GE Nuclear Energy

General Electric Company
175 Curtner Avenue, San Jose CA 95125

July 13, 1989

MFN No. 050-89

Docket No. STN 50-605

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

Attention: Charles L. Miller, Director
Standardization and Non-Power Reactor Project Directorate

Subject: **Submittal of Responses to Additional Information as Requested in NRC Letter from Dino C. Scaletti, Dated May 16, 1989**

Dear Mr. Miller:

Enclosed are thirty four (34) copies of the Responses to Request for Additional Information (RAI) on the Standard Safety Analysis Report (SSAR) for the Advanced Boiling Water Reactor (ABWR). These responses principally pertain to Chapters 7 and 8.

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

Sincerely,

J. S. Gay, Acting Manager
Licensing and Consulting Services

cc: D. R. Wilkins (GE)
F. A. Ross (DOE)
J. F. Quirk (GE)
D. C. Scaletti (NRC)

D028
1/34

QUESTION
420.003 (7) Identify the topical reports that will be provided to support any aspects of the design that are substantially different relative to designs previously reviewed by the staff. Subjects addressed in these topical reports should include but not necessarily be limited to the following:
Failure modes and effects analysis for the I&C system.

RESPONSE
420.003 The failure modes and effects analysis is contained in Appendix 15B, Section 15B.4. No separate topical reports will be provided.

QUESTION
420.004 (7) Identify the topical reports that will be provided to support any aspects of the design that are substantially different relative to designs previously reviewed by the staff. Subjects addressed in these topical reports should include but not necessarily be limited to the following:
A defense-in-depth analysis, demonstrating the diversity in the system that precludes the likelihood of common mode failures.

RESPONSE
420.004 In response to this question, refer to Appendix 7A, Section 7A.7 under the heading: "Items 7A.5(4) and 7A.6(4)". Detail information may be found in the ABWR Specifications referenced in Section 1.1.3.

QUESTION
420.010 (7) Identify the topical reports that will be provided to support any aspects of the design that are substantially different relative to designs previously reviewed by the staff. Subjects addressed in these topical reports should include but not necessarily be limited to the following:
Task analysis for the man/machine interface to the system.

RESPONSE
420.010 Collectively, the instrumentation and controls for the plant systems form the man/machine interface for the plant. This man/machine interface is largely, but not completely, contained in the control room. In this SSAR, the subjects of the plant MMI and control room configuration are not dealt with in Chapter 7 but are covered in Chapter 18. MMI and other aspects of the design of the control and instrumentation are described in the design documentation. There are no topical reports which describe significant differences between the ABWR and previous BWR designs. However, Table 7.1-1 of the SSAR compares the ABWR I&C design with that of GESSAR II.

QUESTION
420.013 (10/87) One of the goals of the ABWR is simplification. The October, 1987 presentation mentions a 60% reduction in instrumentation. Which plants is this referenced to? Provide a description of the instrumentation which is no longer considered necessary.

RESPONSE
420.013 The instrument reduction occured within the design phases of the ABWR itself. The basic configuration of the initial design of the ABWR NBS instrumentation and related systems' initiation logic is very similar to that of the BWR/5 and BWR/6 (and GESSAR II Standard).

As part of the ABWR cost analysis justification study, the number of transmitters required to provide the primary Nuclear Boiler System (NBS) instrumentation functions was reduced from 84 to 30. These substantial (i.e., 64%) reductions in the NBS instrumentation were accomplished without impairment of safety or compromise of reliability of any system and will result in both an inital savings in sensor, instrument rack and installation costs and, in the longer term, a saving in manpower to conduct periodic maintenance and calibration work.

These reductions in NBS instrumentation were primarily accomplished through the broad scope sharing of transmitters such that individual transmitters now provide inputs to a number of different systems and functions. This is possible because of the four independent divisions and two-out-of-four logic adopted for the RPS and ESF Systems in the ABWR control and instrumentation design.

QUESTION
420.017 (7) Describe the trade-off analyses leading to the selection of an analog or digital approach for implementing the logic of the safety system. Describe the major criteria that the tradeoff was based on. Show how the tradeoff criteria is in accordance with applicable design criteria.

RESPONSE
420.017 DESIGN CRITERIA FOR ABWR SAFETY SYSTEM LOGIC

In comparison with BWR/5 plant designs:
1. Reduce control room equipment volume.
2. Reduce quantity of system cabling.
3. Reduce inadvertent reactor trips
4. Permit proper interface with advanced operator benchboard design; i.e., high speed communication with CRT displays and flat screen touch panels.
5. Improve man-machine interface.
6. Improve availablity (reduce downtime).

TRADEOFF CONSIDERATIONS

Since the safety system logic is separated into four divisions, with 2-out-of-4 trip logic in each division, a digital design similar to the Clinton Nuclear System Protection System (NSPS) was considered advantageous. NSPS uses discrete solid-state logic for trip decisions, thus eliminating a large number of relays, but still has hardwired

analog signals to the control room. NSPS also has a digital, on-line, self-diagnostic system that permits complete testability of the four logic divisions in a manner not practical for analog/relay systems.

When multiplexing was considered as a means to reduce cable volume, it was decided to use microprocessor logic to permit proper interfacing to the multiplexing system and to integrate more system functions into a smaller quantity of equipment, eliminating all relay cabinets for RPS and ESF functions. Multiplexing also permits local digitizing of plant variables near their transmitters and digital transmission of encoded signals over a low noise, high speed, fiber optic cable.

A list of other tradeoffs between analog and digital technologies is shown below:

Tradeoffs:
A. DIGITAL:

PRO:
-Stable.
-No drift.
-Accurate setpoints.
-Precise hysteresis.
-Low noise.
-Serial communication (less cable).
-Data multiplexing.
-Easy implementation of bypassing.
-Self-diagnostics (improves MTTR).
-Auto-calibration.
-Improved man-machine interface (graphical displays, prompting help, digital data entry).
-Future updates made via software (no wiring changes or extra hardware).
-Less equipment (more functions integrated into software logic).
-Lower power requirements (CMOS logic, less equipment).

CON:
-Complex, safety-related software (V&V program required).
-Complex, subtle failure modes, difficult to identify.
-Complex testability, logic points not available to technician with simple measuring instruments.
-Complex equipment for troubleshooting, requiring skilled personnel (Interrelationships and responses of logic functions not obvious to technician unless source code and logic analyzer are available).
-Jumpering of logic for temporary testing not possible.
-Repair is limited to module replacements, which must be kept as spares, since repair of modules is not practical on-line.

B. ANALOG

PRO:
-Simple, proven technology.
-Easy troubleshooting and repair.
-Analog displays are low cost and easily implemented.
-Status of analog signals or relay coils and contacts is readily determined at any point in instrument loop.
-Measurements possible with simple instruments by relatively unskilled technicians.
-Simple parts replacement.

CON:
-Signals and setpoints subject to drift.
-Constant calibration required.
-Electromechanical analog meters have low resolution and reliability and may become slow and inaccurate over time.
-Complex logic for interlocks and controls involving interdivisional signals requires large quantities of relays and wiring and is not easily testable automatically.

CONCLUSIONS

The complexities of a software-based, microprocessor-controlled system are compensated for by its higher performance, greater stability and accuracy, and reduced quantity of equipment. System inputs and outputs can be added or deleted without wiring changes. System functions can be changed in software ("firmware") without using extra hardware. These advantages, plus the availability of self-diagnostics, greater automation of functions,and improved man-machine interface, led to the selection of a digital system.

QUESTION
420.022 (7) Provide a table of conformance to IEEEE 603 and ANSI/IEEE 7-4.3.2.

RESPONSE
420.022 Conformance with IEEE 603 and ANSI/IEEE 7-4.3.2 is discussed in Appendix 7A, Section 7A.7.

QUESTION
420.024 (7) Are any artificial intelligence features provided in the proposed system, whereby probabilistic judgements are made by the system, or whereby the system can "learn" during its operational life?

RESPONSE
420.024 No. As explained in the response to Question 420.021, the microprocessors are used only for making simple logic decisions. Artificial intelligence features are not used in the ABWR safety system design.

QUESTION
420.025 (7) Is credit taken in the safety analysis for any rotating memory devices such as disk drives?

RESPONSE
420.025 No. As indicated in the response to 420.021, no safety action is dependent on computations from the central processor. Therefore, no safety credit is taken for rotating memory devices. The control programs for SSLC are contained in ROM as firmware.

QUESTION
420.026 (7.1.2.1.6) What is the definition of "Safety Associated" as used in SAR Section 7.1.2.1.6?

RESPONSE
420.026 The self-test subsystem (STS) is classified as "Safety Associated" because its function is not safety related, yet it is intimately interconnected with functions which are safety related (i.e., the safety system logic & control network which controls RPS and ESF functions).

Since the STS hardware is qualified Class 1E, and receives its power from the divisional buses, the subsystem may be considered Class 1E so far as IEEE 384 is concerned.

QUESTION
420.027 (7) Specify which parameters are to be triplicated. At what point does the triplication start (flow orifice, sensor?) and end (transmitter, trip logic?). If there is triplication of sensors is there diversity between sensors?

RESPONSE
420.027 Some of the non-safety-related process systems use triplicated logic; however, the safety systems, which are the subject of these questions, have sensors and logic in four protection divisions and will be addressed in this response.

The sensors are not diverse among divisions, but are powered separately by the divisional power sources. The logic for most parameters is 2-out-of-4 in each division. Thus, the output of the sensor trip logic for each variable in a division is sent to the other divisions of the particular system. The resulting 2/4 coincidence trip signal is applied to energize the driven equipment in each division. For ESF functions, the driven equipment within a division is not replicated, but the coincidence trips are processed in dual logic processors with a 2-out-of-2 voted output to prevent inadvertent initiation of pumps or valves. In case one processor fails, automatic bypass permits temporary 1-out-of-1 output until repair is accomplished.

For RPS and MSIV, input logic is 2-out-of-4 as above, but the output load drivers which energize various groups of solenoids are also arranged in a 2-out-of-4 grouping. This permits bypassing a full division of logic while still maintaining control of all solenoids with 2-out-of-4 input logic and 2-out-of-3 output logic.

QUESTION
420.028 (15.A) Section 15.A.2.2 defines "Safety" and "Power Generation." The staff did not locate definitions for "important to safety" and "safety related" which are used in Chapter 7.

RESPONSE
420.028 "Safety-related" is the correct term in accordance with the explicit definition in 10CFR50.49(b)(1). "Basic component" defined in 10CFR21 and used in the Potentially Reportable Condition process is equivalent to "safety-related".

In the past, the term "important-to-safety" was used by GE Nuclear Energy as a synonym for "safety-related". However, to avoid confusion, this term should not have been used in the ABWR SSAR. The staff did not indicate where this term was found, except that it was "...used in Chapter 7". GE will change such terms to "safety-related" as they become known. Meanwhile, expressions such as "safety essential,", "essential," "safety grade," and "nuclear safety-related" should be considered synonymous with the term "safety-related".

QUESTION
420.029 (7.1.1) For those systems where it has not already been done (example 7.1.1.3.5) clarify whether manual or automatic initiation will be used.

RESPONSE
420.029 The following systems definitions in Section 7.1.1 have been expanded to state manual or automatic initiation as indicated below:

SECTION	SYSTEM	INITIATION
7.1.1.3.1	ECCS	Automatic
7.1.1.3.2	LDS	Automatic
7.1.1.3.5	SGTS	Automatic safety portion
7.1.1.3.6	DG	Automatic
7.1.1.3.7	RCW	Automatic safety portion
7.1.1.3.8	HVAC	Automatic safety portion
7.1.1.3.9	HECW	Automatic safety portion
7.1.1.3.10	HPIN	Automatic safety portion
7.1.1.4.1	ARI	Automatic
7.1.1.4.4	RSS	Manual
7.1.1.6.1	NMS	Automatic trip to RPS
7.1.1.6.2	FRPM	Automatic trip to RPS
7.1.1.6.4	FPC	Automatic temperature control
7.1.1.6.5	WDVBS	Automatic
7.1.1.6.6	CAMS	Continuous/Automatic
7.1.1.6.7	SPTM	Continuous

QUESTION
420.031 (7.1.2.3.2) For section 7.1.2.3.2(1)(c,d,e) and (2)(a) define "sufficient".

RESPONSE
420.031 In this definition of safety design bases for leak detection & isolation system (LDS) for redundancy, "sufficient" means at least one redundant channel is required to satisfy the single failure criteria. However, for the ABWR design for LDS, at least 2 or more redundant channels are provided to satisfy this requirement.

QUESTION
420.032 (7.1.2.3.2) The listed design basis should include instrumentation necessary to inform the operator that isolation has been completed and control should provide ability for operator to reset (with adequate safeguards against inadvertently breaking isolation).

RESPONSE
420.032 The following has been added to Section 7.1.2.3.2(1) Safety Design Bases: "Provide interlocks to assure reset capability is only possible after clearence of isolation signals."

The following has been added to Section 7.1.2.3.2(2) Nonsafety-Related Design Bases: "Provide status information to annunciator and process computer."

QUESTION
420.033 (7.1.2.3.2) Add to 7.1.2.3.2(2)(c)..."without causing plant shutdowns" or reducing safety margins.

RESPONSE
420.033 The addition to the text has been added as shown in attached mark-up of this section.

QUESTION
420.034 (7.1.2.3.7) For Section 7.1.2.3.7(1)(b) provide a listing of the nonessential parts of the cooling water system which should be isolated. List any nonessential parts for which isolation is not provided.

RESPONSE
420.034 The non-essential parts of the cooling water system which are isolated are listed in Tables 9.2-4a, b and c. The non-essential cooling loads, which are not automatically isolated, are the CRD pump oil coolers, the CUW pump coolers, the instrument air system coolers and the service air system coolers. These groups of coolers which are not automatically isolated comprise less than 1% of the total heat load during LOCA.

QUESTION
420.035 (7.1.2.6.5) Is the wetwell to drywell vacuum breaker control manual or automatic?

RESPONSE

420.035 The wetwell-to-drywell vacuum breaker system (WDVBS) is passive, in that no external power or control is used. When the pressure difference between drywell and wetwell reaches a predetermined setpoint, the WDVBS automatically opens allowing the flow of air back into the drywell thus slowing down its depressurization, and eventually reaching a steady state. For additional information, see Subsection 6.2.1.1.4.1.

QUESTION

420.037 (7.1.2.6.7) What is the immediate safety action required by relief valve leakage and is it automatic?

RESPONSE

420.037 SRV leakage can be detected by either (a) high SRV discharge line temperature alarm, (b) SRV not fully closed alarm, or (c) observing the SRV position indication. SRV position indication is provided by a qualified Class 1E position transmitter on each valve. Continuous SRV leakage will result in a rise in the suppression pool temperature. High bulk average suppression pool temperature will be annunciated in the main control room.

SRV leakage does not require immediate safety control action and there is no automatic control actions initiated. The operator is required to monitor and control suppression pool temperature. The operator can initiate supression pool cooling by operating the residual heat removal (RHR) system in the suppression pool cooling mode. If SRV leakages to the suppression pool exceed the cooling capability of the RHR, suppression pool temperature will increase. High suppression pool temperature condition will be annunciated and it would provide an entry condition to the symptom-based emergency operating procedures. According to the BWROG Emergency Procedure Guidelines, Revision 4, approved by the NRC, the operator actions for suppression pool temperature control can be summarized as follows:

1. Operate all available RHR for suppression pool cooling,

2. Before suppression pool temperature reaches the boron injection initiation temperature (a curve of suppression pool temperature vs reactor power), scram the reactor, and

3. When suppression pool temperature and RPV pressure cannot be maintained below the heat capacity temperature limit (a curve of suppression pool temperature vs RPV pressure), perform a reactor depressurization.

QUESTION

420.038 (Table 7.1-2) The table indicates RG 1.151 applies only to safety related display and Non-1E control systems. Section 7.1.2.10.11 refers to other safety systems including RPS and ECCS. Clarify which systems RG 1.151 is to apply to.

RESPONSE

420.038 Table 7.1-2 is formatted in accordance with the Standard Review Plan in conjunction with the Licensing Review Bases document for the ABWR.

Protection systems (including RPS and ECCS) instruments which require sensing lines are shared, and are contained within the nuclear boiler system (NBS). The NBS conforms with Regulatory Guide 1.151 as described in Subsection 7.7.2.1.2(2).

QUESTION

420.039 (Table 7.1-2) The table lists few systems for which RG 1.97 is applicable. Address the RG 1.97 for all categories and variables.

RESPONSE

420.039 Table 7.1-2 is formatted in accordance with the Standard Review Plan and in conjunction with the Licensing Review Bases document for the ABWR.

The post-accident requirements of Regulatory Guide 1.97 involve instrumentation from many systems within the plant. Signals from these many instruments converge into both safety-related and non-safety-related display systems in the control room. Since Regulatory Guide 1.97 involves only displays, (and the instruments which support them), it is appropriate to address its requirements from the vantage point of the monitoring displays, rather than from each of the C&I systems. We assumed this is why the SRP required that Regulatory Guide 1.97 only needed to be addressed in Section 7.5. We have therefore provided a full assessment of the guide for all categories and variables, in association with the displays and supporting instruments, in Section 7.5.

QUESTION

420.040 (7.3.1.1.1.1) The HPCF pump is interlocked (7.3.1.1.1.1(3)(c)) with the undervoltage monitor. If the breaker cannot close will it retry and what information is available to the operator if it doesn't close that would indicate an undervoltage problem?

RESPONSE

420.040 The HPCF pump starting logic waits for the main bus voltage to be available. As soon as voltage is available the starting cycle is initiated, assuming all other requirements for starting the pump have been met. Bus undervoltage alarms are provided in the control room.

QUESTION

420.041 (7.3.1.1.1.1) Does the 36 seconds (7.3.1.1.1.1(3)(e)) include time for diesel generator to start?

RESPONSE
420.041 Yes, the start time of the diesel is included in the 36 seconds.

QUESTION
420.043 (7.3.1.1.1.2(3)(c)) Manual pushbuttons are provided to initiate ADS immediately if required. Describe when manual action is required before the 29 second timer actuates ADS.

RESPONSE
420.043 Manual actuation of the ADS is not required. The manual actuation switches are included to meed the requ rements of Paragraph 4.17 of IEEE 279. The EPGs (Emergency Procedure Guidelines) call for operator action to depressurize the reactor under some conditions by using individual manual control switches which are provided for each of the 18 safety relief valves (SRVs). The manual pushbuttons for ADS, which operate 8 SRVs simultaneously, can be considered to be a backup method to individual SRV operations when following EPGs.

QUESTION
420.044 (7.3.1.1.1.3(4)(a)) One pressure sensor is used to detect low RCIC system pump suction pressure. Explain the criteria used to justify a single pressure sensor.

RESPONSE
420.044 The RCIC is part of the emergency core cooling system (ECCS) network which consists of 3 high pressure systems and 3 low pressure systems. One RCIC and 2 HPCF loops comprise the high pressure ECCS while the low pressure ECCS are the 3 RHR loops.

The subject sensor is located on the pump suction to provide a turbine trip signal on low suction pressure (and eventually stop the RCIC pump). The intent of this instrument is to protect the pump from cavitation. Since RCIC is a single loop, redundant suction pressure instruments are not necessary. The single failure is based on the loss of one ECCS loop. That is, if RCIC is lost, 5 more ECCS loops are available to perform core cooling. The same configuration is true for BWR6 designs.

QUESTION
420.045 (7.3.1.1.1.3(6)) Define analog indication. Is this an analog system or digital simulation?

RESPONSE
420.045 For the ABWR, the control room indications are digital. However, all primary sensors (pressure transmitters, level transmitters, flow transmitters, differential transmitters, etc.), are analog instruments. Output signals from the primary sensors are multiplexed and digitized, and then sent to the control room through fiber-optic cables.

QUESTION
420.046 (7.3.1.1.1.4(3)(g)) The injection valves cannot be opened at normal pressure. Is this because of interlocks or because of motor size?

RESPONSE
420.046 The RHR injection valves cannot be opened at normal reactor operating pressure (1040 psia) for both reasons. A pressure interlock prevents the valve from opening above a low pressure value (approximately 436 psig), and the specified valve operating differential pressure is approximately 550 psid.

QUESTION
420.047 (7.3.1.1.4) Is the suppression pool cooling automatically initiated? The SAR describes the system as being used to reduce the suppression pool temperature immediately after a blowdown. Section 5.4.7.1.1.5 indicates automatic initiation.

RESPONSE
420.047 Revision C of Section 5.4.7.1.1.5 of the SSAR has been corrected to be consistent with Section 7.3.1.1.4, which describes the manual-only initiation of this mode of RHR. The third sentence has been revised to read, "This subsystem is initiated manually." The remainder of 5.4.7.1.1.5 has been deleted.

QUESTION
420.048 (7.1.2.1.6) SAR 7.1.2.1.6(2) appears to define "fault" as the "...inability to open or close any control circuit." Explain the basis for this definition and the extent of its use in the FMEAs. Are there any other potential failure modes excessive time to close a circuit?

RESPONSE
420.048 There are two types of operations for the self-test subsystem (STS). Subsection (1) of 7.1.2.1.6 describes the on-line STS and Subsection (2) describes the manually-initiated off-line STS.

The "fault" definitions in (1) and (2) differ slightly in that (2) also exercises the trip outputs. Neither definition specifically includes a time-delay test. However, any excessive time delays in either test would be detected as a fault since the test system must cycle from circuit-to-circuit very rapidly (i.e., in the order of milliseconds).

FMEAs for the reactor internal pump (RIP), the multiplex (MUX) and the fine-motion control rod drive (FMCRD) systems are included in Section 15B.4. Portions of the SSLC are included in the FMEA for the MUX. We do not intend to perform separate FMEAs for the STS alone.

QUESTION

420.049 (7) Describe the fault tolerant features of the digital design. Describe the types of faults that are tolerated by these design features. Show how these features would respond to various faults, and show that the effectiveness of the safety system is not compromised.

RESPONSE

420.049 FAULT TOLERANT FEATURES:

HARDWARE:

a. Four-division replication of sensors and logic with 2-out-of-4 voting to confirm trip in each division.

b. Division-of-sensors bypass results in 2-out-of-3 voting.

c. Division logic bypass for de-energize-to-trip funtions results in 2-out-of-3 voting at trip channel outputs

d. Redundant (dual channel) multiplexing in each division with automatic reconfiguration and restart.

e. Energize to trip functions are implemented in redundant channels with 2-out-of-2 voting for confirmation; fails automatically to 1-out-of-1 to maintain availability.

f. Allocation of fail-safe (RPS, MSIV and other PCV isolations) and fail-as-is (ECCS, Aux. ESF) functions to separate microprocessors within each division.

g. Physical separation of divisional instruments prevents damage to redundant instrument loops.

SOFTWARE:

a. Empty memory filled with jump-to-reset instructions.

b. Error checking/correcting of inputs and outputs.

c. On detected fault, retry or roll-back to last known correct state.

d. Continuous self-diagnostics with auto-switchover to good channel.

TYPES OF FAULTS TOLERATED:

HARDWARE:

a. Single failure in any division, including inadvertent trip and loss of power.

b. Loss of digital trip logic in any division; can use maintenance bypass for on-line calibration or repair.

c. Single failure of essential multiplexing system in any division with no effect on safety system operation.

d. Single failure of logic channel in any division with no effect on system operation.

e. Single failure without accidental trip.

f. Failure of some system functions will leave others unaffected.

SOFTWARE:

a. Restart without lockup on fault such as EMI.

b. Detects and corrects data transmission errors with no effect on system operation.

c. Attempts to continue operation through transient fault.

d. Attempts to continue operation through permanent fault.

e. Software transient in any single microprocessor will not cause or prevent reactor trip, nuclear system isolation, or ECCS initiation.

f. Detects failures of plant variables produced by process transmitters or transducer elements through reasonability and range checking.

SYSTEM RESPONSE TO FAULTS:

As described above, the safety system is not compromised by faults because of the multi-divisonal logic configuration and 2-out-of-four coincidence logic in each division. Therefore, single microprocessor instrument failures or some multiple failures within a single division, whether they result in tripped or untripped states, will not result in improper system response.

QUESTION
420.053 (7) Is a diverse (hardware implemented) watchdog timer provided in the design for detecting system stall?

RESPONSE
420.053 A hardware watchdog timer is implemented in each controller of SSLC and the multiplexing system; the timer detects stall within that controller. Thus, a hardware or software fault can be detected and alarmed at a particular system unit without bringing down the entire system.

For example, an individual Trip Logic Unit can be taken out of service on a watchdog timer alarm (using the appropriate bypass function) without disrupting operation of the Digital Trip Module and its communication with the other divisions.

The individual watchdog timer outputs permit differing responses to component failure. Certain timer outputs may cause automatic bypass of a logic channel; others result only in an alarm indication to the operator. Typical responses are as follows:

1. RPS DTM - Alarm output to operator; manual division-of-sensors bypass reverts remaining logic to 2/3.

2. ESF DTM - Same as above.

3. RPS TLU - Alarm output to operator; manual bypass reverts ouput logic to 2/3, while input logic remains 2/4 (DTMs are all assumed operable).

4. ESF SLU 1 & 2 - Alarm output of either SLU 1 or SLU 2 results in automatic bypass of the failed channel at the 2/2 voter (load drivers). Bypass means that load driver of the failed channel is energized. Alarm output to operator is provided, with manual bypass as a backup to the auto function.

QUESTION
420.057 (7) What provisions have been made in the design process to preclude the introduction of a software virus that could affect the system when operational?

RESPONSE
420.057 As indicated in the responses to 420.025 and 420.021, no safety action is dependent on computations from the central processor. The control programs for SSLC are contained in ROM as firmware. Software instructions such as setpoints, etc., are not programmable in the field, but are burned on individual chips in the factory before shipment. This is considered to be adequate safeguard against the introduction of software viruses.

QUESTION
420.061 (7.1.2.2) Explain section (h) further. Does this mean one 480V bus, 4160 bus the generator? Same question at 7.2 3.2(2)(b).

RESPONSE
420.061 [We assume the second sentence should say ".. 4160 bus or the generator?" We also assume the reference to '7.2.3.2(2)(b)" should be "7.1.2.3.2(2)(b)".]

The electrical distribution system has three completely separate and redundant divisions of 6.9 kV buses and diesel generators. There are four divisions of 480 volt AC buses. However, the fourth division 480 volt AC bus receives power from the Division I 6.9 kV AC bus. There are also four completely separate and redundant 125 Vdc battery buses.

The RPS logic actuates on any 2-out-of-4 "failsafe" (logic "0") signals. Power for the RPS and other ESF systems comes from the 4-divisional safety system logic and control (SSLC) power buses. Thus, loss of any one bus or power source (i.e., 6.9 kV bus, 480 bus, diesel generator, or battery) would not result in an inadvertant scram nor a failure to scram when required. This is further explained in Section 7.2.

The leak detection and isolation system (LDS) utilizes various portions of all four buses depending on the power supplies for the isolation valves with which it interfaces [See Subsection 7.3.1.1.2(2)]. No single failure of any power source will result in failure to isolate a pipe system when needed. See Subsection 7.3.1.1.2 for more details describing the LDS system and each of its individual isolation functions.

QUESTION
420.063 (7) What are the reliability/availability goals for the reactor protection and engineered safety features systems?

RESPONSE
420.063 Reliability/Availability Goals

The ABWR RPS and ESF functions were to incorporate the performance features and equipment reduction advantages of the digital, multiplexed design while providing at least the reliability and availability of BWR/5 designs. Particularly with the RPS design, these goals were easily met because of four division, 2-out-of-4 configuration used.

For I&C equipment, studies have shown that the following reliabilities and availabilities are achievable when using equipment with the following failure characteristics (numbers for MTBF are meant to be very conservative figures; much higher MTBFs are known to be achievable in this type of equipment):

Individual controller: MTBF - 10,000 hours
Essential Multiplexing System: MTBF - 100,000 hours
All equipment: MTTR - 10 hours
Probability of detecting equipment failure - 0.9

RPS
Availability (4 div.) A = 0.999999
Reliability an order of magnitude better than BWR/5 (extra degree of redundancy for A and B trips)

ESF
Availability A = 0.9994
Probability of spurious trip avoidance = 0.999992

QUESTION
420.065 (7) What methodology is used in determining the system reliability/availability?

RESPONSE
420.065 Reliability Methodology (follows ANSI/IEEE Std. 352-1987):

a. FMEA for Essential Multiplexing System

b. Probabilistic Risk Assessment (PRA) for Safety System

c. Quantitative Analysis (assumed NUMAC-type instrumentation)

- Manual Calculation

- Computer Calculation (Markov Models for Essential Multiplexing System)

QUESTION
420.066 (7) Describe the data validation features in triplicated sensors.

RESPONSE
420.066 The safety systems use quadruple and not triplicated sensors, one set in each of the four protection divisions. Within each division, data is first validated after the analog to digital conversion process in the Remote Multiplexing Units. Converted signals must fall within the full scale analog range of 4-20 mA; otherwise a gross failure of the sensor is assumed. Digital inputs (contact closures) are filtered and de-bounced to eliminate transient signals.

The formatted digital words are assembled with parity bits and checksum or CRC bits before transmission from the local areas to the control room over the essential multiplexing system. The control room multiplexing units (CMUs) then check transmission quality over the dual channel multiplexing network, where one channel is considered the Master channel (normally on-line) and the other, the Standby channel. Transmission checks typically include frequency of checksum errors and hardware self-test results. At some predetermined error rate, data is taken from the Standby channel instead of the Master channel. Transfer of data from the CMUs to the SSLC logic processors is checked in essentially the same manner.

For a manual check of data plausibility, equivalent sensor data from the four divisions can be compared in the control room logic processors (data is exchanged among the divisions through isolated serial communication links).

QUESTION
420.067 (7) What testing will be done to demonstrate reliability? What is the specific scope of these tests?

RESPONSE
420.067 Testing of Safety System Logic and Control (SSLC) includes integration testing of the hardware and software of each controller and system testing of the interconnected network of controllers, including the fiber optic essential multiplexing system.

Specific testing will check conformity to the system design specifications. Both normal and abnormal responses to input stimuli will be monitored by injecting a defined sequence of test patterns. Test patterns will simulate the various modes of each processed system as defined in its respective design specification and interface block diagram (IBD). Responses to trip conditions in each division will confirm 2/4 coincidence logic. Appropriate fail-safe and fail-as-is response will be noted, including response to power failure. (See Appendix 7A, Section 7A.2, Response 8, for discussion of system response following power failures.)

Reliability testing: EMI/RFI/ESD, power transients, environmental (temp., RH), seismic, radiation, system burn-in, V&V of software.

Degraded mode testing will be performed. System response to multiplexing system failure will be monitored.

Response to manual control switch inputs will be tested.

Transfer of data to non-safety systems will be tested (process computer, control complex, annunciators, process control systems).

Specific to SSLC, bypassing of sensors, trip logic, and dual safety system channels will be tested. System failures will be simulated to confirm proper operation of self-diagnostic features.Automatic failover of MUX will be confirmed for input and output failures. Dual channel ECCS/ESF processing will be tested and failure response will be noted.

Response time testing will be performed.

Sequence of events monitoring will be verified.

Test inputs will include the full range of sensor types. Interlock permissives from motor control centers and valve limit switches will be simulated for testing under realistic conditions.

QUESTION
420.068 (7) What is the effect upon the number of spurious trips generated by the RPS if the digital design replaces the previous analog design? Provide comparison.

RESPONSE
420.068 The digital RPS reduces the number of spurious trips when compared to previous analog designs mainly because of the 2-out-of-4 input coincidence logic and 2-out-of-4 output coincidence logic required for a valid trip condition. This arrangement permits both a bypassed division due to a single failure and a single failure in another division to exist simultaneously without causing a trip.

Other factors for digital over analog:
low drift
low noise
more accurate
fewer components

QUESTION
420.070 (7.1.2.1.6) Is there any system for in-service testing of the ARI?

RESPONSE
420.070 Yes. The design of the ARI function incorporates testability, up to, but not including, the ARI valves, per the requirements of LTR NEDE 31906-P-A.

QUESTION
420.071 (7.1.2.1.6) Is the CRD scram discharge high water level used as the example of the fifth test valid given that there is no scram discharge volume?

RESPONSE
420.071 The reference to scram discharge volume was in error. This has been corrected in Revision B of this section.

QUESTION
420.072 (7.1.2.1.6) Section (1) of 7.1.2.1.6 states that normal surveillance can identify failures. Discuss whether this system has the capability of transmitting this information to the plant computer so that an immediate alarm can be given in addition to waiting for the scheduled surveillance.

RESPONSE
420.072 The statement concerning "normal surveillance" applied to intermittent failures for which the STS is capable of detecting and logging without stopping system operation. All other self-test failures (except intermittent failures) are annunciated to the operator at the main control room console and logged by the process computer.

QUESTION
420.073 (7.1.2.1.6) Section (4) notes that the four divisions are tested in sequence. When the thirty minute sequence is complete does the test system start over again or is this an operator initiated test?

RESPONSE
420.073 In the section referenced, the test starts over again automatically; testing is continuous.

PLEASE NOTE:

The concept of automatic self-test, as applied to ABWR safety systems, has changed since this section was written. The tests described are similar to the Clinton Nuclear System Protection System (NSPS) arrangement, which used an external test controller to periodically inject narrow pulses into the logic inputs and monitor the resulting outputs at the load drivers (the narrow pulses were too short to fully turn the load drivers off or on). NSPS functional logic was implemented with discrete logic gates and was static (not clock driven). The periodic, end-to-end, cross-divisional testing was necessary to confirm system continuity and verify the integrity of logic inputs and outputs and 2-out-of-4 interdivisional wiring.

The ABWR design for SSLC permits a different approach to testing of safety system logic:

a. The real-time, microprocessor-based, software-driven controllers contain powerful, internal, self-diagnostics that perform continuous monitoring of program flow, voltage levels, and inputs and outputs.
b. Serial, multiplexed, data communication allows continuous error checking and correcting of all transmitted and

received data.

c. System functions are distributed among several microprocessor-based chassis. Bypassing permits various controllers to be removed from service for maintenance without affecting system operation. Internal self-diagnostics permit continued testing of the remaining controllers. An external tester would require interruption or complex reconfiguration to continue operation.

d. Experience with GE's NUMAC instruments has proven the reliability of software diagnostics running as a low priority background task. Using external self test would complicate verification and validation of the functional software, since lack of interference with self test would have to be proven for various credible faults.

QUESTION

420.074 (7.1.2.1.6) Section (5) notes that only one division shall be bypassed at any one time. Describe the interlock protection or administrative controls which assure this.

RESPONSE

420.074 A separate manual keylock switch in each of the four divisions provides means to bypass that division. Isolated fiber-optic interface signals provide interlocks between the four divisions to prevent bypass of any two or more divisions at the same time. Once a bypass of one division has been established, bypasses of any of the remaining three divisions are inhibited.

QUESTION

420.076 (7.1.2.3.2) For section 7.1.2.3.2(1)(c,d,e) and (2)(a) define "sufficient".

RESPONSE

420.076 This question should be deleted because it is the same as 420.031. Refer to response 420.031.

QUESTION

420.077 (7.1.2.1.4.1) One of the reasons stated for the utilization of microprocessors for the implementation of instrumentation and logic functions is that less uncertainty exists in the margins between actual safety limi and the limiting safety trips. The margins are stated to be set from experimental data on setpoint drift (see Section 7.1.2.1.4.1) and from quantitative reliability requirements for each system and its components.
Provide the documented bases for this procedure.

RESPONSE

420.077 Setpoint drift does not exist, since the setpoints are programed digitally into non-volatile data storage memory in the Digital Trip Module.

Accuracy is improved over digital systems since setpoints can be programmed precisely and in engineering units.

Trip point accuracy is improved since the digitized sensor signal is compared precisely with the digital setpoint.

Hysteresis is adjustable in small increments and is stable. Upscale and downscale trip points can be accurately programmed.

The digitized sensor signals are accurate to the appropriate linear or non-linear characteristics since the A/D converters and amplifiers use auto-zeroing and auto-calibration.

QUESTION

420.082 (7.1.2.3.3) In section 7.1.2.3.3(1)(c) is manual control required only after 30 minutes? Why isn't automatic control also provided?

RESPONSE

420.082 Drywell or wetwell spray is not required before 30 minutes for the postulated break sequences. Drywell and wetwell sprays are directed by the symptom-based Emergency Operating Procedures.

Automatic initiation of the containment sprays was judged to not be an effective approach.

Fast operator response time is not required. For comparison, the GESSAR BWR-6 containment design pressure of 15 psig resulted in a lower margin for steam bypass capability and required automatic containment spray. The ABWR has a higher (45 psig) containment design pressure and, relatively, a lower steam bypass leakage area requirement which will allow more time for operator action. Manual initiation of drywell/wetwell sprays 30 minutes after the initiation of the event will be sufficient to control and limit the pressure rise below the design value.

The ABWR design allows for easy procedural valve alignment by the operator to achieve the containment spray modes. The heat exchanger is always in the flow path, and only the drywell and/or wetwell spray valves must be opened to initiate spray.

The design is simpler without automatic initiation.

QUESTION

420.083 (7.1.2.3.4) Is the suppression pool cooling also provided with automatic control?

RESPONSE

420.083 The suppression pool cooling is not provided with automatic control.

Non-automated suppression pool cooling is consistent with the GESSAR II design which was granted an FDA by the NRC (See GESSAR II FSAR, Section 7.3.1.1.5).

QUESTION

420.097 (7.3.1.1.4(h)) This refers to Section 3.11 for EQ. Section 3.11 invokes IEEE 323 as a basis for qualification. IEEE 323 was written assuming 40 year life. Address how this standard is to be extrapolated to a 60 year design life for the ABWR.

RESPONSE

420.097 IEEE 323 is a consensus national standard, endorsed by the NRC, which provides an acceptable approach to demonstrating that a component is capable of performing its intended safety function, in a given environment, for a given time. Since historically, most applicants have sought a 40-year operating license for their facility, associated qualification activities have been based on a need to demonstrate a 40-year operating life. However, IEEE 323 is not premised on a specific life; in fact, devices undergoing qualification using the approach presented in this standard often will show qualified life times less than 40 years while others will show a qualified life of significantly greater than 40 years.

With respect to the ABWR, the designed life is intended to be 60 years. It is intended that IEEE 323 will be used to demonstrate that IE devices in the plant will have a qualified life, with appropriate margin, equal to or greater than that period of time. Devices or components for which such a demonstration can not be made will either be redesigned to show this condition, or will (in the case of consumables) be administratively controlled for periodic changeout.

QUESTION

420.099 (7) While a computer-based system can provide more effective man/machine interface, the internal system operation is more complex, and can be more obscure to the operator or maintenance person if he is required to intervene at a complex level.
Have the operator tasks with regard to interfacing with the safety system been analyzed? What was the result of the analysis? How did the result of the analysis affect the requirements, design and implementation of the safety system?

RESPONSE

420.099 Tasks analyses have been performed in support of the design of the man-machine interface. The purpose of the task analyses is to tabulate the controls, indications and alarms needed to monitor and operate the safety systems and to allocate the various tasks comprised among hardware, software and operators. The information is then used to help define man-machine interface requirements for the hardware and software to be incorporated in the detailed design of the main control room and local area panels. The basis for task analysis includes normal system operating procedures and sympton-based emergency operating procedures. The results of the task analyses of the safety systems is contained in

auditable design record files.

Based upon the results of the task analyses, the man-machine interface requirements for a specific system are specified in the system's design specification. The man-machine interface requirements specification for a specific system and interface requirements specified in the task analysis report for a specified system constitute the top level man-machine interface requirements for that particular system. These requirements are then integrated into the operator interface panel design. The man-machine interface requirement specifications for the safety systems are contained in auditable design record files.

QUESTION
420.100 (7) While a computer-based system can provide more effective man/machine interface, the internal system operation is more complex, and can be more obscure to the operator or maintenance person if he is required to intervene at a complex level.
Describe the hardware design features that provide administrative control of devices capable of changing the data or program in the computer-based safety system.

RESPONSE
420.100 Data Security Features:

a. Front panel keylock control to enable keypad input [places instrument in off-line (tripped) mode].
b. Multi-level password control (factory and user settings).
c. Control programs, algorithms, and data tables in PROM for protected storage.

QUESTION
420.101 (7) While a computer-based system can provide more effective man/machine interface, the internal system operation is more complex, and can be more obscure to the operator or maintenance person if he is required to intervene at a complex level.
What data or program elements are adjustable/selectable by the operator?

RESPONSE
420.101 a. Setpoints accessible from front panel for reading (can be changed through keylock/password control).
b. Calibration inputs from front panel (accessible through keylock/password control).
c. Manual self-diagnostics (off-line access through keylock control).
d. Cross-channel check of sensor data (read only).
e. Manual trip of inoperable instrument channel (single data variable within a logic processing instrument).

The operator cannot access the program to change program flow or operation of any logic function shown on an IBD.

QUESTION
420.102 (7) While a computer-based system can provide more effective man/machine interface, the internal system operation is more complex, and can be more obscure to the operator or maintenance person if he is required to intervene at a complex level.
What capability of providing a permanent and current record of the system data base is provided in the system?

RESPONSE
420.102 Each safety system controller is a real-time, computer-based device equipped with both permanent data storage capability and volatile program memory.

Permanent data storage within SSLC:
a. The control programs, algorithms, and data tables of each system controller are in PROM.
b. Setpoints are EEPROM (EAROM).

The contents of PROM and EEPROM can be downloaded to the process computer for archiving or analysis upon operator request. A system fault or internal controller fault, including power failure, that causes an inoperative condition will result in PROM, EEPROM, and RAM data being automatically downloaded to the process computer.

QUESTION
420.103 (7) While a computer-based system can provide more effective man/machine interface, the internal system operation is more complex, and can be more obscure to the operator or maintenance person if he is required to intervene at a complex level.
Provide the basis for assumed operator response times.

RESPONSE
420.103 The safety systems are initiated automatically when required. There are no assumed operator response times used in the task analyses of the safety systems since they are initiated automatically. Manual actuation capability of safety systems is provided in accordance with Paragraph 4.17 of IEEE 279.

QUESTION
420.104 (7) While a computer-based system can provide more effective man/machine interface, the internal system operation is more complex, and can be more obscure to the operator or maintenance person if he is required to intervene at a complex level.
Discuss the range of possible scenarios for transferring the system from automatic to manual mode (and vice versa) and the potential for error or disturbance during such a transfer. Describe any differences characterized by these transfers with respect to BWR designs previously reviewed by the staff. For example, discuss consideration of I&E Bulletin 80-06, "Engineered Safety Features Reset Controls".

RESPONSE

420.104 In the standby safety systems, automatic and manual modes coexist;no transfer is required. Manual control of reactor emergency shutdown or initiation of the emergency core cooling systems is always available to the operator. Manual control is implemented both at the system and individual equipment level. Manual functions do not require the 2-out-of-4 voting of the automatic signals. However, various interlocks from valve limit switches, pump status indicators, or other sensors limit the operator's responses to safe actions.

QUESTION

420.106 (7) Define the logic by type and verify the diversity of the reactor internal pump trip circuits. If software is to be a part of this design, identify the form and diversity to be applied to this function.

RESPONSE

420.106 Referring to the attached figure on recirculation pump trip (RPT) logic, redundant inputs and diverse logic are provided in the RPT design. For example, the use of four sensors to monitor turbine stop valve (TSV) positions and two-out-of-four trip logic in the reactor protection system insulates the RPT signal from the effect of either two sensor failures in the non-trip condition, or one sensor failure in the trip condition. Furthermore, a two-out-of-four trip logic is provided in the RFC system to protect the divisional failure in the reactor protection system (RPS). This same degree of tolerance is available to the TCV fast closure and wide range water level sensors. For the high dome pressure and L3 RPT trip, the failure of one of three sensors in either the trip or non-trip condition is tolerable by the two-out-of-three logic.

Since all trip logic will be performed by application software embedded in dedicated microprocessors, logic redundancy depends only on the voting algorithm for the processor outputs. With both the RPS and SSLC (Safety System Logic & Control) outputs being voted upon by two-out-of-four logic in the recirculation flow control (RFC) system, failure in two divisions of RPS or SSLC processing channels, multiplexer, or data bus in the non-trip condition (a very remote possibility), or one channel of the same in the trip condition can be tolerated. Similarly, with the voting of the RFC system, feedwater flow control (FWC) system and steam bypass & pressure control (SB&PC) system controllers' outputs being performed by two-out-of-three logic, failure in one processing node in each controller will not result in a loss of system function.

Trip diversification is accomplished by planned distribution of trip logic. Multiple failures in the TCV pressure sensors, TSV position switches, or RPS, SB&PC or FWC processors will not cause the loss of more than five RIPs, and multiple failures in the SSLC processors will not cause more than six staggered pump trips. By separating the L2, L3 and high pressure RPT trip logic from the RPS system, no common mode failure can cause a loss of both reactor scram and ATWS RPT functions upon command. Also, by delaying the pump trip in three RIPs with hardware built into the ASD, no multiple failures in the RPT trip logic could cause a simultaneous trip of more than 5 RIPs.

QUESTION
420.107 (9.3.5.2) Describe procedural controls considered adequate to control the keylocked SLCS.

RESPONSE
420.107 The operation of the Standby Liquid Control System (SLCS) is governed by the symptom-based Emergency Operating Procedures (EOPs). NEDO-31331, "BWR Owners Group: Emergency Procedure Guidelines", Rev. 4, March 1987, has been approved by the NRC. These guidelines (which were originally developed for general application for BWRs) have been incorporated for the SLCS system in the ABWR Emergency Procedure Guidelines (See Section 1.1.3).

There are four entry conditions, any one of which would cause the operator to initiate emergency procedures. These are:

1) RPV water level below Level 3,
2) RPV pressure above the high pressure setpoint,
3) Drywell pressure above the high pressure setpoint, or
4) Reactor power greater than specified limits or unknown.

It is the fourth entry condition which could cause a need for SLCS. Once the operator has entered the EOFs he is instructed to monitor and control the following:

1) RPV water level,
2) RPV pressure, and
3) RPV power.

The EOP specifies numerous ways to lower power while continuing attempts to get the control rods in. The operator also monitors the suppression pool temperature during this procedure. Before the pool reaches a specified limit SLCS is initiated.

These symptom-based EOPs provide procedural controls that are adequate to control the keylocked SLCS.

QUESTION
420.108 (7.1.2.2) In section (m) consider replacing "obviate" with prevent or preclude.

RESPONSE
420.108 "Obviate" has been replaced with "prevent" as shown is attached mark-up of text.

QUESTION
420.109 (7.1.2.3.1) In Section 7.1.2.3.1(c), describe how provision for manual control limits dependence on operator judgement in times of stress.

RESPONSE

420.109 Strictly speaking, provision for manual control need not be mentioned under the heading "limit dependence on operator judgement in times of stress...". However, the intent was that the operator would be less stressed knowning such provision was available, even though the ECCS initiation is fully automated.

QUESTION

420.110 (7.1.2.3.1) For Section 7.1.2.3.1(2), describe any precautions taken to prevent or minimize inadvertent initiation of non-safety systems during accidents.

RESPONSE

420.110 The non-safety systems primarily consist of control systems that continuously operate during normal reactor power operation. These are described in Section 7.7. It is desirable, but not essential, that these systems continue to operate during postulated accident events in order to preclude the need for (or reduce the load on) the protection systems. Therefore, the question is not applicable to these systems.

As indicated in Section 9.5.1.1, the fire protection systems are designed so that their inadvertent operation or the occurrence of a single failure in any of these systems will not prevent plant safe shutdown.

QUESTION

420.111 (7.1.2.3.7) Why isn't the requirement to meet the Seismic Category I design requirements (7.1.2.3.7(1)(c)) listed in the other applicable sections?

RESPONSE

420.111 The seismic category I requirement is generally applied to all safety related instrumentation and control equipment as stated generically in Section 7.1.2.11.4 and in Section 3.10. It is usually not considered a design basis for each safety system since it is already imposed as a qualification requirement for the safety system's components. The statement in 7.1.2.3.7(1)(c) is therefore unnecessary, though it is true. To be consistent with the other sections, and avoid the erroneous implication that other safety systems may not meet such requirements, this statement has been removed as shown in attached mark-up.

QUESTION

420.112 (7.1.2.4.3) Are the other sections to be revised to include the normal operation parameters similar to 7.1.2.4.3(1)(a)?

RESPONSE
420.112 We do not anticipate such revisions for the following reason:

The safety design bases for the protection systems described in this section generally pertain to accident (abnormal) conditions. Few, if any, "normal" operation parameters are defined for such systems, other than to monitor for detection of an abnormal condition. An exception, as indicated, is the RHR shutdown cooling mode which has a safety function to remove residual heat from the reactor vessel during normal shutdown.

Normal operating parameters are generally handled by the control systems described in Section 7.7. These systems design bases are just the opposite, in that they generally have no safety design bases except to assure their functions do not preclude the operation of safety-related systems. [See Section 7.1.2.7(1).]

QUESTION
420.113 (7.1.2.6.1.1) Has consideration been given to providing the annunciators with backup diesel or battery power? (Ref. 7.1.2.6.1.1(2)(g))

RESPONSE
420.113 Yes. All control room annunciators shall be powered uninterruptably.

QUESTION
420.114 (7A.1-1) The copy of Section 7 provided to the staff did not include Appendix 7A nor an indication that it was to be provided later. Provide this section or a schedule for providing it.

RESPONSE
420.114 Appendix 7A was submitted to the NRC Staff in March, 1989.

QUESTION
420.115 (7.3 1.1.1.3(4)(e)) In the discussion about torque switches and thermal overloads, there is a reference to Section 3.8.4.2 which is the applicable codes and standards for seismic qualification of the Reactor and Control Buildings. What is the correct reference?

RESPONSE
420.115 The reference has been corrected to say "(For more information on valve testing, see Section 3.9.3.2)"

QUESTION
420.116 (1.2.2.4.8.1.2) The forth paragraph seems to imply that all three systems are needed to mitigate a LOCA. Is that accurate?

RESPONSE

420.116 The previous text was misleading. Section 6.3.1.1 provides a more accurate and detailed discription of the redundant features of the ECCS network. The last sentence of the fourth paragraph of 1.2.2.4.8.1.2 has been replaced with the following:

"These high pressure systems, combined with the RHR low pressure flooders and ADS, make up the ECCS network which can accommodate any single failure and still safely shut down the reactor. (See Section 6.3.1.1 for detail description of ECCS redundancy and reliability.)"

QUESTION

420.117 (9.3.5.1.1) Describe interlocks and indications used to prevent injection of the testing mode demineralized water instead of boron.

RESPONSE

420.117 Control room indications in conjunction with the EOPs prevent the unlikely occurrence of injecting the test tank demineralized water instead of boron.

When the SLCS has been initiated from the main control room, the injection valve and the pump suction valve will open to begin injection of the sodium pentaborate solution. In the unlikely event that the test tank suction valve were open, then neither the injection valve nor the pump suction valve would open and demineralized water would be circulated back to the test tank. However, the test tank suction valve is a manually operated valve whose position (full open or full closed) is indicated in the control room. To inhibit boron injection under this condition, the plant operators would have had to have left the test tank valve open after testing, and the control room operators would have had to ignore the valve position indicator. This is an extremely unlikely scenario.

In addition to the above, the operators operating under the EPGs (See response to Question 420.107) are instructed to confirm boron injection by monitoring the solution water level in the tank.

Therefore, the operating procedures and indicators will prevent the injection of the testing mode demineralized water instead of boron.

QUESTION

420.119 (7.4.1.2(7)) Are there any other valves which must isolate upon initiation of the SLCS?

RESPONSE

420.119 Only the reactor water cleanup isolation valve must close upon initiation of the SLCS. However, given the initiation of the SLCS the operator will be monitoring and controlling many functions of the plant, (See response to Question 420.107), such as managing the RPV water level, to bring the plant to a safe shutdown. These other actions may involve isolating other systems to maximize the benefits of the SLCS.

QUESTION

420.121 (7.3.1.2(7)) The first paragraph states that pipe break outside containment and feedwater line break are discussed below. The staff could not locate these items.

RESPONSE

420.121 The following additional section has been added to 7.3.1.2(7):

"(f) Pipe Break Outside Containment and Feedwater Line Break

For any postulated pipe rupture, the structural integrity of the containment structure is maintained. In addition, safety/relief valves (SRVs) and the reactor core isolation cooling (RCIC) system steamline are located and restrained so that a pipe failure would not prevent depressurization. Separation is provided to preserve the independence of the low-pressure flooder (LPFL) systems.

For high energy piping systems penetrating through the containment, such as the feedwater lines, isolation valves are located as close to the containment as possible. The pressure, water level, and flow sensor instrumentation for essential systems, which are required to function following a pipe rupture, are protected.

Pipe whip protection is detailed in Section 3.6."

7.1 INTRODUCTION

This chapter presents the specific detailed design and performance information relative to the instrumentation and control aspects of the safety-related systems utilized throughout the plant. The design and performance considerations relative to these systems' safety function and their mechanical aspects are described in other chapters.

7.1.1 Identification of Safety-Related Systems

7.1.1.1 General

Instrumentation and control systems are designated as either nonsafety-related systems or safety systems depending on their function. Some portions of a system may have a safety function while other portions of the same system may be classified nonsafety-related. A description of the system of classification can be found in Chapter 15, Appendix A.

The systems presented in Chapter 7 are also classified according to NRC Regulatory Guide 1.70, Revision 3 (i.e., reactor protection (trip) system (RPS), engineered safety feature (ESF) systems, systems required for safe shutdown, safety-related display instrumentation, all other instrumentation systems required for safety, and control systems not required for safety). Table 7.1-1 compares instrumentation and control systems of the ABWR with those of the GESSAR II 238 Nuclear Island. Differences and their effect on safety-related systems are also identified in Table 7.1-1.

Each individual safety-related system utilizes redundant channels of safety-related instruments for initiating safety action. The automatic decision making and trip logic functions associated with the safety action of several safety-related nuclear steam supply systems (NSSS) are accomplished by a four-division correlated and separated protection logic complex called the safety system logic and control (SSLC). The SSLC multidivisional complex includes divisionally separate control room and other panels which house the SSLC equipment for controlling the various safety function actuation devices. The SSLC receives input signals from the redundant channels of instrumentation in the safety-related system, and uses the input information to perform logic functions in making decisions for safety actions.

Divisional separation is also applied to the essential multiplexing system (EMS), which provides data highways for the sensor input to the logic units and for the logic output to the system actuators (actuated devices such as pump motors and motor operated valves). Systems which utilize the SSLC are the reactor protection (trip) system, the high pressure core flooder system, the residual heat removal system, the automatic depressurization system, the leak detection and isolation system and the reactor core isolation cooling system which are defined in the following subsections and discussed in other sections of this chapter.

7.1.1.2 Reactor Protection (Trip) System (RPS)

The reactor protection (trip) system instrumentation and controls initiated an automatic reactor shutdown via insertion of control rods (scram) if monitored system variables exceed preestablished limits. This action avoids fuel damage, limits system pressure and thus restricts the release of radioactive material.

7.1.1.3 Engineered Safety Features (ESF) Systems

7.1.1.3.1 Emergency Core Cooling Systems (ECCS)

420.029

Instrumentation and controls provide automatic initiation and control of specific core cooling systems such as high-pressure core flooder (HPCF) system, automatic depressurization system (ADS), reactor core isolation cooling system (RCIC) and the low-pressure coolant injection flooders of the residual heat removal system provided to cool the core fuel cladding following a design basis accident.

7.1.1.3.2 Leak Detection and Isolation System

Instrumentation and controls monitor selected potential sources of steam and water leakage or other conditions and automatically initiate closure of various ~~automatic~~ isolation valves if monitored system variables exceed preestablished limits. This action limits the loss of coolant from the

reactor coolant pressure boundary and the release of radioactive materials from either the reactor coolant pressure boundary or from the fuel and equipment storage pools.

7.1.1.3.3 Wetwell and Drywell Spray Mode of RHR

Instrumentation and control provides manual initiation of wetwell spray and manual initiation of drywell spray (when high drywell pressure signal is present) to condenses steam in the containment and remove heat from the containment. The drywell spray has an interlock such that drywell spray is possible only in the presence of a high drywell pressure condition.

7.1.1.3.4 Suppression Pool Cooling Mode of RHR (SPC-RHR)

Instrumentation and control is provided to manually initiate portions of the RHR system to effect cooling of the suppression pool water.

7.1.1.3.5 Standby Gas Treatment System

Instrumentation and control is provided to maintain negative pressure in the secondary containment and for limiting airborne radioactivity release from containment if required.

7.1.1.3.6 Emergency Diesel Generator Support Systems

Instrumentation and control is provided to assure availability of electric control and motive power under all design basis conditions. The function of the diesel generator is to provide emergency AC power supply for the safety-related loads (required for the safe shutdown of the reactor) when the offsite source of power is not available.

7.1.1.3.7 Reactor Building Cooling Water System

Instrumentation and control is provided to assure availability of cooling water for heat removal from the nuclear system as required.

7.1.1.3.8 Essential HVAC Systems

Instrumentation and control is provided to maintain an acceptable thermal environment for safety equipment and operating personnel.

7.1.1.3.9 HVAC Emergency Cooling Water System

Instrumentation and control is provided to assure that adequate cooling is provided for the main control room, the control building essential electrical equipment rooms, and the diesel generator cooling coils.

7.1.1.3.10 High Pressure Nitrogen Gas Supply System

Instrumentation and control is provided to assure adequate instrument high pressure nitrogen is available for ESF equipment operational support.

7.1.1.4 Safe Shutdown Systems

7.1.1.4.1 Alternate Rod Insertion Function (ARI)

Though not required for safety, instrumentation and controls for the ARI provide a function for mitigation of the consequences of anticipated transient without scram (ATWS) events. Upon receipt of an initiation signal (high reactor dome pressure or low reactor water level), the fine-motion control rod drive (FMCRD) motor shall drive all rods full-in. This provides a method, diverse from the hydraulic control units (HCUs) for scramming the reactor.

7.1.1.4.2 Standby Liquid Control System (SLCS)

Instrumentation and controls are provided for the manual initiation of an independent backup system which can shut the reactor down from rated power to the cold condition in the event that all withdrawn control rods cannot be inserted to achieve reactor shutdown.

7.1.1.4.3 Residual Heat Removal (RHR) System / Shutdown Cooling Mode

Instrumentation and controls provide manual initiation of cooling systems to remove the decay and sensible heat from the reactor vessel.

7.1.1.4.4 Remote Shutdown System

Instrumentation and controls are provided outside the main control room to assure safe shutdown of the reactor in the event the main

control room should become uninhabitable.

7.1.1.5 Safety-Related Display Instrumentation

Safety-related display instrumentation is provided to inform the reactor operator of plant conditions and equipment status so that it can be determined when a manual safety action should be taken or is required.

7.1.1.6 Other Safety-Related Systems

7.1.1.6.1 Neutron Monitoring System (NMS)

The neutron monitoring system (NMS) monitors the core neutron flux from the startup source range to beyond rated power. The neutron monitoring system provides logic signals to the reactor protection system (RPS) to shut down the reactor when a condition necessitating a reactor scram is detected. The NMS is composed of four subsystems:

(1) startup range neutron monitoring (SRNM),

(2) local power range monitoring (LPRM),

(3) automated traversing incore probe (ATIP), and

(4) average power range monitoring (APRM).

7.1.1.6.2 Process Radiation Monitoring System Instrumentation and Controls (PRM)

The process radiation monitoring system monitors the main steam lines, vent discharges and all liquid and gaseous effluent streams which may contain radioactive materials. Main control room display, recording and alarm capability is provided along with trip inputs to the reactor protection system and leak detection and isolation systems.

7.1.1.6.3 High Pressure/Low Pressure Systems Interlock Protection Function

Instrumentation and controls provide automatic control of the RHR/LPFL system valves thereby providing an interface between this low-pressure system and the reactor coolant pressure boundary to protect it from overpressurization.

7.1.1.6.4 Fuel Pool Cooling and Cleanup System

The fuel pool cooling function maintains the fuel storage pool below a desired temperature necessary to service and store the fuel bundles. The cleanup function consists of filter demineralizer units which treat the water and recirculated it back to the fuel pool.

7.1.1.6.5 Wetwell-to-Drywell Vacuum Breaker System

This system is provided to prevent the occurrence of harmful pressure differences across the diaphragm floor.

7.1.1.6.6 Containment Atmospheric Monitoring System

The containment atmospheric monitoring system (CAMS) measures and records radiation levels and the oxygen/hydrogen concentration in the primary containment under post-accident conditions. It is automatically put in service upon detection of loss-of-coolant accident (LOCA) conditions.

7.1.1.6.7 Suppression Pool Temperature Monitoring System

Instrumentation is provided to maintain operator awareness of pool temperatures and level under all operating and accident conditions.

7.1.2 Identification of Safety Criteria

7.1.2.1 General

Design bases and criteria for instrumentation and control equipment design are based on the need to have each system perform its intended function while meeting the applicable general design criteria, regulatory guides, industry standards, and other documents.

The safety design basis for a safety system states in functional terms the unique design requirements that establish the limits within which the safety objectives shall be met. The general functional requirement portion of the safety design basis presents those requirements

Specific Regulatory Requirements:

The specific regulatory requirements applicable to the controls and instrumentation for the ECCS are shown on Table 7.1-2.

(2) Nonsafety-Related Design Bases

None.

7.1.2.3.2 Leak Detection and Isolation System (LDS) ~~(LD&IS)~~ Instrumentation and Control

(1) Safety Design Bases

The general functional requirements of the LDS ~~LD&IS~~ instrumentation and control are to detect, indicate and alarm leakage from the reactor primary pressure boundary and, in certain cases, to initiate closure of isolation valves to shut off leakage external to the containment.

In order to meet the safety design basis, the LDS ~~LD&IS~~ instrumentation and control system shall be designed (as a minimum) to:

(a) provide direct and accurate measurements of parameters which are indicative of a reactor coolant pressure boundary (RCPB) leak or a leak of reactor coolant outside the containment and then provide automatic ~~prompt~~ isolation of the affected system or area;

(b) monitor predetermined parameters with precision and reliability and respond correctly to the sensed parameters;

(c) provide a sufficient number of independent monitors sensing each parameter to ensure accurate measurement and preclude the possibility of a failure to isolate due to instrumentation failure;

(d) provide a sufficient number of redundant and/or diverse monitors sensing each parameter to ensure that the condition requiring isolation cannot disable the monitors necessary to cause isolation;

(e) provide an isolation control system with sufficient redundancy to ensure the LDS ~~LD&IS~~ can perform its intended function, assuming a single failure caused by any of the design basis events or a single power supply failure;

(f) provide an isolation control system which will ensure that isolation of the containment and/or reactor vessel will occur once initiated;

(g) provide instrumentation and control to permit the operator to manually initiate isolation if necessary.

(g) Provide interlocks to assure reset capability is only possible after clearance of isolation signals.

Specific Regulatory Requirements

Specific regulatory requirements applicable to this system are shown in Table 7.1-2.

(2) Nonsafety-Related Design Bases

The LDS ~~LD&IS~~ instrumentation and control is designed to:

(a) provide sufficient redundancy of instruments to avoid unnecessary plant shutdowns due to instrument malfunctions;

(b) avoid plant shutdowns due to a single power supply failure; and

(c) provide the capability to maintain, calibrate, or adjust system monitors while operating without causing plant shutdowns for reducing safety margins.

(d) provide status information to annunciator and process computer.

420.032

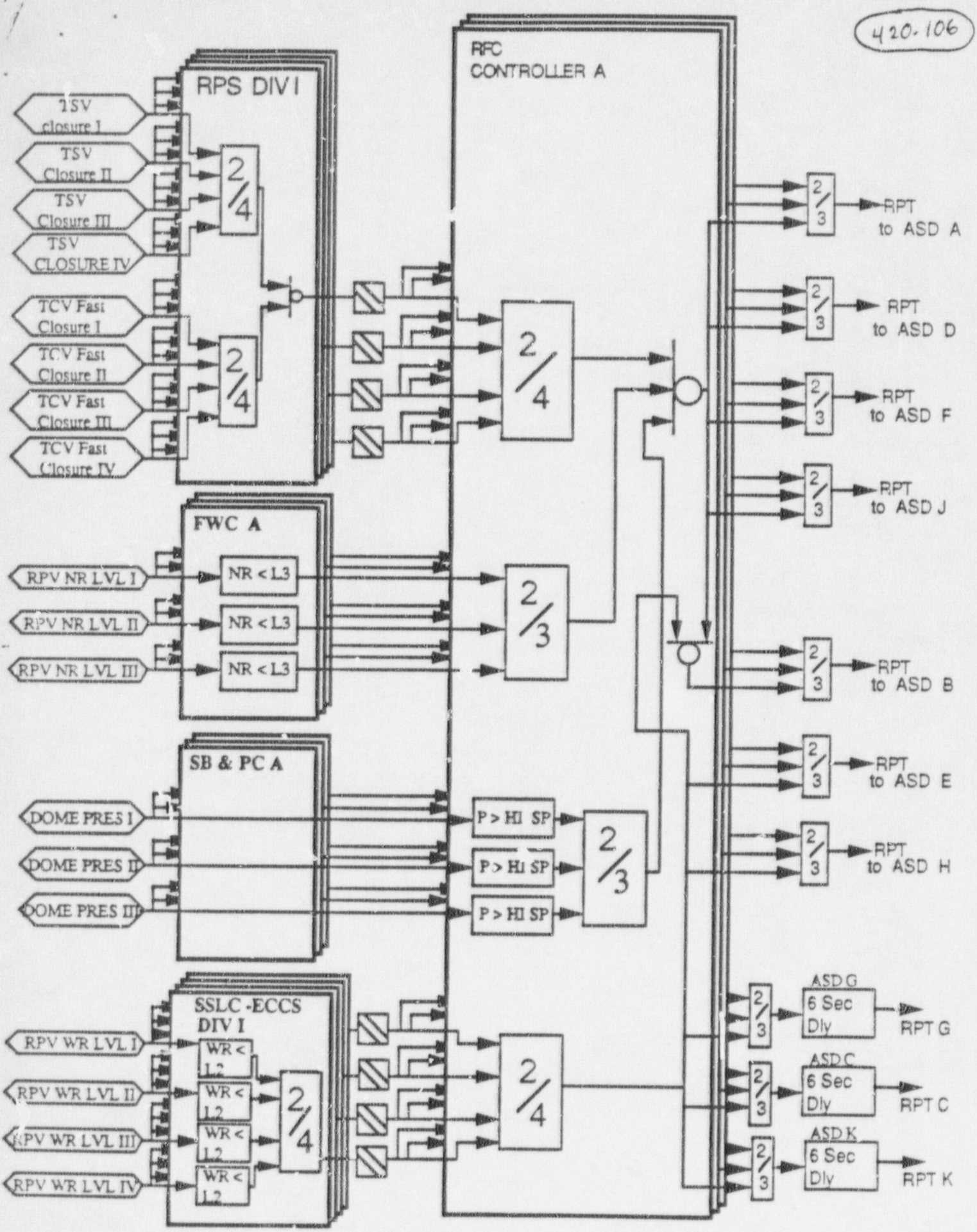
420.033

7.1.2.3.3 RHR Wetwell and Drywell Spray Cooling Mode (CS RHR) Instrumentation and Controls

(1) Safety Design Bases

The general functional requirements of the wetwell and drywell cooling mode of the RHR system shall provide instrumentation and controls to:

(a) initiate wetwell and drywell spray as required to avoid environmental conditions of pressure and temperature that would threaten the integrity of the containment during a transient or accident condition;



ABWR RPT LOGIC

sients, or physical events from impairing the ability of the system to respond correctly.

(k) Earthquake ground motions, as amplified by building and supporting structures, shall themselves initiate reactor scram, and shall not impair the ability of the RPS to otherwise initiate a reactor scram, with the exception of turbine building trips which originate from a non-seismic building. These shall be backed up by diverse variables such as reactor pressure and power trips.

(l) No single failure within the RPS shall prevent proper reactor protection system action when required to satisfy Safety Design Bases as described by the first three bullets under 1(a) above.

(m) Any one intentional bypass, maintenance operation, calibration operation, or test to verify operational availability shall not ~~obviate~~ prevent the ability of the reactor protection system to respond correctly.

420.108

(n) The system shall be designed so that two or more sensors for any monitored variable exceeding the scram setpoint will initiate an automatic scram.

The following bases reduce the probability that RPS operational reliability and precision will be degraded by operator error:

(o) Access to trip settings, component calibration controls, test points, and other terminal points shall be under the control of plant operations supervisory personnel.

(p) Manual bypass of instrumentation and control equipment components shall be under the control of the control room operator. If the ability to trip some essential part of the system has been bypassed, this fact shall be continuously annunciated in the main control room.

Specific Regulatory Requirements:

The specific requirements applicable to the RPS instrumentation and control are shown in Table 7.1-2.

(2) Nonsafety-Related Design Bases

The RPS is designed with the added objective of plant availability. The setpoints, power sources, and control and instrumentation shall be arranged in such a manner as to preclude spurious scrams insofar as practicable and safe.

7.1.2.3 Engineered Safety Features (ESF)

7.1.2.3.1 Emergency Core Cooling Systems Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The ECCS control and instrumentation shall be designed to meet the following requirements:

(a) automatically initiate and control the emergency core cooling systems to prevent fuel cladding temperatures from reaching the limits of 10CFR50.46.

(b) respond to a need for emergency core cooling regardless of the physical location of the malfunction or break that causes the need;

(c) limit dependence on operator judgement in times of stress by:

indication of performance of the ECCS by main control room instrumentation; and

provision for manual control of the ECCS in the main control room.

applicable to the diesel generator and its auxiliaries are listed in Table 7.1-2.

(2) Nonsafety-Related Design Bases

There is no power generation design basis for this system.

7.1.2.3.7 Reactor Building Cooling Water System - Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the instrumentation and controls of this system shall be to:

(a) maintain control of cooling water to equipment that requires cooling during reactor shutdown modes and following a LOCA;

(b) provide for the automatic isolation of the non-essential parts of the reactor building cooling water system (except CRD pump oil coolers and instrument air coolers) from the essential parts during LOCA or upon detection of a major RCW leak in the non-essential system;

(c) satisfy Seismic Category I design requirements

Specific Regulatory Requirements:

The specific regulatory requirements applicable to the system instrumentation and controls are given in Table 7.1-2.

(2) Nonsafety-Related Design Bases

(a) Controls and instrumentation shall be provided to control and monitor the distribution of reactor building cooling water to remove heat from plant auxiliaries during normal plant operation.

(b) The essential service water system shall be capable of being tested during normal plant operation.

7.1.2.3.8 Essential HVAC Systems-Instrumentation and Controls

(1) Safety Design Bases

See Subsections 9.4.1.1.1 and 9.4.5.1.1.

7.1.2.3.9 HVAC Emergency Cooling Water System-Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the HVAC emergency cooling water system instrumentation and controls shall provide control for cooling units that ensure a controlled environment for essential equipment and control room areas following a loss-of-coolant accident, loss of preferred power, or isolation of normal heating, venting, and air conditioning (HVAC).

Specific Regulatory Requirements:

The specific regulatory requirements applicable to the system instrumentation and control are given in Table 7.1-2.

(2) Nonsafety-Related Design Bases

The system shall provide a continuous supply of chilled water to the cooling coils of air conditioning systems which provide a controlled temperature environment and proper humidity to ensure the comfort of the operating personnel and to provide a suitable atmosphere for the operation of control equipment.

7.1.2.3.10 High Pressure Nitrogen Gas Supply System - Instrumentation and Control

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the instrumentation and controls shall provide automatic and manual control of the nitrogen gas supply to assure its operation during

damaged by overheating at reduced RCIC pump discharge flow, a pump minimum flow bypass is provided to route the water discharged from the pump back to the suppression pool.

The minimum flow bypass is controlled by an automatic DC motor-operated valve. The control scheme is shown in Figure 7.3-3 (RCIC IBD). The valve is automatically closed at high flow or when either the steam supply or turbine trip valves are closed. Low flow combined with high pump discharge pressure opens the valve.

To prevent the RCIC steam supply pipeline from filling up with water and cooling excessively, a condensate drain pot, steamline drain, and appropriate valves are provided in a drain pipeline arrangement just upstream of the turbine supply valve. The controls position valves so that during normal operation steamline drainage is routed to the main condenser. The water level in the steamline drain condensate pot is controlled by a level switch and a direct acting solenoid valve which energizes to allow condensate to flow out of the drain pot. Upon receipt of an RCIC initiation signal and subsequent opening of the steam supply valve, the drainage path is shut off by redundant valves.

To prevent the turbine exhaust line from filling with water, a condensate drain pot is provided. The water in the turbine exhaust line condensate drain pot is routed to the clean radwaste system. RCIC initiation and subsequent opening of the steam supply valve causes the condensate drainage line to be shut off by redundant valves.

During test operation, the RCIC pump discharge is routed to the suppression pool. Two DC motor-operated valves are installed in the pump discharge to suppression pool pipeline. The piping arrangement is shown in Figure 5.4-8 (RCIC P&ID). Upon receipt of an RCIC initiation signal, the valves close as shown in Figure 7.3-3 (RCIC IBD). The pump suction from the condensate storage pool is automatically closed or interlocked closed if the suppression pool suction valve is fully open. Various indications pertinent to the operation and condition of the RCIC are available to the main control room operator. Figure 7.3-3 (RCIC IBD) shows the various indications provided.

(d) Redundancy and Diversity

On a network basis, the HPCF is redundant and diverse to RCIC for the ECCS and safe shutdown function. Therefore, RCIC as a system by itself is not required to be redundant or diverse although the instrument channels are redundant for operational availability purposes.

The RCIC is actuated by high drywell pressure or by reactor low water level. Four nuclear boiler system sensors monitor each parameter and combine in two sets of two-out-of-four logic signals in the safety system logic and control (SSLC). A permissive signal from either set initiates the RCIC. The sensor outputs themselves are shared by other systems in common with each division (see NBS P&ID Figure 5.1-3).

(e) Actuated Devices

All automatic valves in the RCIC are equipped with remote manual test capability so that the entire system can be operated from the control room. Motor-operated valves are equipped with limit and torque switches. Limit switches turn off the motors when movement is complete. In the closing direction, torque switches turn the motor off when the valve has properly seated. Thermal overload devices are used to trip motor-operated valves during testing only ~~(see Section 3.6.4.2)~~. All motor-operated and air-operated valves provide control

(For more information on valve testing, see section 3.9.3.2)

420.115

operates automatically in time and with sufficient coolant flow to maintain adequate water level in the reactor vessel for events defined in Section 5.4.

1.2.2.4.8 Emergency Core Cooling Systems (ECCS)

In the event of a breach in the reactor coolant pressure boundary that results in a loss of reactor coolant, three independent divisions of ECCS are provided to maintain fuel cladding below the temperature limit as defined by 10CFR50.46 . Each division contains one high pressure and one low pressure inventory makeup system. The systems are:

1.2.2.4.8.1 High Pressure

1.2.2.4.8.1.1 High-Pressure Core Flooder (HPCF) System

HPCF are provided in two divisions to maintain an adequate coolant inventory inside the reactor vessel to limit fuel cladding temperatures in the event of breaks in the reactor coolant pressure boundary. The systems are initiated by either high pressure in the drywell or low water level in the vessel. They operate independently of all other systems over the entire range of system operating pressures. The HPCF system pump motors are powered by a diesel generator if auxiliary power is not available. The systems may also be used as a backup for the RCIC system.

1.2.2.4.8.1.2 RCIC Description

One division contains the RCIC system which consists of a steam-driven turbine which drives a pump assembly and the turbine and pump accessories. The system also includes piping, valves, and instrumentation necessary to implement several flow paths. The RCIC steam supply line branches off one of the main steam lines (leaving the reactor pressure vessel) and goes to the RCIC turbine with drainage provision to the main condenser. The turbine exhausts to the suppression pool with vacuum breaking protection. Makeup water is supplied from the condensate storage pool (CSP) or the suppression pool with the preferred source being the CSP. RCIC pump discharge lines include the main discharge line to the feedwater line, a test-return line to the suppression pool, a minimum flow bypass line to the suppression pool and a cooling water supply line to auxiliary equipment.

Following a reactor scram, steam generation in the reactor core continues at a reduced rate due to the core fission product decay heat. The turbine bypass system diverts the steam to the main condenser, and the feedwater system supplies the makeup water required to maintain reactor vessel inventory.

In the event the reactor vessel is isolated, and the feedwater supply is unavailable, relief valves are provided to automatically (or remote manually) maintain vessel pressure within desirable limits. The water level in the reactor vessel drops due to continued steam generation by decay heat. Upon reaching a predetermined low level, the RCIC system is initiated automatically. The turbine-driven pump supplies water from the suppression pool or from the CSP to the reactor vessel. The turbine is driven with a portion of the decay heat steam from the reactor vessel, and exhausts to the suppression pool.

In the event there is a LOCA, the RCIC system in conjunction with the two HPCF systems, is designed to pump water into the vessel from approximately 150 psig to full operating pressure. This combination of systems provides adequate core cooling until vessel pressure drops to the point at which the low pressure flooder loop (LPFL) subsystems of the RHR can be placed in operation.

During RCIC operation, the wetwell suppression pool acts as the heat sink for steam generated by reactor decay heat. This results in a rise in pool water temperature. Heat exchangers in the residual heat removal (RHR) system are used to maintain pool water temperature within acceptable limits by cooling the pool water directly.

1.2.2.4.8.2 Automatic Depressurization System (ADS)

The ADS rapidly reduces reactor vessel pressure in a loss-of-coolant accident, enabling the low-pressure RHR to deliver cooling water to the reactor vessel.

420.116

"These high pressure systems, combined with the RHR low pressure flooders and ADS, make up the ECCS network which can accommodate any single failure and still safely shut down the reactor. (See Section 6.3.1.1 for detail description of ECCS redundancy and reliability.)"

To protect ESF systems in the event of a postulated fire, the redundant portions of the systems are separated by fire barriers. If an internal fire were to occur within one of the sections of the main control room panel or in the area of one of the local panels, the ESF systems functions would not be prevented by the fire. The use of separation and fire barriers ensures that, even though some portion of the system may be affected, the ESF system will continue to provide the required protective action. The remote shutdown system provides redundancy in the event of significant exposure fires in the control room.

The plant fire protection system is discussed in Section 9.5.

A

The following ESF system instrument taps and sensing lines are located inside the drywell and terminate outside the drywell. They could be subjected to the effects of a design basis loss-of-coolant accident (LOCA):

Reactor vessel pressure

Reactor vessel water level

Drywell pressure

These items have been environmentally qualified to remain functional during and following a LOCA as discussed in Section 3.11.

~~(f) Pipe Break Outside Containment and Feedwater Line Break~~

(8) Minimum Performance Requirements

The instrumentation and control for the various systems described in this section

Trip points are within the operating range of instruments with full allowance for instrument error, drift, and setting error.

7.3.1.3 System Drawings

A list of the drawings is provided in Section 1.7. P&IDs are provided within Chapters 5, 6, and 9, and are referenced where appropriate in Chapter 7. All other diagrams, tables, and figures are included in Chapter 7 as appropriate. Subsection 1.7.3 provides keys for the interpretation of symbols used in these documents.

7.3.2 Analysis

Failure modes and effects analyses for ESF systems are provided in Chapter 15.

7.3.2.1 Emergency Core Cooling Systems Instrumentation and Controls

7.3.2.1.1 General Functional Requirements Conformance

Chapters 15, "Accident Analysis," and 6, "Engineered Safety Feature Systems," evaluate the individual and combined capabilities of the emergency cooling systems. For the entire range of nuclear process system break sizes, the cooling systems provide adequate removal of decay heat from the reactor core.

Instrumentation for the emergency core cooling systems must respond to the potential inadequacy of core cooling regardless of the location of a breach in the reactor coolant pressure boundary. Such a breach inside or outside the containment is sensed by reactor low water level. The reactor vessel low water level signal is the only emergency core cooling system initiating function that is completely independent of breach location. Consequently, it can actuate HPCF, RCIC, ADS and LPFL.

(f) Pipe Break Outside Containment and Feedwater Line Break

For any postulated pipe rupture, the structural integrity of the containment structure is maintained. In addition, safety/relief valves (SRVs) and the reactor core isolation cooling (RCIC) system steamline are located and restrained so that a pipe failure would not prevent depressurization. Separation is provided to preserve the independence of the low-pressure flooder (LPFL) systems.

For high energy piping systems penetrating through the containment, such as the feedwater lines, isolation valves are located as close to the containment as possible. The pressure, water level, and flow sensor instrumentation for essential systems, which are required to function following a pipe rupture, are protected.

Pipe whip protection is detailed in Section 3.6.

QUESTION

435.023 Section 8.3.1.2.1 states that there are four 6.9 kV electrical divisions, three of which are independent load groups backed by individual diesel generator sets. Figure 8.3-2 entitled "6.9 kV System Single Line" however shows only the three divisions backed by diesel generators. It does not show the fourth 6.9 kV division referred to in section 8.3.1.2.1 Please clarify this discrepancy and show the fourth division, if it exists, in Figures 8.3-1 and 8.3-2.

RESPONSE

435.023 Section 8.3.1.2.1 was incorrect and has been revised in accordance with attached mark-up. There are only three 6.9 kV electrical divisions. Figures 8 3-1 and 8.3-2 are correct as shown.

QUESTION

435.024 In section 8.3.1.2.1 it is stated that the standby power system redundancy is based on the capability of any two of the four divisions (two of three load groups) to provide the mininum safety functions necessary to shut down the unit in case of an accident and maintain it in the safe shutdown condition. Why can't the unit be shut down in case of an accident with only one of the three load groups available? Identify the systems or loads needed that require that two of the three load groups be available.

RESPONSE

435.024 Section 8.3.1.2.1 was incorrect and has been revised in accordance with attached mark-up. The reactor can be safely shut down from the control room with any one of the three load groups available.

QUESTION

435.029 (a) Section 8.3.1.3.1 discusses the means used to physically identify safety related power systems equipment. It states that all cables for Class 1E systems and asociated circuits (except those routed in conduit) are tagged every 15 ft. In addition all cables are tagged at their terminations with a unique identifying number. R.G. 1.75, Rev. 2 states that these cables should be marked at intervals not to exceed 5 ft. and the preferred method of marking the cable is color coding. IEEE 384-1974 also states that these cable markings shall be applied prior to or during installation. Please verify that these recommendations are met or justify the differences. If exception is taken to position C.10 of R.G. 1.75, Rev. 2 regarding cable marking, the exception should be identified in section 8.1.3.1.2.2 and wherever the exception is applicable.

(b) Section 8.3.1.3.1 also describes the marking of conduit and cable trays. Please verify that in accordance with the requirements of IEEE 384-1974 these markings are applied prior to the installation of cables.

(c) The identification requirements for instrumentation and control system cables and raceways described in items (3) and (4) of section 8.3.1.3.2.1 should be the same as those for power systems provided in section 8.3.1.3.1 subject to the above comments.

RESPONSE

435.029 Sections 8.3.1.3.1 and 8.3.1.3.2.1 have been revised as shown on attached. The identification criteria fully complies with the requirements of R.G. 1.75, Rev. 2, and IEEE 384-1974 regarding marking of cables, conduit, cable trays and raceways.

QUESTION

435.030 Provide a description of the ABWR cable spreading areas in the ABWR SSAR. Describe how the requirements specified in section 5.1.3 of IEEE 384-1974 (as modified by position C.12 of R.G. 1.75) are met.

RESPONSE

435.030 A description of the cable spreading areas is not applicable to the ABWR because a majority of the signals will be multiplexed to the control room. A cable spreading area is not in the plant layout.

QUESTION

435.035 Item (4) of section 8.3.1.4.2.3.1 states that the scram solenoid conduits will have unique identification but no specific separation requirements, and the scram group conduits may run in the same raceway with other divisional circuits. If the scram group conduits are run in the same raceway with other divisional circuits or if they have less than the minimum separation from Class 1E circuits, they must be treated as associated circuits and must meet the requirements specified in section 4.5 of IEEE 384-1974. Please verify that this is the case, and identify the specific separation requirements that will be applied to the scram group conduits when they become associated circuits.

RESPONSE

435.035 The statement in item (4) related to "no specific separation requirements" was not correct. There are specific separation requirements for the conduits containing the RPS wiring associated with each of the four scram groups, i.e., the conduits required from the scram actuating devices to the scram solenoid fuse panels, and from the fuse panels to the two solenoids of each of the individual scram pilot valves. Section 8.3.1.4.2.3.1 has been completely revised as per attached pages.

Individual grounded steel conduits will be provided to contain the scram solenoid wiring of each of the four scram groups to protect this wiring from hot shorts to any other wiring. Individual conduits will also be provided for the A solenoid wiring and for the B solenoid wiring in the same scram group.

The scram group conduits will have unique identification and will be treated essentially as if they are separate enclosed raceways, i.e., the conduits containing the scram solenoid group circuit wiring will be physically separated from raceways which contain either divisional or "non-divisional" (non-safety-related) circuits. Any scram group conduit may be routed alongside of any raceway containing either safety-related circuits (of any division), or any raceway containing non-safety-related circuits, as long as the conduit itself is not within the boundary of the raceway which contains either the divisional or non-safety-related circuits. Each scram conduit will be physically separated by at least one (1) inch from either metal enclosed raceways

or non-enclosed raceways.

(b) Conformance: The AC power system is in compliance with these GCDs, in part, or as a whole, as applicable. The GDCs are generically addressed in Subsection 3.1.2.

(2) Regulatory Guides (RGs):

(a) RG 1.6 - Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems

(b) RG 1.9 - Selection, Design, and Qualification of Diesel-Generator Units Used as Standby (Onsite) Electric Power Systems at Nuclear Power Plants

(c) RG 1.32 - Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants

(d) RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

(e) RG 1.63 - Electric Penetration Assemblies in Containment Structures for Light-Water-Cooled Nuclear Power Plants

(f) RG 1.75 - Physical Independence of Electric Systems

(g) RG 1.106 - Thermal Overload Protection for Electric Motors on Motor-Operated Valves

(h) RG 1.108 - Periodic Testing of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Power Plants

(i) RG 1.118 - Periodic Testing of Electric power and Protection Systems

Regarding Position C-1 of Regulatory Guide 1.75, see Section 8.1.3.1.2.2 (6). Otherwise, the onsite AC power system is designed in accordance with recommendations of this guide, and with the other listed Regulatory Guides.

There are ~~four~~ three 6.9 KV electrical divisions, ~~three of~~ which are independent load groups backed by individual diesel-generator sets. The low voltage AC systems ~~of all~~ consist of four divisions which are backed by independent DC battery, charger and inverter systems.

435.023

The standby power system redundancy is based on the capability of any ~~two~~ one of the four divisions (~~two~~ one of three load groups) to provide the minimum safety functions necessary to shut down the unit from the control room in case of an accident and maintain it in the safe shutdown condition.

435.024

There is no sharing of standby power system components between load groups, and there is no sharing of diesel-generator power sources between units, since the ABWR is a single-plant design.

Each standby power supply for each of the three load groups is composed of a single generator driven by a diesel engine having fast-start characteristics and sized in accordance with Regulatory Guide 1.9.

Table 8.3-1 and 8.3-2 show the rating of each of the Division I, II and III diesel generators, respectively, and the maximum coincidental load for each.

(3) Branch Technical Positions (BTPs):

(a) BTP ICSB 8 (PSB) - Use of Diesel-Generator Sets for Peaking

(b) BTP ICSB 18 (PSB) - Application of the Single Failure Criterion to Manually-Controlled Electrically-Operated Valves.

(c) BTP ICSB 21 - Guidance for Application of Regulatory Guide 1.47

(d) BTP PSB 1 - Adequacy of Station Electric Distribution System Voltages

(e) BTP PSB 2 - Criteria for Alarms and Indications Associated with Diesel-Generator Unit Bypassed and Inoperable Status

formers, distribution panels, batteries, chargers) is tagged with an equipment number the same as indicated on the single-line diagrams.

(3) The nameplates are laminated black and white plastic, arranged to show black engraving on a white background for non-Class 1E equipment. For Class 1E equipment, the nameplates have color coded background with black engraving.

All cables for Class 1E systems and associated circuits (except those routed in conduits) are tagged every 25 ft. All cables are tagged at their terminations with a unique identifying number (cable number), in addition to the marking characteristics shown below.

All conduit is similarly tagged with a unique conduit number, in addition to the marking characteristics shown below, at 25 ft intervals, at discontinuities, at pull boxes, at points of entrance and exit of rooms and at origin and destination of equipment. Conduits containing cables operating at above 600V (i.e., 6.9kV) are also tagged to indicate the operating voltage.

All cable trays are marked with their proper raceway identification at 15 ft intervals on straight sections, at turning points and at points of entry and exit from enclosed areas.

To help distinguish the neutron-monitoring and scram solenoid cables from other type cables, the following unique voltage class designations are used in the cable routing program:

Type of Special Cables	Unique Voltage Class
Neutron-monitoring	VN
Scram solenoid cables	VS

Neutron-monitoring cables are run in their own divisional conduits and cable trays, separately from all other power, instrumentation and control cables. Scram solenoid cables are run in a separate conduit for each rod scram group.

In addition, the cables of the rod control and information system in the hydraulic control unit (HCU) are also placed in separate conduits and cable trays.

The redundant Class 1E, equipment and circuits, assigned to redundant Class 1E divisions and non-class 1E system equipment and circuits are readily distinguishable from each other without the necessity for consulting reference materials. This is accomplished by color coding of equipment, nameplates, cables and raceways, as described above.

8.3.1.3.2 Instrumentation and Control Systems

Major electrical and control equipment, assemblies, devices, and cables grouped into separate divisions per Table 8.3-1 shall be identified so that their electrical divisional assignment is apparent and so that an observer can visually differentiate between Class 1E (or 1E-associated) equipment and wiring of different divisions, and between Class 1E and non-Class 1E (or between 1E-associated and non-Class 1E) equipment and wires. The identification method shall be placed on color coding. All markers within a division shall have the same color. For associated cables treated as Class 1E, there shall be an A appended to the divisional designation (e.g., A1). The latter A stands for associated and ND for nondivisional. Associated cables are uniquely identified by a longitudinal stripe and/or the date on the label. The color of the cable marker for associated cables shall be the same as the related Class 1E cable. Divisional separation requirements of individual pieces of hardware are shown in the system elementary diagrams. Identification of raceways, cables, etc., shall be compatible with the identification of the Class 1E equipment with which it interfaces. Location of identification shall be such that points of change of circuit classification (at isolation devices, etc.) are readily identifiable.

8.3.1.3.2.1 Identification

(1) Panels and racks

Panels and racks associated with the nuclear safety-related systems shall be labeled with marker plates which are conspicuously different from those for other similar panels The difference may be in color, shape, or

color of engraving fill. The marker plates shall include identification of the proper division of the equipment included.

(2) Junction or pull boxes

Junction and/or pull boxes enclosing wiring for the nuclear safety-related systems shall have identification similar to and compatible with the panels and racks.

(3) Cables

Cables external to cabinets and/or panels for the safety-related systems shall be marked as indicated in Section 8.3.1.4 to distinguish them from other cables and identify their separate division as applicable. This identification requirement does not apply to individual conductors.

(4) Raceways

Those trays or conduits which carry nuclear safety-related system wiring shall be identified as indicated in section 8.3.1.4 at room entrance points through which they pass (and exit points unless the room is small enough to facilitate convenient following of cable) with a permanent marker identifying their assigned division.

(5) Sensory equipment grouping and designation letters

Redundant sensory logic/control and actuation equipment for safety-related systems shall be identified by suffix letters.

8.3.1.4 Independence of Redundant Systems

8.3.1.4.1 Power Systems

The Class 1E onsite electric power systems and major components of the separate power divisions is shown on Figure 8.3-1.

Independence of the electric equipment and raceway systems between the different divisions is maintained primarily by firewall-type separation where feasible and by spatial separation, in accordance with criteria given in Subsection 8.3.1.4.2, where firewalls are not feasible. Where spatial separation cannot be maintained in hazardous areas (e.g., potential missile areas), physical isolation between electrical equipment of different divisions is achieved by use of a 6-inch minimum thickness reinforced concrete barrier.

The physical independence of electric power systems complies with the requirements of IEEE Standards 279, 308, 379, 384, General Design Criteria 17, 18 and 21 and NRC Regulatory Guides 1.6 and 1.75.

8.3.1.4.1.1 Class 1E Electric Equipment Arrangement

(1) Class 1E electric equipment and wiring is segregated into separate divisions so that no single credible event is capable of disabling enough equipment to hinder reactor shutdown, removal of decay heat from the core, or isolation of the containment in the event of an accident. Separation requirements are applied to control power and motive power for all systems involved.

(2) Equipment arrangement and/or protective barriers are provided such that no locally generated force or missile can destroy any redundant RPS, NSSS, ECCS, or ESF functions. In addition, arrangement and/or separation barriers are provided to ensure that such disturbances do not affect both HPCF and RCIC systems.

(3) Routing of wiring/cabling is arranged such as to eliminate, insofar as practical, all potential for fire damage to cables and to separate the redundant divisions so that fire in one division will not propagate to another division.

(4) An independent raceway system is provided for each divisions of the Class 1E electric system. The raceways are arranged, physically, top to bottom, as follows (based on the function and the voltage class of the cables):

(a) V4 = Medium voltage power, 6.9kV (8kv insulation class).

435.035

435.035

35 Section 8.3.1.4.2.3.1 has been revised as follows:

"8.3.1.4.2.3.1 Reactor Protection (Trip) System (RPS)

The following separation requirements apply to the RPS wiring:

(1) RPS sensors, sensor input circuit wiring, trip channels and trip logic equipment will be arranged in four functionally independent and divisionally separate groups designated Divisions I, II, III and IV. The trip channel wiring associated with the sensor input signals for each of the four divisions provides inputs to divisional logic cabinets which are in the same divisional group as the sensors and trip channels and which are functionally independent and physically separated from the logic cabinets of the redundant divisions.

(2) Where trip channel data originating from sensors of one division are required for coincident trip logic circuits in other divisions, Class 1E isolation devices will be used as interface elements for signals sent from one division to another such as to maintain electrical isolation between divisions.

(3) Sensor wiring for several trip variables associated with the trip channels of one division may be run together in the same conduits or in the same raceways of that same and only division. Sensor wiring associated with one division will not be routed with, or in close proximity to, any wiring or cabling associated with a redundant division.

(4) The scram solenoid circuits, from the actuation devices to the solenoids of the scram pilot valves of the CRD hydraulic control units, will be run in grounded steel conduits, with no other wiring contained within the conduits, so that each scram group is protected against a hot short to any other wiring by a grounded enclosure. Short sections (less than one meter) of flexible metallic conduit will be permitted for making connections within panels and the connections to the solenoids.

(5) Separate grounded steel conduits will be provided for the scram solenoid wiring for each of four scram groups. Separate grounded steel conduits will also be provided for both the A solenoid wiring circuits and for the B solenoid wiring circuits of the same scram group.

(6) The scram group conduits will have unique identification and will be treated essentially as if they are separate enclosed raceways. The conduits containing the scram solenoid group circuit wiring will be physically separated by a minimum separation distance of one inch from either metal enclosed raceways or non-enclosed raceways which contain either divisional or "non-divisional" (non-safety-related) circuits.

(7) Any scram group conduit may be routed alongside of any cable or raceway containing either safety-related circuits (of any division), or any cable or raceway containing non-safety-related circuits, as long as the conduit itself is not within the boundary of any raceway which contains either the divisional or the non-safety-related circuits and is physically separated from

said cables and raceway boundaries by a minimum separation distance of one inch. Any one scram group conduit may also be routed along with scram group conduits of the same scram group or with conduits of any of the three other scram groups as long as the minimum separation distance of one inch (2.5 cm.) is maintained.

(8) The standby liquid control system redundant Class 1E controls will be run as Division I and Division II so that no failure of standby liquid control (SLC) function will result from a single electrical failure in a RPS circuit.

(9) The startup range monitoring (SRNM) subsystem cabling of the NMS and the rod control and information system (RC&IS) cabling under the vessel is treated as divisional. The SRNM cables will be assigned to Divisions I, II, III and IV, and the RC&IS cables to Divisions 1 and II. Under the vessel, cables will not be placed in any enclosure which will unduly restrict capability of removing probe connectors for maintenance purposes.