

Docket file



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

February 18, 1992

Docket No. 50-605

APPLICANT: General Electric Company (GE)  
PROJECT: Advanced Boiling Water Reactor (ABWR)  
SUBJECT: SUMMARY OF MEETING HELD ON NOVEMBER 20 AND 21, 1991

On November 20 and 21, 1991, members of the Nuclear Regulatory Commission (NRC) staff met with General Electric Company (GE) representatives at GE's offices in San Jose, California. The purpose of the meeting was to discuss open items from the staff's review of the Advanced Boiling Water Reactor (ABWR) Standard Safety Analysis Report (SSAR). Enclosure 1 is a list of the attendees, Enclosure 2 is the meeting agenda, and Enclosure 3 was used as a handout during the discussions.

The following is a list of the discussion topics and actions assigned as a result of the meeting:

(1) Thermal Hydraulic Stability Question - GE will submit to the staff their formal response to this issue by December 6, 1991.

(2) Control Rod Design - GE indicated that they would have difficulty providing a representative control rod design for the ABWR. GE will coordinate with the staff to schedule a follow-up meeting at NRC hearing rooms to discuss this issue.

(3) SLCS System - GE will submit to the staff an amendment to the ABWR SSAR which indicates that the SLCS design incorporates automatic initiation.

(4) Reactor Core Isolation Cooling (RCIC) System - GE stated that the information in SSAR Section 5.4.6.1 which indicates that the RCIC is designed to accommodate a loss of AC power for 30 minutes, will be corrected to indicate 8 hours. GE will also provide information to demonstrate that 8 hours is acceptable.

(5) Residual Heat Removal (RHR) System - GE indicated that they would revise SSAR Section 5.4.7.1.3 to adequately address RSB 5-1 of SRP 5.4.7 regarding the design of relief valves in discharge piping. GE discussed the design features of the RHR system including a methodology to address the Intersystem Loss Of Coolant Accident (ISLOCA) concerns described in

DFD  
11

February 18, 1992

SECY-90-016. The staff indicated that GE's methodology, if systematically applied to ABWR piping designs, should adequately address the staff's ISLOCA concerns. GE indicated that it would submit to the staff a comprehensive ISLOCA assessment of the ABWR design.

(6) Automatic Depressurization System (ADS) Timer - GE indicated that the 29 seconds reflects the Diesel Generator start, loading and emergency core cooling system (ECCS) start and valve opening time. The time delay also prevents pump spurious actuation of ADS. This time is not for operator action to inhibit ADS but is included as an improvement for normal sequencing. The staff indicated that GE should develop an ITAAC to ensure that the 29 second time setting is incorporated into the design.

(7) Automatic Depressurization System (ADS) - GE stated that their initial response to the staff's question regarding the efficacy of the ADS was to include an additional high pressure core makeup system. GE stated that in addition, the ADS logic would be modified to include an 8 minute bypass timer, similar to current BWR-6 designs. This change would result in ADS actuation if low vessel water level were to exist for greater than 8 minutes. The staff requested that GE submit the proposed ADS design changes and include design calculations to support the ADS logic modification. The staff also requested that GE ensure that the ABWR probabilistic risk assessment incorporates the failure of the redundant (3) high pressure core makeup systems in sequences which result in challenges to ADS.

(8) REDYA and ODYNA Codes - GE and the staff agreed to coordinate a date and agenda to facilitate an audit of these codes by the staff. Tentative audit dates of January 12-13, 1992, were established.

(9) Loss of Feedwater Heater Transient - GE stated that the ABWR design requirement limiting feedwater temperature drop to 100°F for transients is conservative. In support of its position, GE presented a heat balance for the steam and power conversion. The staff indicated that it would consider GE's response to this issue and determine the acceptability of the heat balance relative to the proposed limit on feedwater temperature.

(10) Limiting Fault Events - GE informed the staff that the Inadvertent RHR Shutdown Cooling Operation and Failure to Initiate RHR Shutdown Cooling events have been reanalyzed as moderate frequency rather than limiting fault events. GE restated its claim that the Pressure Regulator Downscale Failure and Trip of All Reactor Internal Pumps events should be considered limiting fault events. With regard to the failure of all RIPs, GE indicated that SSAR Appendix 15C was submitted to show that the event is a low probability event.

(11) Credit for Non-Safety Grade Equipment - The staff indicated that a strict interpretation of the General Design Criteria would result in no credit being given for non-safety systems mitigation of events. Further

February 18, 1992

discussions led to a revised staff position that GE should provide additional information and justification in the SSAR for the credit being sought for non-safety systems.

(12) Rod Block Monitor (RBM) Algorithm - GE discussed this issue using the enclosed handout. The information appeared to provide a detailed explanation of terms and methodology for the RBM algorithm. The staff requested that GE formally submit this information for staff review.

(13) Slow Turbine Control Valve Closure Event - GE stated that it would provide information to the staff which indicates that this event is bounded by the "fast-closure" of turbine control valve event.

(14) ARI, RPT and SLCS Design - GE indicated that to mitigate the effects of an anticipated transient without scram (ATWS), the reactor internal pump logic would be modified to cause the pumps to run-back upon receipt of an ATWS signal. The staff reiterated that it requires GE to submit its ATWS analysis (SSAR Chapter 15E) to complete its review. In addition, the staff noted that it requires GE to submit its response to instrumentation and controls (SSAR Chapter 7) open issues to complete its integrated assessment of ARI, RPT and SLCS which will be included in FSER Section 15.8.

(15) Shutdown Risk (SDR) - GE expressed concern that the scope of information required by the staff to address SDR for the ABWR was inconsistent. GE reviewed the design features selected to reduce the risk to the ABWR design during shutdown and presented the areas it planned to incorporate into the ABWR SDR assessment. The staff questioned whether GE's approach would produce a comprehensive identification of shutdown vulnerabilities. The staff also informed GE that the Grand Gulf SDR assessment would not be sufficiently complete to be useful in GE's assessment of risk for the ABWR.

(16) Capability of RHR Systems to mitigate ATWS - This issue deals with the number of RHR heat exchangers necessary to remove containment heat loads in the event of an ATWS without boron injection. GE stated that an ATWS event with no boron injection is a seriously degraded and beyond design basis event. GE indicated that it is extremely unlikely that containment design pressure level would be reached since the time required to reach the containment design pressure limit is sufficient for alternate insertion of boron. GE also indicated that it would formally submit a response to the staff for review.

(17) Loss-of-Coolant Accident (LOCA) in Reactor Water Cleanup (RWCU) System - GE stated that a 2-inch RWCU System line break is bounding. This is based upon the diameter of the opening in the reactor-vessel lower head connected to the RWCU system line. GE indicated that a break of this line is considered in the LOCA analysis and that a response to the staff's concerns will be formally submitted for review.

February 18, 1992

(18) Accident Management - The staff outlined the information required from GE to adequately address this issue as part of severe accident closure for the ABWR. There was general agreement on the scope and purpose of information needed to address the concerns described in SECY-89-012. The staff and GE also agreed to include this issue as an agenda item for the next NRC/GE management meeting.

Original Signed By:

Victor M. McCree, Project Manager  
Standardization Project Directorate  
Division of Advanced Reactors  
and Special Projects  
Office of Nuclear Reactor Regulation

Enclosures:  
As stated

cc w/enclosures:  
See next page

DISTRIBUTION:

Docket File	PDST R/F	DCrutchfield	WTravers
NRC PDR	CPoslusny	VMcCree	TMurley/FMiraglia
RNease	JNWilson	RPierson	TBoyce
RBorchardt	FHasselberg	THiltz	TKenyon
MMalloy	SStein	GGrant, EDO	PShea
TWambach	JHWilson	JMoore, 15B18	EJordan, MNBB3701
ACRS (10)	LShao, NLO07	RBosnak, NLO07	JOBrien, NL271A
ZRosztoczy, NLS169	BSheron, RES	JMurphy, NLS007	BHardin, NLS169
RVan Houten, SECY	JLyons	WBeckner	JKudrick
AD'Angelo	AEL-Bassioni	RPalla	GKelly
CMcCracken			

OFC:	LA:PDST:DAR	PM:PDST:DAR	SC:PDST:DAR
NAME:	PShea:tz	VMcCree	JNWilson
DATE:	02/14/92	02/17/92	02/18/92

OFFICIAL DOCUMENT COPY: RSBMTGSU.VM

General Electric Company

Docket No. STN 50-605

cc: Mr. Patrick W. Marriott, Manager  
Licensing & Consulting Services  
GE Nuclear Energy  
175 Curtner Avenue  
San Jose, California 95125

Mr. Robert Mitchell  
General Electric Company  
175 Curtner Avenue  
San Jose, California 95114

Mr. L. Gifford, Program Manager  
Regulatory Programs  
GE Nuclear Energy  
12300 Twinbrook Parkway  
Suite 315  
Rockville, Maryland 20852

Director, Criteria & Standards Division  
Office of Radiation Programs  
U. S. Environmental Protection Agency  
401 M Street, S.W.  
Washington, D.C. 20460

Mr. Daniel F. Giessing  
U. S. Department of Energy  
NE-42  
Washington, D.C. 20585

Mr. Steve Goldberg  
Budget Examiner  
725 17th Street, N.W.  
Room 8002  
Washington, D.C. 20503

Mr. Frank A. Ross  
U. S. Department of Energy, NE-42  
Office of LWR Safety and Technology  
19901 Germantown Road  
Germantown, Maryland 20874

Mr. Raymond Ng  
1776 Eye Street, N.W.  
Suite 300  
Washington, D.C. 20006

## ATTENDEES

## MEETING WITH GENERAL ELECTRIC

November 20-21, 1991

<u>NAME</u>	<u>ORGANIZATION</u>
J. E. Lyons	NRR/DST/SPLB
V. M. McCree	NRR/DAR/PDST
W. Beckner	NRR/DREP/PRAB
J. Kudrick	NRR/DST/PRAB
A. D'Angelo	NRR/DST/PRAB
A. El-Bassioni	NRR/DREP/PRAB
R. Youngblood	BNL
T. Pratt	BNL
R. Palla	NRR/DREP/PRAB
G. Kelly	NRR/DREP/PRAB
J. Gabor	Gabor, Kenton & Assoc./ARSAP
C. Buchholz	GE
C. McCracken	NRR/SPLB

**GE Meeting with NRC Reactor Systems Branch  
ABWR Open Items  
San Jose**

8:30 AM - 5:00 PM  
Building J, Room 1010

Questions	GE Representative	Duration
<b>Wednesday, November 20</b>		
(6) ADS timer	FM Paradiso	8:30-9:30
(7) ADS System		
(17) LOCA in RWCU System		
(19) Accident management	PD Knecht JF Quirk	9:30-10:30
<b>Break</b>		
(18) Emergency Procedure Guidelines	CK Tang CE Buchholz	10:45-11:30
(16) Capability of RCIC/RHR System to mitigate ATWS	CE Buchholz	11:30-12:00
<b>Lunch - GE Cafeteria</b>		
(8) REDYA and ODYNA codes	RW Schrum P. Huang	1:00-1:45
(4) RCIC System	EV Nazareno	1:45-2:30
<b>Break</b>		
(11) Credit for Non-Safety Grade Equipment Topics from Thursday as needed	CD Sawyer RL Huang	2:45-3:30 3:30-5:00
<b>Thursday, November 21</b>		
(2) Control Rod Design	JS Charnley	8:30-9:00
(5) RHR System	WE Taft	9:00-9:30
<b>Break</b>		
(15) Shutdown Risk	Vishu Visweswaran	9:45-10:30
(1) Thermal Hydraulic Stability	RL Huang	10:30-12:00
(3) SLCS System		
<b>Lunch - GE Cafeteria</b>		
(9) Loss of FW Heater Transient	RL Huang	1:00 - 2:30
(10) Limiting Fault Events		
<b>Break</b>		
(12) Rod Block Monitor Algorithm	RL Huang / FC Chao	2:45 - 3:30
(13) Slow Turbine Control Valve Closure Event	RL Huang	3:30 - 5:00
(14) ARI, RPT and SLCS Design		

## NRC Reactor Systems Branch - ABWR Open Items

GE Responsibility

Topic

RL Huang

### (1) Thermal Hydraulic Stability Question

We have had no response as yet on the staff question on thermal-hydraulic stability, in which we asked for a review of the ABWR instability protection system in light of the improved understanding of the problem area developed over the past several years by GE and the BWROG, and the developments in "long term solution" methods and methodologies. An initial attempt at a telephone discussion was cancelled several months ago and no interaction or response to the question has since been indicated.

JS Charnley

### (2) Control Rod Design

There has been an open item in the staff review of the ABWR control rod design. GE has proposed a set of design criteria (presented in SSAR Appendix 4C) for the ABWR control rod similar to those proposed (for GESTAR II) for current BWRs. These criteria are similar in nature to those approved (and accepted for GESTAR II) by the staff for new fuel designs for current reactors (with a parallel set approved for the ABWR). However, the staff has not reviewed the control rod criteria for current BWRs and there is, therefore, currently no basis for review of a similar set for the ABWR. This situation is not likely to change in the near future since the staff currently believes the design criteria path is not suitable for control rod review. We have heard nothing from GE on this subject, and GE may not be aware of the likely permanent nature of the criteria rejection. We believe they should remove it from the SSAR and replace it by referencing a representative design similar to one currently accepted for current BWRs (suitably modified for the ABWR, e.g., no velocity limiter).

RL Huang

### (3) SLCS System

The SSAR indicates that SLCS is started manually rather than automatically as required by ATWS Rule 10 CFR 50.62 for new plants. GE has informally indicated that the SLCS design will be modified for automatic SLCS initiation. GE needs to docket this design change in a supplement to the SSAR (4.6, 9.3.5).

EV Nazareno

### (4) RCIC System

In SSAR Section 5.4.6.1 design basis, it is stated that RCIC is designed for loss of AC power of 30 minutes only. This statement should be revised to address the staff position that the RCIC System must perform its function without the availability of any AC power for a reasonable time (5.4.6).



## NRC Reactor Systems Branch - ABWR Open Items

GE Responsibility

Topic

WE Taft

### (5) RHR System

GE response to the staff questions sent on September 6, 1991 is required. RHR system design should be assessed relative to the Generic Issue 105 "Interface LOCA", compliance with SECY 90-016. The RHR relief system design should be assessed relative to RSB 5-1 position.

FM Paradiso

### (6) ADS timer

The staff requires that GE justify the adequacy of the 29 second time setting with regard to human factors (6.3). The ADS timer is set at 29 seconds rather than 120 seconds for current operating BWRs. 29 seconds is a very short time for operator intervention to prevent ADS.

FM Paradiso

### (7) ADS System

GE should demonstrate that high drywell pressure will be present for all situations requiring ADS or provide modifications to ADS required by TMI action item II.K.3.18 (6.3).

RW Schrum  
RL Huang

### (8) REDYA and ODYNA codes

These transient analysis codes are under staff review. NRC, with support from BNL, will audit GE's changes to these codes for modeling ABWR transients (15).

RL Huang

### (9) Loss of FW Heater Transient

For this transient, GE assumed 100°F (55.6°C) drop in feedwater temperature. However, a drop of 150°F has occurred at a domestic Boiling Water Reactor. The staff requires that GE analyze the transient for 150°F drop of feedwater temperature, or provide justification on their choice of limiting temperature drop (15).

RL Huang

### (10) Limiting Fault Events

GE analyzed the following as limiting fault events rather than moderate frequency events, as specified in the SRP: Inadvertent RHR Shutdown Cooling Operation; Failure to RHR Shutdown Cooling; and Pressure Regulatory Downscale failure and trip of all reactor internal pumps. This is a significant deviation from SRP guidance. The staff requires that GE provide a detailed justification to support the frequency attributed to these events (15).

## NRC Reactor Systems Branch - ABWR Open Items

GE Responsibility

Topic

CD Sawyer

### (11) Credit for Non-Safety Grade Equipment

In response to staff questions regarding credit given to non-safety grade equipment in safety analysis, GE responded that credit was given in their analyses for some equipment which is not safety grade. The most important of these are the turbine bypass valves, and recirculation pump trip on load/turbine trip. GDCs 1-4 requires that components important to safety shall be designed to quality standards etc. and GDC-21 requires that the protection system shall be designed for high functional reliability. GE should provide appropriate transient and accident evaluations, only taking credit for response of safety grade components and systems (15).

RL Huang  
FC Chao

### (12) Rod Block Monitor Algorithm

From the November 7, 1991 letter from GE to R. Pierson, "GE Response to GE/NRC Reactor System Branch Conference Call of September 6, 1991."

The proposed "Insert A" for Discussion Item 7, RBM algorithms, provides a reasonable "summary description" of the calculational algorithm, suitable for insertion in the SSAR. However, an expanded, detailed explanation of several of the terms in the algorithm is needed to provide a clearer understanding of the methodology for the staff review. This includes "A<sub>0</sub>" from formula 1, and "B(X), M<sub>p</sub>, and MAPRAT<sub>i</sub>(X)" from formula 2. In particular, an explanation of "known function" for these parameters and a definition of "margin factor" is required. This information can be provided in a letter rather than as part of the SSAR.

RL Huang

### (13) Slow Turbine Control Valve Closure Event

A slow turbine control valve closure causes a slow increase in reactor pressure with a corresponding slow increase in neutron flux. The reactor scram could be delayed until the high pressure scram setpoint is reached. A large increase in surface heat flux could result in large change in CPR. We require GE to analyze the slow control valve closure event for ABWR, or show that it is bounded by another moderate frequency event (15).

RL Huang

### (14) ARI, RPT and SLCS Design

Adequacy of ARI, RPT and SLCS design relative to compliance with ATWS Rule 10 CFR 50.62 (15.8).

Vishu  
Visweswaran

### (15) Shutdown Risk

The staff sent questions to GE on September 11, 1991. GE should provide a response to these questions.

## NRC Reactor Systems Branch - ABWR Open Items

GE Responsibility

Topic

CE Buchholz

### (16) Capability of RCIC/RHR Systems to mitigate ATWS

During the GE presentation to the staff on ABWR PRA on August 6, 1991, GE referred to an INEL analysis which showed that RCIC was capable of preventing core damage. INEL performed the analysis of a high pressure ATWS with very low makeup flow to support GE's PRA assessment of the ABWR during degraded conditions. (Ref. DOE/ID 10211, October 1988.) The conclusion of the analysis was that based upon a constant vessel superheat of 175 K, the equivalent of 3.45 heat exchangers are necessary to keep the peak containment pressure below the design pressure. Confirm that the three heat exchangers as presently designed having sufficient heat removal capacity to mitigate ATWS.

FM Paradiso

### (17) LOCA in RWCU System

During the ACRS subcommittee meeting on September 18, 1991, Dr. Michelson requested the staff to confirm that the Reactor Water Clean-up System suction line from the reactor bottom is covered in the LOCA analysis. The reactor water clean-up system suction line (from the reactor bottom) pipe size is about 3-1/2 inches and not 2 inches as originally designed. Confirm that the cleanup pipe break is considered in the LOCA analysis. Which break size considered in the LOCA analysis bounds the cleanup pipe break?

CK Tang  
CE Buchholz

### (18) Emergency Procedure Guidelines

(Conference call to Containment Systems Branch). Requirements for shutdown EPGs. Chapter 18A EPGs.

PD Knecht  
JF Quirk

### (19) Accident management

Defined in SECY-89-012, involves actions taken by plant staff to:

- (1) prevent core damage,
- (2) terminate progress of core damage and retain the core within the vessel,
- (3) maintain containment integrity, and
- (4) minimize offsite release.

A comprehensive accident management plan is an important element for severe accident closure on the ABWR design. The staff would expect to review a detailed accident management plan as part of the first COL review for an ABWR application. Prior to completion of our design review, please provide GE's planned approach and strategy for assuring that each of the five elements of accident management defined in SECY-89-012 will be appropriately addressed by the vendor/licensee. Identify the respective responsibilities of GE and of the licensee for addressing each of the elements and projected schedules, and any methods and/or guidance that are expected to be used in this process.

## NRC Reactor Systems Branch - ABWR Open Items

GE Responsibility

Topic

---

(e.g., the "Process for Evaluating Accident Management Capabilities" developed by NUMARC, the "Severe Accident Management Guidance Technical Basis Report" developed by EPRI, or the accident management guidelines now under development by each of the reactor vendors as part of the industry Accident Management Program).

### ATWS without Boron Injection

---

**Issue:** INEL Report DOE/ID10211 interpreted as showing that 3.45 heat exchangers are necessary to remove heat from the containment during an ATWS event with no boron injection.

INEL analysis indicates that:

- 3.45 heat exchangers are needed to maintain containment pressure below design limit.
- 3 heat exchangers limits containment pressure to 72 psig.
- With 3 heat exchangers containment pressure will not exceed design for almost 6 hours.

CEB-1  
11/20/91

### ATWS Without Boron Injection (continued)

---

GE position:

- This event is a seriously degraded event - well beyond the design basis
- Success criteria for the PRA use realistic limits rather than licensing or design basis limits
- Peak pressure predicted using three heat exchangers is below service level C
- Further, time until design level is reached is adequate for the alternate insertion of boron, so it is extremely unlikely that even the design limit will be reached

Three heat exchangers have  
adequate heat removal capacity to  
mitigate ATWS

CEB-2  
11/20/91

ABWR SHUTDOWN RISK

PRESENTED TO NRC

OCTOBER 9, 1991

S. VISWESWARAN

GENERAL ELECTRIC NUCLEAR ENERGY

SAN JOSE, CALIFORNIA

## ABWR SHUTDOWN RISK

### NRC ISSUES

1. DESIGN FEATURES WHICH MINIMIZE RISK
2. DETAILED SHUTDOWN RISK ASSESSMENT

# ABWR SHUTDOWN RISK

## DESIGN FEATURES

### 1. ISSJE:

- A) DESIGN MODIFICATIONS SELECTED TO REDUCE SHUTDOWN RISK
- B) INSTRUMENTATION TO MONITOR REACTOR DURING SHUTDOWN EVENTS

### GE RESPONSE:

MANY FEATURES PROVIDED IN ABWR DESIGN. EXAMPLES ARE THIRD DIESEL GENERATOR, COMBUSTIBLE GAS TURBINE GENERATOR, ELIMINATION OF EXTERNAL RECIRCULATION PIPING AND INCREASED PRESSURE VESSEL ISOLATION CAPABILITY ON LOW WATER LEVEL. ROLE OF DESIGN FEATURES IN MITIGATING SHUTDOWN RISK WILL BE DESCRIBED IN SSAR.



## ABWR SHUTDOWN RISK

### DESIGN FEATURES (CONTINUED)

#### 2. ISSUE:

- A) TECHNICAL SPECIFICATIONS FOR SHUTDOWN CONDITIONS
- B) EPGs FOR SHUTDOWN CONDITIONS

#### GE RESPONSE:

ABWR TECHNICAL SPECIFICATIONS FOLLOW BWROG IMPROVED TECHNICAL SPECIFICATION RECOMMENDATIONS. HOWEVER, THIRD DIVISION OF ECCS PROVIDES MORE FLEXIBILITY COMPARED TO CURRENT PLANTS AND ENSURES ADDITIONAL SAFETY.

CURRENT EPGs DO NOT APPLY TO SHUTDOWN CONDITIONS. UTILITIES REFERENCING ABWR SSAR WILL ADOPT NUMARC GUIDELINES WHICH ARE CURRENTLY UNDER DEVELOPMENT. GE WILL ASSIST UTILITIES IN ADOPTING THESE GUIDELINES.

## ABWR SHUTDOWN RISK

### DESIGN FEATURES (CONTINUED)

#### 3. ISSUE:

- A) RAPID ISOLATION CAPABILITY WHEN FUEL IN-VESSEL
- B) REDUCED LIKELIHOOD AND CONSEQUENCE OF LOSS OF AC POWER DURING SHUTDOWN
- C) CONSIDERATION OF DEMANDS ON EQUIPMENT DURING SHUTDOWN CONDITION
- D) DECAY HEAT REMOVAL CAPABILITY DURING VARIOUS MODES OF OPERATION
- E) MINIMAL ISOLATION NEEDED FOR OUTAGE AND MAINTENANCE ACTIVITIES
- F) PROTECTION AGAINST "FREEZE SEAL" FAILURE
- G) REDUCED LIKELIHOOD OF DROPPING HEAVY LOADS ON DRYWELL HEAD

#### GE RESPONSE:

AVAILABLE FEATURES WILL BE DESCRIBED IN SSAR

## ABWR SHUTDOWN RISK

### DESIGN FEATURES (CONTINUED)

#### 4. ISSUE:

SPECIFIC ANALYSES TO DEVELOP BASES FOR SHUTDOWN PROCEDURES, INSTRUMENT INSTALLATION AND RESPONSE, EQUIPMENT/NSSS INTERACTION AND RESPONSE, AND LCO FOR TECHNICAL SPECIFICATIONS RELATIVE TO SHUTDOWN

#### GE RESPONSE:

MOST SHUTDOWN SITUATIONS ARE BOUNDED BY SITUATIONS AT POWER. SPECIFIC ANALYSES PERFORMED ONLY WHEN UNIQUE CONDITIONS MAY EXIST DURING SHUTDOWN CONDITIONS

## ABWR SHUTDOWN RISK

### SHUTDOWN RISK ASSESSMENT

#### ISSUE:

#### DETAILED SHUTDOWN RISK ASSESSMENT TO INCLUDE:

- LOCAs
- LOSS OF SUPPORT SYSTEMS
- OVERPRESSURE EVENTS
- TECHNICAL SPECIFICATIONS
- FIRE/FLOOD EVENTS
- ETC.

## ABWR SHUTDOWN RISK

### SHUTDOWN RISK ASSESSMENT (CONTINUED)

#### GE RESPONSE:

- 0 FOCUS ON IMPROVED DESIGN FEATURES
- 0 CATALOG ALL SIGNIFICANT SHUTDOWN EVENTS IN OPERATING PLANTS AND DEMONSTRATE FEATURES TO PREVENT OR MITIGATE SUCH EVENTS.
- 0 USE GRAND GULF SHUTDOWN PRA TO IDENTIFY DOMINANT SEQUENCES AND IDENTIFY ABWR DESIGN FEATURES THAT PREVENT OR MITIGATE SUCH SEQUENCES
- 0 IMPROVE DESIGN WHERE NEEDED
- 0 NO NEED FOR SHUTDOWN PRA

### (9) Loss of FW Heating Transient

For ABWR design, the following design requirement is specified for the FW heating system design :

"No single operator error or equipment failure shall cause loss of more than 55 °C (100 °F) feedwater heating ."

The reference steam and power conversion system shown in Figures 10.1-1 to 10.1-3 meets this requirement. In fact, the FW temperature drop based on the reference heat balance shown in Figure 10.1-2 is as follows:

- isolation of one low pressure heater < 15 °F
- isolation of one high pressure heater < 28 °F
- isolation of one low pressure heater string < 53 °F
- isolation of one high pressure heater string < 53 °F

Therefore, the use of 100 °F temperature drop in the transient analysis is conservative.

A drop of 150 °F occurred at a domestic BWR was a unique condition for that particular plant design. That unique condition will not occur in the ABWR design.

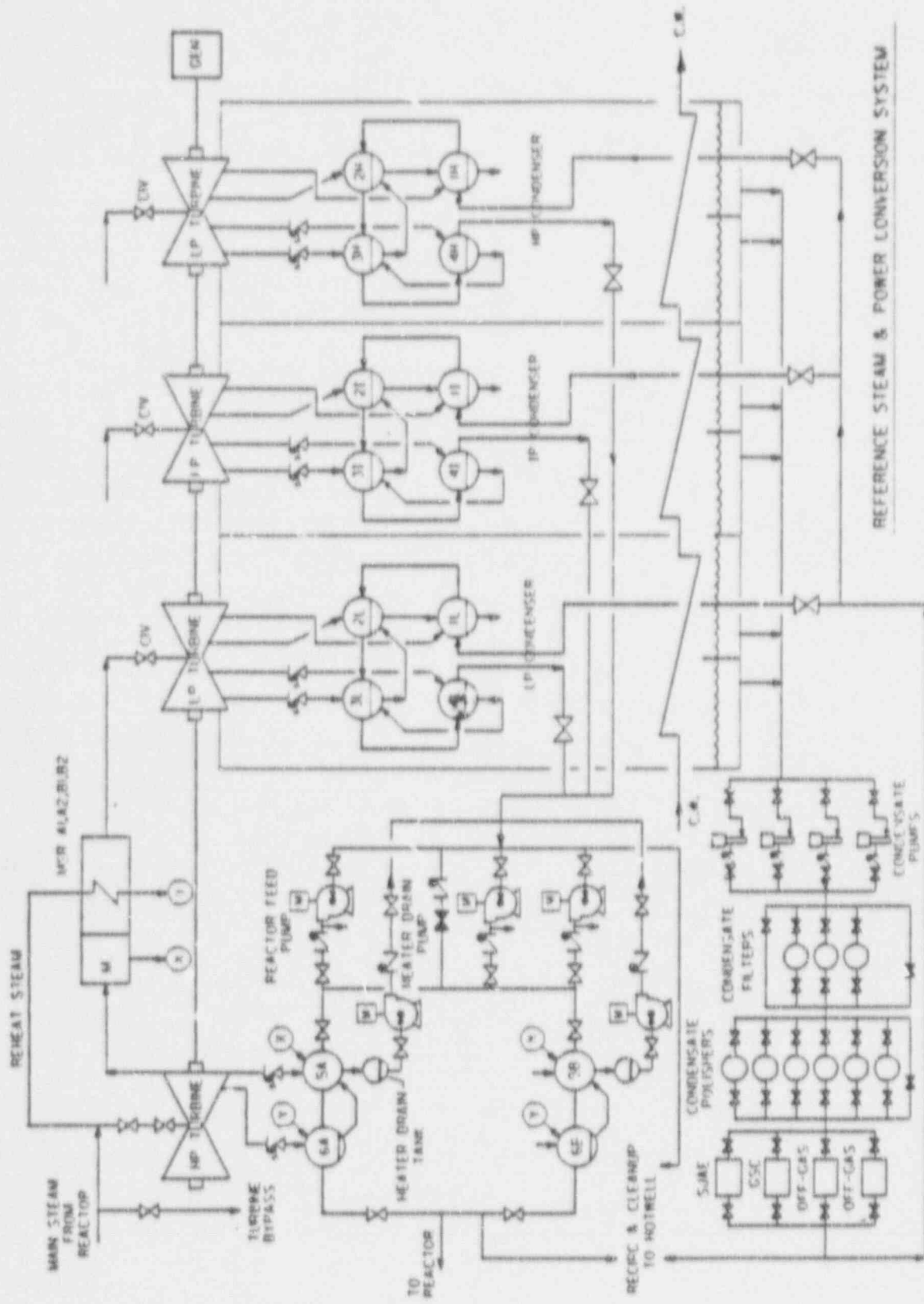


Figure 10.1-1 REFERENCE STEAM & POWER CONVERSION SYSTEM





		<u><math>\Delta T / \text{stage}</math></u>	<u><math>\Delta T / \text{heats}</math></u>	<u><math>\Delta T / \text{string}</math></u>
	124.27° F			
1	168.27° F	43.40° F	<u>19.467° F</u>	
2	208.02° F	39.75° F	13.250° F	
3	244.79° F	36.77° F	12.257° F	
4	283.06° F	38.27° F	12.757° F	52.731° F
	313.11° F			
5	368.43° F	55.32° F	<u>27.66° F</u>	
6	420.00° F	51.57° F	25.785° F	53.465° F



4.13.9 The automatic flow control range shall be from 70% to 100% rated power (100% rod line).

4.13.10 The minimum RIP speed shall be greater than or equal to 450 RPM.

4.14 Core Flow Measurement Requirements

4.14.1 Core flow measurement shall be provided to deliver inputs for scram trip as shown in Figures 1.4 and 1.5.

4.14.2 The required measurement accuracy shall be within the requirements specified in Section 2.1.2.c.

4.14.3 The design basis maximum sensor response time shall be less than or equal to 0.25 second. (Analysis condition for E/PA = 1.0 second)

4.15 Feedwater Requirements

4.15.1 Trip of main feedwater pumps shall be initiated upon the condition of high vessel water level (Level 8). This function may be designed as a non-safety related trip. However, the design of this trip function shall be highly reliable.

4.15.2 The trip signal shall be the same signal to be supplied for the high vessel water level turbine trip (see Section 4.10).

4.15.3 The maximum feedwater runout capacity with a dome pressure of 74.9 Kg/cm<sup>2</sup>g (1065 psig) shall be less than or equal to 130 percent of rated. The change of flow below the pressure specified above shall be less than 2.8% flow/Kg/cm<sup>2</sup> (0.2% flow/psi). E/P analysis may take credit of the maximum flow limit (110%) imposed by the feedwater control system.

4.15.4 Following a trip of one main feedwater pump, the minimum feedwater available to the vessel shall be greater than or equal to 75% of rated.

4.15.5 A six-heater feedwater heating system shall be designed to provide at least 215.5°C (420°F) feedwater at the rated condition.

\* 4.15.6 No single operator error or equipment failure shall cause loss of more than 55°C (100°F) feedwater heating.

4.15.7 The 1σ (standard deviation) uncertainty for the feedwater flow measurement system shall be less than or equal to 1.76% of rated feedwater flow.

4.16 Auxiliary Water Makeup Requirements

4.16.1 The Reactor Core Isolation Cooling (RCIC) system shall be initiated upon the condition of low vessel water level (Level 2).

NRC REACTOR SYSTEMS BRANCH MEETING  
SAN JOSE, NOV. 20-21, 1991  
RHR SYSTEM

FOR BRANCH TECHNICAL POSITION RSB 5-1 OF SRP 5.4.7;

SSAR SECTION 5.4.7.1.3 WAS REVISED:

RELIEF VALVES IN THE DISCHARGE PIPING ARE SIZED  
TO ACCOUNT FOR LEAKAGE PAST THE CHECK VALVE AND  
ARE CODED IN ACCORDANCE WITH THE ASME BOILER AND  
PRESSURE VESSEL CODE, SECTION III.

NRC REACTOR SYSTEMS BRANCH MEETING  
SAN JOSE, Nov. 20-21, 1991  
RHR SYSTEM

INTERSYSTEM LOCA

SECY-90-016 SATISFIED:

- 1) ISOLATION VALVE LEAK TESTING CAPABILITY
- 2) ISOLATION VALVE POSITION INDICATION  
AVAILABLE IN THE CONTROL ROOM
- 3) HIGH PRESSURE ALARMS FOR LOW PRESSURE  
REGIONS

FURTHERMORE

- 1) PROVIDE PIPING TO WITHSTAND THE ULTIMATE  
RUPTURE STRENGTH (URS) OF THE FULL REACTOR  
PRESSURE. (1025 PSIG)
- 2) ASSUME AT LEAST ONE VALVE REMAINS CLOSED IN  
A PATH TO THE LOW PRESSURE CONTAINMENT.



NRC REACTOR SYSTEMS BRANCH MEETING  
 SAN JOSE, NOV. 20-21, 1991  
 RHR SYSTEM

NC-3640 PRESSURE DESIGN OF PIPING PRODUCTS

NC-3641 Straight Pipe

NC-3641.1 Straight Pipe Under Internal Pressure. The minimum thickness of pipe wall required for Design Pressure and for temperatures not exceeding those for the various materials listed in Tables I-7.0, including allowances for mechanical strength, shall not be less than that determined by Eq. (3) as follows:

PIPES

$$t_m = \frac{PD_o}{2(S + Py)} + A \quad (3)$$

where

$t_m$  = minimum required wall thickness, in. If pipe is ordered by its nominal wall thickness, the

$P$  = internal Design Pressure, psi

$D_o$  = outside diameter of pipe, in. For design cal-

$S$  = maximum allowable stress for the material at the Design Temperature, psi (Tables I-7.0)

$A$  = an additional thickness to provide for material removed in threading, corrosion or erosion allowance, and material required for struc-

$y$  = a coefficient having a value of 0.4, except that, for pipe with a  $D_o/t_m$  ratio less than 6, the value of  $y$  shall be taken as

$$y = \frac{d}{d + D_o} \quad (6)$$

NC-3321

VESSEL

1989 SECTION III,

TABLE NC-3321-1  
 STRESS LIMITS FOR DESIGN AND SERVICE LOADINGS<sup>1</sup>

Service Limit	Stress Limits [Note (2)]
Design and Level A	$\sigma_m \leq 1.0 S$ $(\sigma_m \text{ or } \sigma_t) + \sigma_s \leq 1.5 S$

$\sigma_m$  = general membrane stress, psi. This stress is equal to the average stress across the solid section under consideration. It excludes discontinuities and concentrations and is produced only by pressure and other mechanical loads.

$S$  = allowable stress value given in Tables I-7.0, psi. The allowable stress shall correspond to the highest metal temperature at the section under consideration during the loading under consideration.

NC-3416

PUMPS

NC-3000 — DESIGN

NC-3423

TABLE NC-3416-1  
 STRESS AND PRESSURE LIMITS FOR DESIGN AND SERVICE LOADINGS

Service Limit	Stress Limits [Note (1)]	$P_{max}$ [Note (2)]
Level A	$\sigma_m \leq S$ $(\sigma_m \text{ or } \sigma_t) + \sigma_s \leq 1.55 S$	1.0

NC-3530

VALVES

1989 SECTION III, DIVISION 1 — NC

NC-3531.4

TABLE NC-3521-1  
 LEVEL A, B, C, AND D SERVICE LIMITS

Service Limit	Stress Limits [Notes (1)-(4)]	$P_{max}$ [Note (5)]
Level A	$\sigma_m \leq S$ $(\sigma_m \text{ or } \sigma_t) + \sigma_s \leq 1.55 S$	1.0

NRC REACTOR SYSTEMS BRANCH MEETING  
SAN JOSE, Nov. 20-21, 1991  
RHR SYSTEM

$$t_m = \frac{P D_o}{2(S + P_y)} + A$$

$$t_m = \frac{(\text{Design Pressure})(D_o)}{2(\text{Allowable Stress})} + A = \frac{(\text{High Pressure})(D_o)}{2(\text{Ultimate Stress})} + A$$

$$\text{High Pressure} = \frac{(\text{Ultimate Stress})(\text{Design Pressure})}{(\text{Allowable Stress})}$$

$$800 \text{ psig} = \frac{60K (200 \text{ psig})}{15K}$$

OR

$$\text{Design Pressure} = \frac{(\text{Allowable Stress})(\text{High Pressure})}{(\text{Ultimate Stress})}$$

$$256 \text{ psig} = \frac{15K (1025 \text{ psig})}{60K}$$

Round up; Consider 300 psig minimum design pressure

November 3, 1989  
File Tabs C and A

SIL No. 502  
Category 1

## SINGLE TURBINE CONTROL VALVE CLOSURE EVENT

GE Nuclear Energy has recently evaluated the safety significance of a single Turbine Control Valve (TCV) slow closure. The evaluation showed that under certain conditions a slow closure of a TCV could cause the Minimum Critical Power Ratio (MCPR) to approach the safety limit. The purpose of this SIL is to discuss this postulated event.

### Discussion

Postulated failures in the turbine and pressure control systems may cause a single TCV to close without initiating the turbine-generator trip scram logic. In such an event, the high neutron flux, high Simulated Thermal Power (STP) available on some plants and high pressure scram are available for plant protection.

A single TCV closure causes an increase in reactor pressure with a corresponding increase in neutron flux. A high neutron flux scram provides quick protection with no significant change in Critical Power Ratio (CPR) for most postulated failures. However, if the postulated failure, and subsequent valve closure, occurs slowly, pressure and neutron flux increases could be such that the flux increase would not reach the high flux scram or STP scram setpoints. In this case the high reactor pressure scram would provide the remaining protection. During such a slow closure event, the remaining TCVs and bypass valves open in response to the turbine pressure control system to compensate for the steam flow reduction that results from the single TCV closure. TCVs and bypass valves open until limited by the control system limiters. A simplified diagram of a typical pressure control system is shown in Figure 1.

If single TCV closure occurs at a power level below about 85% of rated power, the turbine and bypass flow adequately handle the steam flow with no significant disturbance. However, when operating at or near full power, the



remaining turbine and bypass flow may not be large enough to accept all of the steam from the reactor. If this occurs, the thermal power may reach a level at which a significant change in CPR could occur. However, this will result in a high reactor pressure scram. Normally, periodic TCV surveillance tests are conducted at reduced power and are not a concern if the tests are conducted according to plant procedures. If tests are conducted near full rated power, a similar, but less severe response would be expected.

The single TCV closure event has not been analyzed specifically for operating BWRs in the FSAR or reload licensing analyses because this event has been assumed to be bounded by the other events which establish the MCPR operating limit.

GE has performed a bounding analysis of this postulated event. The analysis was based on full power, a typical GE Mark II turbine electro-hydraulic control system, a limiter value of 100% of nuclear boiler rated (NBR) steam flow for the turbine flow reference limiter in combination with a Maximum Combined Flow Limiter (MCFL) value of 115% NBR steam flow. The analysis assumed a value of 85% of NBR steam flow through the three remaining TCVs (typical for GE turbines). The analysis took no credit for the power reduction response which would occur if recirculation flow control were in the automatic flux control mode. GE concluded the following from this analysis:

1. BWR/2 through BWR/5 plants have sufficient MCPR margin to stay above the MCPR safety limit with a nominal MCFL setting of 115% of NBR steam flow.
2. BWR/6 plants also have sufficient MCPR margin if the steam flow through the three TCVs plus the steam flow through the bypass valves is greater than 97% of NBR steam flow. Note that 97% of NBR steam flow is the value referenced to an initial turbine inlet pressure.

The MCFL setting determines the total steam flow available to the pressure controls. GE usually has specified the MCFL value of 115% of NBR steam flow as an upper limit in the FSAR case for the "Pressure Regulator Failure - Open" (PRFO) event. The purpose of this upper limit is to avoid too rapid a vessel depressurization, which would result if the MCFL setting were higher. The MCFL value is not included in plant technical specifications because the PRFO event is not limiting and a higher MCFL limit can be shown to be adequate.

Because BWR/6 plants have less MCPR margin for this event than BWR/2 through BWR/5 plants, BWR/6 turbine pressure control system settings should receive additional attention. As is shown in Figure 1, steam flow for pressure control purposes is affected not only by the MCFL setting but also by other control signal adjustments or limits.

Review of a single TCV slow closure event emphasizes the importance of the lower bound of the MCFL value and other settings because they determine the amount of steam flow available to the pressure controls. Because it is possible that some plants may operate with lower than the specified MCFL setting, GE Nuclear Energy is issuing this SIL to inform all BWR owners of the need to maintain the MCFL setting at the value specified by GE. This action should avoid the potential for exceeding the technical specification MCPR safety limit if the postulated slow failure of a single TCV were to occur.

#### Recommended Action

GE recommends that BWR owners implement the following actions:

1. BWR/2 through BWR/6 plants:

Check the current value of the MCFL setting. If the current value is lower than 115% of NBR steam flow, raise the setting to at least 115% of NBR steam flow.

2. BWR/6 plants

Adjust the MCFL value and other settings, if necessary, to ensure that the total steam flow through the three TCVs plus bypass flow is greater than 97% of NBR steam flow with the pressure regulator output saturated at its MCFL value.

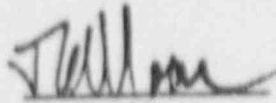
To receive additional information on this subject or for assistance in implementing a recommendation, please contact your local GE Nuclear Energy Service Representative.

Technical Source: E. C. Eckert

#### Notice

This SIL pertains only to GE BWRs. GE Nuclear Energy prepared this SIL exclusively as a service for owners of GE BWRs. GE Nuclear Energy has not considered or evaluated the applicability, if any, of information contained in this SIL to any plant or facility other than GE BWRs. Determination of applicability of information contained in this SIL to a specific BWR and implementation of recommended action are the responsibilities of the owner of that BWR.

Issued by:



J. G. Moore

Customer Service Communications Manager

Product Reference:

C85: Steam Bypass and Pressure Control

A62: Plant Requirements

Figure 1

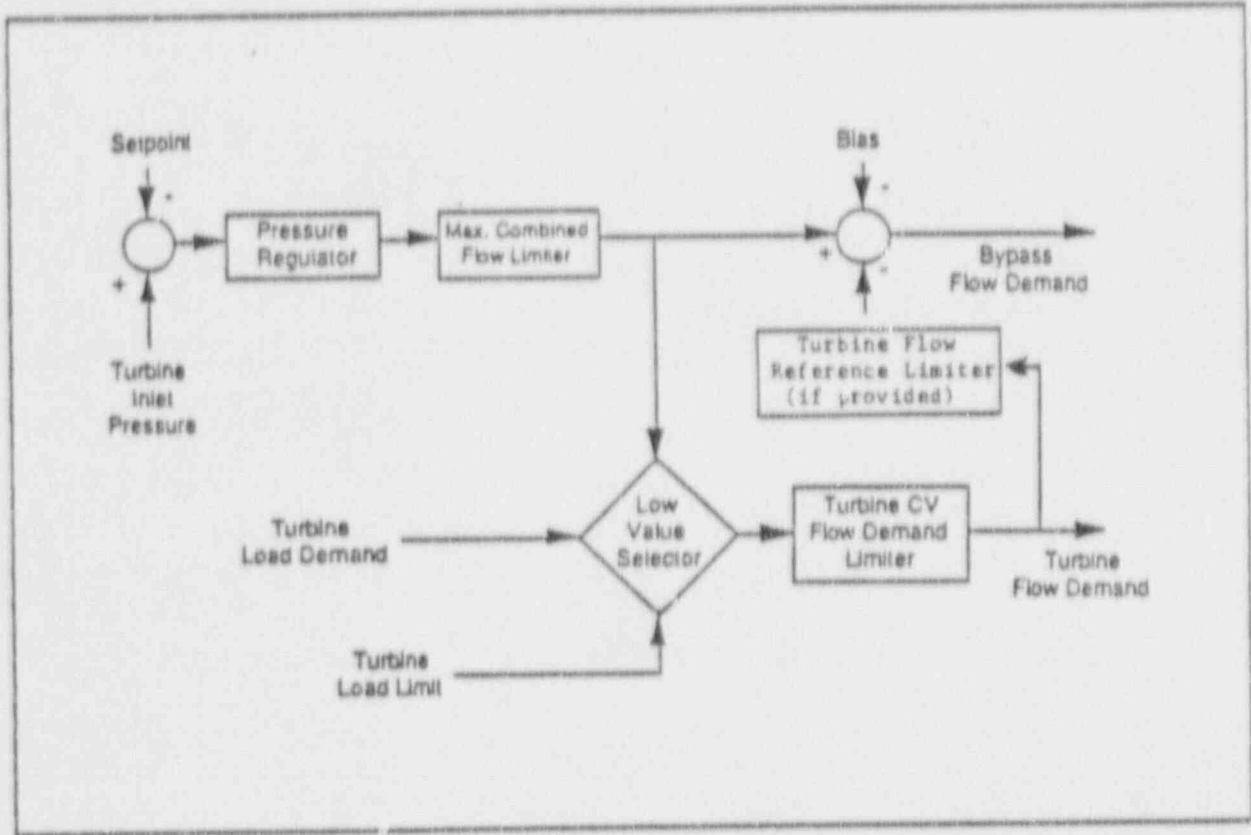


Diagram of the Pressure Control System

DESCRIPTION OF THE ABWR ROD BLOCK MONITOR (ATLM) ALGORITHM

Automated Thermal Limit  
Monitor

NRC REACTOR SYSTEMS BRANCH MEETING

NOV. 21, 1991

## OLMCPR RBS Calculation Methodology

### A) Formula

The formula for calculating the OLMCPR RBS is

$$RBS_o = \frac{LPRM_1 * A_o * RMCPR_1}{OLMCPR}$$

### B) Algorithm Analytical Basis

The critical power ratio (CPR) is related to the bundle power by the following relationship (See note):

$$CPR = X_c / X$$

where X is the nodal quality and is proportional to the ratio of bundle power divided by channel flow, or

$$X = \text{constant} * P / W$$

Consequently,

$$CPR = \text{constant} * \frac{X_c}{P / W}$$

For two different power conditions:

$$\frac{CPR \text{ limit}}{CPR} = \frac{(P/W)}{(P/W) \text{ limit}} * \frac{X_c \text{ limit}}{X_c}$$

Assuming that flow change caused by control rod withdrawal is very small and that  $X_c$  change is negligible, then

$$\frac{P_{\text{limit}}}{P} = \text{constant} * \frac{CPR}{CPR \text{ limit}}$$

The above equation says that the bundle power is inversely proportional to the CPR of the bundle, with a constant.

OLMCPM RES Calculation Methodology (Continued)

If there is axial power peaking shift caused by adjacent control rod motion, then

$$\frac{P_{\text{limit}}}{P} = K_a \frac{\text{CPR}}{\text{CPR limit}}$$

Also, when a control rod is being withdrawn next to a LPRM string, the true bundle power around this rod next to the LPRM string are under-measured by this LPRM string by a factor of C. This factor is primarily a function of control rod density change next to the LPRM string.

Then,

$$\frac{\text{LPRM limit}}{\text{LPRM}} = C \cdot \frac{P_{\text{limit}}}{P}$$

Combining the above two equations,

$$\begin{aligned} \frac{\text{LPRM limit}}{\text{LPRM}} &= C * K_a * \frac{\text{CPR}}{\text{CPR limit}} \\ &= A * \frac{\text{CPR}}{\text{CPR limit}} \end{aligned}$$

"A" value is a function of power, flow, and control rod pull distance, etc. If there is no control rod motion in a specified core region (16 bundles), then "A" value will have the value of unity.

The above explains the analytical basis of the A factor. However, for actual plant application for CPR monitoring during control rod operation, the A value is determined based on a semi-empirical approach where a statistical value is determined based on a set of representative data base.

C) Determination of A value

The purpose of the ATLM is to provide on-line thermal limit protection based on actual operating plant data. It requires quick calculation with a simple algorithm. It is thus not practical to calculate the above C and  $K_a$  values in order to obtain the A value. A semi-empirical statistical approach is used instead. The principle is similar to the method used in deriving the BWR/5 Rod Block Monitor setpoint. Instead of deriving a single worst bounding case, the "A" value is determined based on a set of realistic control rod withdrawal cases at various operating conditions.

A family of operating power and flow conditions with corresponding typical rod patterns are developed using the GE core simulator code. The rod patterns are developed based on BWR standard rod withdrawal sequence procedure and ABWR rod and gang groups, consistent with ABWR reactivity control requirements. This data base consists of various power and flow conditions covering the ABWR power-flow map. From these initial conditions, control rod withdrawal cases are developed using the simulator code, which include both four-rod gang and eight-rod gang withdrawal cases from various initial rod positions. Also, conditions of both initial core design and equilibrium core design are included in the data base. With this set of control rod withdrawal studies, a family of "A" values are obtained. Based on this set of "A" values, a statistical analysis is performed to derive a bounding "A" value curve as a function of relative control rod withdrawal distance. A typical "A" value curve based on ABWR reference core and fuel design is shown in Figure 1. This curve will be updated based on the most current fuel design for actual ABWR plant application.

Due to the use of the statistical data base, the "A" value obtained is conservative for MCPR protection. This is why the "A" value is also referred to as a margin factor. The "A" value curve will be programmed into the microprocessor-based ATLM instrument as a "known function" for a particular core and fuel design.

---

Note: The relationship between CPR and critical quality can be found in MCPR calculation method description document on GE Process Computer P1 program

## OLMLHGR RES Calculation Methodology

### A) Formula

The formula for calculating the OLMLHGR RBS is

$$RBS_m(X) = \frac{LPRM_1(X) * B_m(X) * M_p}{MAPRAT_1(X)}$$

### B) Algorithm Analytical Basis

The average planar LHGR (APLHGR) is a calculated bundle average fuel pellet power density (KW/FT). The maximum APLHGR in the region (RAPLHGR) monitored by the LPRM is proportional to the LPRM output:

$$LPRM = \text{constant} * RAPLHGR$$

For two different power levels,

$$\frac{LPRM_1}{LPRM_2} = \frac{RAPLHGR_1}{RAPLHGR_2}$$

However, when a control rod is withdrawn next to a LPRM string, the true fuel power density of the fuel section around this rod is under-measured. This under-measured factor is B. For two power conditions with one being the limiting condition, then

$$\frac{LPRM_{limit}}{LPRM} = B * \frac{RAPLHGR_{limit}}{RAPLHGR}$$

By definition,

$$MAPRAT = RAPLHGR / MAPLHGR$$

where MAPLHGR is the maximum APLHGR.



## OLMLHGR RBS Calculation Methodology (Continued)

Consequently,

$$\frac{\text{LPRM}_{\text{limit}}}{\text{LPRM}} = B * \frac{\text{MAPRAT}_{\text{limit}}}{\text{MAPRAT}}$$

"B" value is a function of power, flow, and control rod pull distance, e't.c. If there is no control rod motion in a specified core region (16 bundles) and segment, then "B" value will have the value of unity.

Also, based on over-power conditions during worst transient at off-rated conditions, an off-rated power multiplier factor for MAPLHGR,  $M_p$ , has to be included in the above equation, or

$$\frac{\text{RBS}}{\text{LPRM}_i} = B * \frac{M_p * \text{MAPRAT}_{\text{limit}}}{\text{MAPRAT}_i} = B * \frac{M_p}{\text{MAPRAT}_i}$$

Where  $M_p$  is determined based on over-power factors during worst transient at off-rated conditions. It is a function of power and flow, or a combined function of power only. (See note.) With the factor  $M_p$  included, the APRM setpoint setdown at off-rated condition for power peaking protection is not required. At rated condition,  $M_p = 1$ . For a typical BWR/5,  $M_p = 1 + .0052 * (P\% - 100)$ . The  $M_p$  curve will be updated for the most current ABWR fuel and core design.

### C) B Value Determination

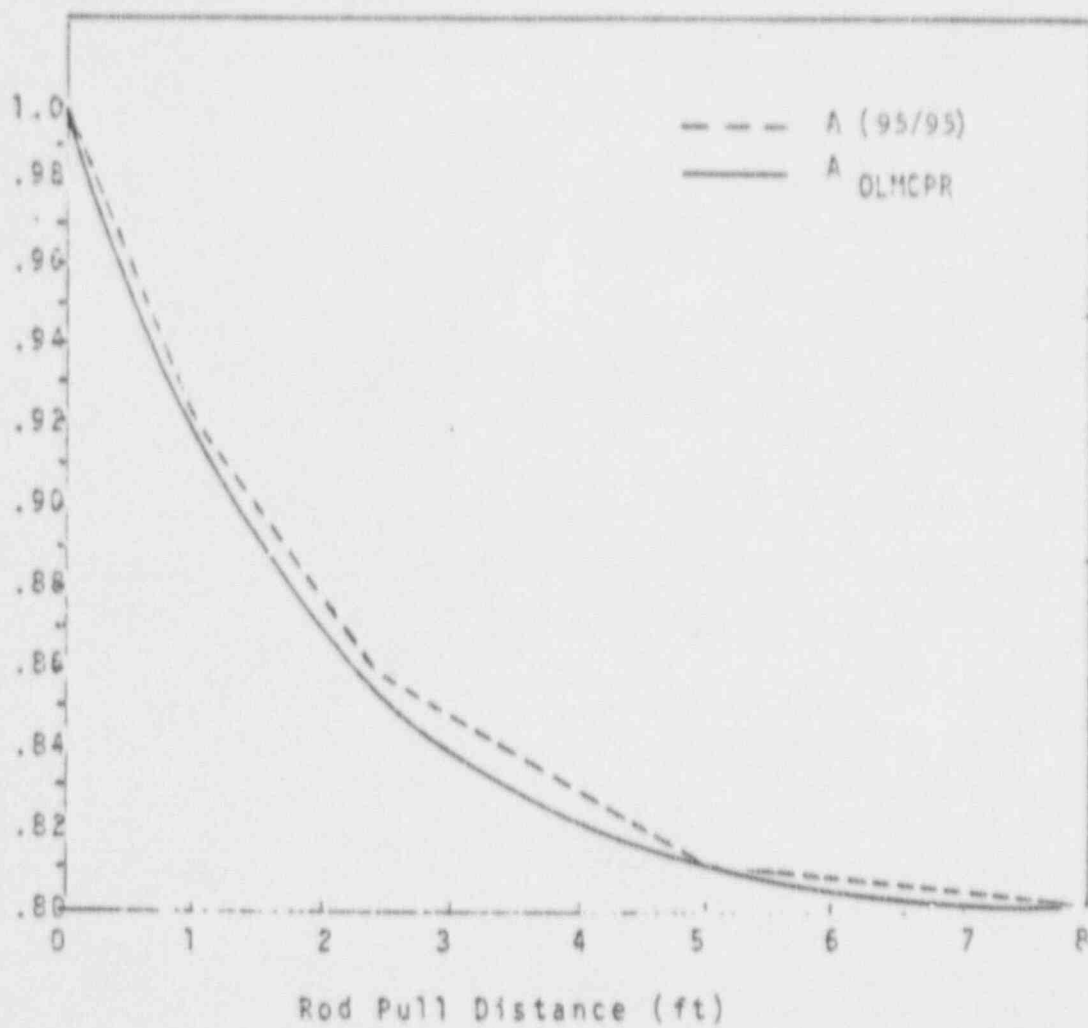
The method used in determining the "B" value is similar to the method used in obtaining the "A" value. Same data base is used. A very conservative bounding curve that cover all "B" values in the data base is developed for each of the four segments of fuel bundles that corresponding to the four LPRM sensor elevations.

A set of "B" value curves based on ABWR reference core and fuel design is shown in Table 1. This table will be updated based on the most current fuel design for actual ABWR plant application.

---

Note: The method of  $M_p$  determination can be found in the licensing report of GE's ARTS Improvement Program.

Figure 1 A-Factor for OLMCPR Protection



1. Considered 15% random LPRM failure
2. Above data included both initial and equilibrium cycle.
3. Above data based on 95% probability 95% confidence.

Table 1 B-Values in  
Setpoint Algorithm For MAPRAT Rod Block

(Initial Cycle Worst KW/FT Peaking & LPRM Average Random  
Failure of 15% Considered )

LEVEL	INITIAL NOTCH	POWER	B-VALUES
A	N <sub>i</sub> < 36	P < 65%	NOTCH 0 32 36 44 48 .95 .95 .80 .80 .95
		P ≥ 65%	NOTCH 0 32 34 48 .96 .96 .94 .94
	N <sub>i</sub> ≥ 36	ALL	0.98
B	N <sub>i</sub> < 28	P < 65%	NOTCH 0 18 26 32 34 40 48 .95 .95 .71 .71 .75 .75 .95
		P ≥ 65%	NOTCH 0 22 26 32 36 42 44 48 .97 .97 .85 .85 .91 .91 .97 .97
	N <sub>i</sub> ≥ 28	ALL	0.95
C	N <sub>i</sub> < 22	P < 65%	NOTCH 0 10 14 16 18 30 48 .95 .95 .82 .82 .85 .85 .94
		P ≥ 65%	NOTCH 0 10 12 32 48 .95 .95 .875 .875 .94
	N <sub>i</sub> ≥ 22	ALL	0.98
D	N <sub>i</sub> < 10	ALL	NOTCH 0 24 48 .85 .85 .95
	10 < N <sub>i</sub> < 12	ALL	NOTCH 0 12 14 24 48 .90 .90 .85 .85 .95
	12 < N <sub>i</sub> < 18	P < 65%	NOTCH 0 12 14 24 48 .90 .90 .85 .85 .95
	12 < N <sub>i</sub> < 18	P ≥ 65%	NOTCH 0 6 8 42 48 .97 .97 .92 .92 .97
	N <sub>i</sub> ≥ 18	ALL	0.98

NOTE: N<sub>i</sub> = Initial control rod notch position before rod pull after  
Predictor MAPRAT update

## 2.2.4 Standby Liquid Control System

The standby liquid control system (SLCS) is design to inject neutron absorbing poison using a boron solution into the reactor and thus provide back-up reactor shutdown capability independent of the normal reactivity control system based on insertion of control rods into the core. The system is capable of operation over a wide range of reactor pressure conditions up to and including the elevated pressures associated with an anticipated plant transient coupled with a failure to scram (ATWS).

The standby liquid control system (SLCS) is designed to provide the capability of bringing the reactor, at any time in a cycle, from full power and at all conditions to a subcritical condition with the reactor in the most reactive xenon-free state without control rod movement.

The SLCS consists of a boron solution storage tank, two positive displacement pumps, two motor operated injection valves which are provided in parallel for redundancy and associated piping and valves used to transfer borated water from the storage tank to the reactor pressure vessel (RPV). The borated solution is discharged through the 'B' high pressure core flooders (HPCF) subsystem sparger. Figure 2.2.4 shows major system components. Key equipment performance requirements are:

- |  |                                 |
|--|---------------------------------|
| a. Pump flow                                 | 100 gpm with both pumps running |
| a. Maximum reactor pressure (for injection)  | 1250 psig                       |
| a. Pumpable volume in storage tank (minimum) | 6100 U.S. gal                   |

The required volume of solution contained in the storage tank is dependent upon the solution concentration and this concentration can vary during reactor operations. A required boron solution volume/concentration relationship is used to define acceptable SLCS storage tank conditions during plant operation.

The SLCS is automatically initiated during an ATWS or can be manually initiated from the main control room. When the SLCS is automatically initiated to inject a liquid neutron absorber into the reactor, the following devices are actuated:

- the two injection valves are opened;
- the two storage tank discharge valves are opened;
- the two injection pumps are started; and
- the reactor water cleanup isolation valves are closed.

When the SLCS is manually initiated to inject a liquid neutron absorber into the reactor, the following devices are actuated by each switch:

- a. one of the two injection valves is opened;
- b. one of the two storage tank discharge valves is opened;
- c. one of the two injection pumps is started; and
- d. one of the reactor water cleanup isolation valves is closed.

The SLCS provides borated water to the reactor core to compensate for the various reactivity effects during the required conditions. These effects include xenon decay, elimination of steam voids, changing water density due to the reduction in water temperature, Doppler effect in uranium, changes in neutron leakage and changes in control rod worth as boron affects neutron migration length. To meet this objective it is necessary to inject a quantity of boron which produces a minimum concentration of 850 ppm of natural boron in the reactor core at 70°F. To allow for potential leakage and imperfect mixing in the reactor system, an additional 25% (220) is added to the above requirement. The required concentration is achieved accounting for dilution in the RPV with normal water level and including the volume in the residual heat removal shutdown cooling piping. This quantity of boron solution is the amount which is above the pump suction shutoff level in the tank thus allowing for the portion of the tank volume which cannot be injected.

The pumps are capable of producing discharge pressure to inject the solution into the reactor when the reactor is at high pressure conditions corresponding to the system relief valve actuation.

The SLCS includes sufficient Control Room indication to allow for the necessary monitoring and control during design basis operational conditions. This includes pump discharge pressure, storage tank liquid level and temperature as well as valve open/close and pump on/off indication for those components shown on Figure 2.2.4 (with the exception of the simple check valves).

The SLCS uses a dissolved solution of sodium pentaborate as the neutron-absorbing poison. This solution is held in a storage tank which has a heater to maintain solution temperature above the saturation temperature. The heater is capable of automatic operation and automatic shutoff to maintain an acceptable solution temperature. The SLCS solution tank, a test water tank, the two positive displacement pumps, and associated valving is located in the secondary containment on the floor elevation below the operating floor. This is a Seismic Category I structure, and the SLCS equipment is protected from phenomena such as earthquakes, tornados, hurricanes and floods as well as from internal postulated accident phenomena. In this area, the SLCS is not subject to conditions such as missiles, pipe whip, and discharging fluids.

The pumps, heater, valves and controls are powered from the standby power supply or normal offsite power. The pumps and valves are powered and controlled from separate buses and circuits so that single active failure will not prevent system operation. The power supplied to one motor operated injection valve, storage tank discharge valve, and injection pump is powered from Division I, 480 VAC. The power supply to the other motor-operated injection valve, storage tank outlet valve, and injection pump is powered from Division II, 480 VAC. The power supply to the tank heaters and heater controls is connectable to a standby power source. The standby power source is Class 1E from an on-site source and is independent of the off-site power.

All components of the system which are required for injection of the neutron absorber into the reactor are classified Seismic Category I. All major mechanical components are designed to meet ASME Code requirements as shown below.

<u>Component</u>	<u>ASME Code Class</u>	<u>Design Conditions</u>	
		<u>Pressure</u>	<u>Temperature</u>
Storage Tank	2	Static Head	150°F
Pump	2	1560 psig	150°F
Injection Valves	1	1560 psig	150°F
Piping Inboard of Injection Valves	1	1250 psig	575°F

Design provisions to permit system testing include a test tank and associated piping and valves. The tank can be supplied with demineralized water which can be pumped in a closed loop through either pump or injected into the reactor.

The SLCS is separated both physically and electrically from the control rod drive system.

### ***Inspection, Test, Analyses and Acceptance Criteria***

Table 2.2.4 provides a definition of the inspections, tests, and/or analyses together with associated acceptance criteria which will be undertaken for the SLCS.

**Table 2.2.4: STANDBY LIQUID CONTROL SYSTEM  
Inspections, Tests, Analyses and Acceptance Criteria**

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
<p>1. The minimum average poison concentration in the reactor after operation of the SLCS shall be equal to or greater than 850 ppm.</p>	<p>1. Construction records, revisions and plant visual examinations will be undertaken to assess as-built parameters listed below for compatibility with SLCS design calculations. If necessary, an as-built SLCS analysis will be conducted to demonstrate the acceptance criteria is met.</p> <p><b>Critical Parameters:</b></p> <p>a. Storage tank pumpable volume</p> <p>b. RPV water inventory at 70°F</p> <p>c. RHR shutdown cooling system water inventory at 70°F</p>	<p>1. It must be shown the SLCS can achieve a poison concentration of 850 ppm or greater assuming a 25% dilution due to non-uniform mixing in the reactor and accounting for dilution in the RHR shutdown cooling systems. This concentration must be achieved under system design basis conditions.</p> <p>This requires that SLCS meet the following values:</p> <p>Storage tank pumpable volume range 6100-6800 gal.</p> <p>RPV water inventory <math>\leq 1.00 \times 10^6</math> lb</p> <p>RHR shutdown cooling system inventory <math>\leq .287 \times 10^6</math> lb</p>
<p>2. A simplified system configuration is shown in Figure 2.2.4.</p>	<p>2. Inspections of installation records together with plant walkdowns will be conducted to confirm that the installed equipment is in compliance with the design configuration defined in Figure 2.2.4.</p>	<p>2. The system configuration is in accordance with Figure 2.2.4.</p>

Table 2.2.4: STANDBY LIQUID CONTROL SYSTEM (Continued)

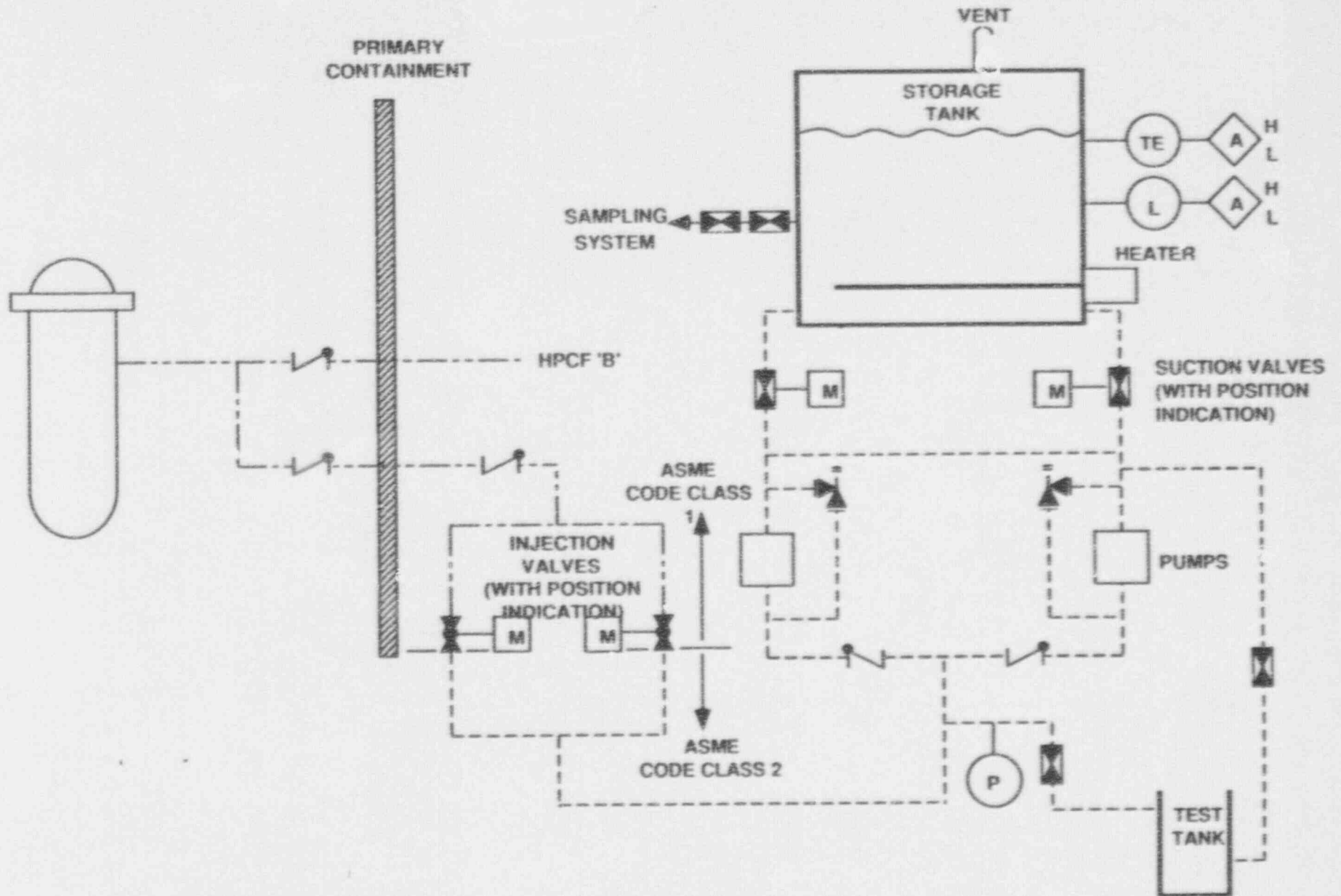
## Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3. SLCS shall be capable of delivering 100 gpm of solution with both pumps operating against the elevated pressure conditions which can exist in the reactor during events involving SLCS initiation.	3. System preoperation tests will be conducted to demonstrate acceptable pump and system performance. These tests will involve establishing test conditions that simulate conditions which will exist during an SLCS design basis event. To demonstrate adequate Net Positive Suction Head (NPSH), delivery of rated flow will be confirmed by tests conducted at conditions of low level and maximum temperature in the storage tank, and the water will be injected from the storage tank to the RPV.	3. It must be shown that the SLCS can automatically inject 100 gpm (both pumps running) against a reactor pressure of 1250 psig with simulated ATWS conditions. It must also be shown that the SLCS pumps can pump the entire storage tank pumpable volume.
4. The system is designed to permit in-service functional testing of SLCS.	4. Field tests will be conducted after system installation to confirm, in-service system testing can be performed.	4. Using normally installed controls, power supplies and other auxiliaries, the system has the capability to: <ul style="list-style-type: none"> <li>a. Pump tests in a closed loop on the test tank and</li> <li>b. Reactor pressure vessel injection tests using demineralized water from the test tank.</li> </ul>
5. The pump, heater, valves and controls can be powered from the standby AC power supply as described in Section 2.2.4.*	5. System tests will be conducted after installation to confirm that the electrical power supply configurations are in compliance with design commitments.	5. The installed equipment can be powered from the standby AC power supply.
6. All SLCS components which are required for the injection of the neutron absorber into the reactor are classified Seismic Category I and qualified for appropriate environment for locations where installed.	6. See Generic Equipment Qualification verification activities (ITA).	6. See Generic Equipment Qualification Acceptance Criteria (AC).

\* This entry may be transferred to the standby AC power ITAAC in Section 2.12.13.



Figure 2.2.4 STANDBY MODE CONTROL SYSTEM (STANDBY MODE)



## 2.2.7 Reactor Protection System

The reactor protection system (RPS) for the Advanced Boiling Water Reactor (ABWR) is a warning and trip system where initial warning and trip decisions are implemented with software logic installed in microprocessors. The primary functions of this system are to: (1) make the logic decisions related to warning and trip conditions of the individual instrument channels, and (2) make the decision for system trip (emergency reactor shutdown) based on coincidence of instrument channel trip conditions.

The RPS is classified as a safety protection system (i.e., as differing from a reactor control system or a power generation system). All functions of the RPS and the components of the system are safety-related. The RPS and the electrical equipment of the system are also classified as Safety Class 3, Seismic Category I and as IEEE electrical category Class 1E.

Basic System Parameters are:

a.	Number of independent divisions of equipment	4
b.	Minimum number of sensors per trip variable (at least one per division)	4
c.	Number of automatic trip systems (one per division)	4
d.	Automatic trip logic used for plant sensor inputs (per division)	2-out-of-4
e.	Separate automatic trip logic used for division trip outputs	2-out-of-4
f.	Number of separate manual trip systems	2
g.	Manual trip logic	2-out-of-2

The RPS consists of instrument channels, trip logics, trip actuators, manual controls and scram logic circuitry that initiates rapid insertion of control rods (scram) to shut down the reactor for situations that could result in unsafe reactor operating conditions. The RPS also establishes the required trip conditions that are appropriate for the different reactor operating modes and provides status and control signals to other systems and annunciators. The RPS related equipment includes detectors, switches, microprocessors, solid-state logic circuits, relay type contactors, relays, solid-state load drivers, lamps, displays, signal transmission routes, circuits and other equipment which are required to execute the functions of the system. To accomplish its overall function, the RPS utilizes the functions of the essential multiplexing system (EMS) and of portions of the safety system logic and control (SSLC) system.

As shown in Figure 2.2.7a, the RPS interfaces with the neutron monitoring system (NMS), the process radiation monitoring (PRRM) system, the nuclear boiler system (NBS), the control rod drive (CRD) system, the rod control and information system (RC&IS), the recirculation flow control (RFC) system, the process computer system and with other plant systems and equipment. RPS components and equipment are separated or segregated from process control system sensors, circuits and functions such as to minimize control and protection system interactions. Any necessary interlocks from the RPS to control systems are through isolation devices.

The RPS is a four division system which is designed to provide reliable single-failure proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures in the RPS. The RPS remains single-failure proof even when one entire division of channel sensors is bypassed and/or when one of the four automatic RPS trip logic systems is out-of-service. All equipment within the RPS is designed to fail into a trip initiating state or other safe state on loss of power or input signals or disconnection of portions of the system. The system also includes trip bypasses and isolated outputs for display, annunciation or performance monitoring. RPS inputs to annunciators, recorders and the computer are electrically isolated so that no malfunction of the annunciating, recording, or computing equipment can functionally disable any portion of the RPS. The RPS related equipment is divided into four redundant divisions of sensor (instrument) channels, trip logics and trip actuators, and two divisions of manual scram controls and scram logic circuitry. The automatic and manual scram initiation logic systems are independent of each other and use diverse methods and equipment to initiate a reactor scram. The RPS design is such that, once a full reactor scram has been initiated automatically or manually, this scram condition seals-in such that the intended fast insertion of all control rods into the reactor core can continue to completion. After a time delay, deliberate operator action is required to return the RPS to normal.

Figure 2.2.7b shows the RPS divisional separation aspects and the signal flow paths from sensors to scram pilot valve solenoids. Equipment within a RPS related sensor channel consists of sensors (transducers or switches), multiplexers and digital trip modules (DTMs). The sensors within each channel monitor for abnormal operating conditions and send either discrete bistable (trip/no trip) or analog signals directly to the RPS related DTM or else send analog output signals to the RPS related DTM by means of the remote multiplexer unit (RMU) within the associated division of essential multiplexing system (EMS). The RPS related bistable switch type sensors, or, in the case of analog channels, the RPS software logic, will initiate reactor trip signals within the individual sensor channels, when any one or more of the conditions listed below exist within the plant during different conditions of reactor operation, and will initiate reactor scram if coincidence logic is satisfied.

- a. Turbine Stop Valves Closure (above 40% power levels) [RPS]

- b. Turbine Control Valves Fast Closure (above 40% power levels) [RPS]
- c. NMS monitored SRNM and APRM conditions exceed acceptable limits [NMS]
- d. High Main Steam Line Radiation [PRRM System]
- e. High Reactor Pressure [NBS]
- f. Low Reactor Water Level (Level 3) [NBS]
- g. High Drywell Pressure [NBS]
- h. Main Steam Lines Isolation (MSLI) (Run mode only) [NBS]
- i. Low Control Rod Drive Accumulator Charging Header Pressure [CRD]
- j. Operator-initiated Manual Scram [RPS]

The system monitoring the process condition is indicated in brackets in the list above. The RPS outputs, the NMS outputs, the PRRM system outputs and the MSLI and manual scram outputs are provided directly to the RPS by hard-wired or fiber-optic signals. The NBS and the CRD system provide other sensor outputs through the EMS. Analog to digital conversion of these latter sensor output values is done by EMS equipment. The DTM in each division uses either the discrete bistable input signals, or compares the current values of the individual monitored analog variables with their trip setpoint values, and for each variable sends a separate, discrete bistable (trip/no trip) output signal to the trip logic units (TLUs) in all four divisions of trip logics. The DTMs and TLUs utilized by the RPS are microprocessor components within the SSLC system.

RPS related equipment within a RPS division of trip logic consists of manual control switches, bypass units (BPUs), trip logic units (TLUs) and output logic units (OLUs). The manual control switches and the BPUs, TLUs and OLU are components of the RPS portions of the SSLC system. The various manual switches provide the operator means to modify the RPS trip logic for special operation, maintenance, testing and system reset. The bypass units perform bypass and interlock logic for the single division of channel sensors bypass function and for the single division TLU bypass function. The TLUs perform the automatic scram initiation logic, normally checking for two-out-of-four coincidence of trip conditions in any set of instrument channel signals coming from the four division DTMs or from isolated bistable inputs from all four divisions of NMS equipment, and outputting a trip signal if any one of the two-out-of-four coincidence checks is satisfied. TLU trip decision logic in all four RPS TLUs becomes a check for two-out-of-three coincidence of trip conditions if any one division of channel sensors has been bypassed. The OLU perform the division trip, seal-in, reset and trip test functions. Trip signals from the OLU within a single division are used to trip the trip actuators, which are fast response,

bistable, solid-state load drivers for automatic scram initiation, and are trip relays for air header dump (back-up scram) initiation. Load driver outputs toggled by a division OLU interconnect with load driver outputs toggled by other division OLU's into two separate arrangements which results in two-out-of-four scram logic, i.e., reactor scram will occur if load drivers associated with any two or more divisions receive trip signals.

The isolated ac load drivers are fast response time, bistable, solid-state, high current interrupting devices. The operation of the load drivers is such that a trip signal on the input side will create a high impedance, current interrupting condition on the output side. The output side of each load driver is electrically isolated from its input signal. The load driver outputs are arranged in the scram logic circuitry, between the scram pilot valves' solenoids and the solenoids ac power source, such that when in a tripped state the load drivers will cause deenergization of the scram pilot valve solenoids (scram initiation). Normally closed relay contacts are arranged in the two back-up scram logic circuits, between the air header dump valve solenoid and air header dump valve dc solenoid power source, such that when in a tripped state (coil deenergized) the relays will cause energization of the air header dump valve solenoids (air header dump initiation). Associated dc voltage relay logic is also utilized to effect scram reset permissives and scram-follow (control rod run-in) initiation.

The RPS design for the ABWR is testable for correct response and performance, in over-lapping stages, either on-line or off-line (to minimize potential of unwanted trips). Access to bypass capabilities of trip functions, instrument channels or a trip system and access to setpoints, calibration controls and test points are designed to be under administrative control.

### ***Inspection, Test, Analyses and Acceptance Criteria***

Table 2.2.7 provides a definition of the visual inspections, tests and/or analyses, together with associated acceptance criteria, which will be used by the RPS.

**Table 2.2.7: REACTOR PROTECTION SYSTEM****Inspections, Tests, Analyses and Acceptance Criteria**

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. RPS safety-related software, which is utilized in effecting individual sensor channel trip decisions and trip system coincidence trip decisions, has been developed and verified, the firmware implemented and validated and then integrated with hardware; all according to a formal documented plan.	1. See Generic Software Development verification activities (ITA).	1. See Generic Software Development Acceptance Criteria (AC).
2. Certain process signals utilized by the RPS are transmitted to RPS sensor channel signal processing equipment by means of four separate divisions of Essential Multiplexing System equipment.	2. See the Essential Multiplexing System verification activities (ITA).	2. See the Essential Multiplexing System Acceptance Criteria (AC).
3. Critical parameter trip setpoints are based upon values used in analyses of abnormal operational occurrences. Documented instrument setpoint methodology has been used to account for uncertainties (such as instrument inaccuracies and drift) in order to establish RPS related setpoints.	3. See Generic Setpoint Methodology verification activities (ITA).	3. See Generic Setpoint Methodology Acceptance Criteria (AC).
4. RPS equipment is designed to be protected from the effects of noise, such as electromagnetic interference (EMI), and has adequate surge withstand capability (SWC).	4. See Generic EMI/SWC Qualification verification activities (ITA).	4. See Generic EMI/SWC Qualification Acceptance Criteria (AC).
5. RPS equipment is qualified for seismic loads and appropriate environment for locations where installed.	5. See Generic Equipment Qualification verification activities (ITA).	5. See Generic Equipment Qualification Acceptance Criteria (AC).

Table 2.2.7: REACTOR PROTECTION SYSTEM (Continued)

## Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
6. RPS components and equipment are kept separate from equipment associated with process control systems.	6. Visual field inspections and analyses of relationship of installed RPS equipment and of installed equipment of interfacing process control systems (and/or tests of interfaces) to confirm appropriate isolation methods used to satisfy separation and segregation requirements.	6. RPS equipment installation acceptable if inspections, analyses and/or tests confirm that any failure in process control systems can not prevent RPS safety functions.
7. Fail-safe failure modes result upon loss of power or disconnection of components.	7. Field tests to confirm that trip conditions and/or bypass inhibits result upon loss of power or disconnection of components.	7. Acceptable if safe state conditions result upon loss of power or disconnection of portions of the RPS.
8. Provisions exist to limit access to trip setpoints, calibration controls and test points.	8. Visual field inspections of the installed RPS equipment will be used to confirm the existence of appropriate administrative controls.	8. The RPS hardware/firmware will be considered acceptable if appropriate methods exist to enforce administrative control for access to sensitive areas.
9. The four redundant divisions of RPS equipment and the four automatic trip systems are independent from each other except in the area of the required coincidence of trip logic decisions and are both electrically and physically separated from each other. Similarly, the two manual trip systems are separate and independent of each other and of the four automatic trip systems.	9. Inspections of fabrication and installation records and construction drawings or visual field inspections of the installed RPS equipment will be used to confirm the quadruple redundancy of the RPS and the electrical and physical separation aspects of the RPS instrument channels and the four automatic trip systems as well as their diversity and independence from the two manual trip systems.	9. Installed RPS equipment will be determined to conform to the documented description of the design as depicted in Figure 2.2.7b.

Table 2.2.7: REACTOR PROTECTION SYSTEM (Continued)

## Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
<p>10. It is possible to conduct verifications of RPS operations, both on-line and off-line, by means of a) individual instrument channel functional tests, b) trip system functional tests and c) total system functional tests.</p>	<p>10. Preoperational tests will be conducted to confirm that system testing such as channel checks, channel functional tests, channel calibrations, coincident logic tests and paired control rods scram tests can be performed. These tests will involve simulation of RPS testing modes of operation. Interlocks associated with the reactor mode switch positions, and with other operational and maintenance bypasses or test switches will be tested and annunciation, display and logging functions will be confirmed.</p>	<p>10. The installed reactor protection system configuration, controls, power sources and installations of interfacing systems supports the RPS logic system functional testing and the operability verification of design as follows:</p> <ul style="list-style-type: none"> <li>a. Installed RPS hardware/firmware initiates trip conditions in all four RPS automatic trip systems upon coincidence of trip conditions in two or more instrument channels associated with the same trip variable(s).</li> <li>b. Installed system initiates full reactor trip and emergency shutdown (i.e., deenergization of both solenoids associated with all scram pilot valves) upon coincidence of trip conditions in two or more of the four RPS automatic trip systems.</li> <li>c. Installed system initiates trip conditions in both RPS manual trip systems if both manual trip switches are operated or if the reactor mode switch is placed in the "shutdown" position.</li> <li>d. Trip system (automatic and manual) trip conditions seal-in and protective actions go to completion. Trip reset (after appropriate delay for trip completion) requires deliberate Operator action.</li> </ul>



Table 2.2.7: REACTOR PROTECTION SYSTEM (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

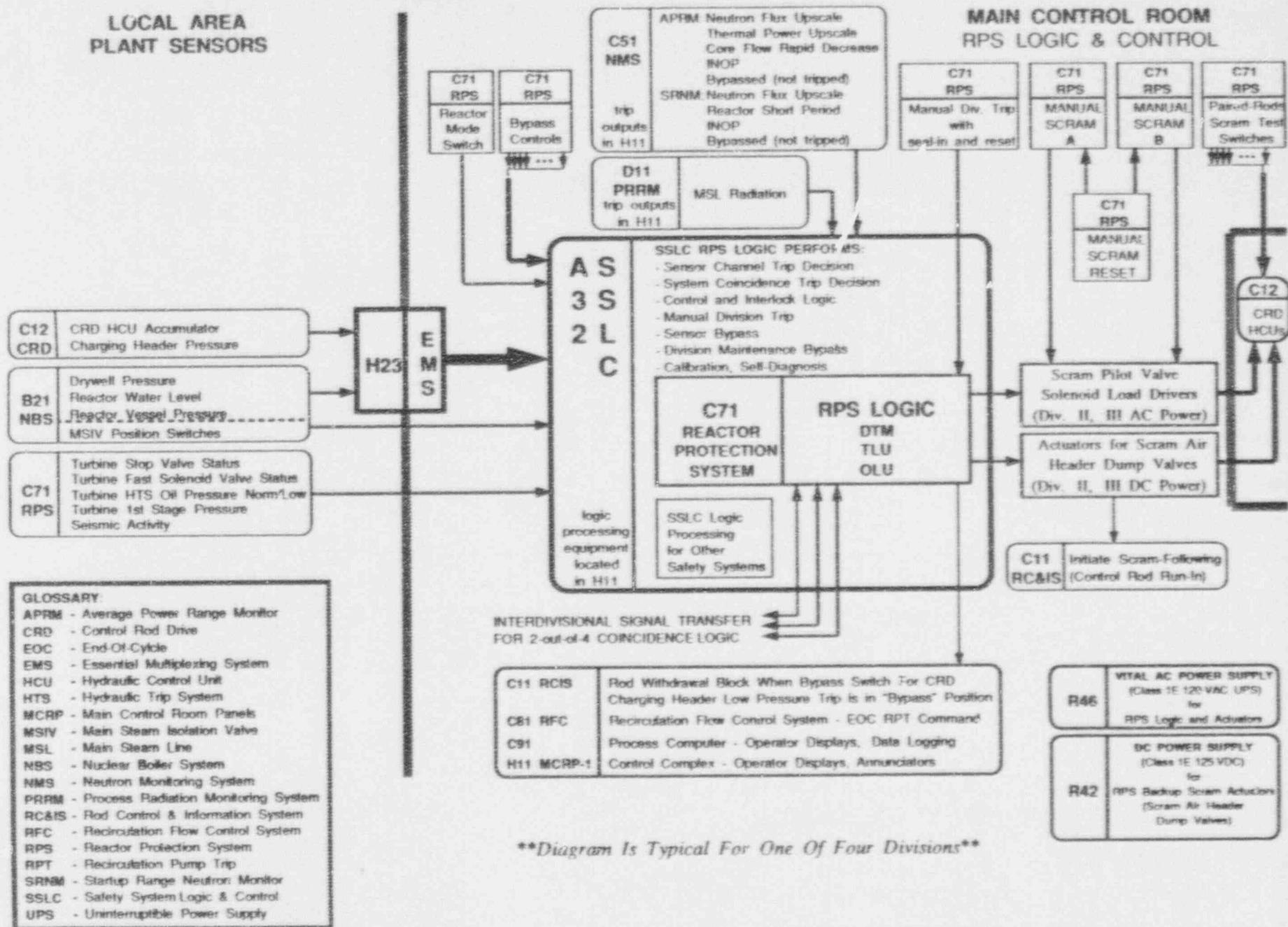
Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
	10. (Continued)	
		e. Installed system energizes both air header dump (back-up scram) valves of the CRD hydraulic system, and initiates CRD motor run-in, concurrent only with a full scram condition.
		f. When not bypassed, trips result upon loss or disconnection of portions of the system. When bypassed, inappropriate trips do not result.
		g. Installed system provides isolated status and control signals to data logging, display and annunciator systems.
		h. Installed system demonstrates operational interlocks (i.e., trip inhibits or permissives) required for different conditions of reactor operation.

Table 2.2.7: REACTOR PROTECTION SYSTEM (Continued)

## Inspections, Tests, Analyses and Acceptance Criteria

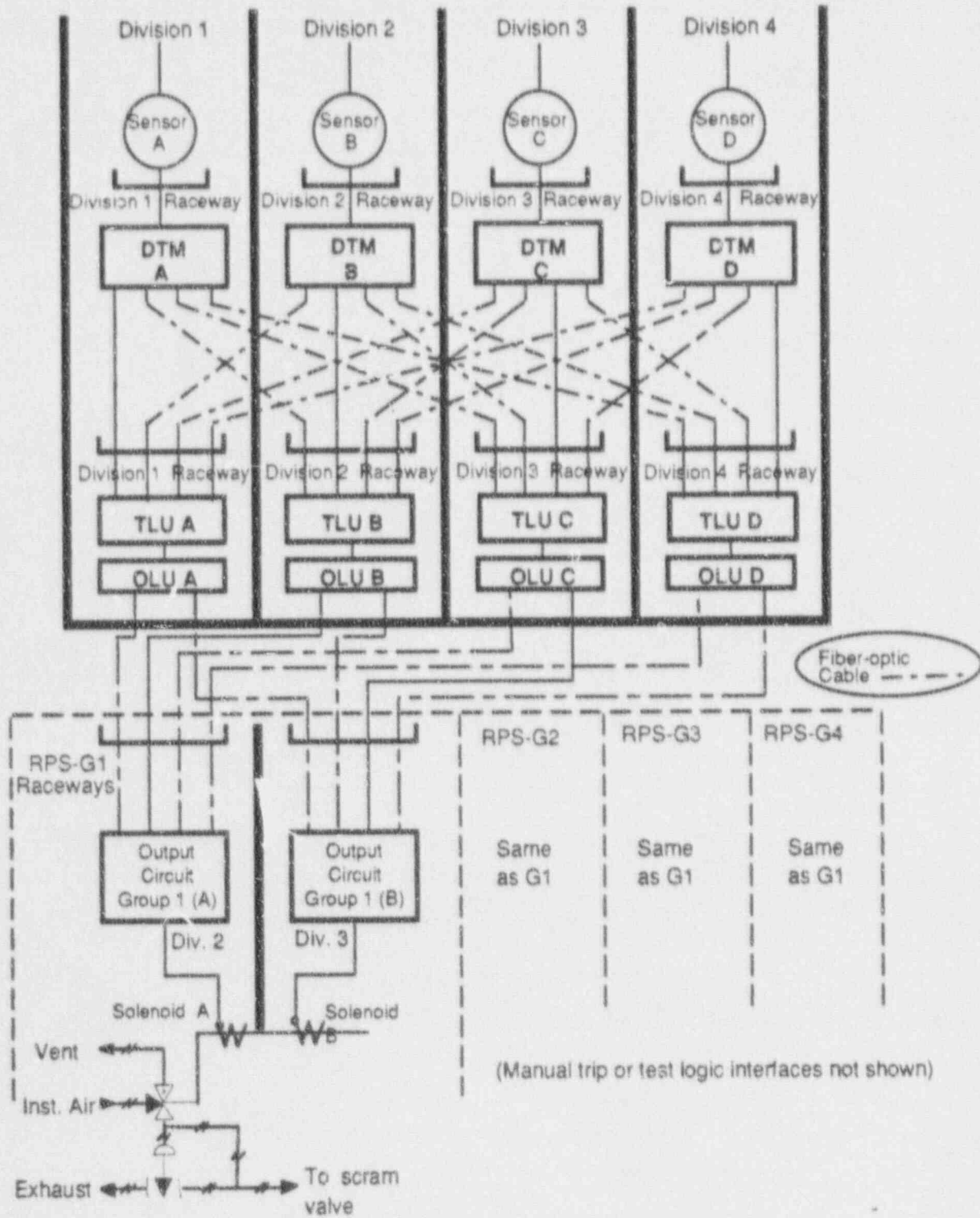
Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11. The RPS design provides prompt protection against the onset and consequences of events or conditions that threaten the integrity of the fuel barrier.	11. Preoperational tests will be conducted to measure the RPS and supporting systems response times to: (1) monitor the variation of the selected processes; (2) detect when trip setpoints have been exceeded; and, (3) execute the subsequent protection actions when coincidence of trip conditions exist.	11. The RPS hardware/firmware response to initiate reactor scram will be considered acceptable if such response is demonstrated to be sufficient to assure that the specified acceptable fuel design limits are not exceeded.
		<b>Validation Attributes:</b>
		Total trip system response, from time when sensor input is beyond setpoint to time of scram pilot valve solenoids deenergization:
		<ul style="list-style-type: none"> <li>- NMS APRM <span style="float: right;">≤ 0.090 sec.</span></li> <li>- Reactor pressure <span style="float: right;">≤ 0.55 sec.</span></li> <li>- Reactor water level <span style="float: right;">≤ 1.05 sec.</span></li> <li>- Turbine stop valve closure <span style="float: right;">≤ 0.060 sec.</span></li> <li>- Turbine control valve fast closure <span style="float: right;">≤ 0.080 sec.</span></li> <li>- Main steam lines isolation <span style="float: right;">≤ 0.060 sec.</span></li> </ul>

Figure 2.2.7a REACTOR PROTECTION SYSTEM



\*\*Diagram Is Typical For One Of Four Divisions\*\*

Figure 2.2.7b REACTOR PROTECTION SYSTEM



### **3.3 CONFIGURATION MANAGEMENT PLAN DAC ITAAC**

This section contains the proposed Configuration Management Plan DAC ITAAC. The DAC ITAAC is included as a section (APPENDIX B) of the generic software ITAAC. The generic ITAAC establishes acceptance criteria for the overall software development process, which includes a Software Management Plan, Configuration Management Plan and Verification and Validation (V&V) Plan. Each ABWR safety system that uses the safety-related software functions of the Safety System Logic and Control (SSLC) equipment will reference the generic software ITAAC as part of that safety system's ITAAC acceptance criteria. The ITAAC of other safety-related equipment that contains software to perform safety functions will also reference the generic software ITAAC.

The generic software ITAAC will reference the DAC ITAAC for Software Management, Configuration Management and V&V, which in turn establish design acceptance criteria that will ensure that proper controls are placed on the step-by-step software development process.

APPENDIX B is an example of a software development DAC ITAAC for the Configuration Management Plan. APPENDIX A for the Software Management Plan DAC ITAAC and APPENDIX C for the V&V DAC ITAAC will be developed later.

**Table 3.3: SOFTWARE FOR PROGRAMMABLE DIGITAL COMPUTERS IN SAFETY-RELATED APPLICATIONS**  
**Inspections, Tests, Analyses and Acceptance Criteria**

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
<p>1. A plan shall be developed for software used in microprocessor-based equipment that performs safety-related functions. The plan shall describe the organizational and procedural aspects of software development and shall comprise the following elements:</p> <ul style="list-style-type: none"> <li>- Software Management Plan</li> <li>- Configuration Management Plan</li> <li>- Verification and Validation (V&amp;V) plan</li> </ul>	<p>1. Review:</p> <ul style="list-style-type: none"> <li>- Software Management Plan</li> <li>- Configuration Management Plan</li> <li>- Verification and Validation Plan</li> </ul>	<p>1. The overall development plan documents the requirements and methodology for achieving the software attributes of consistency, accuracy, error tolerance and modularity. The plan includes the methodology for assuring the software is both auditable and testable during the design, implementation and integration phases. Each element of the plan contains the following items as a minimum:</p> <ul style="list-style-type: none"> <li>a. Software Management Plan establishes standards, conventions and design processes for the design, development, and maintenance of safety-related software. The plan meets the design acceptance criteria described in Appendix A.</li> <li>b. Configuration Management Plan establishes a formal set of standards and procedures to provide visible status and control of software documentation. The following basic elements are addressed:               <ul style="list-style-type: none"> <li>1) Unique identification of each software documentation item</li> <li>2) Management of software documentation change control</li> <li>3) Accounting methods to provide visibility and traceability for all changes to baseline product software</li> <li>4) Verification steps required to assure proper adherence to software design requirements</li> </ul> </li> </ul>

Table 3.3: SOFTWARE FOR PROGRAMMABLE DIGITAL COMPUTERS IN SAFETY-RELATED APPLICATIONS (Continued)

## Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
		1. (Continued)
		The plan meets the design acceptance criteria described in Appendix B.
		c. Verification and Validation Plan establishes verification reviews and validation testing procedures with the following components: <ol style="list-style-type: none"> <li>1) Independent design verification</li> <li>2) Baseline reviews</li> <li>3) Testing</li> <li>4) Firmware issue and validation procedure               <ol style="list-style-type: none"> <li>a) Unstructured testing</li> <li>b) Formal validation testing</li> </ol> </li> <li>5) Procedure for future revisions</li> </ol>
		The plan meets the design acceptance criteria described in Appendix C.
2. The software design documentation meets the requirements of the development plan.	2. Review design documentation: <ul style="list-style-type: none"> <li>- Hardware/Software System Specification</li> <li>- Software Requirements Specification</li> <li>- Software Design Specification</li> <li>- Hardware Requirements Specification</li> <li>- Hardware Design Specification</li> </ul>	2. The documentation complies with the requirements in the Certified Design Commitments. The design documentation allows correlation of the design elements with each specific software requirement as determined by the V&V process described in Appendix C.
		The computer system hardware documentation identifies the hardware requirements that impact software.
3. Details of software implementation and the integration of hardware and software into the final product shall be addressed in Tier 2.	3. Tier 2 requirement	3. Tier 2 requirement

Table 3.3: SOFTWARE FOR PROGRAMMABLE DIGITAL COMPUTERS IN SAFETY-RELATED APPLICATIONS (Continued)

## Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
<p>4. The assembled, final production computer system shall be exercised through static and dynamic simulations of input signals present during normal operation and design basis event conditions requiring computer system action.</p> <p>The validation test plan shall identify the validation tests for each safety-related, software-based system component.</p>	<p>4. Review formal (verified) validation test report.</p>	<p>4. The test report summarizes the results of the computer system validation testing and shows how the system is in compliance with the requirements.</p> <p>The test report identifies the validation tests for each computer system and safety system requirement. In addition, the required input signals and their values, the anticipated output signals, and the acceptance criteria are stated.</p> <p>The test report identifies the hardware and software used, test equipment and calibrations, simulation models used, test results, and discrepancies and corrective actions.</p> <p>The test plan was developed, the tests executed, and the test results evaluated by individuals who did not participate in the design or implementation phases.</p>



**Table 3.3: SOFTWARE FOR PROGRAMMABLE DIGITAL COMPUTERS IN SAFETY-RELATED APPLICATIONS****APPENDIX A: SOFTWARE MANAGEMENT PLAN DESIGN ACCEPTANCE CRITERIA****Inspections, Tests, Analyses and Acceptance Criteria**

Certified Design Commitment

Inspections, Tests, Analyses

Acceptance Criteria

[LATER]

Table 3.3: SOFTWARE FOR PROGRAMMABLE DIGITAL COMPUTERS IN SAFETY-RELATED APPLICATIONS

## APPENDIX B: CONFIGURATION MANAGEMENT PLAN DESIGN ACCEPTANCE CRITERIA

## Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. Development of software for the microprocessor-based safety systems shall be controlled according to a configuration management plan.	1. A review shall be performed of the contents of the configuration management plan.	1. A configuration management plan has been issued.
2. The configuration management plan will define the purpose and scope of the plan with emphasis on the groups to which it applies and the specific product which is to be developed. The product description shall include both executable and non-executable material	2. A review shall be performed of the contents of the configuration management plan.	2. The configuration management plan identifies each group which develops and/or maintains software for safety systems. The plan includes both executable and non-executable portions of the design.
3. The configuration plan shall describe the organizational responsibilities. The organizational independence or dependence of the groups responsible for the software configuration management shall be specifically described. The plan shall describe a function independent of the software designers that is responsible for verifying that the software is maintained under this plan. The plan shall detail the relationships of the configuration control with the software QA, development and other groups.	3. A review shall be performed of the contents of the configuration management plan.	3. The configuration plan describes the organizational independence and responsibilities.

Table 3.3: SOFTWARE FOR PROGRAMMABLE DIGITAL COMPUTERS IN SAFETY-RELATED APPLICATIONS

## APPENDIX B: CONFIGURATION MANAGEMENT PLAN DESIGN ACCEPTANCE CRITERIA (Continued)

## Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
4. Applicable procedures, such as standards for the designation of software versions, shall be described in the plan or specifically referenced. All software shall be identified such that the version can be verified directly, either embedded in the software if in a non-programmable/erasable format or permanently inscribed directly on the component.	4. A review shall be performed of the contents of the configuration management plan.	4. The plan describes the procedures for implementation of the plan.
5. The plan shall describe the audits and reviews that are to be performed to verify that the software is being maintained under configuration management. The plan shall describe a procedure for corrective actions if any problems are discovered.	5. A review shall be performed of the contents of the configuration management plan.	5. The plan describes audits and reviews and describes a procedure for corrective actions.
6. The configuration management of tools, techniques, and methodologies shall be specifically delineated. The plan shall address control of development methods to used (such as formal specification) and tools (such as compilers).	6. A review shall be performed of the contents of the configuration management plan.	6. The plan describes control of tools and methodologies.
7. The plan shall describe the method of records collection and retention.	7. A review shall be performed of the contents of the configuration management plan.	7. The plan describes the record storage plan.

Table 3.3: SOFTWARE FOR PROGRAMMABLE DIGITAL COMPUTERS IN SAFETY-RELATED APPLICATIONS

## APPENDIX B: CONFIGURATION MANAGEMENT PLAN DESIGN ACCEPTANCE CRITERIA (Continued)

## Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
8. The plan shall address control of the final user documentation and the information to be supplied. The method of informing the user of each product of known faults, failures, and changes shall be specifically described.	8. A review shall be performed of the contents of the configuration management plan.	8. The plan will identify the method by which faults, failures, and changes are identified to the affected user.
9. The configuration management plan shall be in place and approved by the implementer prior to the first concept development phases of software development.	9. A review shall be performed of the contents of the configuration management plan.	9. The configuration management plan will be approved and in place at the beginning of the project.
10. The configuration management plan shall require that the design documents (such as software requirements specifications) shall provide specific reference to the applicable configuration management plan. The plan shall define procedures for change control, including change request, evaluation, approval, and implementation.	10. A review shall be performed of the contents of the configuration management plan.	10. The plan will require that the design documents reference the configuration management plan.

**Table 3.3: SOFTWARE FOR PROGRAMMABLE DIGITAL COMPUTERS IN SAFETY-RELATED APPLICATIONS**

**APPENDIX C: VERIFICATION AND VALIDATION PLAN DESIGN ACCEPTANCE CRITERIA**

**Inspections, Tests, Analyses and Acceptance Criteria**

Certified Design Commitment

Inspections, Tests, Analyses

Acceptance Criteria

[LATER]

φ