GE Nuclear Energy

General Electric Company
175 Curtner Avenue, San Jose, CA 95125

August 23, 1989

MFN No. 061-89

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 further responses to the subject Request for Additional Information (RAI) on the Standard Safety Analysis Report (SSAR) for the Advanced Boiling Water Reactor (ABWR). These responses pertain to Chapters 7 and 8.

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

Sincerely,

R. C. Mitchell

R. C. Mitchell, 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
420.005 (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:

System (and significant component) reliability goals, assumptions, methodology, model, analysis, and evaluation.

RESPONSE
420.005 No topical reports will be provided. However, the information is provided in the responses to other similar questions as follows:

Reliability goals - (See response to 420.063)
Model/Assumptions - (See response to 420.064)
Methodology - (See response to 420.065)
Test/Evaluation (See response to 420.067)

Additional information may be found in Appendix 7A and the design specifications and analysis documents referenced in Section 1.1.3.

QUESTION
420.006 (App 3I) 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:

Methodology, basis and acceptance criteria for qualifying the system and equipment to the design basis electromagnetic interference (EMI) environment.

RESPONSE
420.006 No topical reports will be provided. However, system tolerance to EMI is discussed in the following sections of Appendix 7A: 7A.2, Response (4); 7A.2, Response (15); 7A.3, Response (6); and 7A.3, Response (8). Additional detail is provided in the design documents referenced in Section 1.1.3.

QUESTION
420.008 (App 3I) 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:

Methodology, basis, and acceptance criteria for qualifying the system and equipment to the design basis thermal environment established by localized heat transfer within electronic equipment, including in non-accident environments; this should also address requirements for humidity controls to preclude damage from electrostatic discharge.

RESPONSE

420.008 The environmental qualification methodology and requirements for systems and equipment are described in Section 3.11 and in the design documents referenced in Section 1.1.3 (in particular, Environmental Quality Requirements for Safety Grade Equipment, BWR Requirements - Equipment Environmental Interface Data and Safety System Logic & Control Design Specification). No additional topical reports will be provided.

The panel internal environment is maintained to ensure that reliability goals are achieved. Thermal margins are such that panel internal cooling by natural convection is sufficient. Fans may be used to improve long term reliability, but no credit is taken for forced-air cooling in the qualification of safety-related functions.

Even heat load distribution is a design goal. Thermal design adequacy will be demonstrated by analysis of heat loads (per circuit module, per bay, per panel) as required by the design specifications. Thermal design will allow for addition of 15 percent more processing modules for future expansion. (See also the response to Question 420.092.)

Voltage potential buildup leading to damage from electrostatic discharge shall be limited by proper grounding of equipment and use of appropriated static control materials and dielectric barriers to ensure that high potentials cannot be coupled to sensitive semiconductor devices. Humidity controls are provided by the normal and emergency HVAC systems; when relative humidity is restricted to the ranges specified for the mild environment locations where the microprocessor equipment will be installed, there will be no unusual static charge buildup.

QUESTION

420.018 (7) For the proposed use of digital computers, show how the digital system is superior to analog alternatives to implementing the logic. Show how the analyses determined that the realiability of the digital computer based system was better than the reliability of the analog system.

RESPONSE

420.018 The analysis showing the superiority of the digital system compared with the analog system is given in the response to Question 420.017.

With regard to reliability, the SSLC facilitates a full "any-2-out-of-4" digital logic for both RPS and ESF systems, which is inherently more reliable than (1/2)X2 logic typically used in the previous analog designs. Distributed microprocessors are used to perform simple logic decisions in much the same way relays were used in earlier designs. The SSLC is not dependent on a centrally located digital computer.

QUESTION
420.030 (7.1.2.2) Define the word "sufficient" used in section (j).

RESPONSE
420.030 With regard to the Reactor Protection (Trip) System (RPS), the statement "...sufficient electrical and physical separation between redundant ..equipment" means that the system design bases is such that a single event caused by the environment, an electrical transient, or physical event such as a missile, will not disable more than one division of the RPS. In reality, the ABWR RPS 2/4 voting logic could permit a loss of two divisions and still function correctly to scram the reactor.

The following description of the ABWR reactor building design illustrates the electrical and physical separation methods used to accomplish this design basis objective.

Each floor of the ABWR reactor building is sectioned with fire walls dividing the redundant mechanical divisions. The placement of electrical equipment, in general, corresponds to the mechanically separated division assigned to each section (i.e., mechanical divisions A1,B,C and A4 correspond with electrical divisions I,II,III and IV, respectively). Some exceptions are necessary where a given area requires more than one electrical division for sensors or other equipment. (For example, redundant leak detection system sensors may be required to be placed within the same partitioned area.) However, electrical separation is maintained between the redundant divisions.

Because of this partitioned design, it is highly unlikely a single event would affect more than one of the partitioned areas, and thus affect more than one of the redundant RPS divisions. Furthermore, it is not considered credible that a single event could effect more than two such partitioned areas in a manner that could disable more than two divisions of RPS.

QUESTION
420.050 (7.1) Describe the self-diagnostic features of the computer-based safety system. Describe the diagnostics that are run on-line, in a background mode and in a maintenance mode. Describe what happens when an on-line diagnostic uncovers an error in the computer system.

RESPONSE
420.050 The self-test subsystem (STS) is described as the "sixth test" in Section 7.1.2.1.6. Additional information is provided in Appendix 7A, Section 7A.2, Responses (6) and (14).

QUESTION
420.051 (7.1) Describe the data buses that are used in the multiplexers. Describe the features that are implemented to ensure that the bus or multiplexer is not cause of a single point failure. Describe what happens when a single card on a data bus fails. Show what design features prevent the error from propagating and not challenging the remainder of the safety system. If specific equipment has not been selected, please pro[illegible]he interface criteria.

RESPONSE

420.051 The data buses that are used in the multiplexers are of two types: (1) The fiber optic links between multiplexers, and (2) the data pathways from the multiplexer bus interface units to their associated input/output system or application processor for a remote multiplexer data station or control room multiplexer data station, respectively. For clarity, the bus interface unit is frequently referred to as the "node" of a data station of a control data network, while the input/output system or application processor is referred to as the "host" of the data station. The data buses therefore consist of (1) the network links between nodes, and (2) the links between nodes and their respective hosts.

As described in the response to question 420.020, divisional redundancy and electrical separation and independence design criteria prevent random failures of a control data network in one division from interfering with the proper operation and execution of multiplexers in another division. This provides the means to satisfy single failure criteria required by regulations for safety, and further failure contingencies are provided only for improvements in equipment reliability and availability.

These latter improvements are provided in each division through selected redundancy and system reconfiguration capability. Redundancy is provided for both the fiber optic links between multiplexers and the multiplexer bus interface units each division. Two control data networks, each with their own fiber optic links and bus interface units, therefore, are provided for transmission of intradivisional signals.

Redundancy is not required, however, for the links between the redundant bus interface units (nodes) and their associated input/output system or application processor (host). This is because the input/output system or application processor itself is not generally redundant (within a given division of instrumentation and control), and because of its higher parts count, has a lower reliability than the data bus connecting it to the bus interface units. The data bus is left to be specified during the detailed design of the procured equipment, and may be either redundant serial links or a shared parallel bus, as examples.

Because the data bus connecting the redundant multiplexer bus interface units to the input/output system or application processor is not necessarily redundant, there is potential, though of relatively small probability, for the failure of a card interfacing with this data bus to cause the loss of the entire data station. System reconfiguration is provided, however, independently within both of the redundant control data networks to drop out the failed station. The control data networks continue to operate with all data stations except the failed one.

Failure of a card must therefore propagate through the data bus between the input/output system or application processor

to the bus interface unit(s) to fail the entire data station, including functions of both the redundant nodes and their associated host. Furthermore, control data network reconfiguration must fail in order for the card failure to propagate to the entire intradivision multiplexing network. This is the most severe, but unlikely outcome of the initiating random card failure. In any event, however, it is not possible for the failure to propagate to another safety division, and capability to perform safety related functions is unaffected despite the single error.

The interface requirements, therefore, are those features described above; that is, redundancy of fiber optic links between multiplexers; redundancy of bus interface units with associated provision for each to communicate to and from the process input/output system or application processor; and capability for control network reconfiguration to drop out a failed bus interface unit (or data station). These requirements apply to each division separately. Furthermore, there are requirements for electrical independence and separation, as well as for autonomous and asynchronous control, of the multiplexing systems in the different divisions, as discussed in response to question 420.020.

QUESTION

420.052 (10/87) As indicated in the October 1987 ABWR presentation, the self-test sequence of the digital processor equipment is supposed to reduce the need for surveillance and monitoring by human personnel. Describe how it was proven that the old and new surveillance schedules are functionally equivalent.

RESPONSE

420.052 As indicated in the response to 420.072, the self-test system sends a signal to the annunciator and the process computer upon detection of failures within the hardware or software. Thus, the need for surveillance and monitoring by human personnel is reduced, in some areas within the Technical Specifications, compared with that required for systems not employing self-test.

The suggested surveillance intervals for the ABWR are based on studies with operating plants and the BWR Owner's Group. Where there are differences with respect to the "old" surveillance schedules, these are identified and justified in Chapter 16 in the bases to the Technical Specifications.

QUESTION

420.054 (7) Does the FMEA consider unusual failure modes and their effects such as system stall, interruption and restoration of power (or function), metastability, or timing errors? Provide a descriptive summary of the failure modes addressed in the FMEA or describe the interface criteria.

RESPONSE

420.054 This response addresses the FMEA for the Essential Multiplexing System (EMS) (see Section 15B.4).

The only two failure modes that need be considered for the EMS are 1) corruption of the signal due to failure of EMS equipment, and 2) loss of signal due to failure of EMS equipment (or power). Such failures could also occur due to severed fiber optic cable and/or misalignment of junctions. These failure modes are analyzed in Section 15B.4.

Graceful degradation is a design feature of I&C microprocessor equipment that causes safe-state output responses to unusual failure modes such as system stall, interruption and restoration of power (or function), metastability and timing errors. This feature is implemented in both hardware and software. Thus, unusual failure modes can be considered to be part of the hypothesized failure modes analyzed in the FMEA.

Watchdog timers detect system stall or timing errors and cause an INOP output for the failed channel. The same type of trip occurs on loss of power to any given channel. When the effects of these trips are propagated to the Safety System Logic & Control equipment, channel input trips will occur. These trips (fail-safe for RPS and fail-as-is for ECCS) force a "half-trip" condition of the 2-out-of-4 coincidence logic for the given channel and simultaneously alert the operator via the annunciators and process computer. The operator may then opt to bypass the failed channel, which causes the logic to revert to 2-out-of-3. Only one channel may be bypassed at any given time.

The power-on logic ensures known and acceptable initial conditions after restoring instrument or system power or inserting a card with power on. On interruption of power and restart, the microprocessor-controlled logic resets to the start of the control program. Time delays are not activated upon application of power Outputs depend only upon sensed inputs. If downstream processors receive erroneous inputs (based on self-checking within each instrument), then the INOP trip described above will be generated by those processors.

QUESTION

420.055 (7) Provide a summary of any graceful degradation features provided in the I&C systems or describe the interface criteria.

RESPONSE

420.055 Test facilities in the control room monitor data transmission of the essential multiplex system (EMS) to ensure that data transport, routing and timing specifications that are out-of-tolerance for a particular input signal will result in an INOP trip condition for that input into the trip logic processors of SSLC. The SSLC will cause protective function activation upon receipt of inoperative signals caused by hardware or software failure of system instruments. The SSLC Self-diagnostics alsocauses protective function activation when software or hardware failures are detected.

Upon loss of AC or DC power, functions which are normally energized, such as reactor trip and main steam line isolation, will provide fail-safe trip action. For such functions, loss of power to a sensor, its channel, or associated logic automatically produces a trip output. For normally de-energized functions, such as emergency core cooling, the

same failures will leave the state of the actuated equipment unchanged. The system is also designed such that subsequent restoration of power does not introduce transients that could cause a change of state in the actuated equipment.

Additional information is available in Appendix 7A, and in the Safety System Logic and Control System Design Specification (Section 1.1.3).

QUESTION
420.056 (7) Demonstrate that the effects of hardware and external failures on software performance have been sufficiently addressed in the FMEA or describe the interface criteria.

RESPONSE
420.056 The answer to this question is included in the response to Question 420.054. In particular, a component failure (integrated circuit or passive part) will result in loss or corruption of data as described in the FMEA. Whether the erroneous data results from associated software failure or damage to the signal path, the effect on downstream processors is the same. External failures are also sensed as erroneous data and will be treated as described previously.

QUESTION
420.059 (7) Describe the methods which are used to assure that equipment which is not qualified for all service conditions will not spuriously operate during exposure to conditions for which the equipment is not required to function to mitigate the effects of accidents or other events.

RESPONSE
420.059 The non-safety feedwater, recirculation flow and turbine control systems utilize triplicated control channels with middle-value voting. This means that a spurious signal from one of the channels, which differs from the other two channel outputs, will be disregarded by the controller.

The Class-1E safety systems are entirely separated from the non-1E control systems such that spurious initiation of non-safety systems has no adverse impact on safety functions.

QUESTION
420.060 (7.1.2.2) Provide examples for section (g) which meet the design bases.

RESPONSE
420.060 The origin for this design basis is Section 4.7.3 of IEEE 279. However, the statement in (g) was less conservative as originally written because it did not mention the degredation of a second random failure. Therefore, (g) has been rewritten to agree with IEEE 279 more precisely (see attached mark-up).

The ABWR reactor protection (trip) system is designed with 2/4 voting logic, and is electrically isolated and physically separated from the plant control systems [see Section 7.2.2.2.3.1(7)]. In addition, the feedwater, recirc flow, and turbine control systems utilize fault tolerant (middle value voting) triplicated instrument channels in their

control schemes (see Section 7.7). As such, there are no single random failure scenerios which could cause a control system action that causes a plant condition that requires a reactor scram, but also prevents action by some RPS channels. (See Section 7.1.2.10.11 relative to instrument lines.)

The system has also been designed to protect against multiple failures resulting from a credible single event (Section 4.7.4 of IEEE 279). This scenerio is discussed in Section 7.2.2.2.3.1(7).

QUESTION
420.064 (7) Describe the reliability model and assumptions used to demonstrate achievement of the reliability goals; this should include a description of the system architecture.

RESPONSE
420.064 The reliability model and assumptions used to demonstrate achievement of the reliability goals are based on the principles and guidelines of IEEE 352.

The system architecture is described in Appendix 7A, Section 7A.2, Responses (10) and (11).

QUESTION
420.075 (7.1.2.2) For section 7.1.2.2(j) clarify that the physical and electrical separation does not preclude the proper environmental qualification of redundant I&C equipment.

RESPONSE
420.075 All I&C equipment associated with the reactor protection system scram function, and all other safety-related functions, is qualified both seismically and environmentally (Sections 3.10 and 3.11), to Class-1E standards. The qualification requirements of such equipment are independent of the separation requirements imposed on the redundant channels of the systems which utilize the equipment.

QUESTION
420.078 (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 limits 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.

Will this precedure be a topical report used as a design tool?

RESPONSE

420.078 The ABWR utilizes the design specifications, integration procedures, implementation procedures and analysis reports as bases for the design, rather than topical reports. These documents are referenced in Section 1.1.3.

QUESTION

420.079 (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 limits 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.

What experimental data has been used to provide inputs to this design approach?

RESPONSE

420.079 The term "experimental data" is misleading in this context, and has been changed to "historical data" as marked in attachment.

Section 4.4 of NEDC-31336 "General Electric Instrument Setpoint Methodology" discusses historical data accumulated from three operating plants amounting to approximately 9 reactor-years of experience. The plants involved were Peach Bottom, Grand Gulf and Nine Mile Point 1. These plants utilize transmitters similar to those of ABWR. However, the data associated with analog trip devices of earlier plant designs is very conservative compared with the ABWR. This is because setpoint drift is non-existent in the Digital Trip Modules (see response to 420.077). The MUX system introduces a slightly lower accuracy than the hard-wired designs, but the overall uncertainties in the margins are significantly improved.

The details for setpoint methodology specific for the ABWR may be found in the "Instrument Setpoints Design Requirements" document identified in the reference in Section 1.1.3.

QUESTION

420.084 (App 3I) What EMI coupling protection is to be provided for the I&C systems and how will its effectiveness for specific installed conditions be verified? (Examples of standards such as FCC docket 20780, Part 15, Subpart J, "Class A Computing Devices" have been identified by industry for computing devices as a source limitation for radiated and conducted noise. Also ANSI C63.12-1984 "Recommended Practice on procedures for Control of System Electromagnetic Capability," is available as a design guidance tool.) Address these effects, possible limitations, and the criteria and standards to be used by GE in the ABWR design for safety systems equipment.

RESPONSE
420.084 System tolerance to EMI, and associated testing, is discussed in the following sections of Appendix 7A: 7A.2, Response (4); 7A.2, Response (15); 7A.3, Response (6); and 7A.3, Response (8).

Units shall undergo standard surge withstand capability tests as defined in IEEE 472. The fiber-optic equipment will undergo EMI and surge testing to the standards identified in NUREG/CR-3453/EGG-2444.

Additional detail is provided in the design documents referenced in Section 1.1.3.

QUESTION
420.086 (7) If hardwired meters are used explain how the adjacent electronics in the control panels are protected from EMI and fault propagation from faulted current transformers.

RESPONSE
420.086 Hardwired analog-type meters and current transformers are not used near sensitive electronics, either on the operator benchboard or back row panels. If hardwired meters are used for backup of a few critical functions, then they will be installed on a separate backup panel. Current transformers and hardwired meters will form instrument loops physically and electrically independent from the multiplexed, microprocessor-based data acquisition and control systems. As discussed in other responses, general EMI protection is provided by fiber-optic data transmission and proper grounding.

QUESTION
420.089 (7) List the design goals for the survivability and continued operation of safety systems equipment in the presence of line switching transients, lightning induced surges and other induced transients within the systems as installed.

RESPONSE
420.089 Surge withstand capability, and associated testing criteria, is discussed in Sections 7A.2 [Response (4)] and 7A.3 [Response (8)] of Appendix 7A.

QUESTION
420.090 (7) Address the possible effects of electrostatic discharge (ESD) at keyboards, keyed switches and other exposed equipment components.

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

However, modern CMOS and other MOS components have internal protection

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

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

QUESTION

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

RESPONSE

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

Voltage potential buildup will be limited by proper grounding of equipment and use of appropriate static control materials and dielectric barriers to ensure that high potentials cannot be coupled to sensitive semiconductor devices (see the response to Question 420.090). Humidity controls are provided by the normal and emergency HVAC systems; when relative humdity is restricted to the ranges specified for the mild environment locations where the microprocessor equipment will be installed, there will be no unusual static charge buildup.

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

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

following minimum capabilities:

Output Voltage - 2 kV to 16.5 kV
Polarity - positive
Energy Storage Capacitor - 150 pF plus or minus 10%
Discharge Resistor - 150 ohms plus or minus 5%
Charging Resistor - 100 Megohms plus or minus 10%
Rise time of discharge current - 5 ns plus or minus 30% at 4 KV
Operating Modes - (1) up to 20 discharges per second for approximately 5 seconds per test; (2) also single pulses with at least 1 sec between succesive discharges.

Acceptance criterion shall be no misoperation during or after test.

QUESTION
420.093 (7) The application of high technology semiconductor materials and related technologies to computing devices has resulted in high current densities in some portions of equipment used in non-nuclear applications. This type of equipment may be used for the ABWR.

Does an analysis of these potential hot spots result in special thermal design constraints?

RESPONSE
420.093 The answer to this question is included in the reponse to Question 420.092.

QUESTION
420.095 (7) The application of high technology semiconductor materials and related technologies to computing devices has resulted in high current densities in some portions of equipment used in non-nuclear applications. This type of equipment may be used for the ABWR.

Since the plant environmental limitations only identify general area temperature ranges, what consideration will be given to localized cooling and heat transfer?

RESPONSE
420.095 The answer to this question is included in the response to Question 420.092.

QUESTION

435.004 (a) In section 8.2.3 of the ABWR SSAR one of the Nuclear Island interfaces identified is four 6.9 kV feeders to four transformers powering ten RIP pumps. However figure 8.3-1 and figure 8.3-2 show motor generator sets between two of the 6.9 kV feeders and the RIP pumps. Please clarify whether the motor generator sets will be used in the ABWR design and if so, describe their function.

(b) Also, with regard to the same subject, section 15.3.1.1.1 states that since four buses are used to supply power to the RIPS, the worst single failure can only cause three RIPs to trip, and the frequency of occurrence of this event is estimated to be less than 0.001 per year. Further down in this same section a statement is made that the probability of additional RIP trips is low (less than .000001 per year). Justify these figures in light of the fact that historically, a total loss of offsite power occurs about once per 10 site-years (NUREG/CR-3992). Also, has the effect of a fault on the common feeder upstream of the 6.9 kV feeders been considered with respect to the coastdown capability of the RIPS and motor generator sets (braking effect)?

RESPONSE

435.004 (a) Motor generator sets are used in the ABWR design. Their primary function is to provide additional mechanical inertia to extend the coastdown time of the connected RIPs during a bus failure transient. With the adoption of motor-generator set design, the probability of having an all RIPs trip is virtually eliminated.

(b) A RIP reliability analysis will be submitted as Appendix 15.C to Chapter 15 of the SSAR. This analysis estimates the probability that exactly 1, 2, ... 10 out of ten RIPs will trip. The results are shown in the following:

# OF PUMPS TRIPPED	PROBABILITY
1	5.57E-3
2	1.07E-4
3	1.64E-3
4	6.44E-6
5	4.36E-5
6	6.37E-7
7	1.41E-7
8	<<1.00E-6
9	<<1.00E-6
10	<<1.00E-6

This analysis includes the effect of a fault on the common feeder upstream of the 6.9 kV feeders. However, the effect of a total loss of offsite power is not included. This is because the reactor system response to a total loss of offsite power is more than a trip of RIPs. For example, a load rejection followed by a reactor scram will be initiated after a loss of offsite power. The complete discussion of the loss of offsite power event is contained in Subsection 15.2.6. A new analysis for Subsection 15.2.6 will be submitted to include the affect of M/G sets.

QUESTION

435.043 Section 8.3.2.1.3.3 states that battery rooms are ventilated to remove the minor amounts of gas produced during the charging of batteries. Verify that, in accordance with position C.1 of R.G. 1.128 the ventilation system will limit hydrogen concentration to less than two percent by volume at any location within the battery area.

Also, in accordance with position C.6.e of R.G. 1.128, verify that ventilation air flow sensors are installed in the battery rooms with their associated alarms installed in the control room.

RESPONSE

435.043 The ventilation system for the battery room will maintain the concentration of hydrogen to less than 2% as a design requirement. The airflow sensors are described in Section 9.4.1.2, which has been revised (per attached) to reflect the 2% limit on hydrogen concentration.

To minimize common mode effects, automatic self-test is performed sequentially on all four division; i.e., one division's test unit will test and monitor logic circuit integrity and circuit continuity in its division and also verify data communication links with the other three divisions. After completion, test control automatically transfers to the next division, and so on until all four divisions have completed testing. A complete self-test sequence through all four divisions takes thirty minutes or less.

(5) Off-line, manual system testing is provided for surveillance and maintenance testing in bypassed channels.

A separate SSLC test unit in the control room is assigned to initiate and evaluate automatic and manual test functions in each division. This achieves the least interference with normal SSLC operation and permits system and interdivisional testing to continue in the presence of failed SSLC protection system logic processing circuitry.

A separate SSLC bypass unit controls manual initiation of division out-of-service bypasses and receives data from other divisions concerning bypass status (only one division shall be bypassed at any given time).

The control room test unit is capable of calibrating all RMU input channels at the sensor inputs in an off-line mode.

7.1.2.2 Reactor Protection (Trip) System (RPS)-Instrumentation and Control

(1) Safety Design Bases (Conformance to the following design bases is discussed in Section 7.2.2.1).

The reactor protection (trip) system (RPS) shall meet the following functional requirements:

(a) to initiate a reactor scram with precision and reliability to prevent or limit fuel damage following abnormal operational transients;

(b) to initiate a scram with precision and reliability to prevent damage to the reactor coolant pressure boundary as a result of excessive internal pressure (i.e., to prevent nuclear system pressure from exceeding the limit allowed by applicable industry codes);

(c) to limit the uncontrolled release of radioactive materials from the fuel assembly or reactor coolant pressure boundary, by precisely and reliably initiating a reactor scram on gross failure of either of these barriers;

(d) to detect conditions that threaten the fuel assembly or reactor coolant pressure boundary from inputs derived from variables that are true, direct measures of operational conditions;

(e) to respond correctly to the sensed variables over the expected range of magnitudes and rates of change;

(f) to provide a sufficient number of sensors for monitoring essential variables that have spatial dependence;

The following bases assure that the RPS is designed with sufficient reliability:

(g) If a single random failure can cause a control ~~failure of a control or regulating~~ action that system causes a plant condition that requires a reactor scram but also prevents action by some RPS channels, the remaining portions of the RPS shall meet the functional requirements (items a, b and c above), even when degraded by a second random failure. 420.060

(h) Loss of one power supply shall neither directly cause nor prevent a reactor scram.

(i) Once initiated, an RPS action shall go to completion. Return to normal operation shall require deliberate operator action.

(j) There shall be sufficient electrical and physical separation between redundant instrumentation and control equipment monitoring the same variable to prevent environmental factors, electrical tran-

which have been determined to be sufficient to ensure the adequacy and reliability of the system from a safety viewpoint. Many of these requirements have been incorporated into various codes, criteria, and regulatory requirements.

7.1.2.1.1 Safety Design Bases for Safety Systems

Safety systems provide actions necessary to assure safe plant shutdown to protect the integrity of radioactive material barriers and/or prevent the release of radioactive material in excess of allowable dose limits. These safety systems consist of components, groups of components, systems, or groups of systems. A safety system may have a power generation design basis which states in functional terms the unique design requirements which establish the limits within which the power generation objective for the system shall be set.

7.1.2.1.2 Specific Regulatory Requirements

The plant systems have been examined with respect to specific regulatory requirements and industry standards which are applicable to the instrumentation and controls for the various systems. Applicable requirements include specific parts or entities from the following:

(1) Title 10 Code of Federal Regulations;

(2) Industry codes and standards; and

(3) NRC Regulatory Guides.

The specific regulatory requirements identified in the Standard Review Plan which are applicable to each system instrumentation and control are specified in Table 7.1-2. For a discussion of the degree of conformance see the analysis subsection for the specific system.

7.1.2.1.3 Nonsafety Design Bases

Nonsafety-related (including power-generation) systems are reactor support systems which are not required to protect the integrity of radioactive material barriers nor prevent the release of radioactive material in excess of allowable dose limits. The instrumentation and control portions of these system may, by their actions, prevent the plant from exceeding preset limits which would otherwise initiate action of the safety systems.

7.1.2.1.4 Instrument Errors

The design considers instrument drift, testability, and repeatability in the selection of instrumentation and controls and in the determination of setpoints. Adequate margin between safety limits and instrument setpoints is provided to allow for instrument error. The safety limits, setpoints, and margins are provided in Chapter 16. The amount of instrument error is determined by test and experience. The setpoint is selected based on the known error. The recommended test frequency is greater on instrumentation that demonstrates a stronger tendency to drift.

7.1.2.1.4.1 Safety System Setpoints

The safety system setpoints are listed in the Chapter 16 for each safety system. The settings are determined based on operating experience and conservative analyses. The settings are high enough to preclude inadvertent initiation of the safety action but low enough to assure that significant margin is maintained between the actual setting and the limiting safety system settings. Instrument drift, setting error, and repeatability are considered in the setpoint determination (Subsection 7.1.2.1.4). The margin between the limiting safety system settings and the actual safety limits include consideration of the maximum credible transient in the process being measured.

The periodic test frequency for each variable is determined from ~~experimental~~ historical data on setpoint drift and from quantitative reliability requirements for each system and its components.

420.079

7.1.2.1.5 Technical Design Bases

The technical design bases for RPS are in Section 7.2, engineered safety features are in Section 7.3, systems required for safe shutdown are in Section 7.4, and other systems required for safety are in Section 7.6.

Recirculation unit for subsystem 1 consists of a prefilter section, a high efficient filter section, an electric heater, a cooling coil, and two 50% capacity supply fans. The supply fans are placed on low-speed when the fans are in the smoke removal mode.

Two 50% capacity return exhaust fans draw air from safety related battery rooms. During smoke removal mode, the fans are placed on low-speed and the air is discharged to atmosphere.

9.4.1.2.3.2 Safety-Related Subsystem 2

Subsystem 2 specifically serves:

(1) Safety-related battery room 2,

(2) Essential chiller room B,

(3) RB cooling water pump and heat-exchanger room B,

(4) HVAC equipment room,

(5) Safety-related electrical equipment room,

(6) Passages,

(7) Non-essential electrical equipment rooms.

Recirculation unit for subsystem 2 consist of a prefilter section, a high efficient filter section, an electric heater, a cooling coil, and two 50% capacity supply fans. The supply fans are placed on low-speed when the fans are in the smoke removal mode.

Two 50% capacity return exhaust fans draw air from the safety-related battery rooms. During smoke removal mode, the fans are placed on low-speed and the air is discharged to atmosphere.

9.4.1.2.3.3 Safety-Related Subsystem 3

Subsystem 3 specifically serves:

(1) Safety-related battery room 3,

(2) Essential chiller room C,

(3) RB cooling water pump and heat-exchanger room C,

(4) HVAC equipment room,

(5) Safety-related electrical equipment room,

(6) Passages,

(7) MGTS equipment at EL. 7200 in CB.

Recirculation unit for subsystems 3 consist of a prefilter section, a high efficient filter section, an electric heater, a cooling coil, and two 50% capacity supply fans. The supply fans are placed on low-speed when the fans are in the smoke removal mode.

Two 50% capacity return exhaust fans draw air from the safety-related battery rooms. During smoke removal mode, the fans are placed on low-speed and the air is discharged to atmosphere.

9.4.1.2.4 Safety Evaluation

The essential electrical HVAC system is designed to ensure the operability of the essential electrical equipment. All safety-related HVAC equipment and surrounding structures are of seismic category I design and operable during loss of the offsite power supply.

The ductwork which services these safety functions is termed ESF ductwork, and is of Seismic Category I design. ESF ducting is high pressure safety grade ductwork designed to withstand the maximum positive and/or negative pressure to which it can be subjected under normal or abnormal conditions. Galvanized steel ASTM A526 or ASTM A527 is used for outdoor air intake and exhaust ducts. All other ducts are welded black steel ASTM A570, Grade A or Grade D. Ductwork and hangers are Seismic Category I. Bolted Flange and welded joints are qualified per ERDA 76-21.

Redundant components are provided where necessary to ensure that a single failure will not preclude adequate heat-exchanger building ventilation.

9.4.1.2.5 Inspection and Testing Requirements

Provisions are made for periodic tests of the outdoor air cleanup fans and filters. These tests include determinations of differential pressure across the filter and of filter efficiency. Connections for testing, such as injection, sampling and monitoring are prop-

concentration and to limit the hydrogen to less than 2% by volume in the battery rooms.

435.043