited is incorrect, as is the two positions discussed. To comply the staff review and the ensuing evaluation, the discussion of the justification for deviation from R.G. 1.118 will have to be corrected by referencing the 1978 version and by providing a clarification of the design deviations from the RG positions. It should be noted that the use of jury-rigged bypasses such as temporary jumpers, the removal of fuses, or removal of connectors is not an acceptable method for standard in-service testing.

RESPONSE

Although the June 1978 revision of Regulatory Guide 1.118 is not part of the design basis of the HCGS, ~~an assessment of a~~ conformance has been prepared. Section 7.1.2.4.g and Table 7.1-2 have been revised to reflect the specified date and to clarify the conformance situation.

In conjunction with the review described in the response to Question 421.22, a review will be performed to determine if bypasses such as temporary jumpers, the removal of fuses, or the removal of connectors may be necessary for HCGS inservice testing. Instances where such bypasses may have to be used will be documented in a revision to this response, and discussions will be provided to justify the use of these bypasses. These justifications will be based on the exceptions authorized by position C14 of Regulatory Guide 1.118:

"a. Temporary jumper wires may be used with portable test equipment where the safety system equipment to be tested is provided with facilities specifically designed for connection of this test equipment. These facilities shall be considered part of the safety system and shall meet all the requirements of this standard, whether the portable test equipment is disconnected or remains connected to these facilities.

"b. Removal of fuses or opening a breaker is permitted only if such action causes (1) the trip of the associated protection system channel or (2) the actuation (startup and operation) of the associated Class 1E load group."

The revised response will be submitted by July, 1984.

This review was conducted and the results are included in that response. Also,

PRELIMINARY

HCGS; however, equipment is qualified following the guidelines of IEEE 323-1971 as discussed in Section 3.11.2. Also refer to Section 3.11 for discussion of the environmental qualification program.

- o. Assessment to Regulatory Guide 1.100, Seismic Qualifications of Electrical Equipment for Nuclear Power Plants, March 1976 - While not a design basis, the extent of conformance to Regulatory Guide 1.100 is discussed in Section 3.10.
- p. Assessment to Regulatory Guide 1.105, Instrument Setpoints, November 1975 - While not a design basis, the design supplied includes the trip setpoint (instrument setpoint), allowable value (Technical Specification limit), and the analytical or design basis limit, which are all contained in Chapter 16, Technical Specifications. These parameters are all appropriately separated from each other based on instrument accuracy, calibration capability, and design drift (estimated) allowance data. The setpoints are within the instrument accuracy range.

The established setpoints provide margin to satisfy both safety requirements and plant availability objectives.

- q. Assessment to Regulatory Guide 1.118, Periodic Testing of Electrical Power and Protection Systems, June 1978 - This regulatory guide, which endorses modified IEEE 338-1977, is not part of the design basis for HCGS. Discussion of IEEE 338 is presented on a system-by-system basis in the analysis portions of Sections 7.2, 7.3, 7.4, and 7.6, with the following clarification of position C.6: The removal of fuses, and/or breakers to prevent the operation of equipment during the performance of tests could be authorized under strict administrative controls and approved procedures. See the response to Question 4.21.22 for additional information on at-power testability.

7.1.2.5 Independence of Safety-Related Systems

The safety-related I&C required to provide protective actions are physically arranged and separated to retain the minimum required

PRELIMINARY

HOPK CREEK GENERATING STATION
FINAL SAFETY ANALYSIS REPORT
TABLE 7.12

CODES AND STANDARDS APPLICABILITY MATRIX FOR NSSS CONTROL AND INSTRUMENTATION EQUIPMENT (1) (2)

	REACTOR PROTECTION TRIP SYSTEM	EMERGENCY CORE COOLING SYSTEM	PRIMARY CONTAINMENT AND REACTOR VESSEL ISO. SYS.	SPRAY COOLING	RHM SUPPRESSION	POOL COOLING	REACTOR CORE ISOLATION COOLING	STANDBY LIQUID CONTROL	RHM REACTOR SHUTDOWN COOLING	SAFETY RELATED DISPLAY INSTRUMENTATION	CONTROL ROD POSITION INDICATING SYSTEM	PROCESS RADIATION MONITORING SYSTEM	HIGH PRESS./LOW PRESS. SYSTEM INTERLOCKS	LEAK DETECTION SYSTEM	NEUTRON MONITORING SYSTEM	RECIRCULATION PUMP TRIP (2)	SAFETY RELIEF VALVES - RELIEF FUNCTION	REDUNDANT REACTIVITY CONTROL SYSTEM
RG 1.95 5/73																		
RG 1.97 5/73	X	X	X	X	X	X	X	X	X									
RG 1.93 5/73	X	X	X	X	X	X	X	X	X									
RG 1.87 10/73	X	X	X	X	X	X	X	X	X									
RG 1.83 10/73 (5)		B	B															
RG 1.90 11/73	A	A	A	A	A	A	A	A	A									
RG 1.73 1/74		A	A	A	A	A	A	A	A									
RG 1.76 1/75 (7)	X	X	X	X	X	X	X	X	X									
RG 1.89 11/74	A	A	A	A	A	A	A	A	A									
RG 1.190 3/78	A	A	A	A	A	A	A	A	A									
RG 1.195 11/75	A	A	A	A	A	A	A	A	A									
RG 1.118 8/78	A	A	A	A	A	A	A	A	A									

NOTES

- (1) All General Design Criteria, selected IEEE standards and Regulatory Guides 1.1 through 1.118 are included in the plant design basis as indicated for each NSSS system.
- (2) The letter X on the table indicates a system requirement and the letter A indicates that the code or standard is not a design basis, but the text provides a description of the extent of design agreement.
- (3) The recirculation pump trip is related to the RPS trip. It is not assessed as the ATWS trip.
- (4) Alternate reactivity control systems do not include SLCS for BWRs, only reactor manual control and recirculation flow control.
- (5) Electric penetration assemblies are BOP work, therefore IEEE 317 and Regulatory Guide 1.63 are not a NSSS design basis. See Table 7.1.3 note. The letter B indicates NSSS systems requiring electrical penetrations.
- (6) The extent of implementation for the requirements of Regulatory Guide 1.75, Revision 1 are as follows:
Physical separation between divisions of essential systems and between essential systems and essential circuits must be maintained for all essential NSSS systems except the neutron monitoring system and the process inhibition monitoring system, which shall be justified by analysis.

(7) The appropriate editions of the referenced IEEE standards applicable to ATWS are IEEE 308-1974, IEEE 323-1974, IEEE 338-1974, IEEE 344-1975.

QUESTION 421.6 (SECTIONS 7.1 - 7.6)

Identify any "first-of-kind" instruments used in or providing inputs to safety-related systems. Identify each application of a microprocessor, multiplexer or computer system where they are in or interface with safety-related systems.

RESPONSE

There are no "first-of-kind" instruments used in or providing inputs to NSSS safety-related systems. Microprocessors are used in the redundant reactivity control system (RRCS). While the RRCS does not perform any reactor control functions, it does provide signals to trip the recirculation system, to runback the feedwater system, to initiate the standby liquid control system, and to initiate alternate rod insertion for mitigation of an ATWS event (see Section 15.8). The performance monitoring system (PMS) is nonsafety-related, and isolation of safety-related inputs to the PMS is shown functionally in the logic diagrams and elementary diagrams provided to the NRC and listed in Table 1.7-3.

1. The non-NSSS safety-related, "first-of-kind" equipment used at HCGS consists of the following:

- a. Bailey 862 solid state logic modules - provide common signal levels, interfaces, and common logic arrays to provide the interface between the engineered safety features (ESF) systems (identified in Section 7.3) and the main control room controls and displays (identified in Section 7.5).

High system reliability is achieved through the use of auctioneered redundant power supplies for the three different dc voltages utilized by the 862 logic modules:

- 1) 125-Vdc for interrogation of field contacts
- 2) 24-Vdc for interrogation of main control room controls; for powering main control room status lights; for powering output driver relays
- 3) 9-Vdc for powering the 862 logic modules (onboard voltage regulators control this at 5-Vdc for the logic and buffer circuitry).

The integrity of each power supply is continuously monitored and any failure is annunciated in the main control room and indicated at the summary alarm panel of the affected logic assembly (cabinet). This summary

4 channels on all systems except in SIC
Checks and offsite/remote
main switches
Technical K-10503
operating system
start/stop
Form 1/84

alarm panel also provides indication of fuse module fuse failure, cooling fan failure, and in which bay (of the 12 bay assembly) the failure occurred.

A digital logic assembly trouble summary alarm is annunciated in the main control room whenever any of the following conditions exist in a Class 1E logic assembly:

- 1) Door open
- 2) Fuse module fuse failure
- 3) Fuse module interlock (fuse module withdrawn)
- 4) Power bus failure
- 5) Power supply failure
- 6) Cooling fan failure
- 7) Optic link failure (optical isolation system trouble).

High system reliability is achieved by segregating control of field devices (e.g., switchgear, MCC, etc.) into different circuits within a logic assembly. Each circuit is composed of a single fuse module and as many logic modules and output driver relays as required to control a field device. Several related field devices may be controlled from the same circuit. The fuse module protects the logic assembly power supplies from individual circuit faults.

Testing of a system circuit from its control switch through the output(s) of the associated logic modules is made possible by a switch on the fuse module which, when operated, disables the output driver relays. This disabling is continuously indicated in the main control room. Light emitting diodes on the face of the logic module indicate the presence or lack of input signals from the associated control switch and the presence or lack of signals to the output driver relays.

The Bailey 862 equipment is functionally described in the logic diagrams provided to the NRC and listed in Table 1.7-3.

Equipment qualification reports are referenced in Sections 3.10 and 3.11.

- b. Bailey 890 system - provides the interface and isolation between the main control room, safety-related instrumentation and the plant computer (control room integrated display system), and the plant annunciator system. The Bailey 890 system is also used to provide isolation between the Class 1E indicating lamp circuits and initiating logic circuits provided for lamp test.

The equipment is functionally described in the logic diagrams provided to the NRC and listed in Table 1.7-3.

Equipment qualification reports are referenced in Sections 3.10 and 3.11.

The Bailey 890 system isolation capabilities are discussed in the response to Question 421.13.

- c. Technology for Energy Corporation (TEC) Model 600 equipment - provides equipment to monitor, perform calculations, provide outputs to operator displays, and provide signal isolation (where required) for the following systems:

- 1) Suppression pool temperature monitoring system - described in Section 6.2.1.1.10.3,
- 2) Reactor building exhaust radiation monitoring system - described in Section 11.5.2.1.3,
- 3) Refueling floor exhaust radiation monitoring system - described in Section 11.5.2.1.2.

Equipment qualification reports are referenced in Sections 3.10 and 3.11.

The TEC Model 600 equipment isolation capabilities are discussed in the response to Question 421.13.

2. The following non-NSSS systems at HCGS interface with safety-related systems using microprocessors, multiplexers, or computers:

- a. Radiation monitoring systems (RMSs) - discussed in Sections 11.5.2.1.3 and 11.5.2.1.2, the Class 1E reactor building exhaust and refueling floor exhaust RMSs utilize TEC Model 600 equipment to provide radiation monitoring and isolation initiation functions.

The TEC Model 600 system is a microprocessor based system using Motorola 68000 microprocessors to provide

data acquisition, signal processing, and signal isolation (where required). See item 1.c. above.

The TEC Model 600 system isolation capabilities are discussed in the response to Question 421.13.

- b. Suppression pool temperature monitoring system (SPTMS) - discussed in Section 6.2.1.1.10.3, the SPTMS utilizes TEC Model 600 equipment to provide reliable indication of suppression pool temperature to meet the requirements of a Regulatory Guide 1.97 (type A, Category 1) variable.

The TEC Model 600 system is a microprocessor based system using Motorola 68000 microprocessors. In the SPTMS, redundant, dedicated microprocessors are used to provide data acquisition, signal processing, operator displays, and signal isolation (where required). See item 1.c. above.

The TEC Model 600 system isolation capabilities are discussed in the response to Question 421.13.

- c. Control room integrated display system (CRIDS) - part of the plant computer systems discussed in Section 7.5.1.3.3, the CRIDS computer interfaces with safety-related systems to provide information to the control room operator in the form of graphic displays and alarming functions. The CRIDS computer is also used to meet emergency response facility requirements (see Section 7.5.1.3.3).

The CRIDS is nonsafety-related and isolation of safety-related inputs is shown functionally in the logic diagrams and elementary diagrams provided to the NRC and listed in Table 1.7-3. See item 1.b. above and the response to Question 421.13 which discusses isolation capabilities of the Bailey 890 system.

- d. Emergency response facility data acquisition system (ERFDAS) - the data acquisition system for the HCGS emergency response facilities (ERF). The CRIDS computer is used to process this information as discussed in Section 7.5.1.3.3.

The ERFDAS uses the "Real Time Peripheral" (RTP) system supplied by Computer Products Inc. (CPI). The RTP uses multiplexers to provide data acquisition and signal isolation.

The CPI RTP system isolation capabilities are discussed in the response to Question 421.13.

e. Startup transient monitoring system (STMS) - discussed in Section 7.5.1.3.5, the STMS uses Validyne Model MC370AD-Q2 remote multiplexers to provide data acquisition and signal isolation of those safety-related signals needed to support plant startup testing.

Isolation capabilities of the Validyne Model MC370AD-Q2 multiplexers are discussed in the response to Question 421.49.

QUESTION 421.7 (SECTIONS 7.1, 7.2, 7.3, 7.4, 7.5 & 7.6)

Section 7.1.2.4 of the FSAR provides a brief discussion on conformance to Reg. Guide 1.47. Discuss in detail the design of the bypassed and inoperable status indication using detailed schematics. Include the following information on the discussion:

1. Compliance with the recommendations of Reg. Guide 1.47 and Reg. Guide 1.22 Position D.3a and 3b.
2. The design philosophy used in the selection of equipment/systems to be monitored, including auxiliary and support systems.
3. How the design of the bypass and inoperable status indication systems comply with Positions B1 through B6 of ICSB Branch Technical Position 21.
4. The list of system automatic and manual bypasses as it pertains to the recommendations of Reg. Guide 1.47.
5. Discuss hardware features employed to provide a consolidated, human factored, display of the bypassed and inoperable status of ESF equipment.

RESPONSE

1. Bypassed and inoperable status indication has been provided on a system level basis for all HCGS safety-related systems meeting the criteria established by Section B of Regulatory Guide 1.47. The bypassed and inoperable status indication system (BISIS), discussed in revised Section 7.5.1.3.2, is the result of the application of the regulatory positions set forth in Section C of Regulatory Guide 1.47 to the HCGS safety-related systems.

The BISIS is a collection of indicating lights from the various safety-related systems (listed in revised Section 7.5.1.3.2) for which bypassed and inoperable status indication is required by Regulatory Guide 1.47. These systems are designed in accordance with the specific requirements of Regulatory Guide 1.22 (including D.3a and 3b) to the degree stated in Section 1.8.1.22.

System design drawings showing conformance to Regulatory Guides 1.22 and 1.47 have been provided to the NRC under separate cover and are listed on Tables 1.7-1, 1.7-2, and 1.7-3.

The BISIS associated indications are included in revised Table 7.5-1.

- 2,3, See Section 7.5.1.3.2 for a detailed description of the
- & 4. HCGS bypassed and inoperable status indications systems. Compliance to BTP 21 is demonstrated in this system description.
5. Section 7.5.1.3.2 provides a discussion of the hardware features employed in the HCGS design for bypassed and inoperable status indication. The results of a HCGS human factors analysis will be provided in Chapter 18.

QUESTION 421.10 (SECTION 7.1 & 7.2)

The staff believes that the physical separation provided in the design of the RPS cabinets may not satisfy the requirements of Regulatory Guide 1.75 or the plant separation criteria and is, therefore, unacceptable. As an example, it has been noted on similar plants that the cabinet lighting and power circuits (which are not treated as associated circuits) becomes associated with Class 1E circuits inside the RPS cabinets. Section 8.1.4.14 includes a brief discussion on the physical separation provided within panels, instrument racks and control boards for the instrumentation and control circuits of different divisions. Review the design of all Class 1E cabinets for separation between non-Class 1E and Class 1E circuits. Provide the staff with a listing of the cabinets which were reviewed and describe in detail how physical separation is maintained within the panels, racks and boards for those cases where a 6 inch air space cannot be maintained. Provide a summary of the analysis and testing performed to support this lesser separation. Include in the discussion the separation provided for associated circuits, internal wiring identification and the use of common terminations.

RESPONSE

The HCGS RPS cabinets (10C609, 10C611, 10C622 and 10C623) meet the requirements of IEEE Standard 384 as modified and endorsed by Regulatory Guide 1.75, as stated in Section 1.8.1.75. Cabinet lighting and receptacle power circuits are physically separated from RPS circuits by being routed in metallic conduit or by structural steel barriers.

Physical separation between non-Class 1E and Class 1E instrumentation and control circuits is provided in panels, instrument racks and control boards in accordance with IEEE Standard 384, as modified and endorsed by Regulatory Guide 1.75 as stated in Section 1.8.1.75. The following is a listing of Class 1E panels, instrument racks and control boards reviewed for the separation requirements of IEEE Standard 384:

Panels

1AC200	H ₂ /O ₂ Analyzer A Panel
1BC200	H ₂ /O ₂ Analyzer B Panel
1CC200	H ₂ /O ₂ Analyzer Heat Trace Panel
1DC200	H ₂ /O ₂ Analyzer Heat Trace Panel
1AC201	SACS Control Panel A
1BC201	SACS Control Panel B
1CC201	SACS Control Panel C
1DC201	SACS Control Panel D
10C202	RACS Heat Exchanger and Pumps Control Panel

1AC213 Instrument Gas Compressor A Control Panel
 1BC213 Instrument Gas Compressor B Control Panel
 1AC215 H₂ Recombiner A Power Distribution Panel
 1BC215 H₂ Recombiner B Power Distribution Panel
 1AC281 Reactor Building Unit Cooler Control Panel
 1BC281 Reactor Building Unit Cooler Control Panel
 1CC281 Reactor Building Unit Cooler Control Panel
 1DC281 Reactor Building Unit Cooler Control Panel
 1AC285 Reactor Building FRVS Control Panel
 1BC285 Reactor Building FRVS Control Panel
 1CC285 Reactor Building FRVS Control Panel
 1DC285 Reactor Building FRVS Control Panel
 1OC286 Reactor Building Equipment Lock Ventilation
 1OC399 Remote Shutdown Panel
 1OC401 Diesel Generator Area Battery Room Panel
 1OC402 Diesel Generator Area Battery Room Panel
 1AC420 Diesel Generator A Exciter Panel
 1BC420 Diesel Generator B Exciter Panel
 1CC420 Diesel Generator C Exciter Panel
 1DC420 Diesel Generator D Exciter Panel
 1AC421 Diesel Generator A Local Engine Control Panel
 1BC421 Diesel Generator B Local Engine Control Panel
 1CC421 Diesel Generator C Local Engine Control Panel
 1DC421 Diesel Generator D Local Engine Control Panel
 1AC422 Diesel Generator A Remote Control Generator Panel
 1BC422 Diesel Generator B Remote Control Generator Panel
 1CC422 Diesel Generator C Remote Control Generator Panel
 1DC422 Diesel Generator D Remote Control Generator Panel
 1AC423 Diesel Generator A Remote Engine Control Panel
 1BC423 Diesel Generator B Remote Engine Control Panel
 1CC423 Diesel Generator C Remote Engine Control Panel
 1DC423 Diesel Generator D Remote Engine Control Panel
 1AC428 Diesel Generator A Load Sequencer Panel
 1BC428 Diesel Generator B Load Sequencer Panel
 1CC428 Diesel Generator C Load Sequencer Panel
 1DC428 Diesel Generator D Load Sequencer Panel
 1AC482 Electric Heater Control Panel 1AVH403
 1BC482 Electric Heater Control Panel 1BVH403
 1AC483 Diesel Area HVAC Control Panel
 1BC483 Diesel Area HVAC Control Panel
 1CC483 Diesel Area HVAC Control Panel
 1DC483 Diesel Area HVAC Control Panel
 1AC485 Control Area HVAC Control Panel
 1BC485 Control Area HVAC Control Panel
 1AC486 Diesel Area Panel Room Supply System
 1BC486 Diesel Area Panel Room Supply System
 1AC487 Water Chiller Panel
 1BC487 Water Chiller Panel
 1AC488 Chiller AK403 Power Panel
 1BC488 Chiller BK403 Power Panel
 1AC489 Electric Heater Control Panel 1AVH407
 1BC489 Electric Heater Control Panel 1BVH407

1AC490 Water Chiller A Control Panel
 1BC490 Water Chiller B Control Panel
 1AC491 Water Chiller A Power Panel
 1BC491 Water Chiller B Power Panel
 1AC492 Electric Heater Control Panel
 1BC492 Electric Heater Control Panel
 1AC493 Control Panel - Auxiliary Building Diesel
 1AC494 Control Panel - Auxiliary Building Diesel
 1AC495 Control Panel - Auxiliary Building Diesel
 1BC495 Control Panel - Auxiliary Building Diesel
 1CC495 Control Panel - Auxiliary Building Diesel
 1DC495 Control Panel - Auxiliary Building Diesel
 1AC515 Traveling Screen Control Panel
 1BC515 Traveling Screen Control Panel
 1CC515 Traveling Screen Control Panel
 1DC515 Traveling Screen Control Panel
 1AC516 Service Water Pump Panel
 1BC516 Service Water Pump Panel
 1CC516 Service Water Pump Panel
 1DC516 Service Water Pump Panel
 1AC581 Intake Structure HVAC Control Panel
 1BC581 Intake Structure HVAC Control Panel
 1CC581 Intake Structure HVAC Control Panel
 1DC581 Intake Structure HVAC Control Panel
 1OC601 RRCS Division 1 Panel
 1OC602 RRCS Division 2 Panel
 1OC604 Class 1E Radiation Monitoring Instrumentation Cabinet
 1OC617 Division 1 RHR and Core Spray Relay Vertical Board
 1OC618 Division 2 RHR and Core Spray Relay Vertical Board
 1OC620 HPCI Relay Vertical Board
 1OC621 RCIC Relay Vertical Board
 1OC622 Inboard Isolation Valve Relay Vertical Board
 1OC623 Outboard Isolation Valve Relay Vertical Board
 1OC628 ADS Division 2 Relay Vertical Board
 1OC631 ADS Division 4 Relay Vertical Board
 1AC633 Post LOCA H₂ Recombiner A Control Cabinet
 1BC633 Post LOCA H₂ Recombiner B Control Cabinet
 1OC640 Division 4 RHR and Core Spray Relay Vertical Board
 1OC641 Division 3 RHR and Core Spray Relay Vertical Board
 1OC650 Main Control Room Vertical Board
 1OC651 Unit Operators Console
 1AC652 1E Solid State Logic Cabinet Channel A
 1BC652 1E Solid State Logic Cabinet Channel B
 1CC652 1E Solid State Logic Cabinet Channel C
 1DC652 1E Solid State Logic Cabinet Channel D
 1AC655 1E Analog Logic Cabinet Channel A
 1BC655 1E Analog Logic Cabinet Channel B
 1CC655 1E Analog Logic Cabinet Channel C
 1DC655 1E Analog Logic Cabinet Channel D
 1AC657 1E Digital Termination Cabinet Channel A
 1BC657 1E Digital Termination Cabinet Channel B
 1CC657 1E Digital Termination Cabinet Channel C

1DC657	1E Digital Termination Cabinet Channel D
1AC680	1E Electrical Auxiliary Cabinet Channel A
1BC680	1E Electrical Auxiliary Cabinet Channel B
1CC680	1E Electrical Auxiliary Cabinet Channel C
1DC680	1E Electrical Auxiliary Cabinet Channel D

Instrument Racks

1OC002	Reactor Water Clean-up Rack
1OC004	Reactor Vessel Level and Pressure A Rack
1OC005	Reactor Vessel Level and Pressure C Rack
1OC009	Jet Pump Rack A
1OC014	HPCI A/HPCI Leak Detection A Rack
1OC015	Main Steam C/D and Recirc A Flow Rack
1OC018	RHR A and ADS Rack
1OC021	RHR B and ADS Rack
1OC025	Main Steam C/D and Recirc A Flow Rack
1OC026	Reactor Vessel Level and Pressure D Rack
1OC027	Reactor Vessel Level and Pressure B Rack
1OC037	RCIC D/RCIC Leak Detection D Rack
1OC041	Main Steam A/B and Recirc B Flow Rack
1OC042	Main Steam A/B and Recirc B Flow Rack
1OC069	RHR D and ADS Rack
1OC208A	RCIC/Reactor Cooling
1OC211	RCIC Pump
1OC212	RCIC Pump

Instrument racks are separated into channels. No two redundant piped or tubed safety-related instruments are located on the same rack.

Where a 6-inch air space cannot be maintained between instrumentation and control circuits of different channels (both Class 1E to Class 1E and Class 1E to non-Class 1E), barriers are provided in accordance with IEEE Standard 384. These barriers are metallic conduit, structural steel barriers, or non-metallic wrap (Havey Industries Siltemp Sleeving Type S or Siltemp Woven Tape Type WT65). The metallic conduit and structural steel barriers are noncombustible materials. The nonmetallic wrap (Siltemp) was successfully tested for use as an isolation barrier (reference Wyle Laboratories Test Report Number 56669).

For certain types of isolation devices, barriers of the type noted above are not feasible. For these cases, requirements of Section 7.2.2.1 of IEEE Standard 384 are met, as follows:

"The separation of the wiring at the input and output terminals of the isolation device may be less than 6 inches (0.15 m) as required in 6.6.2 provided that it is not less than the distance between input and output terminals.

Add statement

421.10-4

Amendment 5

421/13
3 cables
3 TEC cables
② Relay as
to contact
1 to 2
inches

Minimum separation requirements do not apply for wiring and components within the isolation device; however, separation shall be provided wherever practicable."

Testing, in accordance with IEEE Standard 472 (Surge Withstand Capability) will be performed to ensure that the Class 1E inputs to the isolation devices are not affected by short-circuit failures, ground faults or voltage surges on the output side of the isolation devices.

The only analysis that will be performed to support air spaces less than 6 inches, since the requirements of IEEE Standard 384 are satisfied, is for the Neutron Monitoring System Panel (10C608) and the Process Radiation Monitoring System Panels (10C635 and 10C636).

No associated circuits have been identified in the non-NSSS panels, instrument racks, or control boards. Internal wiring identification is done using color coded insulation or insulation marked with color coded tape. For panel sections of one channel only, internal wiring identification may not be done. Where common terminations are used, the requirements of IEEE Standard 384 are satisfied as stated above.

Electrical equipment and wiring for the reactor protection system (RPS), the nuclear steam supply shutoff systems (NSSSS) and the engineered safeguards subsystems (ESS) are segregated into separate divisions designated I and II, etc., such that no single credible event is capable of disabling sufficient equipment to prevent reactor shutdown, removal of decay heat from the core, or closure of the NSSSS valves in the event of a design basis accident.

No single control panel section (or local panel section or instrument rack) includes wiring essential to the protective function of two systems that are backups for each other (Division I and Division II) except as allowed below:

- a. If two panels containing circuits of different separation divisions are less than 3 feet apart, there shall be a steel barrier between the two panels. Panel ends closed by steel end plates are considered to be acceptable barriers provided that terminal boards and wireways are spaced a minimum of one inch from the end plate.
- b. Floor-to-panel fire proof barriers must be provided between adjacent panels having closed ends.
- c. Penetration of separation barriers within a subdivided panel is permitted, provided that such penetrations are sealed or otherwise treated so that an electrical fire could not

As noted above here

reasonably propagate from one section to the other and destroy the protective function.

- d. Where, for operational reasons, locating manual control switches on separate panels is considered to be prohibitively (or unduly) restrictive to normal functioning of equipment, then the switches may be located on the same panel provided no single event in the panel can defeat the automatic operation of the equipment.

With the exception of panels 10C608, 10C635 and 10C636, internal wiring of the NSSS panels and racks has color-coded insulation. Associated circuits are treated within a panel or rack in the same manner as the essential circuits. Where common terminations are used, the requirements of IEEE Standard 384 are satisfied.

QUESTION 421.9 (SECTION 7.1)

Provide an overview of the plant electrical distribution system with emphasis on the reactor protection system (i.e., reactor trip, engineered safety features actuation and supporting features) instrumentation including the sensors, logic, and actuation relay power supplies and divisional separation as a background for addressing FSAR Chapter 7 concerns. Use on-line diagrams and other drawings as appropriate.

RESPONSE

Section 7.1.2.8 has been added to provide the requested information.

Electrical distribution is shown on the following figures:

- Figure 8.3-8 Single Line Meter & Relay Diagram 125 Vdc System
- Figure 8.3-9 Single Line Meter & Relay Diagram ± 24 Vdc System
- Figure 8.3-11 Single Line Meter & Relay Diagram 120 Vac Instrumentation & Miscellaneous Systems
- Figure 8.3-13 Reactor Protection System Power Supply

*test response
are due in September*

accepted

QUESTION 421.13 (SECTION 7.1, 7.3, 7.4, 7.5 & 7.6)

Various instrumentation and control system circuits in the plant rely on certain devices to provide electrical isolation capability in order to maintain the independence between redundant safety-related circuits and between safety-related circuits and nonsafety-related circuits. Provide the following information:

1. Identify the types of isolation devices which are used as boundaries to isolate nonsafety-related circuits from the safety-related circuits or to isolate redundant safety-related circuits.
2. Provide a summary of the purchase specifications for each isolation device identified in response to part (1) above.
3. Describe the type of testing that was conducted on the isolation devices to ensure adequate protection against the effects of electromagnetic interference, short-circuit failures (line to line and line to ground), voltage faults, and/or surges.

RESPONSE

Non-NSSS:

For part (2) of this question, "summary of purchase specifications" has been inferred as requiring qualification requirements (seismic and environmental) for each isolation system listed below. For each isolation system discussion on seismic qualification, individual isolation devices are qualified to Required Response Spectra (RRS) curves generated for the device location(s). Environmental qualification is discussed for each isolation device in succeeding paragraphs.

Electrical isolation between redundant non-NSSS safety-related circuits and between non-NSSS safety-related circuits and non-safety-related circuits is provided by the following:

- a. Bailey Solid State Interposing Logic System (SSILS) and Analog Instrumentation System (AIS) - these two systems utilize the Bailey 890 system for 1E to non-1E, and non-1E to 1E isolation. The basic components of the 890 system are input/output multiplexing modules and transmitter/receiver modules. Transmission is by fiberoptic cable. The transmitter module provides 1E to non-1E isolation; the receiver module provides non-1E to 1E isolation. The fiberoptic cable provides additional electrical isolation although it itself is not formally qualified.

Seismic qualification for this isolation system is in accordance with qualification procedures and acceptance criteria defined in IEEE Standard 344-1975, and implemented by Regulatory Guide 1.100, Revision 1.

This isolation system is located in and qualified for a mild environment as defined in Sections 3.11.2.4 and 3.11.2.5. The worst-case specified environmental conditions in which this isolation system is designed to operate are as follows:

Pressure: Atmospheric plus fractional inch of H₂O

Temperature:	104°F maximum	} these conditions may exist 24 hours per year
	40°F minimum	
	83°F ± 2°F	

Relative Humidity: 50% maximum (summertime)
20% minimum (wintertime)

Nuclear Radiation: 175 Rads Carbon (40 year TID)
88 Rads Carbon - Beta (180 day TID)
2.5 Rads Carbon - Gamma (180 day TID)

(TID = Total Integrated Dose)

Testing in accordance with SAMA Standard PMC 33.1-1978 will be completed by June, 1984, to ensure that this isolation system is adequately protected against the effects of electromagnetic interference (EMI).

Testing in accordance with IEEE Standard 472-1974 will be completed by June, 1984, to ensure that this isolation system is adequately protected against the effects of short-circuit failures, voltage faults and/or surges.

- 7-10-84*
- b. Computer Products Inc. (CPI) Emergency Response Facilities Data Acquisition System (ERFDAS) - this system utilizes the CPI real time peripheral (RTP) system for 1E to non-1E isolation. The basic components of the RTP system are analog and digital surge cards (qualified to IEEE Standard 472-1974 requirements), analog input cards and optically isolated digital input cards, distributed input/output controllers (DIOC) and transformer-coupled multi-drop limited distance modems (MDLDM). The MDLDMs provided the 1E to non-1E isolation. Data transmission to receiving MDLDMs is by twisted-shielded pairs.

Seismic qualification for this isolation system is in accordance with qualification procedures and acceptance criteria defined in IEEE Standard 344-1975, and implemented by Regulatory Guide 1.100, Revision 1.

This isolation system is located in and qualified for a mild environment as defined in Sections 3.11.2.4 and 3.11.2.5. The worst-case specified environmental conditions in which this isolation system is designed to operate are as follows:

Pressure: Atmospheric plus fractional inch of H₂O

Temperature: 104°F maximum } these conditions may
40°F minimum } exist 24 hours per year
83°F ± 2°F }

Relative Humidity: 50% maximum (summertime)
20% minimum (wintertime)

Nuclear Radiation: 175 Rads Carbon (40 year TID)
88 Rads Carbon - Beta (180 day TID)
2.5 Rads Carbon - Gamma (180 day TID)

Testing in accordance with SAMA Standard PMC 33.1-1978 will be completed by August, 1984, to ensure that this isolation system is adequately protected against the effects of electromagnetic interference (EMI).

Testing in accordance with IEEE Standard 472-1974, will be completed by February, 1984, to ensure that this isolation system is adequately protected against the effects of short-circuit failures, voltage faults and/or surges. These tests will be performed on the analog and digital surge cards and the transmit/receive circuits of the MDLDMs.

- c. Technology for Energy Corporation (TEC) Radiation Monitoring System (RMS) - this system utilizes three separate isolation methods depending upon the type of isolation required:
- 1) 1E to 1E isolation - for this type of isolation, Hewlett Packard HFBR 1000 and HFBR 2001 isolators are used. Optical coupling is used to provide the isolation.
 - 2) 1E to non-1E annunciator outputs - for this type of isolation, Agastat Model EGP isolation relays are used. Relay coil to contact separation provides the isolation.
 - 3) 1E to non-1E communication - for data transmission between the TEC 1E microprocessor and the non-1E host computer, TEC Synchronous Data Link Control, serial communications modules 600-1200 are used. Transformer coupling provides the isolation for the transmit circuits. Optical coupling provides the isolation for the receive circuits.

Seismic qualification for these isolation systems is in accordance with qualification procedures and acceptance criteria defined in IEEE Standard 344-1975, and implemented by Regulatory Guide 1.100, Revision 1.

These isolation systems are located in and qualified for a mild environment as defined in Sections 3.11.2.4 and 3.11.2.5. The worst-case specified environmental conditions in which these isolation systems are designed to operate are as follows:

Temperature:	104°F maximum	} these conditions may exist 24 hours per year
	40°F minimum	
	76°F ± 2°F	

Relative Humidity: 50% maximum
20% minimum

Testing in conformance with Military Standards 461B and 462 on the effects of EMI will be completed by July, 1984.

Testing in accordance with IEEE Standard 472-1974, will be completed by July, 1984, to ensure that these isolation systems are adequately protected against the effects of short-circuit failures, voltage faults and/or surges.

---d. Remote control panels - two isolation methods are provided for remote control panels requiring 1E to non-1E isolation.

- 1) Digital 1E to non-1E isolation - for this type of isolation, Struthers Dunn type 219, Allen Bradley model 700-200A12P, and General Electric model HEA99 isolation relays are used. Relay coil to contact separation provides the isolation.
- 2) Analog 1E to non-1E isolation - for this type of isolation, TEC analog isolators, model 156, are used. Transformer coupling is used to provide the isolation.

Seismic qualification for these isolation systems is in accordance with qualification procedures and acceptance criteria defined in IEEE Standard 344-1975, and implemented by Regulatory Guide 1.100, Revision 1.

The Struthers Dunn type 219 and General Electric model HEA99 isolation relays are located in and qualified for a mild environment as defined in Sections 3.11.2.4 and 3.11.2.5. The worst-case specified environmental conditions in which these isolation relays are designed to operate are as follows:

Struther Dunn Type 219

Temperature: 104°F ± 2°F maximum
40°F ± 2°F minimum

Relative Humidity: 90% maximum
20% minimum

Nuclear Radiation: 200 Rads (40 year TID)

GE HEA99

Temperature: 104°F maximum
60°F minimum

Relative Humidity: 90% maximum
20% minimum

Nuclear Radiation: 200 Rads Gamma (40.5 year TID)

Environmental qualification as defined in IEEE Standard 323-1974, and implemented by Regulatory Guide 1.89, Revision 0, is required for the Allen Bradley model 700P-200A12P isolation relay. The worst-case specified environmental conditions in which this isolation relay is designed to operate are as follows:

		<u>Normal</u>	<u>Abnormal</u>	<u>Accident</u>
Temperature,	Minimum	40°F	110°F	148°F
	Maximum	80°F		
	Average	69°F		
Pressure,	Minimum	-0.25 in. H ₂ O		-3 psig
	Maximum	1.0 in. H ₂ O	0 psig	1.0 in. H ₂ O
Relative Humidity,	Minimum	20%		
	Maximum	90%	100%	100%
Radiation,	Total dose	8.8x10 ² rads		1.7x10 ⁵ rads gamma
	Duration	40 yr		180 days

The TEC model 156 analog isolators are located in and qualified for a mild environment as defined in Sections 3.11.2.4 and 3.11.2.5. The worst-case specified environmental conditions in which these isolators are designed to operate are as follows:

Temperature: 104°F ± 2°F maximum
40°F ± 2°F minimum

Relative humidity: 90% maximum
20% minimum

Nuclear radiation: 200 Rads (40 year TID)

No testing was conducted on the effects of EMI on the Struthers Dunn type 219, Allen Bradley model 700-200A12P, or General Electric model HEA99 isolation relays. By design, these relays should be immune to the effects of EMI.

Generic EMI susceptibility and emissions test were conducted on the TEC model 156 analog isolators following procedure 156-QP-04, "Electromagnetic Interference (EMI) Test for TEC Model 156 Analog Signal Isolator Module," which is Appendix B to test report 31041-QP-01, "Qualification Test Report for Environmental and Seismic Testing of the TEC Model 158 Analog Isolation System." Results of these tests are available for review at Technology for Energy Corporation, Knoxville, Tennessee.

Testing in accordance with IEEE Standard 472-1974, will be performed to ensure that the Struthers Dunn Type 219 and General Electric model HEA99 isolation relays are adequately protected against the effects of short-circuit failures, voltage faults and/or surges.

The following test was performed on the Allen Bradley model 700P-200A12P isolation relay to ensure adequate protection against the effects of short circuit failures, voltage faults and/or surges:

- 1) Test type - 100% high potential test
- 2) Test characteristics - 2700 V applied for one second between points of opposite polarity and to ground.

Testing in accordance with IEEE Standard 472-1974, will be performed to ensure the TEC model 156 analog isolators are adequately protected against the effects of short circuit failures, voltage faults and/or surges.

e. Equipment air lock isolation dampers HD-9450A and B interlock with receiving bay door #4323A - Potter Brumfield model MDR isolation relays are utilized to provide both non-1E to 1E and 1E to non-1E isolation as shown below:

- 1) Non-1E to 1E - receiving bay door #4323A (non-1E coil) permissive to equipment air lock isolation dampers HD-9450A and B (1E contact)
- 2) 1E to non-1E - equipment air lock isolation dampers HD-9450A and B (1E coil) permissive to receiving bay door #4323A (non-1E contact)

These two relays were purchased from General Electric.

words needed regarding testing
HCGS FSAR

4/84

- f. Startup Transient Monitoring System (STMS) - The qualification requirements of isolation devices, used by the STMS are described in Section 7.5.1.3.5.

NSSS:

are these the same as RAGS

The isolation devices used to electrically separate nonessential and essential circuits are pursuant to the guidelines of IEEE Standard 384. Both relay and optical isolation devices are employed. The optical isolators utilize a fiber-optic light pipe to electrically separate the input from the output. For example, an essential logic signal activates a light emitting diode, the light is transmitted through the light pipe to a photo switch and the switch changes state on receipt of the light signal and either blocks or transmits.

The relay isolation devices provide the same degree of separation and are used typically for control voltage separation applications, i.e., 120-Vac and 125 Vdc essential to nonessential and redundant essential circuits. The relays are mounted so that a metal barrier separates the coil from the contacts with a minimum distance of one inch between the coil and barrier and between the contact and barrier.

Summary of Purchase Specification:

- | a. RELAY | b. ISOLATOR |
|---|--|
| 1. Design Specification
a) MIL-R-19523
b) Contact Specification
c) Coil Specification
d) Insulation Specification
e) Design Life
f) Reliability | 1. Bill of Material |
| 2. Class 1E Safety Function
a) Functional Specification
b) Reliability | 2. Purchase part drawings 204B6186 and 204B6188 |
| 3. Qualification Testing
a) Ambient and Design Environments
b) Application Configuration | 3. Qualification Testing
a) Tested as a panel subassembly |

The optical isolator is comprised of semiconductors, resistors, and capacitors mounted on a printed circuit board. As designed, this device satisfies electrical isolation requirements.

Both isolation devices satisfy the concern of susceptibility to noise, shorts, surges, and faults. Adverse conditions affecting the coil or the semiconductor device cannot propagate through the isolation barrier (i.e., metal enclosure or fiber-optic light pipe). Conversely, adverse conditions affecting the contacts or receiving semiconductor cannot propagate through the isolation barrier and affect the coil or transmitting semiconductor. Therefore, essential systems or circuits are electrically isolated from nonessential and/or redundant systems or circuits.

Optical isolators were tested as part of the redundant reactivity control system (RRCS) panel qualification tests. The capability of the optical isolators to prevent propagation of a failure to other circuits was demonstrated as follows:

The isolators were exposed to a maximum switch-voltage of ~~140~~ 140-Vdc or 132-Vac, at approximately 200 mA, during the RRCS panel functional testing. Monitoring of other panel functions during these switching activities showed no detrimental effects on other circuitry. Test results are documented in GE files. An additional 5-kV breakdown-voltage test will be completed by September 1984.

480VAC surge for 1 second

QUESTION 421.17 (SECTIONS 7.2 AND 7.3)

Section 7.2.1.3.6.3 of the FSAR states that the structures containing RPS components, except for the turbine building, have been seismically qualified. Therefore, the turbine scram inputs are not guaranteed to function during a seismic event. The NRC staff recognizes that full conformance to IEEE 279 and associated standards is not possible in those plants where the turbine building is not a Seismic Category I structure. The acceptability of these limitations is subject to the implementation of a system which is as reliable as reasonably achievable. To assure adequate reliability, verify that the design up to the trip solenoids conforms to those Sections of IEEE 279 concerning single failure (Section 4.2), Quality (Section 4.3), Channel Integrity (Section 4.5 excluding seismic), Channel Independence (Section 4.6), and Testability (Section 4.10).

Further:

1. Verify that the design includes a highly reliable power source which assures availability of the system.
2. Using detailed drawings, describe the routing and separation for this trip circuitry from the sensor in the turbine building to the final actuation in the reactor trip system.
3. Discuss how the routing within the non-seismically qualified turbine building is such that the effects of credible faults or failures in the area on these circuits will not challenge the reactor trip system and/or degrade the reactor trip system performance. This should include a discussion of isolation devices.
4. Identify any other sensors or circuits used to provide input signals to the reactor protection system (reactor trip, engineered safety features and supporting features, RCIC) or perform a safety-related function which are located or routed through non-seismically qualified structures. Discuss the degree of conformance to IEEE 279 and associated standards.

RESPONSE

General - Conformance to the requirements of IEEE 279 for the reactor protection system is discussed in Section 7.2.2.2.1.

Specifically:

1. The RPS power supply is discussed in Section 8.3.1.5.

2. The cables for the main (turbine) stop valve closure and turbine control valve fast closure trip signals are run in protective conduit from the sensors to the RPS control panels in the main control complex. Each channel is run in its own conduit to maintain separation.

Drawings showing the cable routing for these trip signals have been previously submitted to the NRC and are listed on revised Table 1.7-1. The specific drawings of concern are as follows:

- a. E-1652-1, sheet 1
- b. E-1653-1
- c. E-1663-1
- d. E-1664-1, sheet 4
- e. E-1730-0
- f. E-1750-0, sheet 1
- g. E-1853-1, sheet 1
- h. E-1863-1, sheet 1
- i. E-1903-1, sheet 1

The following table identifies the sensor being referenced in parts (2) and (3) of this response:

<u>Sensor</u>	<u>Function</u>	<u>Location</u>
SB-ZS-N006A	Main (Turbine) Stop Valve Closure	Turbine Building
SB-ZS-N006B	Main (Turbine) Stop Valve Closure	Turbine Building
SB-ZS-N006C	Main (Turbine) Stop Valve Closure	Turbine Building
SB-ZS-N006D	Main (Turbine) Stop Valve Closure	Turbine Building
SB-ZS-N006E	Main (Turbine) Stop Valve Closure	Turbine Building
SB-ZS-N006F	Main (Turbine) Stop Valve Closure	Turbine Building
SB-ZS-N006G	Main (Turbine) Stop Valve Closure	Turbine Building
SB-ZS-N006H	Main (Turbine) Stop Valve Closure	Turbine Building
SB-PS-N005A	Turbine Control Valve Fast Closure	Turbine Building
SB-PS-N005B	Turbine Control Valve Fast Closure	Turbine Building
SB-PS-N005C	Turbine Control Valve Fast Closure	Turbine Building
SB-PS-N005D	Turbine Control Valve Fast Closure	Turbine Building

3. The routing of the cables is such that each channel is routed in its own conduit with a minimum separation of at least 1 inch between redundant channel conduits. The only credible failures that could challenge the system are: 1) a safe shutdown earthquake, 2) a turbine missile, or 3) a high energy line break. The expected failure mode caused by these events would be loss of the sensor due to loss of continuity (i.e., wire broken or cable severed), which would result in a reactor trip signal being generated.

If the trip sensor failed closed or shorted due to the fault, the high reactor pressure and high reactor power

trips, which are diverse (see Sections 7.2.1.1.4 and 7.2.1.1.5), would still function providing adequate reactor protection. Further, shorting of a single sensor would not prevent protective action by the other related sensors.

Each sensor input to the RPS logic is isolated from other sensor inputs by the use of interposing relays. This prevents a fault on a particular sensor cable causing an entire trip logic channel to be disabled.

4. The following table lists other RPS powered sensors located in non-seismically qualified structures:

<u>Sensor</u>	<u>Function</u>	<u>Location</u>
SB-PT-N052A	Main (Turbine) Stop Valve Closure and Turbine Control Valve Fast Closure Trips Bypass	Turbine Building
SB-PT-N052B	Main (Turbine) Stop Valve Closure and Turbine Control Valve Fast Closure Trips Bypass	Turbine Building
SB-PT-N052C	Main (Turbine) Stop Valve Closure and Turbine Control Valve Fast Closure Trips Bypass	Turbine Building
SB-PT-N052D	Main (Turbine) Stop Valve Closure and Turbine Control Valve Fast Closure Trips Bypass	Turbine Building
SM-PT-N076A	MSIV*-Low Steam Line Pressure Trip (PCRVICS)**	Turbine Building
SM-PT-N076B	MSIV*-Low Steam Line Pressure Trip (PCRVICS)**	Turbine Building
SM-PT-N076C	MSIV*-Low Steam Line Pressure Trip (PCRVICS)**	Turbine Building
SM-PT-N076D	MSIV*-Low Steam Line Pressure Trip (PCRVICS)**	Turbine Building
SM-PT-N075A	MSIV*-Low Condenser Vacuum Trip (PCRVICS)**	Turbine Building
SM-PT-N075B	MSIV*-Low Condenser Vacuum Trip (PCRVICS)**	Turbine Building
SM-PT-N075C	MSIV*-Low Condenser Vacuum Trip (PCRVICS)**	Turbine Building

SM-PT-N075D MSIV*-Low Condenser Vacuum Trip Turbine Building
(PCRVICS)**

- * MSIV = Main Steam Isolation Valve
** PCRVICS = Primary Containment and Reactor Vessel Isolation Control System

Conformance to the requirements of IEEE Standard 279 and associated standards are discussed in Sections 7.2.2.2.1 (RPS Sensors) and 7.3.2.1.2 (PCRVICS sensors).

5. The cables for the trip signals from the sensors listed in part (4) are run in protective conduit from the sensors to the RPS control panels in the main control complex. Each channel is routed in its own embedded conduit with a minimum separation of at least 1 inch between redundant channel conduits. The cable routing for these signals is shown on the following drawings (listed on revised Table 1.7-1):
- a. E-1804-1, sheet
 - b. E-1854-1
 - c. E-1865-1
 - d. E-1875-1

The expected failures, as described in part (3), paragraph (1), would cause loss of the sensor(s) due to loss of continuity (i.e., wire broken or cable severed). This condition would cause no adverse affects on the RPS if the plant was operating at power since the normal condition of sensors SB-PT-N052 (A-D) is deenergized. The open condition on the PCRVICS sensor (SM-PT-N075 (A-D) and SM-PT-N076 (A-D)) circuits could result in a reactor scram, due to main steam isolation valve closure, if an open existed on at least one sensor circuit in each of the two NSSS trip systems.

If the two RPS sensor circuits in the same RPS trip system (SB-PT-N052A and C or SB-PT-N052B and D) were to fail closed, due to the event, the main stop valve closure and turbine control valve fast closure scrams would be rendered inoperable. However, automatic reactor scram would still be provided by the diverse trip signal of reactor high pressure. Manual reactor scram is also available.

Should the event result in the worst case condition of a short circuit (failed closed) condition of all the PCRVICS sensor circuits (SM-PT-N075 (A-D) and SM-PT-N076 (A-D)) in

one or both NSSSS trip systems, automatic isolation would still be provided by the diverse trip signal of reactor vessel low water level (level 1). Manual isolation is also available.

Each sensor input to the RPS or NSSSS logic is isolated from other sensor inputs by the use of interposing relays. This prevents a fault on a particular sensor cable causing an entire trip logic channel to be disabled.

QUESTION 421.18 (SECTIONS 7.2 AND 7.3)

Provide a detailed discussion on the methodology used to establish the technical specification trip setpoints and allowable values for the Reactor Protection System (including Reactor Trip and Engineered Safety Feature channels) assumed to operate in the FSAR accident and transient analyses. Include the following information:

1. The trip setpoint and allowable value for the technical specifications.
2. The safety limits necessary to protect the integrity of the physical barriers which guard against uncontrolled release of radioactivity. The safety limits should be the limits established for licensing purposes, for example the technical specification safety limits on minimum critical power ratio (1.06), and reactor coolant system pressure (1325 psig).
3. The values assigned to each component of the combined channel error allowance (e.g., modeling uncertainties, analytical uncertainties, transient overshoot, response time, trip unit setting accuracy, test equipment accuracy, primary element accuracy, sensor drift, nominal and harsh environmental allowances, trip unit drift), the basis for these values, and the method used to sum the individual errors. Where zero is assumed for an error a justification that the error is negligible should be provided.
4. The margin (i.e., the difference between the safety limit and the setpoint less the combined channel error allowance).
5. Identify any trip for which the setpoint and allowable value in the technical specifications will be assigned best estimate values and for which you do not have an analysis of errors and/or uncertainties to confirm that the trip function will occur before the actual value of the measured parameter exceeds that assumed in the plant safety analysis. Provide justification for this nonanalytical approach.

RESPONSE

Public Service Electric and Gas is currently participating with a number of other utilities and the General Electric Company in generic discussions with the NRC staff concerning the methodology used to establish the technical specification trip setpoints and allowable values for the reactor protection system. All the issues raised by this question are being covered by these generic discussions. After they are concluded, the resolutions of the

generic issues will be applied to the HCGS, as appropriate; any HCGS-specific details the NRC may request will be supplied.

QUESTION 421.19 (SECTION 7.2, 7.3 & 7.4)

Identify each case where instrument sensors or transmitters supplying information to more than one protection channel are located in a common instrument line or connected to a common instrument tap. Verify that a single failure in a common instrument line or tap (such as break or blockage) cannot defeat required protection system redundancy.

RESPONSE

For non-NSSS, the ESF and EAS systems are designed such that no two protection channels of the same system have sensors which share a common instrument line or tap. Therefore, no single failure of an instrument line or tap can cause a loss of required protection system redundancy for any non-NSSS ESF or EAS system. A walkdown will be performed to verify that installation is in accordance with the design.

For NSSS, there are three cases where sensors share common instrument lines, two in the reactor protection system (RPS) and one in the nuclear steam supply shutoff system (NSSSS).

RPS

As shown on Figure 7.1-1, it is permissible for the RPS sensors A and B or C and D to share common instrument lines because of the use of one-out-of-two-twice, fail-safe logic and the manner of allocating the related relays to the RPS logic channels ensures that no single-line failure would prevent the RPS from functioning.

RPS Case 1 Four pressure transmitters (C71-N052 A through D) at the first stage of the main steam turbine provide interlocks for the scram trip functions of the main stop valve and the control valve and for the end-of-cycle recirculation pump trip (RPT). See Section 7.6.1.5. The scram trip and the RPT are prevented when the first-stage turbine pressure is below the setpoint.

In this case, an instrument line fault would not prevent the scram function because of the one-out-of-two-twice logic arrangement. An instrument line fault could disable one of the two RPT systems, but the other would function normally to trip both recirculation pumps.

Diversity for the scram trip functions of the main stop and control valves is provided by high reactor pressure sensed by four pressure transmitters. Redundancy for the RPT function is provided by the ATWS RPT initiated by the redundant reactivity control system. See Section 7.6.1.7.2.

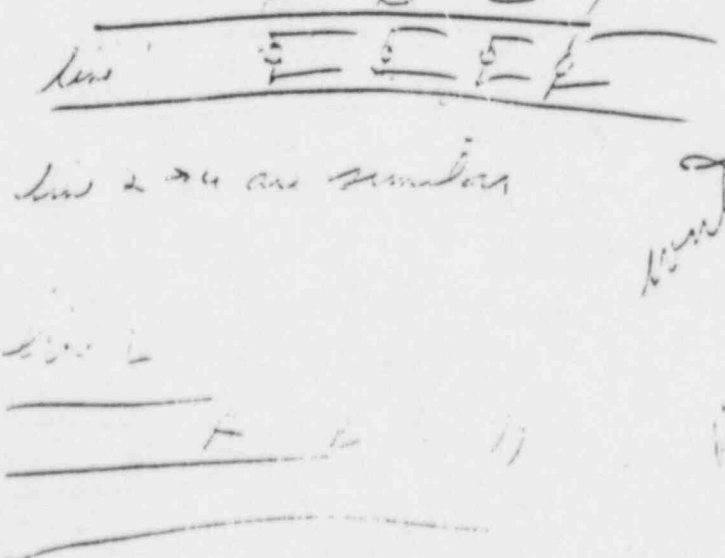
RPS Case 2. Eight differential-pressure transmitters, four for each recirculation pump, provide recirculation suction-flow input to the four flow units in the neutron monitoring system (NMS). These transmitters (B31-N014 A through D and B31-N024 A through D) and the associated flow-sensing units provide input to the APRM scram trip channels, biasing the trip setpoints according to the suction flow rate. Diversity for the APRM (NMS) scram trips is provided by high reactor pressure sensed by four pressure transmitters.

NSSSS

Sixteen differential-pressure transmitters, four in each main steam line, would identify a line break by sensing high flow. As for RPS, it is permissible for the A and B sensor and the C and D sensors to share instrument lines because of the one-out-of-two-twice, fail-safe logic arrangement. Redundancy and diversity for the isolation trip function of these transmitters (B21-N086 A through D, B21-N087 A through D, B21-N088 A through D, and B21-N089 A through D) is provided by four temperature sensors for each steam line that would sense high temperature in the main steam tunnel and by four pressure sensors that would sense low pressure at the input to the main stop valve.

For the remaining NSSS sensors, ESF and RPS systems are designed such that no two protective channels of the same system in separate divisions have sensors that share a common instrument line or tap. Therefore, no single failure of an instrument line or tap can cause a loss of required protection system redundancy for any NSSS, ESF, or RPS system.

L could have credibility (perhaps to wipe out all 4 - share same instrument wires)



write this in ESF. Instrument exist for steam flow monitoring diversity

in B CTS

QUESTION 421.21 (SECTIONS 7.2, 7.3, 7.4, 7.5)

Provide an evaluation of the effects of high temperatures on reference legs of water level measuring instruments subsequent to high-energy line breaks, including the potential for reference leg flashing/boil off, the indication/annunciation available to alert the control room operator of erroneously high vessel level indications resulting from high temperatures, and the effects on safety systems acuation (e.g., delays).

RESPONSE

ATTACHED

~~An evaluation of this issue is in progress. Based on the results of this analysis, proposed modifications, if any, to the HCGS level monitoring instrumentation design will be provided to the NRC when available. This is estimated to be about August, 1984.~~

PRELIMINARY

PRELIMINARY

An evaluation of the effects of high temperatures on reference legs of water level measuring instruments subsequent to High Energy Line Breaks (HELBS) must be divided into two parts: 1) the effects of temperature alone, and 2) the effects of flashing/boiloff.

High temperature effects (without flashing/boiloff)

An increase in the temperature of the dry well will cause a heat up of the fluid in the instrument sensing lines, contributing to sensor error. The HCGS instrument sensing line design reduces this error by routing the variable leg and the reference leg lines with equivalent elevation drops in the drywell. The only exceptions to this design are the upset range transmitters reference leg sensing lines. Physical configuration prevents equivalent routing of these lines. However these transmitters are used exclusively for indication and will not present any challenges to plant safety.

A high dry well temperature alarm is computer generated from the input of 0

PRELIMINARY

Class 1E transmitters. Class 1E temperature recorders located in the main control room provide a continuous display of drywell temperature.

Flashing / Boil off Effects.

The effect of flashing / boil off of the instrument line reference leg is to cause the level instruments to indicate erroneously high levels. The amount of error is directly related to the length of piping physically located within the drywell (i.e. amount of piping boiled dry).

HCGS has re-routed two channels of reactor pressure vessel (RPV) level instrumentation sensing lines to provide a maximum 1 ft elevation drop in the drywell. A worst case analysis of the effects of the boil off of that portion of the sensing line inside the drywell, indicates that the instruments using the re-routed lines will indicate a level 1 ft higher than actual. The 1 ft error will be taken into account in the emergency operating procedures.

PRELIMINARY

All transmitters used for post-accident monitoring use the re-routed lines and thus will provide an unambiguous display of level even after partial flashing of the reference legs.

Flashing / boiloff of the reference legs, that were not re-routed may cause a level 8 (LB), high RPV level trip of the high pressure coolant injection (HPCI) system. The effect of this trip depends on safety system response to various different high energy line break (HELBS) scenarios.

In response to a HELB of a large or intermediate sized line (see figure 15.9-43) the low pressure coolant injection (LPCI) and core spray are initiated by low water level 1 (L1) or high drywell pressure signals. For these postulated events, HPCI is assumed to be unavailable and thus a high level trip signal from any of the transmitters will not compromise the safe shutdown

of the plant.

PRELIMINARY

Two different response paths must be considered for a small break accident (SBA).

The first response path ~~considers~~ considers an SBA with HPCI available. The emergency core cooling system (ECCS) response to an SBA is outlined in FSAR chapter 15 in response to event 42 (Figure 15.9-93). Core spray and LPCI are initiated by high drywell pressure. HPCI is initiated on receipt of a low level 2 or high drywell pressure signals. HPCI continues to operate until the reactor vessel pressure is below the pressure at which LPCI or core spray operation can maintain core cooling. LPCI and core spray are designed to begin injecting water into the RPV when the differential pressure between the RPV and the suppression chamber is approximately 35 PSI or design requirements (see FSAR chapters 6.3 & 6.4).

PRELIMINARY

For an SBA the containment temperature is assumed to be a constant 340°F in the drywell. At this maximum drywell temperature flashing of the instrumentation line reference legs will occur when the reactor pressure is less than 118 PSIA. Flashing of the RPV level sensing line reference legs will cause a high level trip of the HPCI turbine. However, LPCI and Core Spray will already be injecting into the RPV and core cooling will be maintained.

The second response path considers a HPCI line SBA that incapacitates HPCI. Accident mitigation requires the actuation of the automatic depressurization system (ADS), LPCI, and core spray. LPCI and core spray are initiated on high drywell pressure or a LI signal. ADS is initiated by a HI and high drywell pressure or a HI ~~and~~ high drywell pressure, and a L3 permissive signal. ~~At~~ At the point flashing could occur the RPV pressure will be low enough that HPI will not be required, before that point level ~~signals~~ ^{signals/actuators} will remain accurate. Since HPCI is not used, a trip of the HPCI turbine will not compromise

PRELIMINARY

the safe shutdown of the plant.

^{HELS} ~~HELS~~ In the event of any ~~HELS~~ credible
~~HELS~~ inside containment, the capability
of the ECCS to mitigate the accident is
not compromised by high dry well temperature
or flashing of the RRV level instrumentation
line reference legs.

QUESTION 421.22 (SECTIONS 7.2, 7.3, 7.4, 7.5, 7.6, & 7.7)

The design of the instrumentation channels, logic and actuation devices of nuclear plant safety systems should include provisions for surveillance testing. Guidance is included in Reg. Guide 1.118 and IEEE Standard 338 for implementing the requirements of IEEE Standard 279, which requires in part that systems be designed to permit periodic testing during reactor operation.

Section 3.1.2.3.2 and 7.2.2.3.2 includes a brief description of the at-power testing capability of the reactor protection system. However, sufficient information has not been provided to determine the acceptability of the at-power testing capabilities provided in the Hope Creek design. Provide a detailed discussion with illustrations from applicable drawings on the at-power testing capability of the reactor trip system, engineered safety features actuation system and auxiliary supporting features, the actuation instrumentation for the reactor core isolation cooling system, and the instrumentation and controls that function to prevent accidents (i.e., high pressure/low pressure interlocks) or terminate transients (i.e., level 8 - turbine trip). This discussion should include the sensors, signal conditioning circuitry, voting logic, actuation devices and actuated components. Include in the discussion those design features that will initiate protection systems automatically, if required during testing, upon receipt of a valid initiation signal.

RESPONSE

As required by IEEE Standard 279, capability for at-power testing has been provided in the design of the HCGS safety systems. Conformance to the guidance specified in Regulatory Guide 1.118 and correspondingly, IEEE Standard 338, is as stated in Section 1.8.1.118.

The analysis portions of the various system descriptions in Chapter 7 for the safety-related systems referenced in the question describe the methods by which the safety system designs satisfy the testability requirements of IEEE Standard 279. The specific sections covering the testability of these systems are listed below:

RPS -	7.2.1.2
ECCS - HPCI	7.3.1.1.1(c)
- ADS	7.2.1.1.1.2(c)
- CORE SPRAY	7.3.1.1.1.3(c)
- RHR-LPCI	7.3.1.1.1.4(c)
PCRVICS	7.3.1.1.2(d)
RHR-CSCM	7.3.1.1.3(c)
RHR-SPCM	7.3.1.1.4(c)

PRELIMINARY

PCIS	7.3.1.1.5(j)
CACS - Supp. Chamber to	7.3.1.1.6.1(c)
Drywell Press. Relief	
- RB to Supp. Chamber	7.3.1.1.6.2(c)
Press. Relief Sys.	
- HOAS	7.3.1.1.6.3(c)
- CHRS	7.3.1.1.6.4(c)
MCRHIS	7.3.1.1.7(j)
MSIVSS	7.3.1.1.8(c)
FRVS	7.3.1.1.9
RBVIS	7.3.1.1.10(h)
EAS - SSWS	7.3.1.1.11.1(c)
- SACS	7.3.1.1.11.2(c)
PCIGS	7.3.1.1.1.11.4(c)
CACWS	7.3.1.1.1.11.5(c)
EACS - RBEAC	7.3.1.1.11.6.1(c)
- ABDA	7.3.1.1.11.6.2(c)
- ABCA	7.3.1.1.11.6.3(c)
- SWIS	7.3.1.1.11.6.4(c)
RCIC	7.4.1.1.3
SLC	7.4.1.2.3
RRCS	7.6.2.7.2(b)
	7.6.2.7.2(n)
	7.6.2.7.4.1

PRELIMINARY

Design drawings in the form of elementary diagrams, P&IDs, logic diagrams, instrument location drawings, and electrical drawings that describe this capability are listed in Tables 1.7-1, 1.7-2, and 1.7-3.

In response to the NRC's request for additional information during the meeting of January 11, 1984, review of the systems identified above, with the exception of the reactor protection system (RPS), reactor core isolation cooling (RCIC) system, standby liquid control (SLC) system, and redundant reactivity control system (RRCS) ~~will be~~^{was} performed. The review ~~will~~^{will be examined} determine the capability for the at-power testing of all circuits and sensors used in these systems. All actuated contacts and devices ~~will be~~^{are} considered. Any system, subsystem, or component that lacks the capability for at-power testing will be identified and a justification will be provided. The results will be documented in a revision to this response to be submitted by July 1984.

¶ The review did not identify any device- or circuit-bypassing methods, other than those specifically permitted by position C6 of Regulatory Guide 1.118, needed for ESF at-power testing. Built-in test jacks, which provide connections for plug-in test switches, built-in test switches, and normal operational equipment, provide this testing capability as shown on the system elementary diagrams. During testing, redundant channels or systems are available to provide the safety function.

INSERT A →

¶ PSE&G plans to conduct that at-power surveillance testing prescribed by the BWR 4 version of the NRC's Standard Technical Specifications. Amendment 5

INSERT A (QUESTION 421.22)

During the review, the at-power testability of an item was established if an affirmative response could be verified for the following three questions:

- a. Is the item sufficiently accessible to conduct the test during normal operation?
- b. Is the item sufficiently isolatable to permit its safety-related function to be verified or is a safety-related system or subsystem encompassing the item isolatable and testable?
- c. Does any bypassing method that must be used to accomplish the test conform to position C6 of Regulatory Guide 1.118?

except only

By these criteria, two items were judged to be untestable at power, the ADS SRVs, which would cause depressurization if tested, and the steam-tunnel temperature elements, which are inaccessible. The reliability and redundancy of the ADS instrumentation, logic, and actuation devices and the multiplicity of the SRVs adequately justify the lack of ADS at-power testability. Adequate element multiplicity and comparison tests of at-power output signals and electrical characteristics preclude the need for change-of-state testability of the steam-tunnel temperature elements.

DBJ:pes/107T
6/19/84

PRELIMINARY

HCGS FSAR

Diversity of reactor scram initiation due to main steam line high radiation is provided by reactor vessel low water level, reactor vessel high pressure, NMS, or manual trip signals.

7.2.1.1.10 Manual Scram

Scram can be initiated manually. There are four manual scram pushbutton switches, one for each of the four RPS trip logic channels. Actuating the manual scram switch for trip logic channel A1 or A2 will deenergize the "A" scram pilot valve solenoid for all control rods. Actuating the manual scram switch for trip logic channel B1 or B2 will deenergize the "B" scram pilot valve solenoid for all control rods. To manually initiate a reactor scram, the manual reactor scram switches from trip logic channels A1 or A2 and B1 or B2 must be actuated.

Manual reactor scram is diverse to all automatic reactor trip signals.

7.2.1.1.11 Reactor Mode Switch Manual Scram

Even though the action is not a safety function, reactor scram can be initiated by placing the mode switch in the "shutdown" position. The mode switch consists of four independent banks of contacts. A "shutdown" position contact from each of the four contact blocks provides an input to its corresponding RPS trip logic channel.

The reactor scram signal, initiated by placing the mode switch in "shutdown", is automatically bypassed after 10 seconds by a timer. This allows the RD hydraulic system valve lineup to be restored to normal, which must occur before the main control room operator can reset the RPS trip logic.

7.2.1.2 RPS System Testability

The RPS can be tested during reactor operation by the methods described in the following paragraphs.

The manual scram test involves depressing the manual scram switch for one trip logic channel, which deenergizes the actuators, opening contacts in the actuator output logic. After the first

HCGS FSAR

trip logic channel is reset, the second trip logic channel is tripped manually, and so forth for the four manual scram switches. The total test verifies the ability to deenergize all eight groups of scram pilot valve solenoids by using the manual reactor scram pushbutton switches. In addition to main control room and computer printout indications, pilot scram valve solenoid group indicator lights deenergize to verify that the actuator contacts have opened.

The calibration test of the NMS is accomplished by means of simulated inputs from calibration signal units. Calibration and test controls for the NMS are located in the main control room. Their physical location places them under direct physical control of the control room operator.

The single rod scram test verifies the capability of each rod to scram. It is accomplished by operating two toggle switches on the hydraulic control unit for the particular CRD. Timing traces can be made for each rod scrambled. Prior to the test, a physics review must be conducted to ensure that the rod pattern during scram testing will not create a rod of excessive reactivity worth.

The sensor test involves applying a test signal to each RPS sensor trip circuit, in turn, and observing that a logic trip results. This test also verifies the electrical independence of the trip logic channel circuitry. The test signals can be applied to the process type sensing instruments (pressure and differential pressure) through calibration taps. To gain access to the setting controls on each transmitter, a cover plate or sealing device must be removed. Only properly qualified plant personnel are granted access for the purpose of testing or calibration adjustments.

Proper transmitter operation will be evaluated during plant operation by comparison of the analog output meters on the individual channel trip units. Any deviation of a reading from the norm (other units) would indicate a malfunction.

Transmitter testing and calibration will be scheduled during plant outage.

The alarm typewriter provided with the process computer allows verification of the correct operation of many sensors during plant startup and shutdown. MSIV position and main stop valve

position can be checked in this manner. The verification provided on the alarm typewriter is not considered in the selection of test and calibration frequencies and is not required for plant safety.

The overall RPS response time is verified during preoperational testing from sensor trip to trip logic channel relay deenergization and actuator logic deenergization, and can be verified thereafter by similar testing.

7.2.1.3 Design Bases

The RPS is designed to provide timely protection against the onset and consequences of conditions that threaten the integrity of the fuel cladding and the RCPB. Chapter 15 identifies and evaluates events that jeopardize the fuel barrier and RCPB. The methods of assessing barrier damage and radioactive material releases, along with the methods by which abnormal events are identified, are presented in Chapter 15.

Variables monitored in order to provide protective actions to the RPS indicating the need for reactor scram are as follows:

- a. Neutron flux
- b. Reactor vessel high pressure
- c. Reactor vessel low water level
- d. Main stop valve closure
- e. Turbine control valve fast closure
- f. Main steam isolation valve closure
- g. Scram discharge volume high level
- h. Drywell high pressure

stop valve automatically resets and reopens, and the inboard injection valve reopens to initiate HPCI flow into the reactor vessel.

The HPCI turbine is functionally-controlled, as shown on Figure 7.3-1, HPCI FCD. The turbine governor limits the turbine speed and adjusts the turbine steam control valve so that design pump discharge flow rate is obtained. The flow signal used for automatic control of the turbine is derived from a differential pressure measurement across a flow element in the HPCI system pump discharge line.

Manual positioning of the flow controller is available to permit the control room operator to manually control the system following initiation.

The turbine is automatically shut down by closing the turbine trip and throttle valve if any of the following conditions are detected:

1. Turbine overspeed
2. High turbine exhaust pressure
3. High water level in the reactor vessel (L8)
4. Low pump suction pressure
5. Auto-isolation signal.

In the event that the main control room becomes uninhabitable, reactor vessel water level would normally be maintained by operation of the RCIC system from the remote shutdown panel (RSP). Should RCIC operation be disrupted due to some failure at the RSP, the HPCI system would still function to maintain reactor vessel water level by automatically cycling on and off at L2 and L8 respectively (see

- c. HPCI testability - The HPCI instrumentation and control system is capable of being tested during normal unit operation to verify the operability of each system component. Testing of the initiation transmitters, which are located outside the drywell, is accomplished by isolating each transmitter, one at a time, and applying a test pressure or differential pressure source. This verifies the operability of the transmitters. Trip units located in the control equipment room are calibrated individually by a

HCGS FSAR

calibration source with verification of setpoint by a digital readout located on the calibration module.

Adequate control room indications are provided. Testing for functional operability of the control logic relays can be accomplished by use of plug-in test jacks and switches in conjunction with single trip unit tests. Availability of other control equipment is verified during manual testing of the system with the HPCI pump discharge returning to the CST. Water is not injected into the reactor vessel by the HPCI system during periodic testing when the plant is at power.

With the following exceptions, test controls are arranged so that the system can automatically fulfill its safety functions.

1. -Flow controller in manual mode
2. Operator-initiated closure of either or both inboard/outboard isolation valves (an alarm sounds when the valves are in any position other than fully open)
3. Test plug inserted and test switch in position to interlock discharge valves (out-of-service annunciator alarms in the main control room to indicate HPCI in test mode).

7.3.1.1.1.2 Automatic Depressurization System

- a. ADS function - The ADS is designed to provide automatic depressurization of the reactor vessel by actuating five main steam safety/relief valves (SRVs). These valves vent steam to the suppressing pool in the event that the HPCI cannot maintain the reactor water level following a LOCA. The ADS reduces the reactor pressure so that flow from the low-pressure ECCS (HPCI and core spray systems) can inject into the reactor vessel in time to cool the core and maintain fuel cladding temperature within allowable limits.

RHR pump A or C or core spray pump A, and RHR pump A or C or core spray pump C.

After receipt of the initiation signals and after a delay provided by time delay relays, each of the two solenoid pilot air valves for all ADS valves are energized. This allows pneumatic pressure from each ADS valve accumulator to act on the air cylinder operator of its respective ADS valve. Each ADS trip system timer can be reset manually to delay system initiation. If reactor vessel water level is restored by the HPCI system prior to the end of the time delay, ADS initiation will be prevented.

The ADS trip system B actuates the A solenoid pilot valve on each ADS valve. Similarly, the ADS trip system D actuates the B solenoid pilot valve on each ADS valve. Actuation of either solenoid pilot valve causes the ADS valve to open to provide depressurization.

Manual initiation of the ADS trip systems or individual ADS valves is possible from the main control room. To manually initiate an ADS trip system, the control room operator must actuate two armed pushbutton switches, one for each of the logic channels associated with that trip system. Manual initiation bypasses the ADS trip system time delay and all the trip logic except that the requirement that a LPCI and/or core spray system be in operation must still be satisfied. The control room operator can manually open an individual ADS valve by depressing one of the two pushbutton switches (one for each pilot solenoid) that will bypass the trip logic and energize the associated pilot solenoid allowing air to open the valve.

- c. ADS testability - The ADS has two complete trip systems, one in trip system B and one in trip system D. Each trip system has two channels, both of which must operate to initiate ADS. One channel contains a time delay relay to delay ADS and give the HPCI system an opportunity to restore reactor vessel level. Four test jacks are provided, one for each channel. To prevent spurious actuation of ADS during testing, only one channel will be tested at a time. An annunciator is provided in the main control room to indicate that a test plug is inserted in both channels of a trip system

at the same time. Operation of the test plug switch and the permissive contacts will close one of the two series relay contacts in the ADS valve solenoid circuit. This will cause a panel light to extinguish indicating proper channel operation and also continuity of the solenoid electrical circuit. Testing of the other channel is similar.

Annunciation is provided in the main control room whenever a test plug is inserted into a test jack to indicate to the operator that the ADS is in a test status. Testing of the ADS does not interfere with automatic operation if required by an initiation signal.

7.3.1.1.1.3 Core Spray System

- a. Function - The core spray system is designed to deliver sufficient water spray to the reactor core in the event of a LOCA. The system includes two spray loops, each physically and electrically separated so that no single event will render both loops inoperable. Each loop includes two core spray pumps, appropriate valves, the piping to route water from the suppression pool to the reactor vessel, a spray sparger, and the necessary controls and instrumentation to start, operate, and test the system.
- b. Operation - The schematic arrangement of system mechanical equipment is shown on Figure 6.3-7, Core Spray P&ID. Component control logic is shown on Figure 7.3-5, Core Spray FCD. Instrument specifications are shown in Table 7.3-4 and Chapter 16. Instrument location drawings and electrical schematics are identified in Section 7.7. Operator information displays are shown on Figures 6.3-6 and 7.3-5.

There are four completely separate core spray control circuits, one for each pump, COOLERS B, C, and D. The control circuit for pump A also controls valves in loop A as required to direct pump discharge flow to the reactor vessel. In a similar manner, the controls for pump B also control loop B valves. The control circuits for pumps C and D control the pumps only.

outside of the primary containment for accessibility. Only the sensing lines penetrate the primary containment.

Drywell pressure is monitored by eight sensors mounted on instrument racks in the reactor building outside of the primary containment. Four pressure-sensing lines penetrate the primary containment to allow the sensors to monitor drywell pressure. Each drywell high pressure sensor provides an input to a trip unit located in the control equipment room.

Reactor pressure is monitored by eight pressure sensors mounted on racks in the reactor building. Two pressure-sensing lines penetrate the primary containment to allow the sensors to monitor reactor vessel pressure. Each pressure sensor provides an input to a trip unit located in the control equipment room.

- c. Core spray system testability - The core spray system is capable of being tested during normal operation. Drywell pressure and low water level initiation transmitters are individually isolated and subjected to a test pressure.

This verifies the operability of the transmitter as well as the calibration range. The trip units mounted in the control equipment room are calibrated individually by a calibration source with verification of setpoint by a digital readout located on the calibration module. Other control equipment is functionally tested during manual testing of each loop. Adequate indications in the form of panel indicating lights, annunciators, and printed computer output are provided in the main control room.

7.3.1.1.1.4 RHR - Low Pressure Coolant Injection Mode

- a. LPCI function - LPCI is an operating mode of the RHR system. The purpose of the LPCI mode is to provide low pressure reactor vessel coolant makeup following a LOCA when the vessel has been depressurized and vessel water level can not be maintained by the HPCI system.

The four valves on the RHR pump suction from the suppression pool have their control switches keylocked in the "open" position, and thus require no automatic open signal for system initiation.

The two series service water cross-tie valves have their control switches keylocked in the close position, and thus require no automatic close signal for system initiation.

The two series containment spray valves, the two series RHR heat exchanger vent valves, and the RHR shutdown cooling mode suction valves are all normally closed and thus require no automatic close signal for system initiation.

The LPCI pump motors and injection valves are provided with manual override controls. These controls permit the operator to manually control the system subsequent to automatic initiation.

- c. LPCI testability - The LPCI is capable of being tested during normal operation. Drywell high pressure and reactor vessel low water level initiation transmitters are individually isolated and subjected to a test pressure. This verifies the operability of the transmitters as well as the calibration range. Trip units mounted in control equipment room panels are calibrated individually by introducing a calibration source and verifying the setpoint by a digital readout located on the calibration module. Other control equipment is functionally tested during manual testing of each loop. Adequate indications in the form of panel indicating lights and annunciators are provided in the main control room.

7.3.1.1.2

Primary Containment and Reactor Vessel Isolation Control Systems

- a. PCRVICES function - PCRVICES provides the means to automatically isolate the primary containment and reactor vessel by closing the inboard and outboard isolation valves of the main steam lines and of the process lines of other systems.

~~No diversity is provided for the main condenser low vacuum trip.~~

- d. PCRVICS testability - The operation of each subsystem up to and including the actuators can be independently verified during normal plant operation. Instrument setpoints are tested by simulated signals of sufficient magnitude to verify the alarm points.

~~7.3.1.1.2 RHR Containment Spray Cooling Mode~~

- a. Containment spray cooling mode function - The containment spray cooling mode is an operating mode of the RHR system. It is designed to condense steam in the suppression chamber air volume and/or the drywell atmosphere following a LOCA. See Section 6.2.2 and Table 7.3-7.
- b. Containment spray cooling mode operation - The containment spray cooling mode is initiated by the control room operator by diverting LPCI flow to either the suppression chamber or the drywell by opening the containment spray valves or by closing the LPCI injection valve and opening the selected containment spray valves. Containment spray will operate upon a permissive signal from the high drywell pressure interlock. The following conditions must exist before the operator can initiate a containment spray cooling loop:
1. The LPCI initiation signal (either manual or automatically from a LOCA signal) must exist.
 2. Drywell high pressure is monitored by two redundant pressure transmitters. One of the two must indicate high pressure. See Table 7.3-7.
 3. The operator must close the LPCI injection valve.

The LPCI mode of operation can be overridden; but only by conscious operator action; that is, several remote manual switches must be operated to bring valves into proper alignment for operation in other modes. The LPCI mode cannot be overridden by any automatic action. Once the LPCI mode is in operation, operator action is required to place the RHR system in any other condition.

In the event that the main control room becomes uninhabitable, the containment spray cooling mode can

also be initiated from the remote shutdown panel (RSP) using RHR loop B (see Section 7.4.1.4). Operation from the RSP is totally operator controlled and is not dependent on the existence of a LPCS initiation signal or a high drywell pressure signal. These signals are disabled for RHR loop B when the Channel B RSP transfer switch is placed in the "Emergency" position.

- c. Containment spray cooling mode testability - Two full-flow test lines are provided to route RHR pump discharge flow to the suppression pool. Flow is capable of being diverted into these test lines to test operations of pumps and major parts of control systems during reactor operation. Other control equipment is functionally tested during manual testing of each loop. Adequate indication in the form of panel indicating lights and annunciators are provided in the main control room.

7.3.1.1.4 RHR Suppression Pool Cooling Mode

- a. RHR suppression pool cooling mode function - The SPCM is an operating mode of the RHR system. It is designed to prevent suppression pool water temperature from exceeding predetermined limits following a reactor blowdown by the ADS or SRVs.
- b. RHR SPCM operation - The RHR-SPCM is initiated by the control room operator either during normal plant operation or following a LOCA, when the suppression pool water temperature monitoring system, as discussed in Section 7.3, indicates that suppression pool water temperature may exceed a predetermined limit.

During normal plant operation, the operator initiates the RHR SPCM as follows:

1. The RHR pump (A or B) is started. The SACS flow is established to the RHR heat exchanger.
2. The appropriate RHR test return line valve is opened.

3. The RHR heat exchanger inlet and outlet valves are opened. The heat exchanger bypass valves are throttled as necessary.

Subsequent to a LOCA, the operator initiates the RHR-SPCM as follows:

1. Once reactor vessel water level has been restored, the LPCI flow must be terminated by closing the LPCI injection valve. Closing the injection valve causes the LOCA initiation logic to be overridden and allows operator control of the system.
2. The RHR test return line valve control logic also has LOCA signal override provisions. This allows the operator to open the valve.
3. The RHR heat exchanger inlet and outlet valves are opened. The heat exchanger bypass valve after a time delay and the test return valve are throttled as necessary. Arrangement of system equipment is shown on Figure 5.4-13, RHR P ID. Component control logic is shown on Figure 7.3-7, RHR FCD. See Table 7.3-8 for instrumentation specifications.

In the event that the main control room becomes uninhabitable, RHR-SPCM loop B can also be initiated from the remote shutdown panel (RSP) (see Section 7.4.1.4). Operation from the RSP is totally operator controlled and all RHR loop B automatic initiation signals are disabled when the Channel B RSP transfer switch is placed in the "Emergency" position.

The RHR-SPCM can be manually initiated locally on RHR loop A as a backup to operation of RHR loop B from the RSP. The RHR loop A local pump and valve controls are identified on Table 7.4-3.

- c. RHR-SPCM testability - The RHR-SPCM is capable of being tested during normal operation. Testing for functional operability can be accomplished by manual testing of each loop. Adequate indication in the form of panel

indicator lights and annunciators is provided in the main control room.

7.3.1.1.5 Primary Containment Isolation System

a. PCIS function - The PCIS is designed to ensure primary containment integrity by initiating closure of non-NSSS primary containment isolation valves following a design basis accident (DBA). Each channel of the PCIS is actuated by the following input signals as shown on Figure 7.3-26:

1. Reactor vessel water level low (L2) (For definition of reactor vessel water level trip functions, see Figure 5.1-4)
2. Reactor vessel water level low (L1)
3. Drywell pressure high
4. Reactor building radiation high-high
5. Refueling floor area radiation high-high
6. Manual initiation

A block diagram of the PCIS is shown on Figure 7.3-13. A specific identification of primary containment isolation is provided in Section 6.2.4.

b. PCIS operation - The PCIS initiates isolation of the following lines penetrating the primary containment:

1. Reactor auxiliaries cooling system (RACS) cooling water supply and return
2. RCPE leak detection system gas sampling and return

In addition to manual initiation, the following initiating signals of reactor low level (L2 and L1), drywell high pressure, reactor building high-high radiation, and refueling floor area high-high radiation are provided to each PCIS initiation channel.

- h. PCIS actuated devices - Table 6.2-16 lists all valves actuated by the PCIS. Figure 6.3-26 shows the PCIS initiation logic and isolation signal fanout.
- i. PCIS separation - Separation is maintained between redundant portions of the PCIS by using physical distance and electrical separation barriers in accordance with the requirements of Regulatory Guide 1.73. The redundant portions of the PCIS are assigned to separate Class 1E electrical channels.
- j. PCIS testability - The three systems providing inputs to the PCIS have testability as described in the following sections:
 - 1. PCRVICES - refer to Section 7.3.1.1.2
 - 2. RMS - refer to Section 11.5.2.1
 - 3. Core spray controls and instrumentation - refer to Section 7.3.1.1.1.3.

The PCIS controls and instrumentation are capable of being tested, from the sensor through actuated devices by the overlap method during normal power operation. The sensors (transmitters) can be valved out of service, one at a time, and functionally tested using an appropriate test source. This test will verify proper circuit operation from the sensor to the input of the actuation device.

The PCRVICES and core spray trip units can be tested by providing an input signal from a calibration device. This test will verify circuit function from the channel trip unit to the input of the actuation device.

Actuated devices can be individually tested from the main control room by manual operation of control switches.

During scheduled plant outages, each PCIS actuation channel and its associated actuated devices can be functionally tested as follows:

- (a) Operation of the PCIS manual initiation switch
- (b) Simultaneous insertion of test signals into the PCRVICS and core spray systems to simulate conditions of reactor vessel water level low (L2) or drywell pressure high
- (c) Manual actuation of the reactor building high-high radiation trips at the local radiation processors (LRPs)
- (d) Manual actuation of the refueling floor area high-high radiation trips at the LRPs (tests the RBVIS function)
- (e) Insertion of test signals into the core spray system to simulate LOCA conditions of reactor vessel water level low (L1) and/or drywell pressure high (tests the LOCA (L1) isolation function)
- (f) Operation of the core spray manual initiation switch.

These tests are performed during plant outages since actual isolation at the system level will occur.

- k. PCIS environmental considerations - The instrumentation and controls of the PCIS are qualified as Class 1E equipment. The sensors are mounted locally or on local instrument racks. The actuation circuitry is located in instrumentation panels in the control equipment room and the main control room. All equipment is qualified.

- c. SCDPR system testability - Each relief valve in the SCDPR system can be tested during normal plant operation from the main control room. Each relief valve has a test pushbutton switch and a solenoid valve associated with it. Depressing the test pushbutton switch energizes the solenoid valve which directs gas from the PCIGS to open the vacuum relief valve. When the test pushbutton is released, the solenoid valve deenergizes, and the relief valve returns to normal operation depending on the primary containment conditions. This test verifies the proper operation of the vacuum relief valve, status lights, and computer input.

7.3.1.1.6.2 Reactor Building to Suppression Chamber Pressure Relief System

- a. Reactor building to suppression chamber pressure relief (RBSCPR) function - The purpose of the RBSCPR system is to limit the differential pressure between the reactor building and the suppression chamber. See Section 6.2.5 for a description of the mechanical system equipment.
- b. RBSCPR operation - The RBSCPR system consists of two vacuum relief assemblies, each providing a ventilation path from the reactor building to the suppression chamber. Each RBSCPR system assembly consists of a check valve and a normally closed butterfly valve.

A differential pressure transmitter senses the pressure differential between the reactor building and the suppression chamber. When this differential reaches a specified limit, a pressure differential switch provides an input signal to a solenoid valve associated with the butterfly valve, which energizes and directs gas from the PCIGS to open the butterfly valve. This allows the reactor building atmosphere to enter the suppression chamber and equalize the pressure difference. The suppression chamber to drywell pressure differential is equalized through the SCDPR system discussed in Section 7.3.1.1.6.1. When the differential pressure is reduced to a specified level, the solenoid valve deenergizes and the butterfly valve returns to the closed position. The check valve prevents the suppression chamber atmosphere from venting into the reactor building should the butterfly

valve fail to close after the differential has been reduced. Valve position switch contacts are monitored on each butterfly valve and each check valve providing fully open and fully closed valve position signals to illuminate valve position indicating lights in the main control room. An input is provided to the computer whenever the butterfly valve is not 100% closed.

- c. RBSCPR system testability - The RBSCPR system controls and instrumentation are capable of being tested from sensors through actuated devices during normal power operation. Each sensor (transmitter) can be valved out of service and functionally tested using an appropriate test source. This test will verify proper circuit operation from the sensor input through the actuated device.

The calibration of the alarm units (differential pressure switches) can be checked from the appropriate cabinet in the control equipment room without initiating operation of the actuated device. When an alarm unit is placed "in test" an output is provided to illuminate an indicating light in the main control room to advise the control room operator of the "in test" status. This indicating light is automatically extinguished when the alarm unit is placed back in operation. See Figure 7.3-14.

Each check valve and butterfly valve in the RBSCPR system can be individually tested from the main control room by the operation of an associated pushbutton test switch. When the pushbutton test switch is depressed, the associated solenoid valve of the valve being tested is energized and directs gas from the PCIGS to open the butterfly or check valve. When the pushbutton test switch is released, the solenoid valve deenergizes and the valve under test returns to its normal operating status. Satisfactory operation is determined by observation of the expected valve position indicating light patterns during the test.

7.3.1.1.6.3 Hydrogen/Oxygen Analyzer System (HOAS)

- a. HOAS function - The purpose of the HOAS is to measure the percentage of hydrogen and oxygen in the primary

Each HOA has a subpanel mounted in a main control room panel section and a remote control cabinet. Control switches and status indicating lights are provided to allow HOA calibration and operation from either location. Percent oxygen and percent hydrogen are indicated on meters at each location for use during calibration and operation. Percent oxygen is repeated on indicating meters located near the drywell equipment hatches. However, the HOA sample and return line containment isolation valves cannot be operated from the remote control cabinet.

A three-pen recorder for each HOA allows a permanent record to be maintained. One pen identifies which sample stream the HOA is analyzing, one pen records the percent oxygen in the sample, and one pen records the percent hydrogen in the sample. The recorder can be turned "on/off" from the remote control cabinet and/or the main control room. Signals from each of the inboard containment isolation valves in the HOA sample lines are interlocked in logic which prevents the sample stream identifying pen from recording an erroneous stream identification should two or more sample lines be open. See Figure 7.3-14.

The following system failures are annunciated at the local control panel and are repeated in the form of a common system trouble alarm in the main control room:

1. HOA pump enclosure pressure high/low
2. HOA calibration and reagent gas pressure low,
3. HOA hot box temperature high/low,
4. HOA cell failure.

The HOA common system trouble alarm in the main control room is also annunciated whenever predetermined levels of hydrogen or oxygen are detected.

- c. HOAS testability - Each HOA in the HOAS is capable of being tested during normal plant operation. With the

HOA warmed up (a minimum six hour warmup is required prior to any testing or calibration) and operating in the standby mode, system flow rates can be checked by placing the main power switch (located on the analyzer sub-panel in the main control room) in the "analyze" position and observing the flow meters on the remote analyzer panel. Needle valves are provided for adjusting the system flows as necessary.

Once proper flow rates are established, the operator can check zero and span calibration by operation of the function selector switch (located on the analyzer sub-panel in the main control room) first to the "zero" position and then to the "span" position. In the "zero" position, the operator should observe 0% readings on the percent H₂ and O₂ indicators located on the analyzer sub-panel in the main control room and on the remote analyzer panel. In the "span" position, the operator should observe readings on the percent H₂ and O₂ indicators corresponding to the calibration gas percentage supplied to the analyzer. Calibration gases of 5% H₂ in N₂ and 5% O₂ in N₂ are provided for initial calibration of the HOAs and for verifying calibration during system operation.

A heated compartment, "hot box", is provided in each HOA to maintain the temperatures of the incoming sample and analyzer cells sufficiently high to prevent condensation of the gases in the system. Proper hot box operation can be verified by removing the hot box cover and measuring the internal temperature with a suitable temperature monitoring device (i.e., calibrated pyrometer).

Proper operation of the HOA sample pump (located in the remote analyzer panel) can be verified by attaching a pressure gauge to the test tee provided at the pump discharge and observing the discharge pressure with the pump running.

7.3.1.1.6.4 Containment Hydrogen Recombination System (CHRS)

- a. Containment hydrogen recombination system (CHRS) function - The function of the CHRS is to reduce the hydrogen concentration of the primary containment atmosphere following a LOCA. See section 6.2.5 for the

Each hydrogen recombiner has a main control panel located in the control room. Control switches, process indicators, and status indicating lights are provided on the control panel, allowing hydrogen recombiner operation from the main control room. The CHRS system is designed for manual initiation, operation, and shutdown from the main control room. However, the hydrogen recombiners are tripped automatically by any of the following conditions:

1. Gas inlet pressure high
2. Blower inlet temperature high
3. Heater wall temperature high-high
4. Reaction chamber shell temperature high-high
5. Return gas temperature high.

An alarm is annunciated (audible and visual) at the CHRS control panel whenever any of the above listed trip conditions or the following non-trip conditions exist during CHRS operation:

1. Reaction chamber gas temperature low
2. Through gas flow low.

Any alarm at the CHRS control panel will also annunciate a common alarm on the main annunciator panel in the main control room.

- c. CHRS testability - The CHRS is capable of being tested during normal plant operations. Control and instrumentation is tested along with the remainder of components in an integrated system test.

- f. MCRHIS bypasses and interlocks - The handswitch of each fan in the CREF system and the main control room HVAC system, when in the "lockout" position, provides inputs to a control room out-of-service display. The isolation system is interlocked with the CREF system to maintain ventilation within the main control room during isolation. The CRS fans are interlocked with the CRRA fans and the chilled water pumps.
- g. MCRHIS redundancy and diversity - To maintain the redundancy of the mechanical equipment, controls and instrumentation are provided on a one-to-one basis with the mechanical equipment they serve. Diversity is not applicable.
- h. MCRHIS actuated devices - The MCRHIS does not actuate any other devices.
- i. MCRHIS separation - The controls, instrumentation, and power supplies of the MCRHIS are physically separated and electrically independent for each of the redundant trip channels. See Section 8.1.4.14 for a discussion of the electrical system separation.
- j. MCRHIS testability - The operability of the isolation initiating circuits of the MCRHIS may be verified by tripping the individual radiation monitor circuits or by manually initiating the channels using handswitches located in the main control room.

Operability of the initiating circuits of the CREF system may be verified by putting each CREF fan in the "auto" mode and tripping the respective isolation channel.

Operability of the initiating circuits of the main control room HVAC fans may be verified by alternately placing each fan in the "auto" mode while the other fan of the pair is shut down. In addition, all fans may be manually tested by handswitches located in the main control room.

- k. MCRHIS environmental consideration - The I&S for the MCRHIS are located in the main control complex. The

A flow element measures the air flow through each subsystem and provides a signal to a flow switch and a timer. Whenever the flow exceeds the setpoint, the timer is started. The timer continues to run as long as the flow is higher than the setpoint. If the timer should run out, the pressure differential control valve will be signaled to close. Thus, gross leakage from the system is prevented. In addition low pressure in any main steam line is alarmed in the main control room. The system would then be manually secured by the control room operator. Each main steam line is capable of being isolated separately.

The inboard and the outboard MSIVSSs are actuated separately. The outboard subsystem is initiated after the inboard subsystem has been started. Either the inboard or the outboard subsystem can perform the entire sealing control function.

Both the inboard and outboard subsystems are provided with RPV and main steam line pressure interlocks to prevent inadvertent system initiation during normal reactor power operation. See Figure 7.3-17.

Controls and indications are located in the main control room. The sensors are located outside the primary containment. Instrument specifications are listed in Table 7.3-11.

The mechanical system description and performance evaluation in Sections 6.7.2 and 6.7.3 provide a detailed discussion of the operator information and of the necessary action to complete the system's function objectives.

- c. MSIVSS testability - The MSIVSS is fully testable during normal power operation by the overlap method. Full system functional testing will be performed during scheduled outage periods.

During normal plant operation, the MSIVSS is tested by introducing a simulated RPV pressure signal from the analog logic cabinet in the main control room in place of the pressure transmitter output from the RPV. This allows actuation of the pressure differential control

HCGS FSAR

valve, admitting gas from the PCIGS gas receiver. Gas passes through the flow elements and is routed through a test line to the PCIGS gas compressor drywell suction line. This test will verify the operability of the modulating pressure control valve. The seal gas supply shutoff valves and MSIV seal gas supply isolation valves are closed during this test. The inboard and the outboard subsystems are tested separately.

Instrument setpoints are tested by simulated signals of sufficient magnitude to verify accuracy.

Placing an alarm or switch unit in test causes an interlock-in-test status light to be illuminated in the main control room, advising the control room operator of the abnormal condition. Placing the alarm or switch unit back in service extinguishes the interlock-in-test status indicating light.

The motor-operated inboard and outboard MSIV seal gas supply isolation valves can be tested during normal power operation. However, this testing requires bypassing of a protective interlock (main steam line high pressure) and requires that the seal gas supply shutoff valve for the subsystem under test be closed. An interlock bypass pushbutton switch has been provided in the main control room for each inboard and outboard MSIV seal gas supply isolation valve. Depressing this switch accomplishes two functions:

1. Enables the protective interlock bypass which allows the control room operator to open the valve
2. Illuminates an indicating light to advise the control room operator of the bypassed condition.

The control room operator can reestablish the protective interlock by depressing either the "close" or "reset" pushbutton for the isolation valve under test. This action also extinguishes the bypass status indicating lamp. See Figure 7.3-17.

d. ~~MSIVSS power sources - The instrumentation and controls of the MSIVSS are powered from Class 1E ac power~~

4. Reactor building/outside differential pressure.

- e. FRVS bypasses and interlocks - The FRVS is interlocked with the reactor building isolation system.
- f. FRVS redundancy and diversity - Controls and instrumentation are provided on a one-to-one basis with the mechanical equipment they serve to maintain the redundancy of the equipment. Diversity is not applicable.
- g. FRVS actuated devices - No additional devices or systems are actuated by the FRVS.
- h. FRVS separation - Separation is maintained for the redundant controls, instrumentation, and power sources of the FRVS by physical barriers and spatial distance. See Section 8.1.4.14 for a discussion of electrical system separation.

- i. FRVS testability - The FRVS is fully testable during normal power operation. All FRVS recirculation and vent system fans can be manually started from the main control room or the entire system can be functionally tested by manually actuating the refueling area radiation monitoring system high-high radiation trips. See Figures 7.3-18 and 7.3-19.

j. FRVS environmental consideration - All instrumentation and controls are selected to meet the normal, accident, and post-accident conditions of pressure, humidity, temperature, radiation, and vibrations expected at their respective locations. See Section 3.11.

- k. FRVS setpoints - For setpoints, see Chapter 16, Technical Specifications.

7.3.1.1.10 Reactor Building Ventilation Isolation System

- a. RBVIS function - The RBVIS, a subsystem of the FCIS, isolates the reactor building following a LOCA or refueling area accident so that potentially radioactive

The PCIS is discussed in Section 7.3.1.1.5. PCIS initiation logic and isolation signal fanout are shown on Figure 7.3-26.

- e. RBVIS redundancy and diversity - See the discussion of redundancy and diversity for the PCIS in Section 7.3.1.1.5.
- f. RBVIS actuated devices - The RBVIS is actuated by the RBVIS.
- g. RBVIS separation - The controls, instruments, and power supplies of the isolation system are physically separated and electrically independent for each of the redundant trip channels. See Section 1.4.14 for a discussion of electrical system separation. See the discussion of separation for the PCIS in Section 7.3.1.1.5.

- h. RBVIS testability - The RBVIS is fully testable during normal power operation. The isolation dampers operated by the RBVIS can be individually tested from the main control room, or the entire system can be functionally tested by manually actuating the reactor building radiation monitoring system high-high radiation trips. See Figures 7.3-18 and 7.3-19.

- i. RBVIS environmental considerations - The controls and instrumentation for the RBVIS are located in the reactor building and the main control complex. The environmental considerations for these areas are listed in Table 3.11.

- j. RBVIS setpoints - See Chapter 16, Technical Specifications, for setpoints.

In the event that the main control room becomes uninhabitable, SSWS loop B can also be initiated from the remote shutdown panel (RSP) (see Section 7.4.1.4). Operation from the RSP is totally operator controlled and all SSWS loop B automatic initiation signals are disabled when the Channel B RSP transfer switch is placed in the "Emergency" position.

SSWS loop A can be manually initiated locally as a backup to operation of SSWS loop B from the RSP. SSWS loop A local pump and valve controls are identified on Table 7.4-3.

- c. SSWS testability - The SSWS is fully testable during normal power operation. System redundancy is such that an entire loop can be placed out of service for testing without disrupting normal plant operation. All safety-related alarm or switch units are supplied with on line testability and when placed in test, signals are provided to the main control room to indicate the in-test status and, where applicable, that a protective interlock has been bypassed. All system setpoints can be checked by insertion of simulated signals of sufficient magnitude to verify accuracy. All SSW pump/valve interlocks can be verified by normal plant operations such as starting up and securing the system.

7.3.1.1.11.2 Safety Auxiliaries Cooling System

SACS function - The purpose of the SACS system is to provide a heat sink for the ESF equipment by circulating demineralized water in a closed loop system. The system is designed with sufficient heat removal capacity to bring the nuclear boiler to cold shutdown condition in the required amount of time. The system also provides for protection of the SACS system from a pipe break in the turbine auxiliaries cooling system (TACS).

- b. SACS operation. Schematic arrangements of system mechanical equipment are shown on Figure 9.2-4. SACS control logic is shown on Figure 7.3-11. Instrument specifications are listed in Table 7.3-13 and Chapter 16, Technical Specifications. Instrument location drawings and electrical schematics are identified in Section 7.7.

In the event that the main control room becomes uninhabitable, SACS loop B can also be initiated from the remote shutdown panel (RSP) (see Section 7.4.1.4). Operation from the RSP is totally operator controlled and all SACS loop B automatic initiation signals are disabled when the Channel B RSP transfer switch is placed in the "Emergency" position.

SACS loop A can be manually initiated locally as a backup to operation of SACS loop B from the RSP. SACS loop A local pump and valve controls are identified on Table 4-3.

- c. SACS testability - The SACS is fully testable during normal power operation. System redundancy is such that

an entire loop can be placed out of service for testing without disrupting normal plant operation. All safety-related alarm or switch units are supplied with on-line testability and when placed in test, signals are provided to the main control room to indicate the in-test status and, where applicable, that a protective interlock has been bypassed. All system setpoints can be checked by insertion of simulated signals of sufficient magnitude to verify accuracy. Total system functional operation can be verified by shifting the system lineup as necessary to observe proper operation of all SACS components.

7.3.1.1.11.3 Class 1E Power Systems

Refer to Chapter 8 for a complete discussion of ESF Class 1E power systems.

7.3.1.1.11.4 Primary Containment Instrument Gas System

- a. PCIGS function - The normal function of the PCIGS is to provide compressed gas from the primary containment to operate pneumatic devices. In the event of a DBA, the PCIGS will provide makeup instrument gas from outside the drywell to the ADS valve actuators inside the primary containment and supply instrument gas to the MSIV seal system outside the primary containment. Many of the normal gas users will be isolated. See Section 9.3.6 for further information.
- b. PCIGS operation - Manual control of the PCIGS compressors is either from the main control room or from a panel located adjacent to the PCIGS compressors. Control of all PCIGS valves is from the main control room at all times. PCIGS system control logic is shown on Figure 7.3-22.
 1. Main control room operation of the PCIGS compressors is by means of a switch having the following functions:
 - (a) "Remote" - The "start" switch on the local panel is interlocked with this switch so that

HCGS FSAR

- (d) PCIGS supply header cross-connecting valves
- (e) PCIGS supply to suppression chamber vacuum relief valves inboard and outboard containment isolation valves
- (f) PCIGS supply to traversing in-core probe (TIP) purge equipment containment isolation valve
- (g) PCIGS to CACS emergency pneumatic supply valves.

An isolation override capability has been provided for the PCIGS compressor start circuitry and the PCIGS instrument gas inboard and outboard containment isolation valves to allow restarting the system following primary containment isolation to enable the system to supply sealing gas to the MSIVSS and instrument gas to the SRVs. All other PCIGS valves that were closed by the primary containment isolation signal remain closed and cannot be reopened until the isolation initiation signals have cleared and the initiation logic has been reset.

The PCIGS compressor suction is manually shifted to the reactor building atmosphere following primary containment isolation and both PCIGS trains are operated in the auto-lead mode.

Any condition of motor overload or control power failure on any PCIGS valve is alarmed individually and annunciated by a common system trouble alarm in the main control room. Any alarm condition at the remote control panel is annunciated in the main control room by a remote control panel trouble alarm.

- c. PCIGS testability - The PCIGS is fully testable during normal operation. Each PCIGS compressor train is capable of supplying the entire PCIGS load requirement. This allows for securing one entire train for maintenance. All system setpoints can be checked by

inserting simulated signals of sufficient magnitude to verify accuracy. PCIGS valve and compressor train functional operation can be verified by startup and normal operation of the system.

7.3.1.11.5 Control Area Chilled Water System - Instrument and Control

- a. CACWS function - The CACWS provides a means of cooling the air supplied to parts of the auxiliary control area. The primary function of CACWS is to provide chilled water to the main control room and control equipment room air conditioning units. The CACWS also provides chilled water to the switchgear room and the reactor building SACS room cooling units. A separate subsystem, the safety-related panel room chilled water system, provides chilled water to the Class 1E panel room and technical support center (TSC) air conditioning units, and the remote shutdown panel (RSP) room cooling units.
- b. CACWS operation - The power for the instruments and controls associated with the CACWS is supplied from the Class 1E power system. See Chapter 8 for a description of the electrical systems.

Equipment design is described in Section 9.2.7.

The CACWS is normally controlled from the main control room. However, the CACWS chillers can be placed in an auto-start condition from their respective remote control panel when a permissive signal from the main control room is present. One chilled circulating water pump and its associated chiller for each CACWS subsystem are started manually from the main control room to correspond with the cooling coils intended for use. The other chilled water circulating pump and chiller for each CACWS subsystem are put in "auto" and "on" respectively. If an associated fan unit fails or is shut down, it sends a "stop" signal to its corresponding chilled water circulating pump and chiller. If a circulating water pump or chiller shuts down, the corresponding fan units shut down and the resulting low chilled water flow in the loop signals the standby circulating water pump and chiller to start. The standby fan units start after chilled water

In the event that the main control room becomes uninhabitable, CACWS loop B can also be initiated from the remote shutdown panel (RSP) (see Section 7.4.1.4). Operation from the RSP is totally operator controlled and all CACWS loop B automatic initiation signals are disabled when the Channel B RSP transfer switch is placed in the "Emergency" position.

CACWS loop A can be manually initiated locally as a backup to operation of CACWS loop B from the RSP. CACWS loop A local pump and chiller controls are identified on Table 7.4-3.

- c. CACWS testability - The CACWS is fully testable during normal power operation. Operability of initiating circuits can be verified by manual testing of the pumps and chillers as follows:
1. Manually start and stop pumps and chillers using handswitches located in the main control room

2. With the system in a normal operating lineup, stop one of the fan units associated with the running chiller and chilled water circulating pump pair and observe that the standby chiller and chilled water circulating pump pair and its associated fan units start.

All CACWS setpoints can be checked by insertion of simulated signals of sufficient magnitude to verify accuracy. All CACWS alarm and/or switch units are provided with on-line testability and when placed in test provide a signal to the main control room to indicate the in-test status and also provide an input, where necessary, to indicate that a protective interlock is in test. See Figure 7.3-23.

7.3.1.1.11.6 ESF Equipment Area Cooling System

The ESF equipment area cooling system comprises the following subsystems:

- a. Reactor building equipment area cooling (RBEAC) system
- b. Auxiliary building diesel area HVAC (ABDA-HVAC)
- c. Auxiliary building control area HVAC (ABCA-HVAC)
- d. Service water intake structure HVAC (SWIS-HVAC).

The purpose of the ESF equipment area cooling system is to provide adequate cooling of ESF equipment by maintaining a suitable ESF equipment ambient temperature environment during normal and abnormal plant operations.

7.3.1.1.11.6.1 Reactor Building Equipment Area Cooling Instrumentation and Control

- a. RBEAC function - The RBEAC system consists of unit cooler pairs providing cooling to the RCIC, HPCI, RHR, core spray, and SACS pump rooms. For description and operation, see Section 9.4.2. The RBEAC unit coolers

The unit cooler fans serving the RCIC, HPCI, RHR, and core spray pump fans are interlocked with and close SACS cooling water valves when in the "stop" position.

Individual unit cooler trouble is annunciated at a remote control panel. An alarm on the remote control panel is annunciated in the main control room by a summary unit cooler trouble alarm.

To maintain the redundancy of the mechanical equipment, controls and instrumentation are provided on a one-to-one basis with the mechanical equipment they serve.

The controls, instrumentation, and power supplies are physically and electrically separated for each of the RBEAC unit coolers. See Section 8.1.4.14 for a discussion of the electrical system separation.

The controls for the subject equipment are located in the reactor enclosure. The environmental consideration for this area and the control qualification summary is provided in Section 3.11. For setpoints, see Chapter 16, Technical Specifications. See Figure 7.3-18, Reactor Building Supply Logic Diagram.

- c. RBEAC testability - The RBEAC system is fully testable during normal power operation. Operability of initiation circuits may be verified when the applicable unit cooler fans are operationally tested. The units may be manually tested using handswitches located on remote control panels. RBEAC system setpoints can be checked by insertion of simulated signals of sufficient magnitude to verify accuracy.

7.3.1.1.11.6.2

Auxiliary Building Diesel Area HVAC Instrumentation and Controls

ABDA-HVAC function - The auxiliary building diesel area HVAC system provides cooling and ventilation to the diesel generator cells, diesel area switchgear rooms, diesel area battery rooms, and diesel area Class 1E panel rooms. The ABDA-HVAC system is required for normal operation and testing of the diesel generators

- c. ABDA-HVAC testability - The ABDA-HVAC is fully testable during normal power operation. Operability of the DRR initiating circuits may be verified as follows:
1. By manually testing the fans using handswitches from the associated remote control panel.
 2. In the "auto" mode, by tripping the diesel start signal or cell high-temperature switch and observing the auto-lead fan start.
 3. In the "standby" mode, by tripping the diesel start signal or cell high temperature switch and then tripping the low flow switch for the auto lead fan and observing that the standby fan starts and the auto-lead fan secures.

Operability of the SRC and DABE fans for elevation 146 feet 0 inches may be verified by observation of normal operation of those units. The units may be tested using handswitches located on remote control panels.

Verification of the operability of the DABE fans for elevation 163 feet 6 inches and the DAPRS units may be made by tripping the low flow switch of an operating unit and verifying that the standby unit starts and the operating unit secures.

~~7.3.1.11.6.3~~

~~Auxiliary Building Control Area HVAC
(ABCA-HVAC)~~

- a. ~~ABCA-HVAC function - The ABCA-HVAC system provides cooling and ventilation to the control area HVAC equipment room and control area battery and electrical equipment rooms. The ABCA-HVAC system is required for normal operation of its service area. For description and operation, see Section 9.4.1.~~
- b. ~~ABCA-HVAC operation - The power for the instruments and controls associated with the DRR portions of the auxiliary building control area ventilation system is supplied from the Class 1E power system.~~

HCGS FSAR

operates continuously in the "run" mode. The second CAGE fan is maintained in an auto-standby mode and will start upon a low air flow signal from a flow switch monitoring the running fan. The fan in trouble is deenergized by the low flow signal.

For each CAGE fan, a low flow alarm is indicated at a remote control panel. Any alarm at the remote control panel is annunciated in the main control room by a system summary trouble alarm.

On a LOP, both CAGE fans will stop. The fan in the run mode will restart upon receipt of a permissive signal from the emergency load sequencer.

To maintain the redundancy of the mechanical equipment, controls and instrumentation are provided on a one-to-one basis with the mechanical equipment they serve.

The controls, instrumentation, and power supplies for the control area HVAC units are physically and electrically separated for each of the systems. See Section 8.1.4.14 for a discussion of electrical system separation.

The controls for the ABCA-HVAC equipment are located in the auxiliary building control area and diesel generator area. The environmental consideration for these areas is provided in Section 3.11.

For setpoints, see Chapter 16, Technical Specifications. See Figure 7.3-15, Auxiliary Building Control Area Logic Diagram.

- c. ABCA-HVAC testability - The ABCA-HVAC is fully testable during normal power operation. Operability of the CERS fans and the CAGE fans may be verified by tripping the low flow switch of an operating unit and verifying that the standby unit starts and the operating unit secures. Setpoints may be checked by insertion of simulated signals of sufficient magnitude to verify accuracy.

The controls for the SWIS-HVAC equipment are located in the service water intake structure. The environmental consideration for these areas is provided in Section 3.11.

The controls, instrumentation, and power supplies for the SWIS-HVAC fans are physically and electrically separated for each of the fan systems. See Section 8.1.14 for a discussion of the electrical system separation.

For setpoints, see Chapter 16, Technical Specifications.

See Figure 7.3-25, Service Water Intake Structure and Miscellaneous Equipment Piping Diagram.

- c. SWIS-HVAC testability - The SWIS-HVAC system is fully testable during normal power operation. Operability of the SWIS-HVAC supply fans may be verified by tripping the room thermostat, thus simulating high room temperature and observing that the SWIS-HVAC supply fan starts automatically.

Operability of each SWIS-HVAC exhaust fan may be verified by starting the associated SWIS-HVAC supply fan and observing that the SWIS-HVAC exhaust fan starts automatically subsequent to the start of the supply fan.

Verification of the operability of the traveling screen motor room fans may be made by tripping the low air flow switch of a running fan and observing that the standby fan starts automatically.

All system setpoints can be checked by insertion of simulated signals of sufficient magnitude to verify accuracy.

7.4.1.1.3 Testability

A design flow functional test of the RCIC system may be performed during normal plant operation by drawing suction from the CST and discharging through a full flow test return line to the CST. The discharge valve to the reactor vessel remains closed during the test, and reactor operation remains undisturbed. All components of the RCIC system are capable of individual functional testing during normal plant operation. Control system design provides automatic return from the test mode to operating mode if system initiation is required during testing.

With the following exceptions, test controls are arranged so that the system can automatically fulfill its safety functions:

- a. Flow controller in manual mode
- b. Operator-initiated closure of either or both inboard/outboard isolation valves. An alarm sounds when the valves are in any position other than fully open
- c. Test plug inserted and test switch in position to interlock discharge valves. Out-of-service annunciator alarms in the main control room to indicate system in "test" mode.

Standby Liquid Control System

7.4.1.2.1 Function

The instrumentation and controls for the SLC system are designed to initiate and continue injection of a liquid neutron absorber into the reactor when manually and/or automatically called upon to do so. This equipment also provides the necessary controls to maintain this liquid chemical solution well above saturation temperature in readiness for injection.

The SLC system process equipment, instrumentation, and controls essential for injection of the neutron absorber (sodium pentaborate solution) into the reactor is designed to withstand Seismic Category I earthquake loads. Any nondirect process

Both loops of the SLC system are automatically initiated by the redundant reactivity control system (RRCS) after a time delay, provided that APRM power is downscale. This automatic initiation signal will override the manually initiated pushbutton control switch; however, the manual shutoff signal will override the automatic initiation signal. Section 7.6.1.7 describes the automatic initiation of SLC system by the RRCS.

When either SLC system switch is actuated to inject liquid neutron absorber into the reactor, the following devices are actuated:

- a. One of the two explosive valves is fired
- b. Either the inboard or outboard reactor water cleanup (RWCU) isolation valve closes
- c. One of the two injection pumps is started
- d. The pressure-sensing equipment indicates that the SLC system is pumping liquid into the reactor.

The SLC system is separated both physically and electrically from the control rod drive (CRD) system. The SLC system instrument channels are separated in accordance with the requirements of Regulatory Guide 1.75. The redundant active components of the SLC system are physically and electrically separated.

7.4.1.2.3

Testability

The SLC system is fully testable, with the exception of the explosive valves, during normal operation. Full system testing, by injection of demineralized water into the reactor pressure vessel (RPV), is performed during shutdown or refueling operations.

~~Logic is powered by 125-V dc from bus 1~~

b. Regulatory Guide 1.22 - Revision 0, Periodic Testing of Protection System Actuation Functions - The RRCS equipment is designed so that integrated system testing can be performed to verify overall system performance.

c. Regulatory Guide 1.29 - Revision 3, Seismic Design Criteria - The sensors, transmitters, trip units and associated logic for the RRCS are classified as Seismic Category I. The feedwater pump trip contacts are high quality but not necessarily safety grade.

d. Regulatory Guide 1.30 - Revision 1, Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment - See Section 7.1.2.4.

e. Regulatory Guide 1.32 - Revision 2, Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants - See Section 7.1.2.4.

f. Regulatory Guide 1.47 - Revision 0, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems - There is no RRCS bypass or operating bypass. The following annunciators are provided to communicate system status to the operating personnel in the main control room.

1. RRCS Manual Initiation Enabled
2. RRCS Potential ATWS (receipt of high pressure or low water level 2)
3. Reactor Recirc Pumps Tripped
4. RRCS FW Runback Initiated
5. RRCS RWCU Isolation Initiated

m. Regulatory Guide 1.105 - Revision 1, Instrument Setpoints - Instrument setpoints (accuracy, margin and drift) for reactor power, water level and pressure are described in the plant Technical Specifications, Chapter 16.

n. Regulatory Guide 1.118 - Revision 1, Periodic Testing of Electric Power and Protection Systems - The RRCS is continually checked by a solid state microprocessor based self-test which is part of the analog trip units. This system checks the RRCS sensors, logic, protective devices and itself.

7.6.2.7.3 Conformance to 10 CFR 50 Appendix A, General Design Criteria

General Design Criteria (GDC), established in Appendix A of 10 CFR 50, which are generally applicable to all safety-related systems, are discussed in Section 3.1. Those with specific impact on the RRCS are described in this section.

a. GDC 1 through 5, 13 and 19 - See Section 7.1.2.2.

b. GDC 20, Protection System Functions - The RRCS is completely automatic.

c. GDC 21, Protection System Reliability and Testability - The RRCS is designed for high functional reliability and its logic can be tested for the safety functions to be performed. No single failure in this two divisional, four channel protection system will result in the loss of the protective functions.

d. GDC 22, Protection System Independence - The RRCS is a two division class 1E system separate and diverse from the RPS. It has functional diversity via ARI, RPT, and feedwater runback.

e. GDC 24, Separation of Protection and Control Systems - The RRCS protection system interfaces with control systems through isolation devices. Specifically, the RRCS signals to the recirculation system pump and the signal to the feedwater control system to initiate

- h. Derivation of System Inputs (Paragraph 4.8) - The RRCS system inputs, reactor pressure, and water level, are derived from pressure and level transmitters that produce signals that are to the extent, feasible and practical, direct measures of these desired variables.
- i. Capability for Sensor Checks (Paragraph 4.9) - The RRCS self-test unit automatically checks the RRCS level and pressure sensors. The automatic check determines if the sensor output is downscale, within normal operating bounds, or too high. If the sensor output is found to be abnormal, an alarm is sounded. The sensor's output can be observed and compared at the middle bay of the RRCS cabinet where the analog trip module diagnostic display is mounted.
- j. Capability for Test and Calibration (Paragraph 4.10) - Each RRCS sensor provides input to an analog trip module (ATM). The ATM electronically monitors the incoming sensor signal level and provides the appropriate output to the RRCS logic if that sensor signal level goes beyond its trip setpoints. Sensor signal level can be read at the ATM and compared to the known characteristics of the transmitter. Trip setpoint can be adjusted at the ATM, and the operability of this trip module is checked repeatedly by the RRCS self-test unit.

RRCS sensors, logic, timers, and actuated devices are continuously checked by the RRCS self-test unit, meeting paragraph 4.10.

- k. Channel Bypass or Removal from Operation (Paragraph 4.11) - The RRCS is designed such that portions may be removed from service for maintenance or testing without initiating the RRCS protective actions at the system level.
- Removal of portions of the RRCS for service will not result in protective actions because the system is normally deenergized.
- l. Operating Bypasses (Paragraph 4.12) - There is no operating bypass affecting the RRCS.
- m. Indication of Bypasses (Paragraph 4.13) - There is no manual bypass of the RRCS.
- n. Access to Means for Bypassing (Paragraph 4.14) - The RRCS cannot be manually bypassed.

QUESTION 421.23 (SECTIONS 7.2, 7.3, 7.4)

Operating reactor experience indicates that a number of failures have occurred in BWR reactor vessel level sensing lines and that in most cases the failures have resulted in erroneously high reactor vessel level indication. For BWRs, common sensing lines are used for feedwater control and as the basis for establishing vessel level channel trips for one or more of the protective functions (reactor scram, MSIV closure, RCIC, LPCI, ADS or HPCS initiation). Failures in such sensing lines may cause a reduction in feedwater flow and consequential defeat of a trip within the related protective channel.

If an additional failure, perhaps of electrical nature, is assumed in a protective channel not dependent on the failed sensing line, protective action may not occur or may be delayed long enough to result in unacceptable consequences. This depends on the logic for combining channel trips to achieve protective actions.

Identify each case where a reactor vessel water level tap or sensing line failure concurrent with an additional random single electrical failure induces a transient and precludes the automatic operation of reactor scram and/or engineered safety feature system. For each case identified provide an evaluation which demonstrates how the redundancy or diversity of the plant design provides for reactor scram or safety system operation within acceptable limits. Where manual action is required by the operators discuss the instrumentation and time available for the operator to take such corrective action.

To reduce the consequences of sensing line failures in combination with a single failure in a protection channel not dependent on the failed sensing line, a modification of the protection system logic may be required.

BWROG generic report SLI-8211 indicates that early operator action would be required to initiate either HPCI or RCIC in the event of a loss of the reference leg connected to the level sensor which is controlling feedwater combined with the failure of a level sensor, control component or power supply bus associated with the intact reference leg instruments. The specific level sensors are N091, A, B, C, D (Figure 5.1-4) and the buses are 125 Vdc A and B. Provide a description of the modifications implemented at Hope Creek as a result of this concern or provide justifications why the modifications discussed in the generic report are not necessary to reduce the consequence of sensing line failures.

PRELIMINARY

RESPONSE

~~The concerns addressed above are being evaluated against the HCGS design. A justification why modifications are not necessary or a description of proposed modifications will be provided by July 1984.~~

An analysis was conducted based on the following assumption that simultaneously:

1. An instrument reference line fails (breaks),
2. A single electrical device also fails (but there is no power supply failure), and
3. There is no operator action.

These postulated multifailures are beyond the design basis for the HCGS; however, an assessment of the plant responses to these types of events was provided.

The instrument reference lines common to feedwater control and to protective system sensors were identified. All the various failure combinations were examined. Two failure combinations that represent the worst postulated failure paths were identified. These two failure combinations are described in what follows.

Failure Combination 1 would be the failure of the division 1 instrument reference line connected to condensing chamber B21-D004A combined with a failure such that it indicates a high water level. In the analysis of this combination, it was assumed that the manual selection switch for feedwater control is on the failed instrument line (division 1) and that the operator does not switch the control to the other instrument line (division 2) as would be expected. This would cause the feedwater controller to respond to the erroneous high-level signal by reducing the feedwater flow.

Following the loss of feedwater flow, the decrease of the water level to level 4 would initiate a low water level alarm. After the water level decreased to level 3, a second low water level alarm would be initiated, but a reactor scram would not occur due to the assumed failures.

failure of high level transmitter

*H=h
K=1/2000*

*ΔP goes up
level goes down
ΔP goes down
level goes up*

When the water level decreased to level 2, a reactor scram would occur due to the alternate rod insertion system, and a third low water level alarm would be initiated. The RCIC system would then automatically start, and both recirculation pumps would trip. However, HPCI system would be unavailable (tripped) due to the assumed failures.

LR-ARI
ACIC
Trip

Core uncover analysis were performed using the REDY program and simulations that represent the beginning-of-cycle (BOC) and end-of-cycle (EOC) void-reactivity coefficients.

The case with the EOC void-reactivity coefficient showed that the minimum water level would be between level 1 and level 2. Figures 421.23-1 and 421.23-2 show the REDY plots for the cases with the BOC void-reactivity coefficient and the EOC void-reactivity coefficient, respectively. The case with the BOC void-reactivity coefficient showed that the minimum water level would be below level 1 outside the shroud and would trigger the closure of the MSIVs.

For the BOC void-reactivity case, a further analysis, based on realistic assumptions, was performed to evaluate the potential for core heatup. This analysis applied the power history that resulted from the core uncover analysis until the level-2 scram signal occurred at approximately 42 seconds. After 42 seconds, the ANS 1979 best-estimate decay-heat values were used.

Handwritten note:
The minimum water level is 2.5 feet below the top of the active fuel (inside the shroud).

Figures 421.23-3 through 421.23-5 show the system pressure, water level inside the shroud, and peak cladding temperature (PCT), respectively, calculated from the core-heatup analysis. The minimum water level in the core would be 2.5 feet below the top of the active fuel (inside the shroud). This uncover level would result in a PCT of 450°F. Since this PCT is less than the initial cladding temperature of 644°F and well below the 2200°F limit, these results are acceptable from an ECCS viewpoint.

Handwritten note:
This is acceptable

Handwritten note:
Shows an HRF
Morton

Failure Combination 2 would be the failure of the division 2 instrument reference line connected to condensing chamber B21-D004B combined with a B21-N097 D- or H-level transmitter failure such that it indicates a high water level. In the analysis of this combination, it was assumed that the manual selection switch for feedwater control is on the failed instrument line (division 2) and that the operator does not switch the control to the other instrument line (division 1) as would be expected. This would cause the feedwater controller to respond to the erroneous high-level signal by reducing the feedwater flow. Following the loss of feedwater flow, the water level would decrease to level 4, initiating a low water level alarm. After the water level decreased to level 3, a second low water level alarm would be initiated, and reactor scram would occur. After the water level decreased to level 2, a third low water level alarm would initiate, the HPCI system would automatically start, and both recirculation pumps would trip. The RCIC system would be unavailable (tripped) due to the assumed failures.

Handwritten note:
scram L3
HPCI L

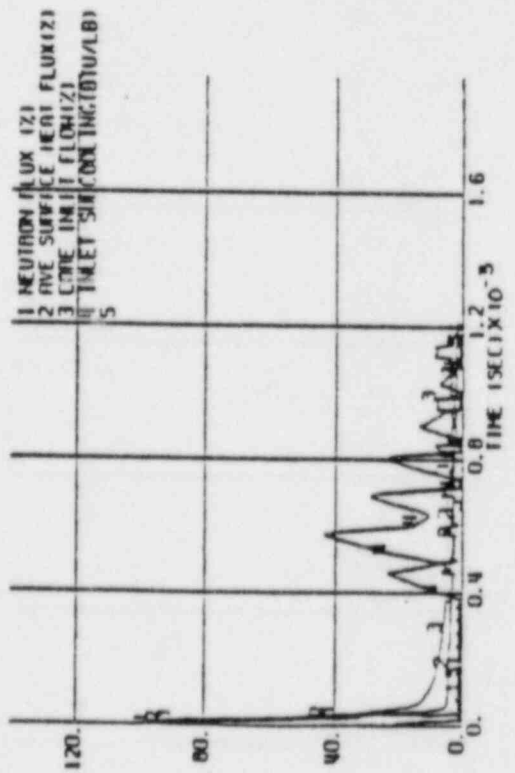
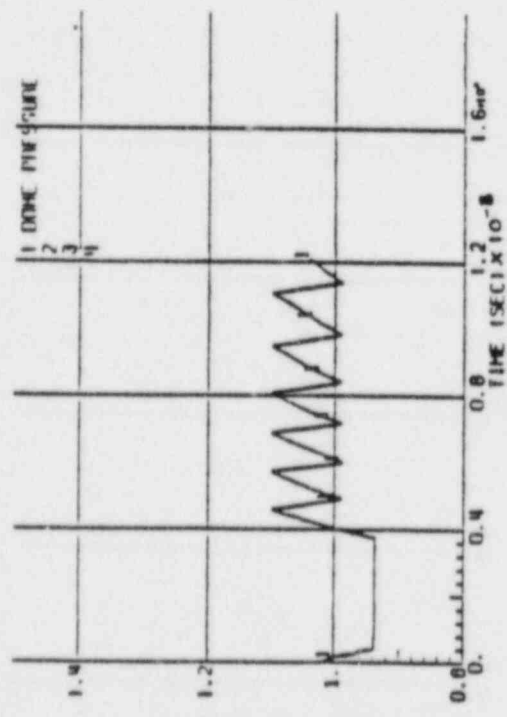
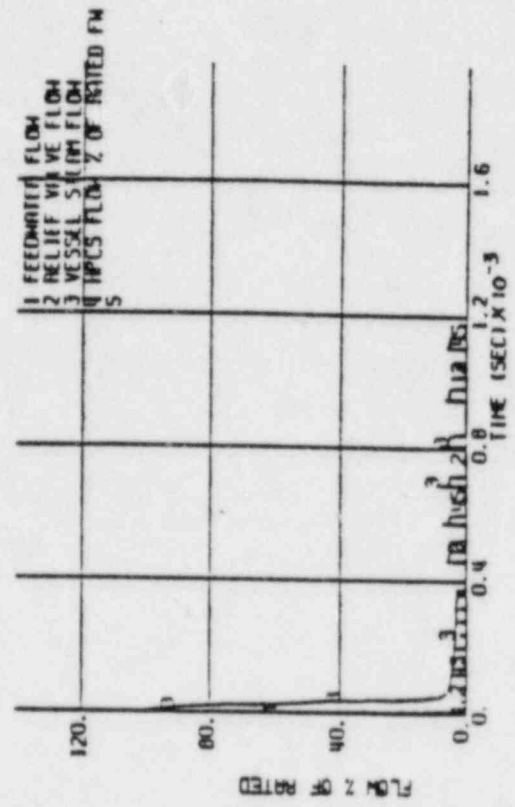
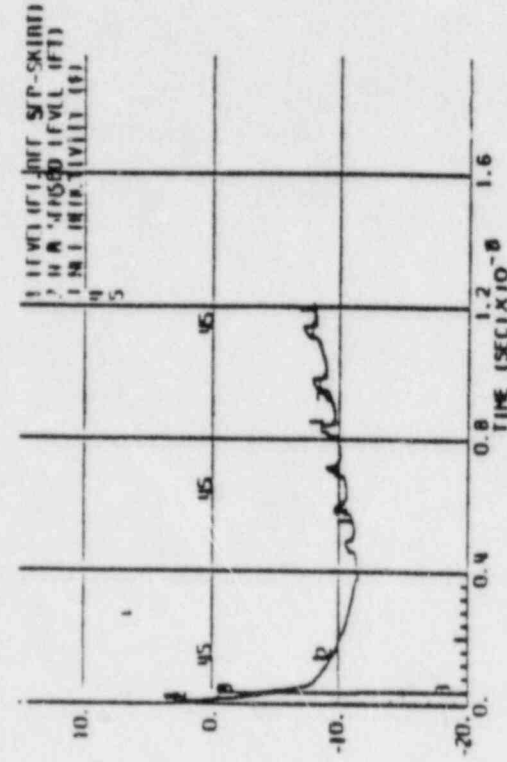
Handwritten note:
Need ARI

A core uncover analysis was performed using the REDY program, and simulating the BOC void-reactivity coefficient only, since it presents the worse reactor condition for this scenario.

Figure 421.23-6 shows the REDY plot for this case. It can be seen that the minimum water level outside the shroud would be about 10 feet above the top of the active fuel. No core uncover was found.

Handwritten note:
Shows 2.5 feet above

PRELIMINARY



PRESSURE (PSI) x 10⁻³

PRELIMINARY

FIGURE 421.23-1 INSTRUMENT LINE BREAK ANALYSES, BOC; NO HPCI; RCIC AVAILABLE WITH ARI

PRELIMINARY

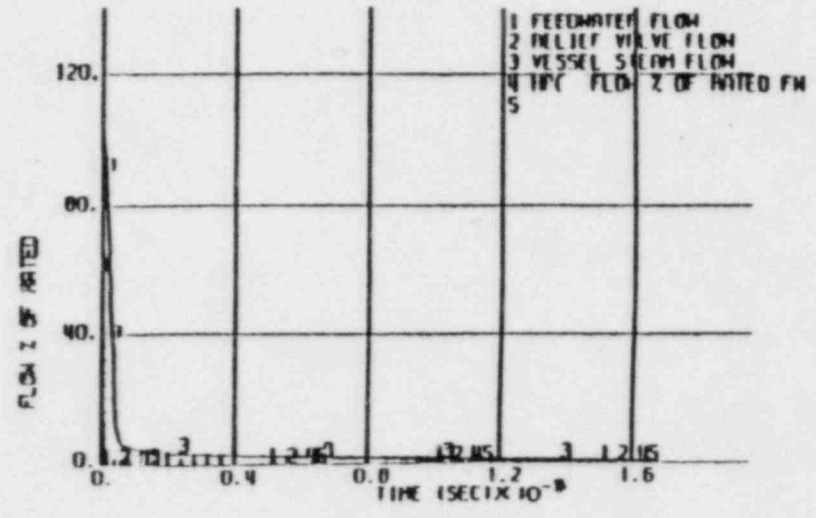
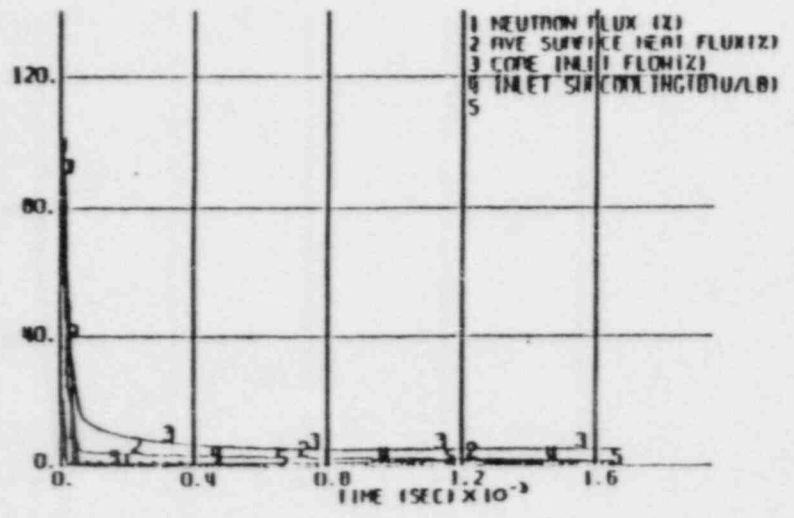
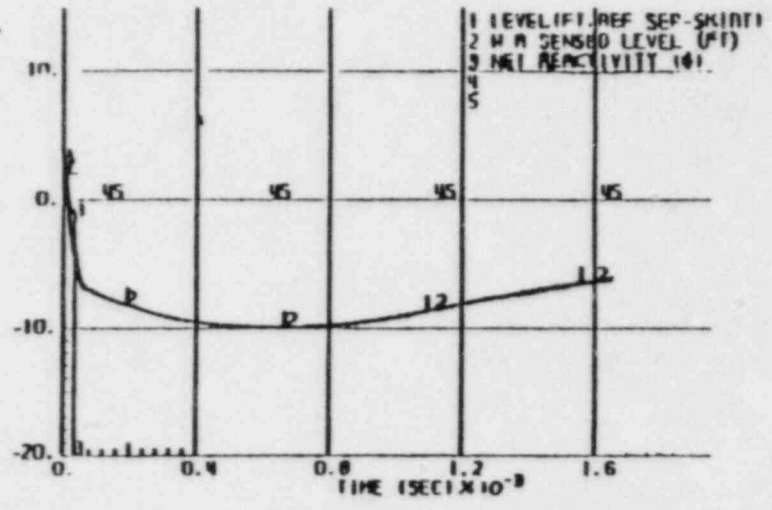
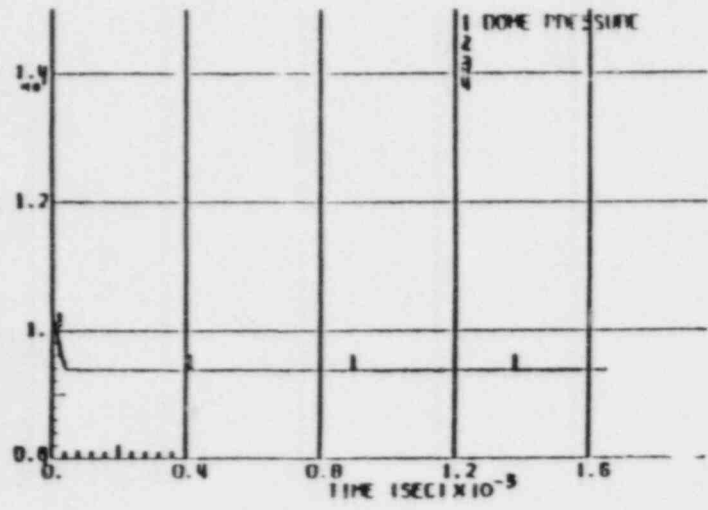


FIGURE 421.23-2 INSTRUMENT LINE BREAK ANALYSES, EOC; NO HPCI; RCIC AVAILABLE WITH ARI

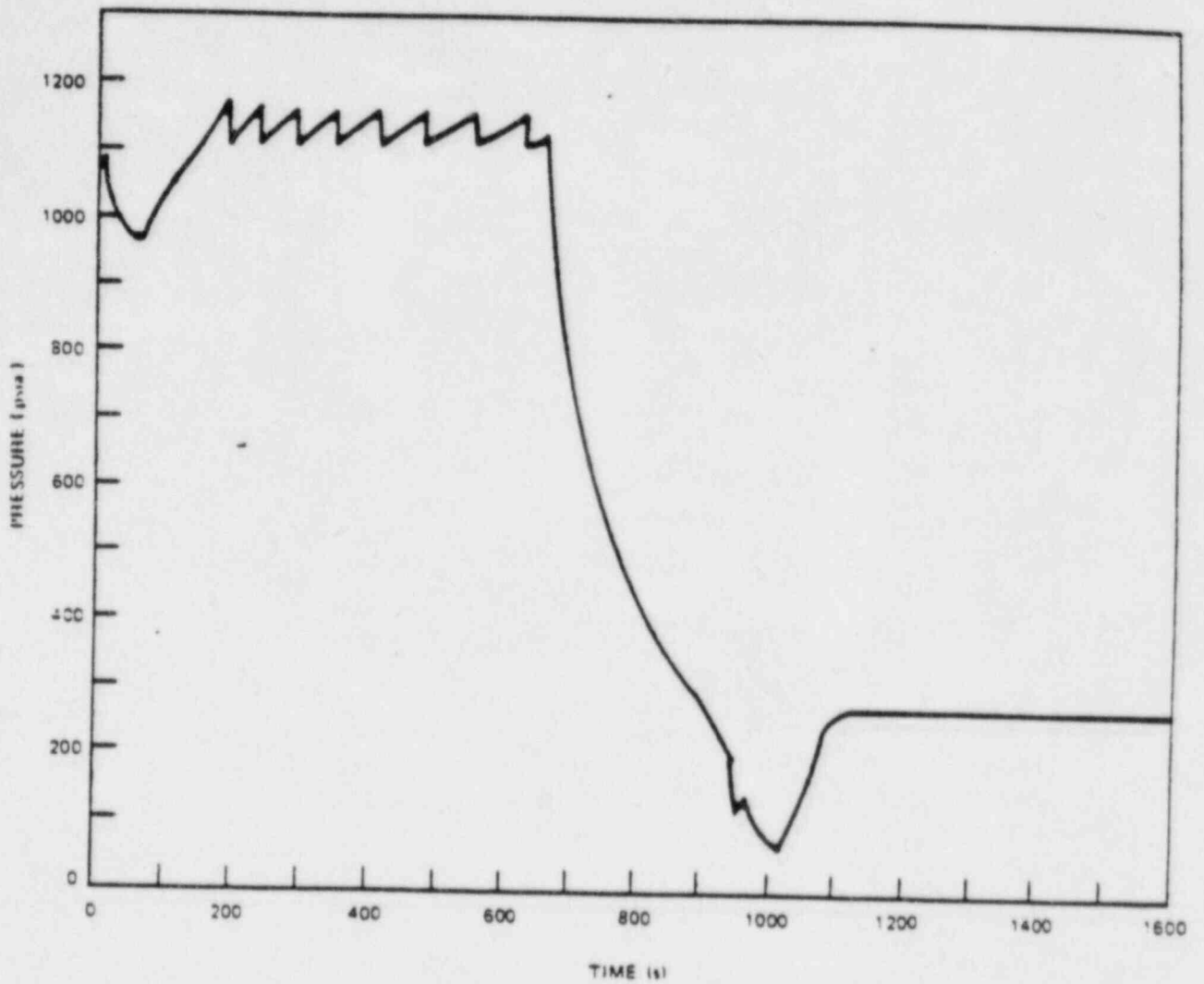


Figure 421.23-3

Vessel Pressure Calculated
from the Core-Heatup Analysis

PRELIMINARY

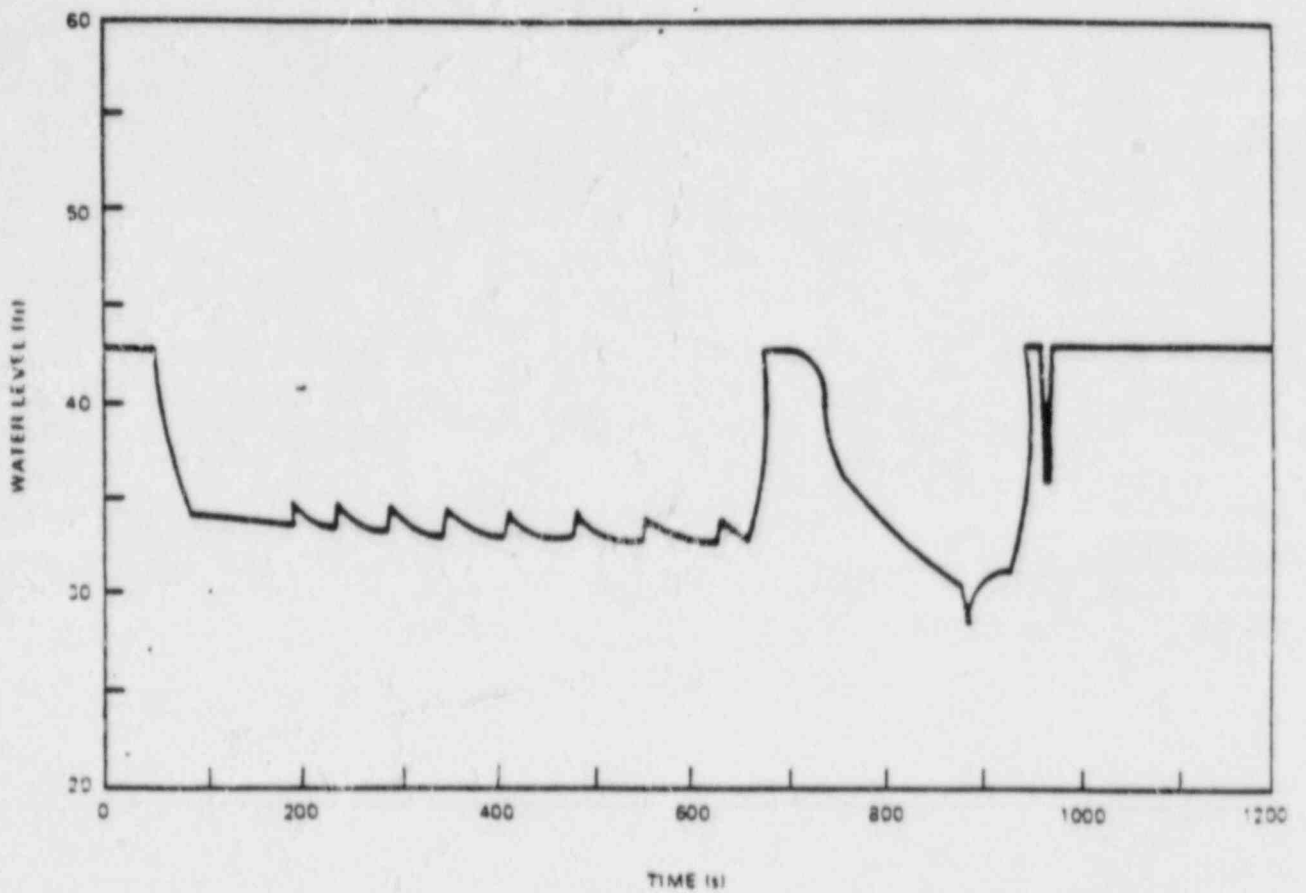


Figure 421.23-4
Water Level Calculated
from the Core-Heatup Analysis

PRELIMINARY

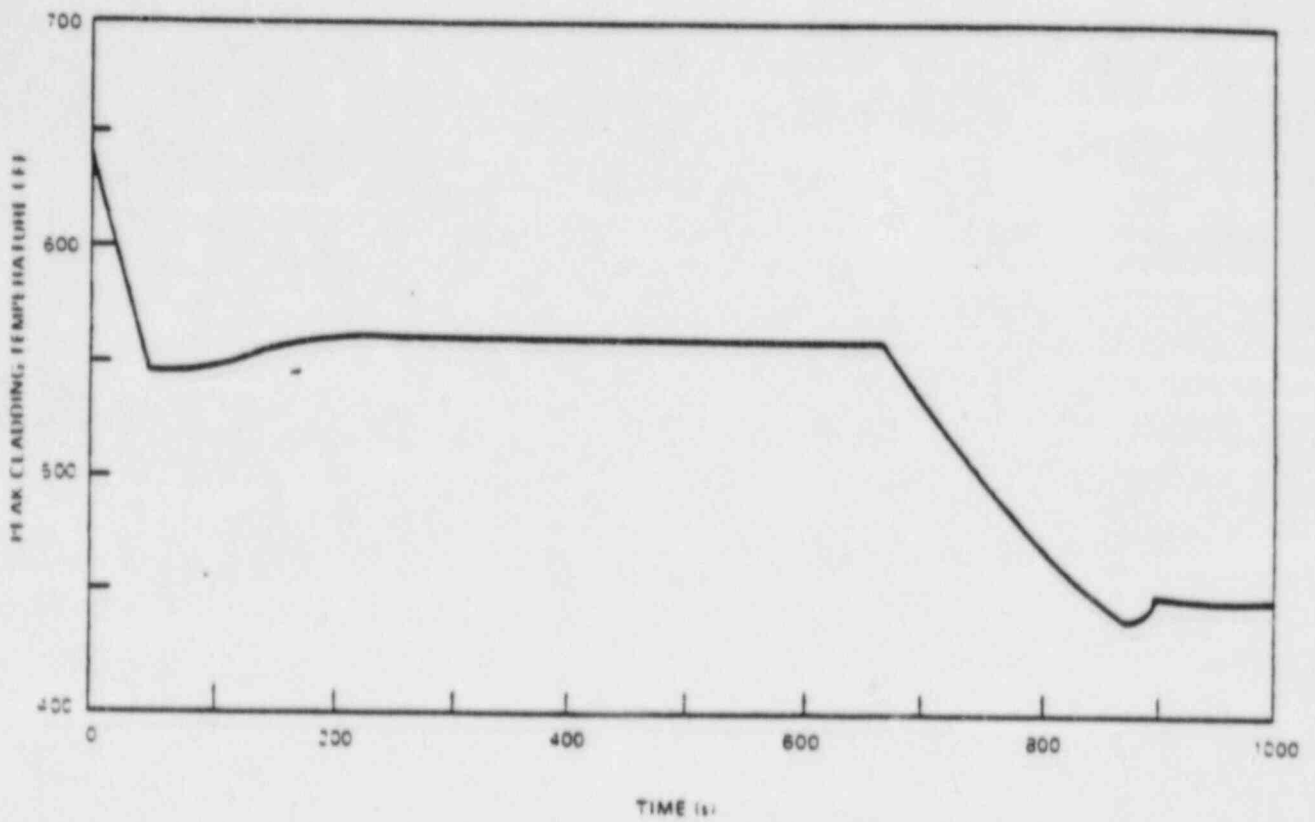


Figure 421.23-5
Peak Cladding Temperature Calculated
from the Core-Heatup Analysis

PRELIMINARY

PRELIMINARY

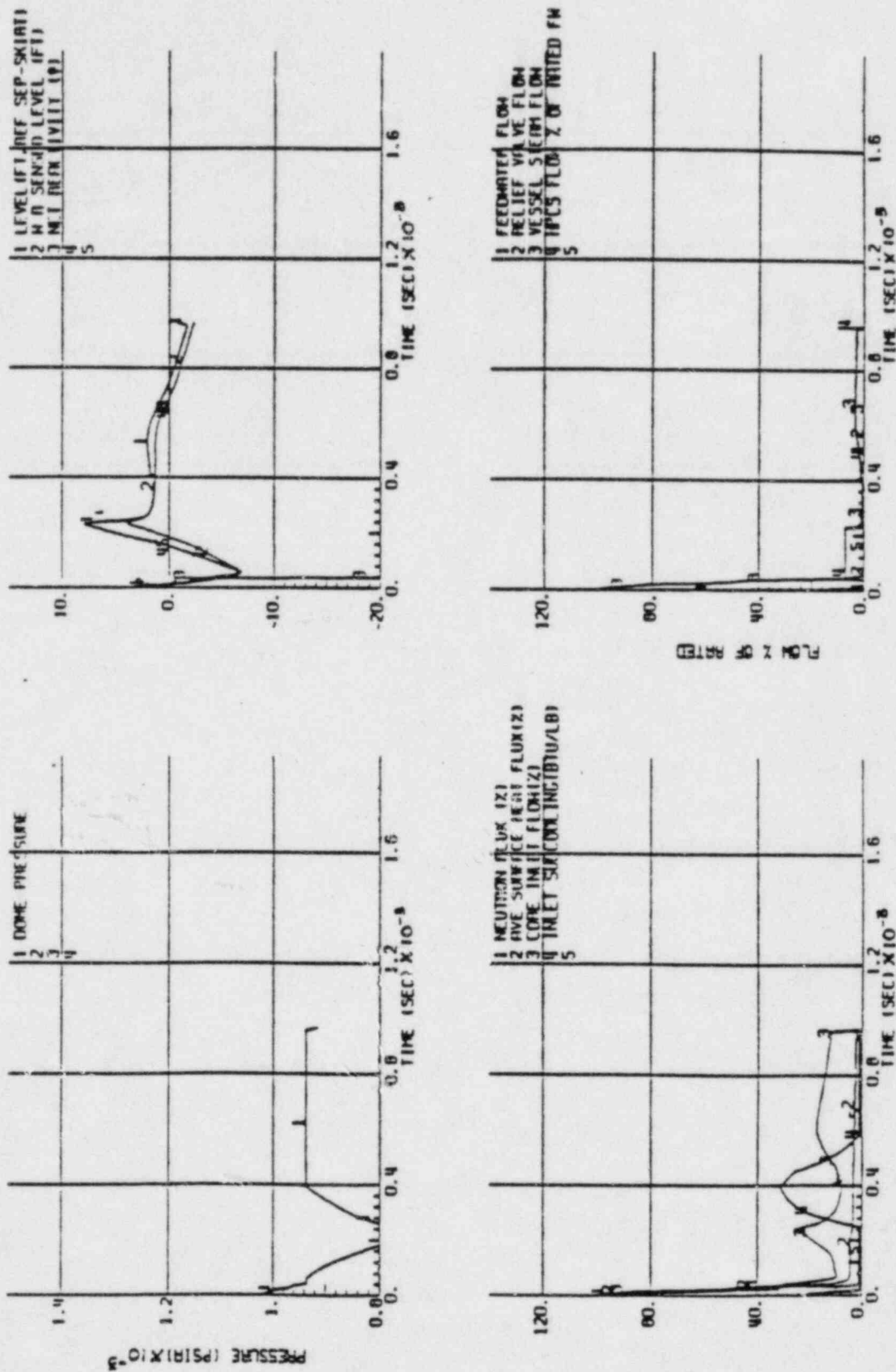


FIGURE 4-1.23-6 INSTRUMENT LINE BREAK ANALYTIC DATA, NO DATA NOT AVAILABLE WITH AHT

Hope Creek 1-42

QUESTION 421.26 (SECTIONS 7.2, 7.3, 7.7)

Mode switch contact and mode switch operating mechanism malfunctions have caused inadvertent protective actions. Similar malfunctions could have rendered redundant channels of protective functions inoperable. IE Information Notice 83-42 provided notification of potentially significant events concerning mode switch malfunctions. Section 7.2.1.1.11 of the FSAR indicates that the reactor mode switch can be used to initiate a reactor scram. Further discussion regarding the reactor mode switch capability to bypass and enable protective functions and provide rod withdrawal interlocks and refueling equipment interlocks is not provided in Section 7.2. Provide a detailed discussion on how the mode switch is incorporated into the overall design, supplemented with detailed drawings and schematics. Please include the following:

1. Identification of the reactor protection system, rod block, refueling interlock and other functions important-to-safety that are dependent on proper mode switch contact operation.
2. Identification of the analyzed transients and accidents where credit is taken for the operation of any function identified in 1 above.
3. The surveillance actions necessary to positively verify mode switch contact positions, detect mode switch contact failures and detect mode switch operating mechanism failures for each function identified in 1 above.

RESPONSE

The reactor mode switch currently installed at HCGS is of the type having the potential for ^{misoperation} ~~malfunction~~ as described in IE Information Notice 83-42. This switch will be replaced prior to fuel load with a modified switch having an identical contact configuration and wiring scheme.

An assessment ^{has been made} of the system impact of postulated mode switch misoperations for the presently installed HCGS mode switch ~~is provided in the report "Assessment of the Effects of Postulated Mode Switch Misoperations" provided below. It provides an~~ ^{This assessment} evaluation of the impact of postulated mode switch misoperations on the analyses described in Chapter 15. It identifies normal switch contact positions for each mode of operation - "RUN", "SHUTDOWN", "REFUEL", and "START" - and summarizes the system consequences should one or more pairs of contacts misoperate. All of the identified misoperations of contacts are detectable by annunciation, instrumentation checks, or surveillance tests. ~~This response will be modified by June 1984 to identify the~~

~~Chapter 15 accident analyses that bound mode switch misoperations.~~

1 Assessment of the effects of Mode Switch Misoperations.

- I. Mode Switch Contacts 1-2, 9-10, 17-18, and 25-26 (Division 1 through 4 respectively).

The contacts listed above are normally closed when the mode switch is in the "RUN" position and are open in all other mode switch positions (i.e., "SHUTDOWN", "REFUEL" and "STARTUP").

- A. If the contacts were to open in the "RUN" mode, then:

1. Scram or half scrams would result as K15 relays are deenergized.
2. The IRM functions would be enabled and the APRMs would revert to setdown trip-level scrams or half scrams if the plant is at greater than 12% to 15% of rated power or IRMs are upscale.
3. A rod block would be annunciated because the RPS signals to the reactor manual control system would incorrectly infer that the mode switch is in the "SHUTDOWN" position.

- B. If the contacts were to close in the "STARTUP", "REFUEL", or "SHUTDOWN" modes, the effects would be similar for all three modes of operation, i.e.,

1. In all three modes, the IRM scram function would be bypassed. This would not be immediately detectable but would be detected at the time of the weekly channel functional tests because half scrams would not result. Weekly channel functional tests will cover IRMs in "STARTUP", "REFUEL" and hot and cold "SHUTDOWN".
2. Assuming two or more contact pairs fail, the "SHUTDOWN" scram would be redundantly bypassed in the "STARTUP" and "REFUEL" modes with no consequence although this would not be immediately detectable. However, if the contacts were closed prior to going to "SHUTDOWN", either no scram or only a half scram could result when the mode switch is placed in "SHUTDOWN", assuming that the contacts remain closed during and after the transfer to "SHUTDOWN".

3. In all three modes ("SHUTDOWN", "REFUEL", and "STARTUP") the APRM setdown scram function would not be in effect, APRM setpoints would be raised to their high setpoint level (approximately 120% of the NB rated power). Again, this condition would not be immediately detectable, but it could be detected at the time of the weekly channel functional tests.
4. In all three modes ("SHUTDOWN", "REFUEL" and "STARTUP") there would be an unannounced capability or permission via the reactor manual control system to move more than one control rod according to the rod pattern control definition. This would be a redundant permission in the "STARTUP" mode. In the "REFUEL" mode, the operator would not be directly aware of this capability unless he attempted to withdraw more than one rod. ~~The scram or half scram from~~ ~~Item A4 above would probably preclude such action.~~ *would* The operator ~~will~~ verify this rod block by an attempt to withdraw a second rod after the first control rod is withdrawn. In the "SHUTDOWN" mode, the operator should be aware of such permission as the normal annunciation of the rod withdrawal block would be present, ~~or would be removed at the same time as the scram or half scram resulting from Item A4 above.~~

C. Conclusions:

1. *INSERT A →* Except for switch closures where the switch is in the "STARTUP" mode, postulated switch failures would result in at least a half scram condition at the time of the switch failure. This would alert the operator to an RPS failure. This conclusion addresses failures only of mode switch 1-2, 9-10, 17-18 and 26-26 contacts.
2. The potential consequences related to bypassed IRM trips and high-setpoint APRM trips, while in the "STARTUP" mode, are not determined in this assessment. These are reported in a separate evaluation.

II. Mode Switch Contacts 3-4, 11-12, 19-20 and 27-28 (Divisions 1 through 4, respectively).

These contacts are normally closed when the mode switch is in the "STARTUP" position and are open in all other mode switch positions (i.e., "SHUTDOWN", "REFUEL", and "RUN".)

INSERT A

1. Addressing only the multiple failures of the mode switch contacts 1-2, 9-10, 17-18, and 25-26, the items of principal concern are:
 - a. The unannounced bypass of the IRM scram function in the "STARTUP," "REFUEL," and "SHUTDOWN" modes.
 - b. The potential failure to scram by positioning the mode switch to "SHUTDOWN."
 - c. The unannounced bypass of the APRM setdown scram function in the "STARTUP," "REFUEL," and "SHUTDOWN" modes.
 - d. The unannounced permission to move more than one control rod in the "REFUEL" mode.
 - e. The annunciated (via the removal of the signal) removal of the normal "SHUTDOWN" mode rod-withdrawal block.

preceding, the time delays relays K16A-D, would also be energized such that after 10 seconds, the second set of contacts in the shutdown scram bypass circuitry would close. At that time, the "SHUTDOWN" scram function would be redundantly bypassed (i.e., already bypassed by the "RUN", "STARTUP" or "REFUEL" modes). When this redundant bypass occurs, the operator would be alerted since the annunciators would indicate "RPS Mode Switch Shutdown Scram Bypass".

4. If the switch were in the "REFUEL" mode, a redundant mode-switch permissive signal to allow bypass of the high water level trip function on the scram discharge instrument volume would occur with no consequence. However, if the permissive signal does exist in the "RUN" or "STARTUP" mode, the bypass switches for the SDV high water level trip must have been incorrectly placed in the bypass position. This switch placement is abnormal for these modes. Such bypass is annunciated and would initiate a rod withdrawal block at the same time.

C. Conclusion:

Addressing only the failure modes of the mode-switch contacts 7-8, 15-16, 23-24 and 31-32, the items of principal concern are the annunciated bypasses of the MSIV closure scram function and steam-line low pressure isolation function when the switch is in the "RUN" mode. Ten seconds later the operator would receive an additional input that something is wrong with the RPS when the annunciation system indicates that the "RPS mode switch shutdown scram bypass" is in effect. *Assessment*

V. Summary and Conclusions of the Mode Switch Misoperation Effects *A*

- A. All failure modes for the mode switch contacts where contacts open that should be closed would result in scrams or half scram depending on the number of contacts that are open. At the same time, for conditions of operation where steam line pressure is low, isolations of the main steam lines would occur.
- B. In the "STARTUP", "REFUEL", and "SHUTDOWN" positions of the mode switch, contact closures of the contacts that should be open, (i.e., contacts 1-2, 9-10, 17-18 and/or 25-26) would result in a bypass of the IRM scram function in one or more of the RPS channels and also would result in raising the setpoint of the normally

similar change in the mode switch contacts.

setdown APRM high flux scram function from 15% to 118% in one or more of the RPS/NMS channels.

- C. In item B above, although the mode switch failure, (i.e., contacts closing), would not be immediately apparent to the plant operator, the failure would be detected during the weekly IRM and APRM channel functional tests. If these tests were performed prior to the power increase and after transferring the mode switch to the "STARTUP" position, then the IRM channel functional tests would detect the failures because no half scram would result. ~~The proposed technical specification requirement will be that the IRM channel functional test and the APRM channel functional test be performed within 24 hours prior to startup, if it has not been performed in the previous seven days. Weekly surveillance would be required for the case whereby the "HOT STANDBY" condition is maintained for long periods of time. Additional information will be provided in June 1984 on the mode switch.~~

- D. In the "RUN" position of the mode switch, contact closures of the contacts that should be open, (i.e., contact closures of all contacts other than 1-2, 9-10, 17-18 and 25-26) would result in the bypass of one or more RPS trip channels related to the MSIV closure scram functions and would also result in the bypass of one or more NSSSS trip channels related to the steam-line low pressure isolation function. Concurrent with the incorrect mode switch contact closures, there would be annunciations that one or more of the RPS MSIV closure scram trip channels have been bypassed. If contacts 7-8, 15-16, 23-24 and/or 31-32 were to close, then the operator would receive additional information that something is wrong approximately 10 seconds after the contacts close with the annunciation that there is a "RPS mode switch shutdown scram bypass". ~~Additional information will be provided in June 1984 on the use of operational procedures~~ of the mode switch.

- E. Closure of several sets of contacts can bypass the "SHUTDOWN" mode scram function. If the contacts remain closed during and after transfer of the mode switch to the "SHUTDOWN" position, such closed contacts would not allow a scram to occur. That is, only a half scram or no scram would result. This fact would be immediately apparent to the operator. *The ability to scram the plant from the mode switch is only one of several backups to the manual scram pushbuttons.*
- F. In the "REFUEL" mode, closure of the mode switch contacts 1-2, 3-4, 25-26 and/or 27-28 would negate the normal "refuel" mode restriction of the "all rods in first, move only one rod at a time" and would allow the

From the positioning of the mode switch

movement of any number of rods within the rod pattern definition existing at the time. This fact would not be apparent to the operator if contacts 3-4 and/or 27-28 were closed. ↑

- G. In the "SHUTDOWN" mode, closure of the mode switch contacts 1-2, 3-4, 5-6, 25-26, 27-28 and/or 29-30 would remove the normal rod withdrawal block restriction of the associated with this mode. This fact would be apparent to the operator because the window for the normal rod withdrawal block annunciator would be extinguished, and its change of state would alert the operator.

However, the rod-block positioning restrictions are only a backup to the strict procedural restrictions on the manual positioning of rods. Also, the technical specifications direct these procedures to require the operator to verify the rod block function by attempting to withdraw a second rod after the first is withdrawn.

INSERT B
HERE →

INSERT B

2. Evaluation of the Impact of the Effects of Mode Switch Misoperation on the Chapter 15 Analyses.

*ICSB
concern*

The potential impacts of the effects of mode switch misoperation on the analyses of transients and accidents presented in Chapter 15 were evaluated. The focus was on certain specific events because of previously expressed NRC concerns with those events or because the events might impact the limiting transients. These specific events were classified into two groups according to the consequences of mode switch misoperation.

I. The Evaluation of Group 1 Events

The events in Group 1 include:

- a. The abnormal startup of an idle recirculation loop.
- b. The failure of the recirculation flow controller with increasing flow.
- c. A rod drop accident.

These are events for which the concern is related to the bypass of the scram function of the intermediate range monitor (IRM) while the mode switch is in the "STARTUP," "REFUEL," or "SHUTDOWN" positions. This would also raise the scram setpoint of the average power-range monitor (APRM) from the 15% "startup" value to the 118% "run" value, which corresponds to the analytical limit of 121% used for the analyses of Chapter 15 transients and accidents.

None of the Chapter 15 analyses of the events in Group 1 takes credit for either the IRM scram function or the APRM scram function with the setpoint setdown to the 15-to-25% level. Events a and b of Group 1 were analyzed from a "RUN"-mode power condition since the Chapter 15 analyses are initiated from about 55% power and 38% core flow. In the "RUN" mode, the IRM trips are bypassed and the APRM flux scram-setpoint is approximately 118% (121% analytical limit). The rod drop accident analysis was initiated from 0% power, (50% rod density); consequently, the mode switch would be in the "STARTUP" position.

No impact would result from the misoperation of the mode switch in the "REFUEL" or "SHUTDOWN" modes.

- A. For the analysis of the abnormal recirculation-loop startup transient, no credit was taken for the flow reference in the scram for high neutron flux. The high neutron flux setpoint of 121% was used. The Analysis of this event was initiated from a power level significantly in excess of where recirculation-loop startups would

normally originate and corresponding to the mode switch in the "RUN" mode. At lower power levels, the consequences of the event would be less severe; consequently, the impact of the mode switch misoperation on the analysis of this event is of no significant consequence.

The initiation of an abnormal recirculation-loop startup transient when the mode switch is in the "STARTUP" position would also be of no consequence since operating procedures would require the initial power level to be less than 15%. The resulting power increase probably would not cause a scram. If the resulting power level were in excess of technical specification requirements related to power, pressure, and core flow, the operator would take corrective action in accordance with those requirements.

- B. The Chapter 15 analyses of the recirculation flow-controller failure with increasing flow were initiated from a 57% power and 40% core flow conditions, with a 121% flux scram terminating the power excursion.
 - Similar events originating from the startup power range of 0 to 15% power would be of lesser consequence. Also, at this low power level, normal operating procedures would infer minimum pump speed with individual loop operation. These operating conditions would lessen the effect of a single-loop flow increase and would preclude the event of flow control failing with increasing flow on both loops.
- C. The analysis in Chapter 15 of the rod drop event only takes credit for the 121% APRM trip and takes no credit for the IRM scram function. The event, as analyzed from the 0% power level, is terminated by the Doppler effect and is of significance only below about 2 to 3% power. At high power levels, the rod drop would be less of a problem because of the influence of the resulting steam voids in the core on the local high reactivity.

II. The Evaluation of Group 2 Events

The events in Group 2 include:

- a. The inadvertent closure of the main steam isolation valve.
- b. The loss of an auxiliary power transformer.
- c. The break of a main steam line outside the containment.
- d. The failure in the open position of the steam pressure controller.

These are events for which the concern is either the bypass of the main steamline isolation function due to low steamline pressure by the nuclear steam supply shutoff system (NS⁴) in the "RUN" mode or the loss of the position scram function of the MSIVs in the "RUN" mode. Only the isolation function that should result whenever the turbine-inlet steamline pressure drops below the (analysis) setpoint level of approximately 825 psig is of concern. No other isolation functions of the NS⁴ are impacted by the potential mode switch misoperations.

- A. The analysis of the MSIV closure event in Chapter 15 does take credit for the scram initiated from limit switches of the MSIV while the mode switch is in the "RUN" mode. Potential mode switch misoperation could cause this scram function to be bypassed while the mode switch is in the "RUN" position. However, this bypass would be annunciated in the control room. The operating procedures would require corrective action since the technical specification requirement that all four channels for the MSIV-closure trip function be operable in the "RUN" mode would be violated. Depending upon the number of inoperable channels, the affected channels and at least one trip system of the reactor protection system (RPS) would have to be placed in the tripped condition within one hour. If both RPS trip systems were affected, the plant would have to be placed in the "STARTUP" condition within 6 hours.

Because of the unique design of the HCGS switchyard (see section 8.1), this event would have the same consequences as the loss of all grid connections. The fast closure of the turbine control valve, a scram, and MSIV closure would be initiated at time zero of the event, irrespective of possible misoperation of the mode switch.

- B. The consequences of the ^{loss of} auxiliary power, as analyzed in Chapter 15, are also not affected by any mode switch misoperation. ~~The scram and isolation that occur at about 2 seconds (or later) are a direct result of the loss of power to the RPS motor-generator sets and the subsequent disconnection of all power to the loads on the RPS bus.~~
- C. The analysis of the main steamline break outside of the containment does not take credit either for the low steamline isolation signal that would probably result from low steamline pressure or for the scram from MSIV closure. In this analysis, the event is initiated at the Level 3 scram to start out with a minimum inventory. At about 0.5 seconds into the event the isolation, is assumed to be initiated because of high steamline flow. Although this is not addressed in the analysis, a level-8 high-water turbine trip would be expected due to sudden depressurization.
- D. Failure of the steam pressure controller in the open position would result in a level-8 high-water turbine trip, which would initiate a scram and a recirculation pump trip. Since the depressurization would be limited to the capacity of the turbine bypass, the low-pressure isolation would be delayed to beyond a minute. Since an annunciation in the control room would have alerted ^{the operator} to the bypass of the isolation function, the operator would be prepared to actuate MSIV closure manually should this event occur.

III. Conclusion of the Event Evaluations

Conclusions from these evaluations are that all misoperations of the mode switch are detectable by one or more of the following means.

- A. The operator would be immediately aware of a problem because of the annunciation of bypasses that should not exist for the given position of the mode switch. All mode switch misoperations that might impact the severity of consequences of transients and accidents analyzed in Chapter 15 are in this category. Hence, the probability of a transient occurring before the operator takes corrective action would be extremely low.
- B. The operator would be immediately aware of a problem in the RPS because of scrams or half scrams, which are also annunciated.
- C. The remaining modes of mode switch misoperation would be detected during the weekly channel functional tests of the NMS channel inputs to the RPS. If these tests were performed prior to the power increase and after the transfer of the mode switch to the "STARTUP" position, the IRM channel functional tests would detect the failures because no half scram would result.

3. Surveillance Actions Necessary to Detect Mode Switch Misoperation

The proposed technical specification requirement is that the IRM channel functional test and the APRM channel functional test be performed within 24 hours prior to startup, if it has not been performed in the previous seven days. Also, weekly surveillance should be required when the "HOT STANDBY" condition has been maintained for long periods of time.

QUESTION 421.30 (SECTION 7.3)

Provide a detailed response to the concerns addressed by IE Bulletin 80-06 (Engineered Safety Feature (ESF) Reset Controls) issued to operating reactors March 13, 1980. For all safety-related equipment which does not remain in its emergency mode following an ESF reset, provide adequate justification for the change of state of each piece of equipment or proposed corrective actions to prevent such changes (e.g., equipment returning to its normal operational status).

RESPONSE

The HCGS non-NSSS ESF and EAS systems were evaluated against the concerns of IE Bulletin 80-06 and no discrepancies were identified.

Section 7.3.2.2 has been revised to include a statement addressing the concerns of IE Bulletin 80-06.

The response to NUREG-0737 Item II.E.4.2 in Section 1.10 provides additional information on this issue relating to primary containment isolation.

A review of current NSSS ESF system design documents for the HCGS identified the following ESF equipment as being capable of automatically returning to its normal (nonemergency), or pre-actuated condition subsequent to the disappearance of the trip-actuating signal(s), and the manual initiation of the associated system reset. This ESF equipment reset action appears to conflict with the intent of NRC's IE Bulletin No. 80-06, "ESF Reset Controls," issued to operating reactors March 13, 1980.

HCGS ESF equipment reset design conflicts with IE Bulletin 80-06 in the following areas:

B21-F013 A through E, Reactor Safety/Relief Valves (5 for ADS)

SV-4310 and SV-4311, Reactor Water Sample Valves, Inboard/Outboard

E11-F079, A/B RHR System Sample Line Isolation Valves, Inboard

E11-F080, A/B RHR System Sample Line Isolation Valves, Outboard

E41-F002 and F003, HPCI Turbine Steam Supply Isolation Valves, Inboard/Outboard

E41-F042, HPCI Pump Suction Valve from Suppression Chamber

E51-F031, RCIC Pump Suction Valve from Suppression Chamber

E51-F007 and F008, RCIC Turbine Steam Supply Isolation Valves, Inboard/Outboard

Although the initiation of an ADS reset returns the safety/relief valves B21-F013A through E to their closed position, this deliberate, predefined operator action to expeditiously close the relief valves and prevent or limit inadvertent reactor depressurization is considered an allowed exception to IE Bulletin 80-06 compliance.

Compliance of the remaining valves identified above, with the exception of the SRVs, with IE Bulletin 80-06 will be complete when the design modifications dictated by the resolution of TMI Item II.E.4.2 are complete. Modifications will be completed prior to fuel load.

*to these tie in with E 42
change to indicate to reflect
that mods will
confirm based on supplying modes
30a - HPII - open temporary*

QUESTION 421.32 (SECTION 7.3)

The information presented in FSAR Table 7.3-15, "Variable Monitored Applicability Matrix for System Actuated to Provide Protective Actions," is inconsistent with the system descriptions of FSAR Section 7.3. As an example, only three variables are shown as applicable to PCIS when according to the staff review, it should be five variables. Correct and update Table 7.3-15 so that it is consistent with the system descriptions.

RESPONSE

Table 7.3-15 has been revised to be consistent with Section 7.3 system descriptions.

Note 7 has been added to Table 7.3-15 identifying that manual initiations are not included in the table.

QUESTION 421.35 (SECTION 7.3)

Section 7.3.2.1.3 of the FSAR includes a discussion of how the Hope Creek design conforms to the recommendations of Reg. Guide 1.62. This discussion does not include the permissive logic. From the staff's review, it appears that the logic for manual initiation for several Engineered Safety Feature (ESF) systems is interlocked with permissive logic from various sensors. In some cases it appears that the permissive logic is dependent upon the same sensors as those used for automatic initiation of the system. It is the staff's position that the capability to manually initiate each safety system should be independent of permissive logic, sensors, and circuitry used for automatic initiation of that system. Identify each safety system at Hope Creek which is interlocked as described above and provide proposed modifications or justification for the existing design.

RESPONSE

Non-NSSS:

The HCGS non-NSSS ESF systems (as defined in Section 7.3.1) are as follows:

- a. Primary containment isolation system (PCIS)
- b. Containment atmosphere control system (CACS)
- c. Main control room habitability and isolation system (MCRHIS)
- d. Main steam isolation valve sealing system (MSIVSS)
- e. Filtration, recirculation, and ventilation system (FRVS)
- f. Reactor building ventilation isolation system (RBVIS).

Of these six systems, only the PCIS, MCRHIS, FRVS, and RBVIS are initiated automatically with the PCIS generating the initiation signals for the MCRHIS, FRVS, and RBVIS. Therefore, the PCIS is the only non-NSSS ESF system receiving automatic initiation signals (see Section 7.3.1.1.5 for a discussion of PCIS operation). Manual initiation at the system level has been provided for the PCIS which duplicates the actions of the automatic initiation signals. Manual initiation is not dependent on the automatic initiation signals.

Conformance to the six positions of Regulatory Guide 1.62 is as follows:

- a. Position 1 - means have been provided for manual initiation of the PCIS at the system level. Means have also been

provided for manual initiation at the component level for all components (valves, pumps) actuated by the PCIS, MCRHIS, FRVS, and RBVIS.

- b. Position 2 - manual initiation of the PCIS performs all actions performed by automatic initiation.
- c. Position 3 - the PCIS manual initiation switches are located on Section C of the operator's console in the main control room and are easily accessible to the operator. The switches are of the armed pushbutton type similar to those used for NSSSS manual initiation. The switch collar must be rotated to "arm" the pushbutton which may then be depressed to provide PCIS actuation. The arming feature prevents inadvertent actuation of the PCIS.
- d. Position 4 - the amount of equipment common to both manual and automatic initiation has been kept to a minimum. Equipment is common from the Bailey 862 logic modules, where the automatic and manual initiation signals are logically combined as shown on Figure 7.3-26, through the actuated devices. Manual initiation is not dependent on any permissive signal common with automatic initiation logic. No single failure within the manual, automatic, or common portions of a PCIS channel will prevent the manual or automatic initiation of the redundant PCIS channels. Further, the only single failure that could affect an entire PCIS channel on a system and component level basis would be a loss of the Class 1E power supply to that channel. More information on the Bailey 862 logic modules is provided in the response to Question 421.6.
- e. Position 5 - manual initiation of the PCIS at the system level requires the operation of a minimal amount of equipment as shown on Figure 7.3-26.
- f. Position 6 - manual initiation of the PCIS at the system level is designed such that once initiated, the protective action goes to completion in conformance with the requirements of Section 4.16 of IEEE Standard 279-1971.

NSSS:

a. ECCS

Each individual subsystem of the emergency core cooling systems (HPCI, ADS, Core Spray, and LPCI) has a provision for its own manual initiation. In addition, no single failure in the initiation portion of the network of systems will prevent manual or automatic initiation of redundant portions of the network.

1. HPCI

The HPCI system is initiated automatically by a LOCA signal (low reactor water level and/or high drywell pressure) or by a system-level remote manual switch. The subsystem can also be initiated by use of an individual remote manual switch for each valve including the turbine-driven pump. In all initiation modes, the system is prevented from operating by high water level (Level 8) using one-out-of-two-twice logic circuitry.

2. ADS

The ADS function is initiated automatically by a LOCA signal (low reactor water level and high drywell pressure) or by system-level remote manual switches. In either mode, the ADS valves are prevented from opening unless both pumps in either of the two core spray loops, or any of the four RHR pumps, are running. In addition, each individual ADS valve can be opened manually without restriction from permissive sensors.

3. LPCI and Core Spray

Low pressure coolant injection (LPCI), an operating mode of the residual heat removal (RHR) system, consists of four independent and redundant loops. Each loop contains a separate suction path from the suppression pool, a motor-driven pump, necessary control and instrumentation devices and valves, and a separate injection path that discharges directly into the reactor. Each loop is assigned to a separate electrical safety division. Logic and motive power for each division is supplied from safeguarded power sources within that division. Each safety division is fully separated (including instrumentation, controls, and power cables) from each of the other safety divisions as required by the HCGS electrical separation criteria. Each LPCI pump will supply 100% of the loop's design flow.

The following discussion describes the initiation and operation of the A LPCI loop only. The three remaining loops are initiated and operated similarly, and each loop is initiated and operated independently of the other loops. The A LPCI loop is automatically initiated when a LOCA condition (reactor vessel low level or containment high pressure coincident with reactor low pressure) exists. LPCI can be manually initiated from the control room by arming and depressing the loop initiation switch.

a LOCA condition (low reactor vessel level or high drywell pressure coincident with low reactor vessel pressure) exists. The A core spray loop can also be manually initiated by arming and depressing the A and C core spray initiation switches (B and D switches for the B loop).

Upon receipt of either the above loop initiation signals in their respective divisions of initiation logic, the A and C core spray pumps start automatically, the core spray test return lines to the suppression pool are automatically isolated, and a signal to open the inboard and outboard loop injection valves is initiated. However, the inboard and outboard injection valves are interlocked to prevent opening if reactor pressure is greater than the core spray piping-design maximum pressure (determined by monitoring reactor pressure) or if power is not available at the 4-kV bus to which the A core spray pump is connected.

When the 4-kV bus is energized and reactor pressure has decreased to below the core spray piping-design maximum pressure, the injection valves will automatically open.

Each of the components in the core spray flow path can also be manually operated from the control room by means of the component's individual control switch. Again, the injection valves are interlocked to prevent opening if reactor pressure is greater than core spray piping-design maximum pressure. The interlocks and control devices used in this manner are the same as those used for automatic operation.

Each loop of either core spray or LPCI in itself is not designed to sustain a single failure and still perform its design functions. Single failures such as loss of one division of safeguarded power, logic circuitry failure in one division, or an instrument failure in one division can disable one loop of core spray and/or one loop of LPCI, including the manual and automatic operation of these loops. For a design basis accident coincident with a worst case single failure, the most demanding and limiting scenarios for low-pressure ECCS are:

1. A pipe break that is not part of the low-pressure ECCS and a single diesel generator failure. Three LPCI loops and one core spray loop would remain.
2. A low-pressure ECCS pipe break and a single diesel generator failure. If the pipe break were in the core spray system, three LPCI loops would remain.

If the pipe break were in LPCI, one core spray loop and two LPCI loops would remain.

For either scenario, the remaining low-pressure ECCS loops are more than sufficient to satisfy the low-pressure coolant flow requirements to reactor.

The above scenarios are more demanding of the low-pressure ECCS than the failure of any one core spray or LPCI instrument. Hence, the consequences of a single core spray or LPCI instrument failure are bounded by the consequences for the above scenarios. Because the low-pressure ECCS is designed with sufficient redundancy and separation to perform its design functions with the worst-case single failure scenarios, no design changes are needed to reduce the consequences of a single failure of a core spray or LPCI instrument.

b. PCRVICS

There are no interlocks involved in manual operation of the PCRVICS.

c. Containment Spray Mode (RHR) and Suppression Pool Cooling Mode (RHR)

These two modes of the RHR system are only initiated manually (no automatic initiation).

d. CONCLUSION

Of the ESF systems, only the HPCI, ADS, CS, AND LPCI systems of the ECCS share permissive logic circuitry between the automatic and system-level manual initiation logic circuitries. The design is acceptable because the individual subsystems of the ECCS are not required to meet the single failure criterion. The ECCS function will be achieved with any one of its subsystems inoperative.

QUESTION 421.38 (SECTION 7.4)

Section 7.4.1.4 of the FSAR provides information on the Remote Shutdown System (RSS). Attachment 1 provides the Instrumentation and Control Systems Branch (ICSB) guidance for remote shutdown capability. The attachment provides guidance for meeting the requirements of GDC 19. Provide supplemental information to identify the extent that the design of the RSS at Hope Creek conforms to the guidance provided in Attachment 1. Include the following information in your discussion using drawings as appropriate:

- a) Design criteria for the remote control station equipment including the transfer switches and separation requirements for redundant functions.
- b) Discuss the separation arrangement between safety-related and nonsafety-related instrumentation and controls on the auxiliary shutdown panel.
- c) Location of transfer switches and the remote control stations.
- d) Description of isolation, separation and transfer/override provisions. This should include the design basis for preventing electrical interaction between the control room and remote shutdown equipment.
- e) Description of the administrative and procedural control features to both restrict and to assure access, when necessary, to the displays and controls located outside the control room.
- f) Description of any communication systems required to coordinate operator actions, including redundancy and separation.
- g) Means for ensuring that cold shutdown can be accomplished.
- h) Description of control room annunciation of remote control or override status of devices under local control.
- i) Discuss the proposed startup test program to demonstrate remote shutdown capability in accordance with the guidance provided in R.G. 1.68.2.
- j) Discuss the testing to be performed during plant operation to verify the capability of maintaining the plant in a safe shutdown condition from outside the control room.
- k) Discuss the equipment classification using the guidelines contained in FSAR Table 3.2-1.

RESPONSE

General - Section 7.4.1.4 has been revised to address the concerns of GDC 19 in accordance with the ICSB guidance provided as Attachment 1 to this question.

Specifically:

- a. See Section 7.4.1.4.3.
- b. See Section 7.4.1.4.3.7.
- c. The transfer switches are located on the remote shutdown panel (RSP). The RSP location is identified in Section 7.4.1.4.5.2. See also Table 7.4-2 and Figure 1.2-22.
- d. See Sections 7.4.1.4.5.3 and 7.4.2.4.4.
- e. Access to the RSP room is discussed in Section 7.4.1.4.5.2. Access to other instrumentation and controls which might be needed during a remote shutdown that are not located in the RSP room is controlled in accordance with plant administrative and security procedures established to allow access only to qualified operating personnel.
- f. See Section 9.5.2.2.4.
- g. See Sections 7.4.1.4.5.1 and 7.4.1.4.5.2.
- h. See Sections 7.4.1.4.5.2 and 7.4.1.4.5.3.
- i. Both the preoperational test program and the startup test program scheduled after fuel load follow the guidance of Regulatory Guide 1.68.2. The preoperational test program is discussed in Section 14.2.12.1.54 and the startup test program is discussed in Section 14.2.12.3.26. Additionally, responses to Questions 640.18 and 640.20, addressed in Amendment 2, provide additional clarification to remote shutdown system testing.
- j. Testing of the remote shutdown panel monitoring instrumentation (e.g., channel checks, channel calibration) will be performed using written procedures in accordance with the frequencies specified in the Hope Creek Technical Specifications.
- k. See part XV of Table 3.2-1.

421.38 ATTACHMENT 1
ICSB GUIDANCE FOR THE INTERPRETATION OF GENERAL DESIGN
CRITERIA 19 CONCERNING REQUIREMENTS
FOR REMOTE SHUTDOWN STATIONS

A. BACKGROUND

GDC 19 requires that equipment at appropriate locations outside the control room be provided to achieve a safe shutdown of the reactor. Recent reviews of remote shutdown station designs have demonstrated that some designs cannot accommodate a single failure in accordance with the guidance of SRP Section 7.4 (Interpretation of GDC-19). The following provides supplemental guidance for the implementation of the requirements of GDC-19 concerning remote shutdown stations. Requirements for remote shutdown capability following a fire are detailed in Appendix R to 10 CFR 50. It should be noted that although GDC 19 and Appendix R requirements are complementary, the potential exists that modifications to bring a design into conformance with GDC 19 will violate Appendix R criteria and vice versa. For example, remote manual devices for a second division of instrumentation and controls added to satisfy single failure requirements would not be acceptable if the added devices were located in the same fire area as existing transfer switches in the redundant division. In addition, transfer switches added to isolate the remote shutdown equipment from the control room fire area would not be acceptable if they disable ESF actuation, unless this is done in accordance with item B6 below. The acceptability of remote shutdown stations designs given a fire is determined by the Auxiliary Systems Branch (ASB) as outlined in Section 9.5.I of the SRP.

B. ICSB GUIDANCE

To Meet GDC-19 (As Interpreted In SRP Section 7.4)

- 1) The design should provide redundant safety grade capability to achieve and maintain hot shutdown from a location or locations remote from the control room, assuming no fire damage to any required systems and equipment and assuming no accident has occurred. The remote shutdown station equipment should be capable of maintaining functional operability under all service conditions postulated to occur (including abnormal environments such as loss of ventilation), but need not be environmentally qualified for accident conditions unless environmental qualification is required for reasons other than remote shutdown. The remote

- shutdown station equipment, including indicators, should be seismically qualified.
- 2) Redundant instrumentation (indicators) should be provided to display to the operator(s) at the remote shutdown location(s) those parameters which are relied upon to achieve and verify that a safe shutdown condition has been attained.
 - 3) Credit may be taken for manual actions (exclusive of continuous control) of systems from locations that are reasonably accessible from the Remote Shutdown Stations. Credit may not be taken for manual actions involving jumpering, rewiring, or disconnecting circuits.
 - 4) The design should provide redundant safety grade capability for attaining subsequent cold shutdown through the use of suitable procedures.
 - 5) Loss of offsite power should not negate shutdown capability from the remote shutdown stations. The design and procedures should be such that following activation of control from the remote shutdown location, a loss of offsite power will not result in subsequent overloading of essential buses or the diesel generator. Manual restoration of power to shutdown loads is acceptable provided that sufficient information is available such that it can be performed in a safe manner.
 - 6) The design should be such that if manual transfer of control to the remote location(s) disables any automatic actuation of ESF equipment, this equipment can be manually placed in service from the remote shutdown station(s). Transfer to the remote location(s) should not change the operating status of equipment.
 - 7) Where either access to the remote shutdown station(s) or the operation of equipment at the station(s) is dependent upon the use of keys (e.g., key lock switches) access to these keys shall be administratively controlled and shall not be precluded by the event necessitating evacuation of the control room.
 - 8) The design should comply with the requirements of Appendix R to 10 CFR 50.

QUESTION 421.39 (SECTION 7.4)

Section 7.4.1.1.2 of the FSAR provides a discussion regarding RCIC automatic suction source switchover from the condensate storage tank (CST) to the suppression pool yet FSAR Section 9.4 indicates that automatic switchover from the CST to the suppression pool is only provided for HPCI. Correct this discrepancy and provide a detailed discussion of the automatic switchover design including the independence between RCIC and HPCI and the precautions taken for the inoperability of these instruments due to cold weather.

RESPONSE

Automatic switchover of the HPCI/RCIC pump suctions is discussed in Section 9.2.6.5.1.

Section 9.2.6.5.1 has been revised to provide information on HPCI/RCIC pump-suction automatic switchover independence and cold weather design precautions and to show that CST low-low level indication has been provided at the remote shutdown panel (RSP).

Section 7.3.1.1.1.1 has been revised to include a reference to the HPCI valve logics.

Sections 5.4.6.1 and 7.4.1.1.2 have been revised to provide a description of the RCIC pump suction automatic switchover function.

Section 7.4.1.4.5.2 has been revised to clarify the description of the CST low-low level indication at the RSP and to clarify the requirements for manually shifting the RCIC pump suction when operating at the RSP.

revised to b
The only heat tracing installed on safety-related instrument sensing lines at HCGS for the purpose of protecting the sensing line from freezing in cold weather is that heat tracing installed on the level sensing line from the condensate storage tank to the reactor building. This heat tracing is powered from a highly reliable battery-backed non-1E power source and is equipped with an alarm monitoring circuit which detects loss of power to the heat tracing or loss of thermostat. The non-1E battery-backed power supply for the alarm circuit is separate from the heat tracing power supply. The sensing line will also be supplied with an RTD to monitor the temperature of the process fluid in the sensing line where the sensing line is exposed to the severe weather conditions. This temperature indication and associated alarm will be available in the main control room via the plant computer.

QUESTION 421.40 (SECTION 7.4)

Section 7.4.1.2.2 of the FSAR states that although the standby liquid control (SLC) system has been designed to a high degree of reliability with many safety system features, it is not required to meet the safety design requirements of the safety systems.

Recent BWR application (e.g., Shoreham and Perry) have indicated that all portions of the SLCS required for the injection of fluid including the switch used to initiate the system are safety-related and the heaters, indicator lights and alarms are not safety-related.

Considering the information provided above, discuss in detail the design criteria and classification of the SLC system in your design. The discussion should include separation between redundant portions of the SLCS.

RESPONSE

The standby liquid control (SLC) system is an independent backup system for the control rod drive system. The SLC system is capable of shutting down the reactor from a full power condition, and maintaining it subcritical until the cold shutdown condition is achieved, without control rod movement. The SLC system is not required to scram the reactor or to operate when the reactor has been shut down by the control rod drive system. In the event of an ATWS, injection of the sodium pentaborate solution can be initiated manually by the operator or it is initiated automatically by the redundant reactivity control system (RRCS). The SLC system is not designed for use as a safety system because of the large number of independent control rods available to shutdown the reactor which provide adequate redundancy. See Sections 9.3.5 and 15.8 for additional system information not contained in Chapter 7.

While the injection portions of the SLC system have been designed electrically as a Class 1E, redundant system, certain safety system design bases are not required and have not been incorporated in the design (e.g., there is no system level redundancy; that is, there is only one tank and one injection point and the heaters are nonredundant and are not Class 1E). The controls and instrumentation required to perform the injection function are redundant and the logic circuitry and instrumentation are separated into Channels A and B so that the failure of any single electrical component will not prevent injection. The injection logic circuitry including the initiation switches, pumps, and squib valves as well as inputs from RRCS are redundant, Class 1E, and electrically and physically separated. Details of the electrical design are contained on the SLC system elementary diagram (791E409AC).

QUESTION 421.42 (SECTION 7.5)

If reactor controls and vital instruments derive power from common electrical distribution systems, the failure of such electrical distribution systems may result in an event requiring operator action concurrent with failure of important instrumentation upon which these operator actions should be based. IE Bulletin 79-27 addresses several concerns related to the above subject. You are requested to provide information and a discussion based on each IE Bulletin 79-27 concern. Also, you are to:

- 1) Confirm that all a.c. and d.c. instrument buses that could affect the ability to achieve a cold shutdown condition were reviewed. Identify these buses.
- 2) Confirm that all instrumentation and controls required by emergency shutdown procedures were considered in review. Identify these instruments and controls at the system level of detail.
- 3) Confirm that clear, simple unambiguous annunciation of loss of power is provided in the control room for each bus addressed in item 1 above. Identify any exceptions.
- 4) Confirm that the effect of loss of power to each load on each bus identified in item 1 above including ability to reach cold shutdown, was considered in the review.
- 5) Confirm that the re-review of IE Circular No. 79-02 which is required by Action Item 3 of Bulletin 79-27 was extended to include both Class 1E and non-Class 1E inverter supplied instrument or control buses. Identify these buses or confirm that they are included in the listing required by Item 1 above.

RESPONSE

*would follow
Limerick
Limerick approved*

An analysis will be conducted based on the General Electric methodology for answering the concerns raised in IE Bulletin 79-27. This methodology has been reviewed and approved by the NRC via a report written for the ~~WNEC~~ project. The methodology provides for a systematic and comprehensive analysis to ensure that, in the event of a single power bus failure, sufficient control room indicators, instruments, and controls exist to achieve a cold shutdown.

An outline of the methodology follows:

1. Review the Class 1E and non-Class 1E busses including inverters supplying power to instrumentation and controls in

systems used in attaining the cold shutdown condition. Identify busses that could affect the ability to achieve cold shutdown. Use plant operating procedures and procedures developed for certain power bus failures to ensure the identification of all critical power busses.

2. Identify the instrumentation and control devices connected to each identified power bus. Evaluate the effects of a loss of power to each load, including the limiting effects on the ability to achieve cold shutdown.
3. Create bus trees denoting the bus hierarchy and the cascading bus configuration of all busses that power instrumentation and controls the operator would manipulate in going to cold shutdown.
4. Determine the annunciators and alarms that would alert the operator to a failure of any of the identified busses.
5. Determine the effects of any single power bus loss on the ability to continue in each particular shutdown path being used at the time the bus loss occurs. Include the cascading effects of any bus loss, and consider alternate indications and controls powered by unaffected busses that may aid the operator in the event of a bus loss. Identify alternative shutdown paths available and existing procedures for restoration of the affected bus.
6. Document the results of the analysis, providing recommendations of hardware or procedural changes as appropriate.

The programs described in the responses to this question and to Questions 421.51 and 421.52 will be conducted as a combined effort that will be completed by December, 1984.

QUESTION 421.49 (SECTION 7.7)*Owner's table*

Describe the installation, operation, and removal of the "star trek" computer system which is used for start-up testing of GE, BWR 4s. Include the following topics:

- (1) Specifications of and Qualification of electrical isolators.
- (2) Separation criteria for permanent and temporary wiring.

RESPONSE

Section 7.5.1.3.5 has been added to describe the HCGS startup and transient monitoring system (GETARS I). This description includes the requested information.

QUESTION 421.51 (SECTION 7.7)

The transient and accident analyses included in the FSAR are intended to demonstrate the adequacy of safety systems in mitigating anticipated operational occurrences and accidents.

Based on the conservative assumptions made in defining these "design bases" events and the detailed review of the analyses by the staff, it is likely that they adequately bound the consequences of single control system failures. To provide assurance that the design basis event analysis for Hope Creek adequately bounds other more fundamental credible failures, provide the following:

- (1) Identify those control systems whose failure or malfunction could seriously impact plant safety.
- (2) Indicate which, if any, of the control systems identified in (1) receive power from common power sources. The power sources considered should include all power sources whose failure or malfunction could lead to failure or malfunction of more than one control system and should extend to the effects of cascading power losses due to the failure of higher level distribution panels and load centers.
- (3) Indicate which, if any, of the control system identified in (1) receive input signals from common sensors. The sensors considered should include common taps, hydraulic headers and impulse lines feeding pressure, temperature, level or other signals to two or more control systems.
- (4) Provide justification that any malfunctions of the control systems identified in (2) and (3) resulting from failures or malfunctions of the applicable common power source or sensor including hydraulic components are bounded by the analyses in Chapter 15 and would not require action or response beyond the capability of operators or safety systems.

RESPONSE

An analysis will be conducted based on the General Electric methodology for answering NRC concerns for common power source failures and common sensor or sensing line failures. This methodology, which received NRC concurrence via reports for the Grand Gulf, Shoreham, and WNP-2 projects, will be used for the Hope Creek project. The methodology is systematic and comprehensive and examines control systems interactions to establish the limiting-case events. The consequences of single power-source or sensing-line failures will be evaluated with respect to control-grade systems and will ensure the limiting-case events are bounded by the events analyzed in Chapter 15.

systems and working up each bus tree to the highest common power level. At each level examine the effects the single bus failure and the consequences of cascading bus failures on all control systems' components.

- 5. Postulate the limiting transient events as a result of the combined effects analysis and compare these events to those analyzed in Chapter 15.

- 6. Perform ~~any~~ additional transient calculations ^{that the worst case limiting event is} or analyses necessary to ensure [^] ~~the postulated limiting events are~~ bounded* by those analyzed in Chapter 15 with the assumption there is a single active failure in a safety system required to mitigate effects of the event.

Handwritten notes:
 - ~~Control System~~
 - ~~System~~
 - ~~Hit~~

- 7. Document the results of the analyses of common power source failure, providing recommendations as appropriate.

QUESTION 421.52 (SECTION 7.7)

If control systems are exposed to the environmental resulting from the rupture of reactor coolant lines, steam lines, or feedwater lines, the control systems may malfunction in a manner which would cause consequences to be more severe than assumed in safety analyses. I&E Information Notice 79-22 discusses certain non-safety grade control equipment, which if subjected to the adverse environment of a high energy line break, could impact the safety analyses and the adequacy of the protection functions performed by the safety-related systems.

The staff is concerned that a similar potential may exist at light water facilities now under construction. You are, therefore, requested to perform a review per the I&E Information Notice 79-22 concern to determine what, if any, design changes or operator actions would be necessary to assure that high energy line breaks will not cause control system failures to complicate the event beyond the FSAR analyses. Provide the results of your review including all identified problems and the manner in which you have resolved them.

The specific "scenarios" discussed in the above referenced Information Notice are to be considered as examples of the kinds of interactions which might occur. Your review should consider analogous interactions as relevant to the BWR design.

RESPONSE

An analysis will be conducted based on the General Electric methodology for answering the concerns raised in IE Information Notice 79-22. The NRC has concurred with this methodology via its review prepared for the Shoreham and Grand Gulf projects. The methodology assures a systematic, comprehensive analysis of high-energy line breaks and the consequential control systems failures. An outline of this methodology follows:

1. Identify all nonsafety control-grade systems and components within these systems whose failure could affect the critical reactor parameters of water level, pressure, and power.
2. Establish assumptions and criteria for determining high-energy lines and pipe break locations and for evaluating the consequences of pipe breaks. Pipe whip, jet impingement, and environmental parameters such as high temperature, high pressure, and high humidity will be considered in the analysis.
3. Identify from appropriate plant drawings those plant locations in which high-energy lines with postulated break

locations coexist with nonsafety components of control-grade systems.

4. Conduct a plant walkdown to verify the locations of control system components and to determine their proximity to high-energy line break locations.
5. Examine, one at a time, high-energy line breaks and establish the worst-case combined effects of each break and the consequential control-system failures.
6. Ensure that the consequences of those pipe-break events are bounded by those of the events analyzed in Chapter 15.
7. Choose two or more of the worst-case scenarios and postulate for each a worst-case additional failure in a safety-related, mitigating system. Ensure that the consequences of these new events do not fall outside the bounds of the capabilities of safety systems or the consequences of the events analyzed in Chapter 15.
8. Document the results of the analysis of the interactions between high-energy line breaks and control systems and recommend actions to be taken as appropriate.

The programs described in the responses to this question and to Questions 421.42 and 421.51 will be conducted as a combined effort that will be completed by December 1984.

QUESTION 421.54 (SECTION 7.7)

Table 7.1-1 of the FSAR lists the safety-related instrumentation and control systems. Nonsafety-related systems are identified in Table 7.7-1. From a review of Chapter 15 of the FSAR the staff has determined that the analysis of certain anticipated operational occurrences (i.e., the feedwater controller failure-maximum demand) and design basis accidents (i.e., recirculation pump seizure) take credit for the operation of nonsafety-related instrumentation and control systems. It is the staff's position that for events classified as anticipated operational occurrences, credit can be taken for nonsafety-related systems to mitigate the event provided only high availability nonsafety-related systems are being relied upon. Therefore, identify each instrumentation and control system/component which is not classified as safety-related but assumed in the FSAR analysed to mitigate the consequences of transients. Provide a justification for the assumption of operability of this equipment based upon system design, equipment quality, and proposed technical specifications. In addition, provide a discussion on the interfaces with the safety-related portions of the Hope Creek design.

It is the staff's position that no credit may be taken for nonsafety-related instrumentation and control systems/components in mitigating the consequences of design bases accidents. Therefore, identify each instrumentation and control system/component which is classified as nonsafety-related but assumed in the FSAR analyses to mitigate the consequences of accidents. Either redo the analysis assuming no credit for the operation of this equipment, or propose modifications to upgrade the equipment to safety-related status.

RESPONSE

The following nonsafety-grade systems/components may be actuated during the course of anticipated operational occurrences (transients) shown in Chapter 15:

- a. Level 8 turbine trip
- b. Level 8 feedwater trip
- c. Turbine bypass
- d. Recirculation runback
- e. Rod sequence control system
- f. Rod block monitor

- g. The relief function of the safety relief valves.

None of these systems are required to mitigate the accidents discussed in Chapter 15.

Table 440.33-1 provided in response to Question 440.33 lists transients where nonsafety-grade systems/components are actuated during the course of the event. The analyses for each of the transients are based on the single-failure criterion associated with the abnormal transients (abnormal transients are defined as events that occur as a result of equipment malfunctions as a result of a single active component failure or operator error). Following this single failure, the resulting transient is simulated in a conservative fashion to show the response of primary system variables and how the various plant systems would interact and function.

Although the analyses of certain transient events assume the operation of specific nonsafety-grade equipment to provide a realistic transient signature, failures of such equipment would not make these events more thermally or pressure limiting than the limiting accidents already addressed in Chapter 15. Periodic testing is prescribed by the NRC's Standard Technical Specifications for Level 8 turbine trip, Level 8 feedwater trip, turbine bypass, the rod sequence control system, the rod block monitor, and the relief function of the safety relief valves.

Meeting Summary Distribution

Docket File

NRC PDR
Local PDR
PRC System
NSIC
LB#2 Reading
Attorney, OELD
A. Schwencer
D. Wagner
E. Hylton
J. Mauck
J. Calvo

RHartfield (Caseload Forecast Panel Visits)
OPA (Caseload Forecast Panel Visits)

NRC Participants

J. Mauck
J. Calvo
A. Schwencer
D. Wagner

bcc: Applicant & Service List