February 3, 1992

MFN No. 025-92
Docket No. STN 50-605
EEN-9212

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Attention: Robert C. Pierson, Director
Standardization and Non-Power Reactor Project Directorate

Subject: **GE Responses to the Additional Items Noted in the Draft SER for Chapter 7**

Reference:
1. D.M. Crutchfield to P.W. Marriott, Draft Safety Evaluation Report on the Advanced Boiling Water Reactor Design, dated October 4, 1991 (SECY-91-294), MFN No. 126-91
2. GE Responses to the Additional Items Notes in the Draft SER for Chapter 7, Proprietary Information, dated 2/3/92, MFN No. 028-92

Enclosed are thirty-four (34) copies of the GE responses to the subject request. The responses are cross referenced with a summary item number corresponding to the review meeting held in San Jose on August 7 & 8, 1991.

Some of these responses contain information that is designated as General Electric Company proprietary information and are primarily corrections or additions to earlier proprietary submittals. This information is being submitted under separate cover (Reference 2).

It is intended that GE will amend the ABWR SSAR with these responses in a future amendment.

Sincerely,

R.C. Mitchell

R.C. Mitchell, Acting Manager
Regulatory and Analysis Services
M/C 382, (408) 925-6948

cc: F. A. Ross (DOE)
N. D. Fletcher (DOE)
C. Poslusny, Jr. (NRC)
J. Stewart (NRC)
R. C. Berglund (GE)
J. F. Quirk (GE)

D026 1/34

CONCERN - DSER Section: 7.1.3.2 , Page # 7-6 (DSER Summary Item # 4.a)
GE should provide additional information for the following items required or discussed by the EPRI RD:

RG 1.106, RG 1.33, GL 83-08, 10CFR50.62, GDC 3, GDC 17, GDC 26, IEEE 730, IEEE 829, IEEE 472, BTPCMEB9.5-1, 10CFR APP B, ISA 67-15, ANSI C96.1, NEMA, DOD 263, IPCEA 561402, NUREG CR4640, NUREG 0993, NUREG CR3958, NUREG CR4385, NUREG CR4386, NUREG CR4387, NUREG 0572, NUREG 0977, NUREG 1000, NUREG 0696, NUREG 1154, NUREG 985, NSAC-39, EPRI 2184-7, MILSPEC 338, MILSPEC 217E, MILSPEC 781, MILSPEC 472, EPRI NP3659, EPRI NP6209, EPRI 5693, EPRI NP3448, EPRI NP3701, EPRI NP3659, AND EPRI RP27057.

CLOSURE PLAN
The review of EPRI requirements will remain as an open issue in the SER. This item will be addressed in the final SER on the ABWR.

RESPONSE
Evaluation of the ABWR against the listed criteria is beyond the SRP/LRB certification requirements. GE will discuss with the NRC to determine the appropriate forum in which to address these issues.

CONCERN - DSER Section: 7.1.3.3 , Page # 7-11 (DSER Summary Item # 5.a)
GE should provide additional information to demonstrate its commitment to GDC 1 for the SSLC and EMS design. The staff noted that there was no evidence in the SSAR that current IEEE and other computer/electronics industry standards related to advanced technology had been considered in the design; for example, no standards were identified regarding electromagnetic compatibility, local area networks, communications protocols, and software design.

CLOSURE PLAN
GE will review ANSI C37.90.2, Mil Spec 461 and 462, and ANSI C63.12 for application to the ABWR regarding EMC. Appendix 7A will be amended to address such standards (or others) deemed appropriate following the review. (See also Item 8.a.)

[ACTION COMPLETED PER MODIFIED RESPONSE]

RESPONSE
(See Proprietary Information in separate submittal.)

CONCERN - DSER Section: 7.1.3.3 , Page # 7-13 (DSER Summary Item # .a)
Prototype testing of new technology is required to confirm expected safety performance, to confirm unforseen systems interactions, and allow the staff to reach its safety determination on systems which may not have extensive operating experience. Based on information currently available, the staff believes that prototypes will be needed to demonstrate acceptable performance of the interconnected RPS, ESFAS, EMS, and SSLC systems.

CLOSURE PLAN

GE will submit "scroll" flow chart consistent with DSER Summary Item 1.e. NRC action to review/assess regulatory process (ITAAC + Q/A). GE will propose up-front confirmatory steps which can be defined now, but be applied post-certification.

[ACTION COMPLETED PER RESPONSE AND RPS PILOT ITAAC EXAMPLE]

RESPONSE

GE submitted a flow chart during the GE/NRC meetings on DSER Chapter 7 concerns that illustrated GE's assessment of the regulatory process before and after certification. As a typical example of commitments that will be made for the inspection and test of installed safety protection system equipment after certification, but prior to plant startup, the pilot ITAAC for the Reactor Protection System (RPS) is attached. This ITAAC describes inspections and tests that are unique to RPS. However, since the RPS function is part of Safety System Logic and Control (SSLC) and the Essential Multiplexing System (EMS), portions of SSLC and EMS are also verified to be acceptable during the performance of RPS procedures. ITAACs for other safety functions will verify other portions of SSLC and EMS. There will, however, be ITAACs that are specific to both of these systems. These ITAACs will provide more detailed inspections and tests for specialized functions within SSLC and EMS, such as bypass, self-test, data throughput rate, error rate, and time response.

CONCERN - DSER Section: 7.2.1 , Page # 7-16 (DSER Summary Item # 1.b)

GE should specify which periodic reactor protection system tests will be used to satisfy technical specification requirements.

CLOSURE PLAN

GE will amend SSAR Section 7.2 to state fault-detection diagnostic testing is not being used to satisfy tech spec requirements for surveillance.

[ACTION COMPLETED PER MODIFIED RESPONSE AND MARKED-UP 7.2]

RESPONSE

Fault-detection diagnostic testing is not being used to satisfy Technical Specification requirements for surveillance. All of the basic periodic RPS surveillance tests will be used to satisfy the these requirements related to RPS channel and trip system operability.

These periodic tests shall include:

a. Channel checks on each shift or twice per day to verify correspondence of the values of the several instrument channels for all analog type scram variables.

b. Channel functional tests to verify operability and decision logic of the various instrument channels and tests of the output logic channels to verify operability of the actuating devices.

c. Channel calibrations to verify the accuracy of the channel trip decision logic. These are primarily verifications of the required trip setpoints in the Digital Trip Modules (DTMs).

d. Outage/Inspection tests conducted during scheduled refueling outages. These tests consist of: (1) Total channel calibrations which include the channel transmitters or other detection devices as well as the DTMs; (2) Complete RPS logic system functional test. This includes testing all coincidence (2/4) logic and non-coincidence (1/n) logic of the several instrument channels and the four trip systems, and the final actuating trip logic using the arrangement of load drivers to effect the final trip system (2/4) trip logic. Functional tests include both the automatic and manual trip systems and testing of all interlocks related to operational and maintenance bypasses, trip seal-in, reset permissives and trip reset logic, etc.; (3) RPS response time testing; and, (4) Other outage type inspection tests such as APRM simulated thermal power time constant verification and Reactor Mode switch operation functional tests.

CONCERN - DSER Section: 7.2.1 , Page # 7-16 (DSER Summary Item # 2.a)
GE should provide additional information on the Reactor Protection System to address the electrical and physical separation between the four channels. Because of the extensive use of multiplexors and software, the staff considers that isolation of information (error handling) to be an essential factor in its safety determination.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
The requested information was provided in the package described in the closure plan for Item 1.e.

CONCERN - DSER Section: 7.2.2.2 , Page # 7-26 (DSER Summary Item # 1.d)
The staff requests that GE formally submit (docket) its undocketed assessment of the loss of all four divisions of the ABWR Essential MUX, which concluded that the plant could be safely shut down from the remote shutdown system.

CLOSURE PLAN
GE will provide the NRC with a draft of Appendix 19K which includes the requested assessment.

RESPONSE
(See Proprietary Information in separate submittal.)

CONCERN - DSER Section: 7.2.2.2 , Page # 7-27 (DSER Summary Item # 1.e)
GE should define the software architecture that runs in the EMS microprocessors. In addition, GE should demonstrate how the decision logic, which in an analog design is a parallel process, would be implemented by the software, which is usually a serial process. GE has provided high level block diagrams of the data signal paths; however, the software implied in the system block diagrams can mask much of the safety system's design complexity. Since the software is an essential line element in the execution of the safety system functions, a definition of the software architecture is required for the staff to make its safety determination. The architecture should include application specific software, operating system software and embedded software.

CLOSURE PLAN

GE will provide the 18 identified MPL documents under proprietary agreement (mechanics of transmittal to be worked out, i.e., by affidavit, etc., later).

[ACTION COMPLETED PER THE FOLLOWING LIST]

LIST OF DOCUMENTS SENT TO NRC VIA AFFIDAVIT (3 COPIES) ON AUGUST 16, 1991

One copy each was sent to Dino Scaletti, Jim Stewart, and Charlie Miller (Central File/Mail Desk).

(Every page of each document was stamped "GENERAL ELECTRIC CO. PROPRIETARY INFORMATION")

Document Number	CE Number	Revision	Arev. Title	ages
23A6710	5.8.2	0	RPS H/S System Spec.	34
23A1317	1.B.14	1	SSLC Design Spec.	45
22A8477	5.6.1	1	NMS Design Spec.	71
299X700-070	5.18.2b	0/2 *	NEMS Design Spec.	22
23A6327	5.2.4	0	EMS/SSLC Interface Req.	21
23A1302	5.8.1	1	RPS Design Spec.	61
23A6301	5.6.2	0	NMS H/S System Spec.	86
23A6229	5.8.8	0	RPS V&V Criteria Spec.	8
23A5759	5.1.5	A	Imp. Procedure for H/S	29
23A5761	5.1.10	A	MUX Application Proc.	14
23A6761	5.6.9	0	NMS V&V Criteria Spec.	30
23A6280	5.2.1c	0	SSLC V&V Criteria Spec.	7
299X701-016	5.1.8	0/1 *	Safety Sys. App. Proc.	8
299X701-015	5.1.6	0/0 *	Imp. Procedure for V&V H/S	17
299X700-071	5.18.2a	0/2 *	EMS Design Spec.	22
23A5727	5.1.1	1	Integration of C&I Design	23
103E1805	5.2.1	(none)	SSLC Block Diagram	5
"Scroll" Draft	(N/A)	R910809	Design & Impl. Chart	11
App. 19K Draft	(N/A)	8/15/91	MUX Common-Cause Failure	21
DAL #1508	(N/A)	(none)	Codes and Standards	4
DAL #1512	(N/A)	(none)	U.S. ABWR Codes & Stds.	2
IF-R-389 (FMEA)	(N/A)	(none)	SSLC Reliability Analysis	192
Position Paper	5.2.2	0	Allocation of DTM to SSLC	13

* Second number is the corresponding revision of the original H/T document

RESPONSE

(See Proprietary Information in sepsrate submittal.)

CONCERN - DSER Section: 7.2.2.2 , Page # 7-28 (DSER Summary Item # 1.f)
GE should define the functional requirements of the EMS, the major parameters that define the data transmission attributes, and the criteria for selecting the data transmission hardware. The staff recognizes that the detail design of the EMS depends on the hardware that is selected; however, the functional requirements for the EMS as part of the ABWR safety systems are not hardware dependent.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
(See Proprietary Information in separate submittal.)

CONCERN - DSER Section: 7.2.2.2 , Page # 7-29 (DSER Summary Item # 6.a)
The staff requests that GE provide information to clarify how the two DTMs in the EMS network arbitrate to determine which will be the MASTER loop. The staff noted that the two EMS network loops are designated MASTER and STANDBY by the receiving fiber optic interface. The designation of which loop is MASTER is on the basis of transmission errors and checksum errors, as well as the results of self test. The hardware diagrams that the staff has reviewed showed that each Digital Trip Module (DTM) in the SSLC has two fiber optic interfaces. The design parameters of how the MASTER loop is designated is important to the evaluation because it could address possible software failure modes like deadly embrace, lockup, and other contention issues that can disrupt communications EMS. This designation is also applicable at the RMU level where ESF equipment actuation commands are received.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
The requested information was provided in the package described in the closure plan for Item 1.e.

CONCERN - DSER Section: 7.2.2.3 , Page # 7-30 (DSER Summary Item # 1.g)
GE should provide information describing in detail the fault tolerant design features of the SSLC system. In response to the staff request (Q420.49) to describe the fault tolerant features of the SSLC system, GE responded that the system will be capable of error correction of inputs and outputs, retry or rollback to last known correct state on fault detection, restart without lockup on fault such as EMI, data transmission error correction, continued operation through transient fault, and continued operation through permanent fault. GE's response should include additional information which describes the SSLC system design features that accomplish the capabilities described above.

CLOSURE PLAN

GE will provide a fault-tolerance review of the specific items listed in the concern, consistent with its present level of definition, as an amendment to GE response 420.49 (or other appropriate area of SSAR if appropriate).

RESPONSE

The process of testing and verifying fault tolerant features will be discussed in the Inspections, Tests, Analysis and Acceptance Criteria (ITAAC) for the Safety System Logic and Control (SSLC).

CONCERN - DSER Section: 7.2.2.3 , Page # 7-30 (DSER Summary Item # 7.a)

The STS should be considered a safety grade system because it is embedded in the SSLC and interfaces directly with the safety system software. The staff noted that when the STS has possession of the EMS token, a non-safety system (the STS) is in control of a safety system (the EMS), albeit only a short time. A failure of the STS to pass on the token would result in the EMS being disabled until the timeout for the lost token expired, and a new one would be generated. Since the STS software was considered a non-safety system, it must be assumed that the STS software will fail in any conceivable mode, including the mode whereby it keeps running tests. The staff also requests that GE provide information which describes how the STS would acquire the token to send an EMS message and specify the duration of the token timeout.

CLOSURE PLAN

GE will amend Section 7.1.2.1.6(6) which now says "The self-test function is classified as safety associated." to "The self-test function is classified as safety related." Note this issue appears twice in the DSER; section 7.2.2.3 (page 7-30), and section 7.2.3.3 (page 7-43).

[ACTION COMPLETED PER RESPONSE CHANGE AND TEXT MARK-UP]

RESPONSE

GE agrees that the self-test software is safety-related. Subsection 7.1.2.1.6(6) has been changed to state "The self-test function is classified as safety related."

However, note that the self-test implementation in the final SSLC design has changed from the concept discussed in the staff comments (see the response to Item 1.q). On-line self-test is now a monitoring or diagnostic-type system embedded in the software of each microprocessor-based controller. Critical circuit nodes and program flow are continuously monitored for deviations from normal states. Thus, self-test is not actively involved with token passing or other aspects of multiplexing.

CONCERN - DSER Section: 7.2.3 , Page # 7-31 (DSER Summary Item # 3.a)
GE should provide Failure Modes and Effects Analysis information in accordance with GDC 23, "Protection System Failure Modes." This information should demonstrate that all postulated RPS and ESF failures result in a known safe state if conditions such as disconnection of the system, loss of energy or a postulated adverse environment are experienced.

CLOSURE PLAN
Same as DSER Summary Item 1.e. Note this issue is shown twice in the DSER; section 7.3.2 (page 7-52), and section 7.2.3 (page 7-31).

RESPONSE
"...all postulated RPS and ESF failures..." would include vendor specific information dependent on the hardware and associated software employed. However, a more detailed FMEA was provided in the package described in the closure plan for Item 1.e.

CONCERN - DSER Section: 7.2.3.1 , Page # 7-32 (DSER Summary Item # 8.a)
GE should provide information which identifies the design bases and criteria for EMC and environmental qualification. The quality levels of the SSLC hardware, thermal design implementation limits and design practices or standards to limit possible EMI effects should also be provided. The lack of design control for these parameters could result in common mode failures for multiple divisions, from such failures as loss of HVAC, and electromagnetic interference pulses from uninticipated field effects common to all divisions The potential for disabling multiple RPS and ESF logic divisions is a critical safety concern that requires additional review.

CLOSURE PLAN
Item 8.a is closed based on resolution of 5.a. In conjunction with 5.a, GE will review ANSI C37.90.2, Mil Specs 461 and 462, and ANSI C63.12 for application to the ABWR regarding EMC. Appendix 7A will be amended to address such standards (or others) deemed appropriate following the review.

[ACTION COMPLETED PER REFERENCES IN RESPONSE]

RESPONSE
For a commitment to thermal design limits, see the response to Item 8.c.

For a commitment to criteria for EMC requirements, see the response to Item 5.a.

CONCERN - DSER Section: 7.2.3.1 , Page # 7-33 (DSER Summary Item # 9.a)
The staff requests GE clarify which RPS signals are multiplexed and which are not. Figure 7A-1 in GE Document No. 23A1317 of undocketed MPL Document A32-4080, showed that many of the RPS related sensors are connected directly to the Digital Trip Modules (DTM) and do not go through the EMS. This was contradicted by Figure 7.A.2-1 in SSAR Chapter 7A which showed all the sensor signals sent via the EMS.

CLOSURE PLAN

GE will review and correct Table 7A.2-1 as required, consistent with the proposed closure response and GE document 23A1317. GE will also submit expanded FMEA on the same basis as DSER Summary Item 1.e.

[ACTION COMPLETED PER RESUBMITTAL OF TABLE 7A.2-1 (FMEA submitted earlier)]

RESPONSE

The following signals are hard-wired directly from the instrument channel sensors output contacts to the Digital Trip Module input terminals:

a. Turbine stop valves limit switch signals;

b. Turbine control valves emergency trip system oil pressure monitoring pressure switch signals.

c. Turbine first stage pressure monitoring transmitters 4-20 milliampere analog value signals; and,

d. Main steam line isolation valves limit switch signals.

The output signals from the four Process Radiation Monitoring System panels in the control room are also wired directly to the DTMs. Here, the DTMs are mainly used only to distribute the signals from each of the four PRRM panels to all four RPS automatic trip systems, since any trip decisions have already been made by the PRRM System.

In the case of the Neutron Monitoring System SRNM and APRM signals, these two trip signals are sent from each NMS division, by isolated wiring, to all four RPS Trip Logic Units (TLUs).

The only instrument channel signals associated with the RPS that are multiplexed, and utilize the Essential Multiplexing System for signal transmission of sensor signals from the transmitters to the DTM input terminals are:

a. Reactor vessel pressure transmitter signals;

b. Reactor narrow range water level transmitter signals;

c. Drywell pressure transmitter signals; and,

d. CRD accumulator charging header pressure transmitter signals.

Criteria used in deciding which instrument channels should or could be hard-wired from sensor outputs to the inputs of the RPS related equipment in the main control room included the following:

A. All turbine building originating variables would be hard-wired. The primary reason being that no EMS remote multiplexing units would be located in the turbine building.

B. All variables with extremely fast instrument channel response time requirements should be hard-wired.

C. For instrument channels where the trip decision is made by the remote sensing device, by itself, e.g., by valve limit switches, by pressure switches, or for

cases where trip decisions are made by equipment of other supporting systems located in the main control room, these instrument channels could be hard-wired.

CONCERN - DSER Section: 7.2.3.1 , Page # 7-33 (DSER Summary Item # 10.a)
CE should provide additional information which describes design features to preclude the common mode failure of software, including an analyses which demonstrates how the SSLC, EMS, ESF, and STS designs comply with NUREG-0493.

Since the ARI function and the SLCS instrumentation are subject to the common mode failure of the EMS and SSLC systems for effects such as EMI or software operational problems, the analysis should consider the detailed effects of such failures and how operation of the systems could continue. The staff also noted the possibility that the EMS and NEMS would use the same software modules and, therefore, upon a software error, could fail simultaneously. This would represent a challenge to defense-in-depth and should be evaluated. Since a detailed failure modes and effects analysis will not be performed for the STS system, it was also unclear to the staff how the SSLC design would mitigate the results of a postulated common mode failure of the STS software (related open item - no. 7).

CLOSURE PLAN
GE will submit appendix to "Design Alternatives Evaluation Report" as part of DSER Summary Item 1.e. GE will submit information showing how NUREG-0493 was used in conjunction with designs for ATWS, SSLC, RSS (per mechanics of 1.e). Control and information systems may also be added (GE's option) in support of the diversity and defense-in-depth argument. Note this issue is stated twice in the DSER; section 7.2.3.1 (page 7-33), and section 7.4.2 (page 7-59).

RESPONSE
An analysis to investigate ABWR compliance with NUREG-0493 is presently being performed by Lawrence Livermore Laboratories (LLL), which will be reviewed by GE. This issue should be closed based on the outcome of that study.

CONCERN - DSER Section: 7.2.3.1 , Page # 7-34 (DSER Summary Item # 1.h)
GE should provide additional information which describes the bus protocol for the SSLC hardware design, bus data capacity, accommodations for hardware level interrupts, size of the memory, speed and size of the microprocessor, format of the status panel, hardware based interlocks, type of display media, and the method of providing the TLU trip status to the operator.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
The requested information was provided in the package described in the closure plan for Item 1.e.

CONCERN - DSER Section: 7.2.3.1 , Page # 7-34 (DSER Summary Item # 1.i)
GE should provide information which describes the design approach employed for the SSLC software. GE should also demonstrate how the decision logic, which in an analog design is a parallel process, will be implemented by the software, which is a serial process. GE should present design documentation of how the listed software elements will interact with each other and what considerations were given to ensure data integrity, error handling, task priority, timing, variable representations, module structures, interrupt handling, and fault tolerance.

CLOSURE PLAN
Same as 1.a. In addition, GE will provide information describing the 10 millisecond time allowance window for 2/4 logic signal arrivals.

RESPONSE
(See Proprietary Information in separate submittal.)

CONCERN - DSER Section: 7.2.3.1 , Page # 7-35 (DSER Summary Item # 1.j)
A top level design of the SSLC software is required for the staff to make its safety determination. The staff acknowledged GE's statements that the software design for the SSLC was not available for review because it is hardware dependent and the hardware had not been selected. The staff also reviewed the SSLC design description presented in the SSLC System Design Specification (SDS) (undocketed). The staff considered the documentation presented for the SSLC to be inadequate for design evaluation and not in conformance with the requirements for level of detail. Because software implements the functionality of computer-based SSLC, the top level design of the software is necessary for the staff review.

CLOSURE PLAN
Same as DSER Summary Item 1.e. Note this issue is stated twice in the DSER; section 7.2.3.1 (page 7-35), and section 7.2.3.2 (page 7-42).

RESPONSE
The requested information was provided in the package described in the closure plan for Item 1.e.

CONCERN - DSER Section: 7.2.3.1 , Page # 7-36 (DSER Summary Item # 1.k)
GE should provide information, in accordance with IEEE Std 7-4.3.2, describing methods to be employed to verify and validate the development of the software which would implement the SSLC and EMS logic functions.

CLOSURE PLAN
Same as DSER Summary Item 1.e. Note this issue is stated twice in the DSER; Section 7.1.3.3 (page 7-11), and section 7.2.3.1 (page 7-36).

RESPONSE
The general V&V plan methodology has already been given to the NRC. (See Appendix 7A, items 7A.5(1) & 7A.7). Additional information was supplied in the package described in the close plan for Item 1.e.

CONCERN - DSER Section: 7.2.3.2 , Page # 7-37 (DSER Summary Item # 1.l)
GE should provide information which describes the EMS fiber optic local area network design requirements upon which the control standard, the software and hardware selection was based. Since the EMS is central to the functioning of all safety systems for the ABWR, the staff has concluded that more detailed specifications of the EMS are required prior to making its safety determination.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
The requested information was provided in the package described in the closure plan for Item 1.e.

CONCERN - DSER Section: 7.2.3.2 , Page # 7-37 (DSER Summary Item # 1.m)
A top level design of the EMS software is required for the staff to make its safety determination. The staff acknowledges GE's statements that the software design for the EMS was not available for review because it is hardware dependent and the hardware had not been selected. However, in the development of computer-based systems, the staff considers it to be good engineering practice to have a top level design of the software as a criteria to be considered in the hardware selection.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
The requested information was provided in the package described in the closure plan for Item 1.e.

CONCERN - DSER Section: 7.2.3.2 , Page # 7-38 (DSER Summary Item # 1.n)
The staff requests that GE clarify the design description presented for the EMS regarding synchronous communication of the local area network. In SSAR Appendix 7A it stated that the "...systems are independent and will run asynchronously..." [page 7A.2-2], in the EMS/SSLC Interface Requirements [MPL A32-4080] it stated that the system timing will be asynchronous...", and [page 5] "all communications shall be asynchronous...". However, in the same document it stated that "...communications processing circuitry... will append

synchronizing and parity checking information" [page 14, Section 3.5.1; and similarly in Section 3.5.3].

CLOSURE PLAN
GE will amend the SSAR with clarifications consistent with the proposed closure response.

[ACTION COMPLETED PER MARK-UP OF 7A.2-2]

RESPONSE
(See Proprietary Information in separate submittal.)

CONCERN - DSER Section: 7.2.3.2 , Page # 7-39 (DSER Summary Item # 1.o)
The staff requests that GE clarify the contradictory design information provided on the Control Multiplexor Unit (CMU), an essential part of the EMS. From the information in Appendix 7A, it was apparent that the EMS consisted of the Remote Multiplexor Unit (RMU), the CMU, and the fiber optic cable connecting the RMU and CMU. However, in most of the drawings reviewed by the staff, the CMU was not shown as a separate component but as an implied part of the SSLC, although the RMU was shown explicitly connected to the multiplexor system (of which the RMU was a part).

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
(See Proprietary Information in separate submittal.)

CONCERN - DSER Section: 7.2.3.2 , Page # 7-39 (DSER Summary Item # 2.b)
GE should clarify design information provided on the issues of electrical, data and control isolation and separation. The manner of sending data to the plant computer was stated in general terms, and key design issues remained unclear. GE stated that the sensor data is taken from the CMU and sent to the plant computer through a data buffer. It was stated that the data buffer provided isolation between the plant computer and the safety system EMS, but no data was provided about the location of the data buffer, how the read/write access was controlled, and which device cleared the buffer.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
See the response to Item 1.v.

CONCERN - DSER Section: 7.2.3.2 , Page # 7-40 (DSER Summary Item # 1.p)
The staff requests GE to clarify a discrepancy in the description of the major components of the EMS. The Multiplixing Control Units (MCU) is discussed in SSAR Section 15.B.4 although it was not discussed as a separate component in SSAR chapter 7. It was unclear whether this was an abstraction to facilitate the FMEA or whether the EMS does indeed contain an element called MCU. The MCU was described as the bridge between the optical and digital signals, with the stated purpose of providing control of the data transmission. Other documentation stated that control of the fiber optic transmission medium was shared between RMUs and CMUs. It was also unclear whether the MCU was the communications module in the RMU and CMU.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
The functions [illegible] described in the Essential Multiplexing Design Specification. [illegible] that these functions may be allocated to the other MUX units [illegible] in the actual design. The final EMS design uses only RMUs and the CMU function.

CONCERN - DSER Section: 7.2.3.2 , Page # 7-41 (DSER Summary Item # 11.a)
GE should provide an I&C failure analysis which includes outages due to I&C maintenance and a discussion of acceptable maintenance practices. The staff noted that additional information provided in response to questions has not provided enough detail for the staff to evaluate the GE findings. The staff also requests that GE clarify its maintenance requirements for Reactor Internal Pump (RIP) maintenance and the associated reliance, in part, on leak detection instrumentation to detect failures. The clarification should also describe the availability of the leak detection system during shutdown maintenance on the RIPs.

CLOSURE PLAN
NRC will review references relating to this concern.

RESPONSE
Maintenance on the ABWR Reactor Internal Pumps (RIP) does not depend on instrumentation for leak detection. The RIPs have leak detection tubes for monitoring leakage during maintenance. These tubes are shown on the Reactor Recirculation System P&ID (please refer to Figure 5.4-4 of the ABWR SSAR). The tubes, which are plugged during plant operation, are unplugged for RIP motor installation. Each tube connects to the space between a flat gasket and an o-ring which is outboard of the gasket. The tubes will detect leakage of the main gasket after the motor is reinstalled and filled with water. This concept has been applied to detect leaks from both the main motor cover and the smaller auxiliary cover located on the bottom center of the motor cover.

Use of these leak detection tubes has been proven in European BWRs with internal recirculation pumps (Asea Brown Boveri plants). In instances where leakage was experienced due to improper installation, the leakage was detected through the leak-off tubes, and the gaskets were replaced prior to plant startup. ABB has

never experienced a leaking main gasket during plant operation. Thus, conventional leak detection instrumentation is not considered necessary for the ABWR RIPs.

CONCERN - DSER Section: 7.2.3.3 , Page # 7-44 (DSER Summary Item # 1.q)
The staff requests GE to clarify its design information on the Self Test System (STS). GE indicated that the STS must cycle from circuit-to-circuit very rapidly. It is not clear to the staff what circuits are referred to since the SSLC is implemented using digital microprocessors. GE did not state if the STS would place the SSLC software in a special testing mode to allow very rapid cycling of the system test.

CLOSURE PLAN
NRC staff will review the latest amendment of SSAR Section 7.1.2.1.6 (sixth test) in conjunction with the SSLC Design Spec (submitted per DSER Summary Item 1.e).

RESPONSE
(See Proprietary Information in separate submittal.)

CONCERN - DSER Section: 7.2.3.3 , Page # 7-44 (DSER Summary Item # 2.e)
GE should provide additional information on the STS and SSLC to address the issue of data and control separation. The staff noted that fiber optical data links will be used to ensure electrical separation; however, the issue of information separation has not been addressed. GE should demonstrate that the STS and SSLC designs preclude adverse effects within the extensive data and control software considering the interconnection of STS modules in each division within the control room. GE should also examine the safeguards incorporated to provide isolation and separation according to IEEE-279.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
Such information is provided in 7A.2(13). Additional information was provided in the package described in the closure plan for Item 1.e.

CONCERN - DSER Section: 7.3.1.10, Page # 7-51 (DSER Summary Item # 8.c)
GE should provide additional information to address design limit(s) for HVAC equipment designs. The staff noted the HVAC cooling design provided in the SSAR represents traditional bWR cooling designs, but does not reflect consideration of any additional cooling required to limit the presence of hot spots due to higher current densities within the digital chip designs employed in the ABWR. The staff also requests GE to comment on any additional HVAC controls and direct cooling requirements.

CLOSURE PLAN

GE will add the requirement for 27 degrees F temperature rise into the ABWR SSLC design spec. The mechanics for reflecting this on the docket will be consistent with DSER Summary Item 1.e.

[ACTION COMPLETED PER ADDITION TO RESPONSE]

RESPONSE

The design responsibility for limiting the presence of hot spots due to current densities within digital chips is with the vendor of the equipment utilizing the chips. The ABWR design specifies the ambient temperature within which the equipment must function properly. The vendor determines if forced cooling is required or if natural convection is adequate. In either case, the cooling is obtained by use of ambient air from the surrounding room.

The digital chip designs for the ABWR should have lower current densities (CMOS) than previous designs. This only affects the sizing of the HVAC equipment, however.

A special ducted cooling system is provided for the reactor internal pump (RIP) power supplies because of the large amount of heat generated by them.

The room ambient temperatures are maintained stable and within the required limits by the use of HVAC systems in conjunction with chilled water systems. The HVAC systems are described in SSAR Section 9.4. The chilled water systems are described in 9.2. The environmental limits, including ambient temperature limits, are given in SSAR Appendix 3I. These systems are conventional nuclear industry HVAC systems without special controls and are not peculiar to the BWR.

In order to bound the requirements for HVAC equipment design in ABWR, the heat rise limits for the digital signal processing units included in Safety System Logic and Control (SSLC) shall be added to the SSLC System Design Specification, GE Document No. 23A1317, Section 2.3.7, Environment, in a new paragraph, as follows:

"2.3.7.3 The heat release by internal panel components shall not raise the internal temperature of the panel to greater than 27 degrees F above external ambient temperature of the control room for electronic components within a chassis or within any printed circuit card file structure."

Note that existing paragraph 2.3.7.1 limits the method of panel cooling to natural convection when qualifying safety-related equipment for Class 1E service. Fans may be used to improve long-term reliability, but no safety credit will be claimed for forced-air cooling in analyses for thermal design adequacy.

CONCERN - DSER Section: 7.3.1.2 , Page # 7-47 (DSER Summary Item # 12.a)
The staff requests that GE clarify an apparent contradiction in the power supply sources for the ADS and RCIC systems. SSAR section 7.3.1.1.1.2 (2) indicates that the ADS is powered from Divisions I & II. However, SSAR Figure 7.2-1 (Amendment 5) indicates that the ADS power supplies are from Divisions 1 and IV. Similarly, the SSAR section 7.3.1.1.1.3 (3) indicates that the RCIC is powered from Division I; however, Figure 7.2-1 indicates that RCIC is powered from Divisions II and IV.

CLOSURE PLAN
Closed based on Amendment 17. No further action required.

RESPONSE
Figure 7.2-1 was modified and submitted with Amendment 17. The text descriptions referenced were correct for both ADS and RCIC, and are now consistent with Figure 7.2-1 following that amendment.

CONCERN - DSER Section: 7.4.1.1 , Page # 7-57 (DSER Summary Item # 1.c)
The staff wants more detailed information on RPS and RC&IS to make its safety determination. The staff will conduct detailed discussions with GE to specify the scope of required information.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
The RC&IS is not a safety system, and should not be included in the staff's safety determination. However, GE supplied the requested information in the package described in the closure plan for Item 1.e.

CONCERN - DSER Section: 7.4.2 , Page # 7-59 (DSER Summary Item # 13.a)
The staff requests that GE provide information which describes how the two Remote Shutdown Panels, which are to be located in separate areas, can be operated simultaneously or in a master/slave arrangement. In addition, the staff requests GE to clearly describe in the SSAR how data is transferred to the two remote shutdown panels in the event that the control room becomes unusable.

CLOSURE PLAN
GE will provide the clarification requested in Section 7.4.1.4.4, consistent with this proposed closure response, and that of 1.r. Note this issue is stated twice in the DSER; section 7.4.2 (page 7-59), and section 7.5.2 (page 7-64).

[ACTION COMPLETED PER LAST PARAGRAPH ADDED TO RESPONSE]

RESPONSE

Two Remote Shutdown System (RSS) panels are provided to interface with equipment in two plant mechanical/electrical divisions. Complete divisional separation is maintained between the two panels. During operation from the RSS, equipment in both divisions will be operated in parallel (i.e., the operator will use controls and indicators provided on both panels). The panels are located in one remote shutdown area with a fire barrier separating them, as shown on the attached diagram. A sliding door forms a part of the fire barrier. The door can be opened during RSS operation to allow the operator to move easily between the two RSS panels. With the door opened, the operator has a clear view of both panels.

RSS control of interfacing systems equipment is accomplished by actuating manual transfer switches on the RSS panels. These transfer switches override the signals from the main control room and transfer control to the RSS. Both equipment control signals and process sensor signals are transferred in this manner. Operation of the transfer switches will initiate an alarm in the main control room.

An addition was made to Section 7.4.1.4.4 of the SSAR, in association with Response 1.r, which clarifies the transfer of control to the remote shutdown panels.

CONCERN - DSER Section: 7.4.2 , Page # 7-60 (DSER Summary Item # 1.r)

The staff requests GE to clarify design information which describes how the transfer of sensor transmitter outputs would occur without the loss of the calibration data updates. The staff notes that the calibration data updates would be stored in the SSLC system microprocessors which would presumably be disconnected from the readouts.

CLOSURE PLAN

GE will review SSAR Section 7.4.1.4.4 (Remote Shutdown System description) and revise, as necessary, to clearly state the system's independence from the SSLC (i.e., fully hard-wired interfaces) following transfer.

[ACTION COMPLETED PER ADDITION TO 7.4.1.4.4(1), AND AS NOTED IN THE ADDITION TO THE PREVIOUS RESPONSE]

RESPONSE

GE assumes this comment relates to transfer of sensor transmitters to the alternate signal path of the Remote Shutdown System. Within SSLC, automatic calibration is applied only to the analog-to-digital converters in the RMUs. When transfer is made to the Remote Shutdown System, the direct 4-20 mA outputs of the transmitters are routed to the analog trip units of the RSS instrument channels. Calibration of sensors and transmitters is performed by conventional, manual means.

The following clarification is added to Section 7.4.1.4.4(1):

Control and process sensor signals are interrupted by the transfer devices at the hardwired, analog loop. Sensor signals which interface with the remote shutdown system are routed from the sensor, through the transfer devices on the remote shutdown panels, and then to the multiplexing system remote multiplexing

units (RMUs) for transmission to the main conrol room. Similarly, control signals from the main control room are routed from the RMUs, through the remote shutdown transfer devices, and then to the interfacing system equipment. Actuation of the transfer devices interrupts the connection to the RMUs and transfers control to the remote shutdown system.

.....

CONCERN - DSER Section: 7.5.1 , Page # 7-62 (DSER Summary Item # 1.s)
GE should provide design information to demonstrate the manner in which safety related data will be processed and displayed, and describe dependencies on the supporting hardware and software. The staff acknowledges that GE has provided a comprehensive list of variables that were considered essential for providing safety related information to the operators. Explicit tables of conformance and specific exceptions to RG 1.97 were provided in the SSAR, and functional requirements for display of data were provided in the process system descriptions in the SSAR.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
The requested information was provided in the package described in the closure plan for Item 1.e.

.....

CONCERN - DSER Section: 7.6.2 , Page # 7-69 (DSER Summary Item # 1.t)
GE should provide design documentation to demonstrate that conformance to appropriate standards will be achieved. The staff acknowledges GE's commitment in the SSAR which states that interlock systems important to safety (i.e., Neutron Monitoring System, Process Radiation Monitoring System, High Pressure/Low Pressure Interlocks, Fuel Pool Cooling and Cleanup System, Drywell Vacuum Relief System, Containment Atmosphere Monitoring System and Suppression Pool Temperature Monitoring System) are in conformance with the applicable GDCs, Regulatory Guides and Branch Technical Positions; however, GE has not provided design information to confirm that these commitments will be manifest in the design.

CLOSURE PLAN
NRC will re-examine the concern on the basis of a docket submittal of the V&V (VISION) documents and DSER Summary Item 1.a. The mechanics of that submittal will be consistent with DSER Summary Item 1.e.

RESPONSE
It was our understanding that when full conformance to criteria is met, a simple declaration of such conformance is sufficient for the analysis sections, because elaborations would tend to be redundant to information already provided in the description sections. However; clarifications, justifications, or exceptions to criteria are elaborated in the analysis sections.

****

CONCERN - DSER Section: 7.7.1.15, Page # 7-77 (DSER Summary Item # 8.d)
GE should define the sensitivity of safety computer systems to electromagnetic fields and provide information to identify acceptable radiation levels and frequency ranges for plant communication transmitters and receivers. Controls, test programs, field measurements and operational descriptions should be employed to implement EMC and avoid effects such as spurious actuation of safety related equipment.

CLOSURE PLAN
Same as 8.a/5.a with additional emphasis on installation procedures, site test procedures, and vendor testing (i.e., site survey data). This is a possible SSAR Chapter 3 amendment.

[ACTION COMPLETED PER MODIFIED RESPONSE]

RESPONSE
(See Proprietary Information in separate submittal.)

****

CONCERN - DSER Section: 7.7.1.3 , Page # 7-71 (DSER Summary Item # 1.u)
GE should provide additional information on the I&C design of the Recirc Flow Control System to facilitate an assessment of possible single failure points of the design such as manual control, automatic speed control input, the interprocessor communication links and load demand signal from main turbine pressure regulator.

CLOSURE PLAN
GE will provide information illustrating single failure potential is negligible for the Recirc Flow Control System. The mechanics of that submittal will be consistent with DSER Summary Item 1.e.

[ACTION COMPLETED PER MODIFIED RESPONSE]

RESPONSE
The description of the Recirculation Flow Control System (RFCS) presented in Section 7.7 has been augmented with the following subsequent information packages sent to the NRC:

a. "Postulated All RIP Trip Event due to Common Cause Failure," Attachment to transmittal from J.N. Fox to D.C. Scaletti, dated March 20, 1991.

b. "Additional Information on Recirculation Flow Control System and RIP Power Supplies," Attachment C. to transmittal from J.N. Fox to D.C. Scaletti, dated May 8, 1991.

The following additional information is provided in accordance with the closure plan determined at the August, 1991, meetings:

The primary design goal for the RFCS is to ensure that any single active component failure will not result in a loss of system function. The RFCS Design Specification includes the following requirements regarding single failure

points and system fault tolerance:

1. The RFCS controller shall ensure that no single active component failure within the RFCS process sensing, control, or communications equipment shall result in a loss of continuous validated demand signals to the RFCS critical operator displays and reactor recirculation system (RRS) actuators.

2. Under normal conditions, no single equipment failure in either the RFCS or RRS shall result in loss of more than three of the recirculation pumps. (Note that loss of three pumps has been analyzed as a normal ABWR transient event.)

3. No single equipment failure in either the RFCS or the RRS shall cause more than one of the recirculation pumps to run out.

The attached figures provide information to support an assessment of possible single failure points within the RFCS. These diagrams emphasize the key areas of interest identified by the NRC staff during the August 7&8, 1991, meetings: the load demand error input signals from the pressure regulator and the speed demand output signals to the recirculation pumps.

Figure 1 shows the RFCS controller design. The RFCS is implemented on the triplicated, microprocessor-based fault tolerant digital controller (FTDC). The ABWR feedwater control system and steam bypass & pressure control (SB&PC) system are also based on the standardized FTDC design. The FTDC includes three identical processing channels, each of which contains the hardware and firmware necessary to perform the system control calculations in parallel, and three identical interface units, which provide the interface with the triplicated non-essential multiplexing system (NEMS) network and other dedicated data links. Interprocessor communication links are provided to exchange data between the FTDC processing channels in order to prevent divergence of outputs. The FTDC channels are powered by redundant power supplies.

Figure 1 also shows the interface between the RFCS and the SB&PC system. This interface is supported by three dedicated data links between the two system controllers. Through these data links, the RFCS and SB&PC system exchange the signals needed for automatic load following operation. When the RFCS is placed in the automatic load following operating mode, redundant signals are sent over the data links to initiate the SB&PC pressure setpoint adjustment logic. The SB&PC system provides redundant load demand error signals to the RFCS for load following control. In addition, the SB&PC system supplies redundant, validated, wide range dome pressure signals through these data links for use in the RFCS pump trip logic.

Figure 2 shows the RFCS interface with the recirculation pumps. The three demand signals generated by the three FTDC processing channels are sent over the triplicated NEMS network to remote, fault-tolerant, output voters. The voters perform a mid-value selection on continuous output signals (e.g., recirculation pump speed demand) and two-out-of-three voting on discrete outputs (e.g., pump trip). This voting scheme assures that an erroneous demand signal resulting from a single failure in the FTDC or the NEMS will not be selected as the final demand signals sent to the actuator. Thus, any single failure in the FTDC or NEMS will not affect the process.

A separate voter is provided for each recirculation pump, so that a voter failure will only impact the control of a single pump. In the event of a voter failure, the RFCS controller will automatically compensate by adjusting the speed demand signal to the other pumps. In addition, a "ringback" feature is provided in which the critical voter output signals are sent back to the FTDC channels in order to detect a voter failure.

The fault-tolerant architecture of the RFCS design assures that no single active component failure with the sensing, control, or communications equipment will result in a loss of system function.

.....

CONCERN - DSER Section: 7.7.2 , Page # 7-78 (DSER Summary Item # 2.c)
GE should provide design information to address the issue of safety system connectivity to non-safety systems. It appears to the staff that the Non-Essential Multiplexing System (NEMS) is directly connected to the EMS through the CMU of the EMS. Since the EMS is used to carry safety system sensor data and to activate the control ESF systems, a failure in the EMS would disable a division. A failure of the NEMS or plant computer could challenge or adversely affect the operation of the EMS, unless the broadcast software had design features that would make such failure propagation improbable. In particular, the staff was concerned with software failures in the NEMS that could lead to undetected software failures in the EMS.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
See the response to Item 1.v.

.....

CONCERN - DSER Section: 7.7.2 , Page # 7-79 (DSER Summary Item # 1.v)
GE should provide additional information to facilitate an evaluation of the EMS/NEMS connection and how it addresses the isolation requirements of IEEE 279.

CLOSURE PLAN
Same as DSER Summary Item 1.e.

RESPONSE
(See Proprietary Information in separate submittal.)

.....

CONCERN - DSER Section: 7.8 , Page # 7-80 (DSER Summary Item # 1.w)
GE should provide additional information which demonstrates that equipment design and installation standards are incorporated to prevent electrostatic discharge (ESD) at keyboards, keyed switches and other exposed equipment components.

CLOSURE PLAN
GE will amend the response to 402.90 to include a reference to IEC 801-2, or other appropriate standard(s).

[ACTION COMPLETED PER MODIFIED RESPONSE]

RESPONSE

The response to RAI 420.090 discussed several precautions to be taken against electrostatic discharge (ESD) in electronic assemblies, and also described typical circuit design and equipment grounding methods to prevent component damage.

The following response is added to the response of RAI 420.090. The additional material includes a reference to industry standards that verify conformance to ESD requirements.

Microprocessor-based control equipment for ABWR is designed under the assumption that users will have taken no precautions against static charge buildup before attempting to operate the equipment. The equipment is designed to tolerate an electrostatic discharge without damage, partly by employing insulation (with no air gaps) over exposed metallic components, but primarily by providing an alternative path for current flow other than through sensitive circuit paths. As discussed previously, this means that all exposed metallic components of the system must be grounded. Low inductance multipoint grounds are used where ESD current flow is desired and single-point grounds where discharge flow is not wanted.

The low power requirements of ABWR control equipment ensure that the integrity of the equipment enclosures is not compromised by large ventilating holes or slots. Special attention is given to hinges, joints, and seams so that the continuity of shielding is maintained.

In the system configuration, where shielded cables transfer data between the equipment enclosures, the cables must be prevented from propagating ESD currents and voltages between system units. For ABWR safety systems, the problem has been minimized by using fiber optic cables as the transmission medium for most critical signals. While the cables may contain metallic supporting members or protective shields, these will not be electrically connected to any equipment or circuit. For certain functions where hardwired cable is required, solid grounding of cable shields to the equipment chassis and bypass capacitors at all inputs and outputs shall be used to divert ESD currents to ground.

These hardware solutions shall be supplemented with firmware ESD solutions to protect against potential upsets such as system lockup if ESD noise causes memory or data flow errors. The methods used are discussed as part of the fault-tolerance issues included in Items 1.g and 1.i.

The susceptibility of ABWR control equipment to electrostatic discharges shall be established using the test procedures included in IEC Publication 801-2, Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment, Part 2: Electrostatic Discharge Requirements. The test procedures of paragraph 8 of this document shall be performed up to and including Severity Level 4, as defined in the document. The following acceptance criteria shall be used:

1. No change in trip output status shall be observed during the test.

2. Equipment shall perform its intended functions after the test.

Note that the safety system control equipment for ABWR has inherent protection against transient ESD effects in that data is continually refreshed throughout the system, including trip, display and indicator status. Further protection is provided by the asynchronous, four-division, 2-out-of-4 channel configuration. Temporarily corrupted data in one division cannot cause an inadvertent trip or permanently disable a required trip. When bad data or equipment damage is detected, the affected division can be bypassed until repaired. In the Reactor Protection System (RPS) and Main Steam Isolation Valve (MSIV) channels, where the final trip outputs are also in a 2-out-of-4 configuration, both the sensor input and trip output sides of each equipment division can be bypassed, thus preventing failure from any cause in one channel from inhibiting or inadvertently causing a trip.

.....

CONCERN - DSER Section: 7.8 , Page # 7-80 (DSER Summary Item # 8.b)
The staff concluded that ESD should not be considered a site specific concern and recommends that it be removed as an interface requirement from Section 7.8 and Table 1.9-1.

CLOSURE PLAN
GE will delete "Interface" comment per NRC recommendation.

[ACTION COMPLETED PER RESPONSE CHANGE AND TEXT MARK-UP]

RESPONSE
The interface defined in 7.8 does not require the methods be generated by the applicant, but was intended to be confirmatory of the methods presented in RAI 420.90. However, the interfaces have been deleted in Table 1.9-1 and Section 7.8.2 as requested.

.....

CONCERN - DSER Section: 7.8 , Page # 7-81 (DSER Summary Item # 2.d)
GE should provide information in Section 7.8 of the SSAR to specifically address non-safety information interfaces; that is, information transfer between safety and non-safety systems. The staff acknowledged that GE performed a study of each of the I&C systems included in Chapter 7 of the SSAR and determined that there are no safety-related electrical signal interfaces and therefore no interface requirements for the utility applicant. However, the SSAR did not address information transfer to equipment outside of the scope of the SSAR.

CLOSURE PLAN
Closed based on "interfaces" definition in proposed closure response. Flectrical interfaces are being addressed per 2.a,b,c, and e; but will not be reflected in Section 7.8, since they are within GE scope and do not affect the utility/applicant.

RESPONSE

The intent of Section 7.8 is to provide a consolidated listing of actions required by the utility/applicant (i.e., "interfaces") to complete the licensing process. Electrical interfaces between Class 1E and non-Class 1E circuits; and between redundant divisions of Class 1E circuits are accomplished through fiber-optic cable links, as described in other sections.

DSER open issues relating to isolation of corrupted data, error handling, etc., will be addressed in conjunction with open items 2.a,b,c, and e.

Table 1.9-1

SUMMARY OF ABWR STANDARD PLANT INTERFACES WITH REMAINDER OF PLANT (Continued)

ITEM NO.	SUBJECT	INTERFACE TYPE	SUBSECTION
5.2	Conversion of Indicators	Procedural	5.2.6.2
5.3	Fracture Toughness Data	Confirmatory	5.3.4.1
5.4	Materials and Surveillance Capsule	Confirmatory	5.3.4.2
6.1	Protection Coatings and Organic Materials	Confirmatory	6.1.3.1
6.2	External Temperature	Confirmatory	6.4.7.1
6.3	Meterology (X/Qs)	Confirmatory	6.4.7.2
6.4	Toxic Gases	Confirmatory	6.4.7.3
7.1	Effects of Sation Blackout on HVAC	Confirmatory	7.8.1
7.2	~~Electrostatic Discharge on Exposed Equipment Components~~ (Deleted)	~~Confirmatory~~	7.8.2
7.3	Localized High Heat Spots in Semiconductor Material for Computing Devices	Confirmatory	7.8.3
8.1	Stability of offsite power system	Confirmatory	8.1.4.1
8.2	Diesel Generator Reliability	Procedural	8.1.4.2
8.3	Class IE Feeder Circuits	Design	8.2.3.1
8.4	Non-class IE Feeders	Design	8.2.3.2
8.5	Specific ABWR Standard Plant/remainder of plant power sysytem interfaces	Design	8.2.3.3
8.6	Interupting Capability of Electrical Distribution Equipment	Confirmatory	8.3.4.1
8.7	Diesel Generator Design Details	Confirmatory	8.3.4.2
8.8	Cerified Proof Tests on Cable Samples	Confirmatory	8.3.4.3
8.9	Electrical Penetration Assemblies	Confirmatory	8.3.4.4
8.10	Analysis Testing for Spatial Seperation per IEEE 304	Confirmatory	8.3.4.5

(6) The sixth test is an integrated self-test provision built into the microprocessors within the safety system logic and control (SSLC). It consists of an on-line, continuously operating, self-diagnostic monitoring network; and an off-line semi-automatic (operator initiated, but automatic to completion), end-to-end surveillance program. Both on-line and off-line functions operate independently within each of the four divisions. There are no multi-divisional interconnections associated with self-testing.

The primary purpose of the self test is to improve the availability of the SSLC by optimizing the time to detect and determine the location of a failure in the functional system. It is not intended that self-test eliminate the need for the other five manual tests. However, most faults are detected more quickly than with manual testing alone.

The self-test function is classified as safety related. ~~However,~~ its hardware and software are an integral part of the SSLC and, as such, are qualified to Class 1E standards.

The hierarchy of test capability is provided to ensure maximum coverage of all EMS/SSLC functions, including logic functions and data communications links. Testing shall include:

(a) On-line Continuous Testing

A self-diagnostic program monitors each signal processing module from input to output. Testing is automatic and is performed periodically during normal operation. Tests will verify the basic integrity of each card or module on the microprocessor bus. All operations are part of normal data processing intervals and will not affect system response to incoming trip or initiation signals. Automatic initiation signals from plant sensors will override an automatic test sequence and perform the required safety function. Process or logic signals are not changed as a result of self-test functions.

Self-diagnosis includes monitoring of overall program flow, reasonableness of process variables, RAM and PROM condition, and verification of 2/4 coincidence logic and device interlock logic. Testing includes continuous error checking of all transmitted and received data on the serial data links of each SSLC controller; for example, error checking by parity check, checksum, or cyclic redundancy checking (CRC) techniques.

A fault is considered the discrepancy between an expected output of a permissive circuit and the existing present state.

Actuation of the trip function is not performed during this test. The self-test function is capable of detecting and logging intermittent failures without stopping system operation. Normal surveillance by plant personnel will identify these failures, via a diagnostic display, for preventive maintenance.

Self-test failures (except intermittent failures) are annunciated to the operator at the main control room console and logged by the process computer. Faults are indentified to the replacement board or module level and positively indicated at the failed unit.

The continuous surveillance monitoring also includes power supply voltage levels, card-out-of-file interlocks, and battery voltage levels on battery-backed memory cards (if used). Out-of-tolerance conditions will result in an inoperative (out-of-service) condition for that particular system function.

Automatic system self-testing occurs during a portion of every periodic transmiss[illegible] period of the data communication networ[illegible] Since exhaustive tests cannot be performed during any one transmission interval, the test software is written so that sufficient overlap coverage is provided to prove system performance during tests of portions of the circuitry, as allowed in IEEE 338.

7.2.1.1.11 Control Room Cabinets and Their Contents

The SSLC logic cabinets, which contain the RPS, for Divisions I, II, III, and IV include a vertical board for each division. The vertical boards contain digital and solid state discrete and integrated circuits used to condition signals transferred to the SSLC from the essential multiplex system (EMS). They also contain combinational and sequential logic circuits for the initiation of safety actions and/or alarm annunciation. Isolators for electrical and physical separation of circuits used to transmit signals between redundant safety systems or between safety and nonsafety systems, and system support circuits such as power supplies, automatic testing circuits, etc. Load drivers with solid-state switching outputs for actuation solenoids, motor control centers, or switchgear may be located in the control room or throughout the plant.

The principal console contains the reactor mode switch, the RPS manual scram push button switches, the RPS scram reset switches and the bypass switches for the low RCS accumulator charging pressure.

7.2.1.1.12 Test Methods that Enhance RPS Reliability

Surveillance testing is performed periodically on the RPS during operation. This testing includes sensor calibration, response-time testing, trip channel actuation, and trip time measurement with simulated inputs to individual trip modules and sensors. The sensor channels can be checked during operation by comparison of the associated control room displays on other channels of the same variable. Fault-detection diagnostic testing is not being used to satisfy tech spec requirements for surveillance.

1.6

7.2.1.1.13 Interlock Circuits to Inhibit Rod Motion

Interlocks between the RPS and RC&IS inhibit rod withdrawal when the CRD charging pressure trip bypass switch is in the "BYPASS" position. These interlocks assure that no rods can be withdrawn when conditions are such that the RPS cannot re-insert rods if necessary.

7.2.1.1.14 Support Cooling System and HVAC Systems Descriptions

The cooling (ventilating) systems important for proper operation of RPS equipment are described in Section 9.4.

7.2.1.2 Design Bases

Design bases information requested by IEEE 279 is discussed in the following paragraphs. These IEEE 279 design bases aspects are considered separately from those more broad and detailed design bases for this system cited in Subsection 7.1.2.2.

(1) Conditions

Generating station conditions requiring RPS protective actions are defined in the Technical Specifications, Chapter 16.

(2) Variables

The generating station variables which are monitored cover the protective action conditions that are identified in Subsection 7.2.1.2.1.

(3) Sensors

A minimum number of LPRMS per APRM are required to provide adequate protective action. This is the only variable that has spatial dependence (IEEE 279, Paragraph 3.3).

(4) Operational Limits

Operational limits for each safety-related variable trip setting are selected with sufficient margin to avoid a spurious scram. It is then verified by analysis that the release of radioactive material following postulated gross failure of the fuel or the reactor coolant pressure boundary is kept within acceptable bounds. Design basis operational limits in chapter 16 are based on operating experience and constrained by the safety design basis and the safety analyses.

(5) Margin Between Operational Limits

The margin between operational limits and the limiting conditions of operation (scram) for the reactor protection system are in Chapter 16, Technical Specifications. The margin includes the maximum allowable accuracy error, sensor response times, and sensor setpoint drift.

leaving the main control room. If this was not possible, the capability of opening the RPS logic input power breakers from outside the main control room can be used as a backup means to achieve initial reactor reactivity shutdown.

(7) The main turbine pressure regulators may be controlling reactor pressure via the bypass valves. However, in the interest of demonstrating that the plant can accommodate even loss of the turbine controls, it is assumed that this turbine generator control panel function is also lost. Therefore, main steamline isolation is assumed to occur at a specified low turbine inlet pressure and reactor pressure is relieved through the relief valves to the suppression pool.

(8) The reactor feedwater system which is normally available is also assumed to be inoperable. Reactor water is made up by the HPCF system.

(9) It shall be assumed that the event causing the evacuation will not cause any failure of the DC or AC control power supplies to the remote shutdown panels or any failure of the DC or AC power feeds to the equipment whose functions are being controlled from the remote shutdown panels.

The above initial conditions and associated assumptions are very severe and conservatively bound any similar postulated situation.

7.4.1.4.3 Remote Shutdown Capability Description

(1) The capability described provides remote control for reactor systems needed to carry out the shutdown function from outside the main control room and bring the reactor to cold condition in an orderly fashion.

(2) It provides a variation to the normal system used in the main control room permitting the shutdown of the reactor when feedwater is unavailable and the normal heat sinks (turbine and condenser) are lost.

(3) Reactor pressure will be controlled and core decay and sensible heat rejected to the suppression pool by relieving steam pressure through the automatic activation of relief valves. Reactor water inventory will be maintained by the HPCF system. During this phase of shutdown, the suppression pool will be cooled by operating the residual heat removal (RHR) system in the suppression pool cooling mode.

(4) Manual operation of the relief valves will cool the reactor and reduce its pressure at a controlled rate until reactor pressure becomes so low that HPCF system operation is discontinued.

(5) The RHR system will then be operated in the shutdown cooling mode using the RHR system heat exchanger in the reactor water circuit to bring the reactor to the cold low pressure condition.

7.4.1.4.4 Remote Shutdown Capability Controls and Instrumentation - Equipment, Panels, and Displays

(1) Main Control Room - Remote Shutdown Capability Interconnection Design Considerations

Some of the existing systems used for normal reactor shutdown operations are also utilized in the remote shutdown capability to shut down the reactor from outside the main control room. The functions needed for remote shutdown control are provided with manual transfer devices which override controls from the main control room and transfer the controls to the remote shutdown control. All necessary power supply circuits are also transferred to other sources. Remote shutdown control is not possible without actuation of the transfer devices. Operation of the transfer devices causes an alarm in the main control room. The remote shutdown control panels are located outside the main control room. Access to this point is administratively and procedurally controlled.

Instrumentation and controls located on the remote shutdown control panels are shown in instrument and electrical diagram Figure 7.4-2.

answer
OE assumes this comment relates to transfer of sensor transmitters to the alternate signal path of the Remote Shutdown System. Within SSLC, automatic calibration is applied only to the analog-to-digital converters in the RMUs. When transfer is made to the Remote Shutdown System, the direct 4-20 mA outputs of the transmitters are routed to the analog trip units of the RSS instrument channels. Calibration of sensors and transmitters is performed by conventional, manual means.

The following clarification is added to Section 7.6.1.4.4(1):

Control and process sensor signals are interrupted by the transfer devices at the hardwired, analog loop. Sensor signals which interface with the remote shutdown system are routed from the sensor, through the transfer devices on the remote shutdown panels, and then to the multiplexing system remote multiplexing units (RMUs) for transmission to the main conrol room. Similarly, control signals from the main control room are routed from the RMUs, through the remote shutdown transfer devices, and then to the interfacing system equipment. Actuation of the transfer devices interrupts the connection to the RMUs and transfers control to the remote shutdown system.

Insert "A"

7.8 INTERFACES

7.8.1 Effects of Station Blackout on the HVAC

A temperature heat rise analysis shall be performed for the station blackout scenario applied to the control room on consideration of the environmental temperatures unique to the plant location. [See Chapter 20, NRC Question 420.14 and Subsection 7.1.2.3.9]

7.8.2 Electrostatic Discharge on Exposed Equipment Components

e-(Deleted)

The response to NRC Question 420.90 provides recommendations for limiting the effects of electrosatatic discharge (ESD) at keyboards, keyed switches and other exposed equipment. The applicant shall provide assurance that the grounding and shielding techniques are consistent with these recommendations, or provide an acceptable alternative plan for controlling ESD. [See Chapter 20, NRC Question 420.90]

7.8.3 Localized High Heat Spots in Semiconductor Materials for Computing Devices

The response to NRC Question 420.92 provides recommendations for limiting high cuurent densities whigh could result in localized heat spots in semiconductor materials used in computing devices. The applicant shall provide assurance that these recommendation are followed, or an acceptable alternative is presented, by the selected equipment vendor(s). To ensure that adequate compensation for heat rise is incorporated into the design, a thermal analysis shall be performed at the circuit board, instrument and panel design stages. [See Chapter 20, NRC Question 420.92]

7.8.4 Safety-Related C&I Interfaces

Each of the systems addressed in Chapter 7 were reviewd for safety-related C&I (signal) interfaces which extend outside the scope of the ABWR Standard Plant. Since the scope of the ABWR Standard Plant includes all of the reactor building, the turbine building and the control building, the study determined there are no safety-related electrical signal interfaces for any of these systems which extend beyond the scope definition.

RESPONSE 420.90

If appropriate countermeasures are not taken, then electrostatic discharge (ESD) can cause damage to electronic components. High impedance devices using MOS (metal-oxide semiconductor) technology are particularly subject to damage. The discharge from an electrically charged human body, when certain areas of electronic equipment are touched (keypads, switches), may open the junctions of CMOS devices or other semiconductors.

However, modern CMOS and other MOS components have internal protection against ESD in the form of diode clamping arrays and current limiting resistors that conduct the discharge away from the junction. In addition, good circuit design practices will include the use of other devices such as transient suppressors [for example, metal-oxide varistors (MOVs), Zener diodes] across critical circuit inputs and outputs that are directly exposed to external transients.

Other precautions against the effects of ESD take the form of adequate i..sulation or proper grounding. Keypads generally have insulating material in the form of a thick plastic covering over the metallic switch contacts. Toggle switches and other controls should have insulating knobs. Various metallic chassis components (front panel, handles, deck, connector shells) should be solidly grounded to each other (the effects of painted and plated surfaces should be considered), and the chassis should be grounded to the appropriate panel or instrument ground bus by metallic ground straps. Panel and instrument mounting hardware should not be depended upon for solid grounds. Printed circuit boards must have the signal commons and ground plane commons properly connected to the common busses and to the low voltage logic power supplies.

I.w/ Insert "A" here →

QUESTION 420.91

Most of the I&C system microprocessor equipment is likely to be located in a mild environment, but survivability requirements or limitations on the voltage potential buildup by humidity control or other measures is not discussed. Also, the data concentrators are provided at remote locations where the environmental control is not clearly described. Identify the criteria, design limits and testing program for this area of ESD controls. (7)

RESPONSE 420.91

The environmental qualification requirements for systems and equipment are described in Secton 3.11 and in the design documents referenced in Subsection 1.1.3 (in particular, BWR Requirements - Equipment Environmental Interface Data and the Safety System Logic & Control Design Specification).

Voltage potential buildup will be limited by proper grounding of equipment and use of appropriate static control materials and dielectric barriers to ensure that high potentials cannot be coupled to sensitive semiconductor devices (see the response to Question 420.90). Humidity controls are provided by the normal and emergency HVAC systems; when relative humdity is restricted to the ranges specified for the mild environment locations where the microprocessor equipment will be installed, there will be no unusual static charge buildup.

The thermal design environments for the SSLC panels themselves are discussed in the response to Question 420.008. The Remote Multiplexing Units (i.e., "data concentrators") of the Essential Multiplexing System are located within the "clean" areas of the Reactor Building outside the secondary containment. The panels containing this equipment will be environmentally qualified and tested in accordance with Regulatory Guide 1.89 and IEEE 323 for the areas in which they are located.

I&C microprocessor equipment will be required to meet the requirements of IEC Standard Publication 801-2, "Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment, Part 2 (Electrostatic Discharge Requirements)". Test equipment shall have the following minimum capabilities:

Record# ANSWER

23. The response to RAI 420.090 discussed several precautions to be taken against electrostatic discharge (ESD) in electronic assemblies, and also described typical circuit design and equipment grounding methods that should be used to prevent component damage.

The following response is added to the response of RAI 420.090. The additional material includes a reference to industry standards that verify conformance to ESD requirements.

Insert "A"

1.W

Microprocessor-based control equipment for ABWR is designed under the assumption that users will have taken no precautions against static charge buildup before attempting to operate the equipment. The equipment is designed to tolerate an electrostatic discharge without damage, partly by employing insulation (with no air gaps) over exposed metallic components, but primarily by providing an alternative path for current flow other than through sensitive circuit paths. As discussed previously, this means that all exposed metallic components of the system must be grounded. Low inductance multipoint grounds are used where ESD current flow is desired and single-point grounds where discharge flow is not wanted.

The low power requirements of ABWR control equipment ensure that the integrity of the equipment enclosures is not compromised by large ventilating holes or slots. Special attention is given to hinges, joints, and seams so that the continuity of shielding is maintained.

In the system configuration, where shielded cables transfer data between the equipment enclosures, the cables must be prevented from propagating ESD currents and voltages between system units. For ABWR safety systems, the problem has been minimized by using fiber optic cables as the transmission medium for most critical signals. While the cables may contain metallic supporting members or protective shields, these will not be electrically connected to any equipment or circuit. For certain functions where hardwired cable is required, solid grounding of cable shields to the equipment chassis and bypass capacitors at all inputs and outputs shall be used to divert ESD currents to ground.

These hardware solutions shall be supplemented with firmware ESD solutions to protect against potential upsets such as system lockup if ESD noise causes memory or data flow errors. The methods used are discussed as part of the fault-tolerance issues included in Items 1.g and 1.i.

The susceptibility of ABWR control equipment to electrostatic discharges shall be established using the test procedures included in IEC Publication 801-2, Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment, Part 2: Electrostatic Discharge Requirements. The test procedures of paragraph 8 of this document shall be performed up to and including Severity Level 4, as defined in the document. The following acceptance criteria shall be used:

1. No change in trip output status shall be observed during the test.

(cont. next page)

(Project "A" Contd)

2. Equipment shall perform its intended functions after the test.

(1.W)

Note that the safety system control equipment for ABWR has inherent protection against transient ESD effects in that data is continually refreshed throughout the system, including trip, display and indicator status. Further protection is provided by the asynchronous, four-division, 2-out-of-4 channel configuration. Temporarily corrupted data in one division cannot cause an inadvertent trip or permanently disable a required trip. When bad data or equipment damage is detected, the affected division can be bypassed until repaired. In the Reactor Protection System (RPS) and Main Steam Isolation Valve (MSIV) channels, where the final trip outputs are also in a 2-out-of-4 configuration, both the sensor input and trip output sides of each equipment division can be bypassed, thus preventing failure from any cause in one channel from inhibiting or inadvertently causing a trip.

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 (TLU's) in all four divisions of trip logics. The DTMs and TLU's 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 (BPU's), trip logic units (TLU's) and output logic units (OLU's). The manual control switches and the BPUs, TLU's and OLUs 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 TLU's becomes a check for two-out-of-three coincidence of trip conditions if any one division of channel sensors has been bypassed. The OLU's perform the division trip, seal-in, reset and trip test functions. Trip signals from the OLU's 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 bistable, solid-state, high current interrupting devices. The operation of 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 devices) to confirm appropriate isolation methods used to satisfy separation and segregation requirements.	6. RPS equipment installation acceptable if inspections, analyses and 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
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.	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.	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: 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). 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. 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. 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.

Table 2.2.7: REACTOR PROTECTION SYSTEM (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

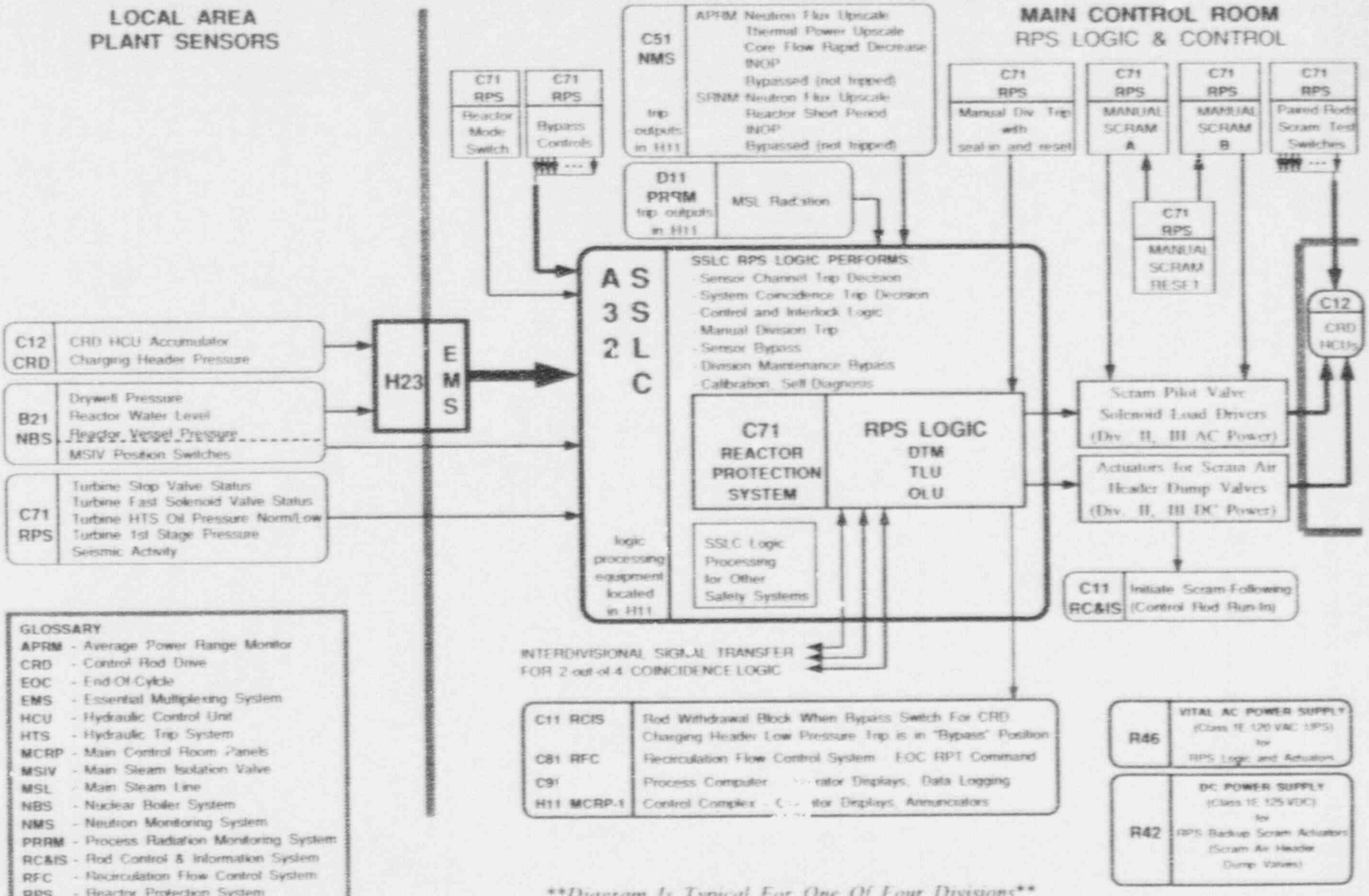
Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
		10. (Continued)
		e. Installed system energizes both air header dump (back-up scram) valves of the CRD hydraulic system, and initiates CRD motor run-in, concurrent only with a full scram condition.
		f. When not bypassed, 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. **Validation Attributes**: Total trip system response, from time when sensor input is beyond setpoint to time of scram pilot valve solenoids deenergization: - NMS APRM ≤ 0.090 sec. - Reactor pressure ≤ 0.55 sec. - Reactor water level ≤ 1.05 sec. - Turbine stop valve closure ≤ 0.060 sec. - Turbine control valve fast closure ≤ 0.080 sec. - Main steam lines isolation ≤ 0.060 sec.

Figure 2.2.7a REACTOR PROTECTION SYSTEM



GLOSSARY

APRM	- Average Power Range Monitor
CRD	- Control Rod Drive
EOC	- End-Of-Cycle
EMS	- Essential Multiplexing System
HCU	- Hydraulic Control Unit
HTS	- Hydraulic Trip System
MCRP	- Main Control Room Panels
MSIV	- Main Steam Isolation Valve
MSL	- Main Steam Line
NBS	- Nuclear Boiler System
NMS	- Neutron Monitoring System
PRRM	- Process Radiation Monitoring System
RC&IS	- Rod Control & Information System
RFC	- Recirculation Flow Control System
RPS	- Reactor Protection System
RPT	- Recirculation Pump Trip
SRNM	- Startup Range Neutron Monitor
SSLC	- Safety System Logic & Control
UPS	- Uninterruptible Power Supply

Diagram Is Typical For One Of Four Divisions

Figure 2.2.7b REACTOR PROTECTION SYSTEM