



General Electric Company  
175 Curtner Avenue, San Jose, CA 95126

March 31, 1994

MFN No. 040-94  
Docket STN 52-004

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

Attention: Richard W. Borchardt, Director  
Standardization Project Directorate

Subject: NRC Requests for Additional Information (RAIs) on the Simplified Boiling  
Water Reactor (SBWR) Design

- References:
1. Transmittal of Requests for Additional Information (RAIs) for the SBWR Design, Letter from M. Malloy to P. W. Marriott dated January 5, 1994
  2. MFN No. 004-94, NRC Requests for Additional Information (RAIs) on the Simplified Boiling Water Reactor (SBWR) Design Letter from J. E. Leatherman to R. W. Borchardt, dated January 17, 1994
  3. Transmittal of Requests for Additional Information (RAIs) Regarding the SBWR Design, Letter from M. Malloy to P. W. Marriott dated March 8, 1994

The Reference 1 letter requested additional information regarding the SBWR I & C design. In partial fulfillment of this request and in accordance with the Reference 2 schedule, GE is submitting Attachment 1 to this letter which contains responses to the following RAIs:

420.4 - .5	420.41 - .64
420.7 - .8	420.66
420.12	420.71
420.14 - .16	420.73 - .74
420.18 - .22	420.85 - .86
420.24 - .33	420.90
420.35 - .37	


The Reference 3 letter requested SBWR core neutronics data on a short-turnaround basis of March 15, 1994 to permit Brookhaven National Laboratory (BNL) to modify the RAMONA - 4B code for the staff's use. In partial fulfillment of this request and with NRC approval, GE has participated in frequent telephone dialog with BNL and submitted draft responses to these RAIs prior to the deadline, and requested NRC teleconferences to receive comments before final transmittal of these responses. Since Ramona - 4B and TRACG are somewhat different in their modeling, and GE does not use RAMONA-B,

9404060124 940331  
PDR ADOCK 05200004  
A PDR

2040  
11

we need to complete this telephone comment cycle with NRC to permit the BNL modeling activity to go forward. Please contact Mr. David Foreman at (408) 925-4722 to arrange for closure of the RAMONA-B dialog.

Sincerely,



J. E. Leatherman, Manager  
SBWR Design Certification  
MC-781, (408)925-2023

Attachment 1, "Responses to NRC RAIs"

cc: M. Malloy, Project Manager (NRC) w/2 copies of Attachment 1)  
F. W. Hasselberg, Project Manager (NRC) (w/1 copy of Attachment 1)

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.4**

Provide a list of all actuation devices of the reactor protection system and engineered safety features actuation system that cannot be fully tested during reactor operation. How will these devices be periodically tested to ensure that they are capable of performing their safety functions, in compliance with the guidance of Regulatory Guide (RG) 1.22?

**GE Response:**

Reactor Protection System (RPS)

There are no safety related RPS actuation devices that cannot be tested during reactor operation. Only the backup scram solenoids, which are non-safety related, are not tested during reactor operation, since their energization necessitates a full scram.

Engineered Safety Features Systems

Automatic Depressurization Subsystem (ADS) - has squib valve booster assemblies for depressurization valves (DPV) B21-F004A, B, C, D and B21-F005A and B which are periodically tested during refueling outages. Gravity-Driven Cooling System (GDCS) has squid booster assemblies for valves E50-F002A, B, C, D, E, F; E50-F006A, B, C and E50-F009A through I which are periodically tested during refueling outages.

Passive Containment Cooling System - has no actuation devices that cannot be tested during reactor operation.

Leak Detection and Isolation System - has no actuation devices that cannot be tested during reactor operation.

Safety System Logic and Control - has no actuation devices that cannot be tested during reactor operation.

Essential Multiplexing System - has no actuation devices that cannot be tested during reactor operation.

Flammability Control System - is being changed to a passive system and has no actuation devices that cannot be tested during reactor operation.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.4 (continued)

The following updated SSAR Subsections and figures are attached:

- 1.2.2.14.1
- 1.2.2.14.7
- 1A.2.13
- 3.1.4.12
- 6.2.5
- 7.3.6.3
- 7.3.6.5
- 7.3.8
- 9A Tables 9A.7-1a and 9A.7-1b
- Chapter 16, Items 3.6 and B3.6
- 19G.2.12
- Figure 6.2-23
- Figures 6.2-24, 6.2-25, 21.7.3-7 and 21.7.3-8 are voided

Thus within the RPS and ESF systems only the squib valves explosive charges for the ADS and GDCS are not fully tested during reactor operation.

However, during reactor operation periodic continuity checks are performed on the explosion initiator electrical circuits of squib valves via SSLC self-test logic. In addition, during each refueling outage, random samples of explosive charges of the squib valves are tested in a laboratory environment. Explosive charges of the squib valves are also replaced with new ones, based on their established qualified life. This type of testing is in accordance with and meets RG 1.22, Regulatory Position D.4

The design value for a maximum steam bypass leakage between the drywell and the suppression chamber through the diaphragm floor including any leakage through the suppression chamber-to-drywell vacuum breakers is limited. Satisfying this limit is confirmed by initial preoperational tests as well as by periodic tests conducted during refueling outages. These tests are conducted at differential pressure conditions between the drywell and suppression chamber that do not clear the drywell-to-suppression chamber horizontal vents.

Equipment is provided to obtain a water tight barrier between the open reactor and the drywell during refueling. This enables the reactor well to be flooded prior to removal of the reactor steam separator, dryer assembly and to facilitate underwater fuel handling operations. Piping, cooling air ducts and return air vent openings in the reactor well platform must be removed, vents closed and sealed watertight before filling the reactor well with water. The refueling bellows assembly is provided to accommodate the movement of the vessel caused by operating temperature variations and seismic activity.

Containment isolation is accomplished with inboard and outboard isolation valves on each piping penetration which are signaled to close on predefined plant parameters. Systems performing a post LOCA function are capable of having their isolation valves reopened as needed.

Drywell coolers are provided to remove heat released into the drywell atmosphere during normal reactor operations.

The Flammability Control System provides recombiners ~~igniters~~ located throughout both the drywell and suppression chamber to prevent any high-energy-release recombinant reactions potentially developing within the containment following a LOCA.

#### 1.2.2.14.2 Containment Vessel

The containment vessel is a reinforced stepped cylindrical concrete vessel (RCCV). The RCCV supports the upper pools whose walls are integrated into the top slab of the containment to provide structural capability for LOCA and testing pressures.

#### 1.2.2.14.3 Containment Internal Structures

The containment system's principal internal structure consists of the structural barrier separating the drywell from the suppression chamber. This barrier is comprised of the suppression chamber ceiling (diaphragm floor) and the inboard wall (vertical vent wall) separating the drywell from the suppression chamber. Both of these structural components are designed as steel structures filled with insulating concrete to minimize long-term heat transfer from drywell to wetwell. The vertical vent wall also provides a durable attachment point for the RPV horizontal stabilizers.

consequent temperature rise in the discharge stream or loss of flow actuates an alarm in the MCR.

Each upper drywell FCU has a cooling capacity of 50% of the upper drywell design cooling load under normal plant operating conditions. Likewise, each lower drywell FCU has a cooling capacity of 50% of the lower drywell design cooling load. All FCUs normally operate. Each FCU is composed of a cooling coil and two fans downstream of the coil. One FCU is supplied by RCCWS loop A and the other by RCCWS loop B. One of the fans operates while the other is on standby status and will automatically start upon loss of the lead fan. During normal operation, if both fans of an FCU are out of commission, or the unit is not in service for some other reason, then both fans on the other unit in the area (upper or lower drywell) operate and the cooling supply transfers to the CWS.

Cooled air/nitrogen leaving the FCUs enter a common plenum and is distributed to the various zones in the drywell through distribution ducts. Return ducts are not provided; the FCUs draw air/nitrogen directly from the upper or lower drywell.

A condensate collection pan is provided with each FCU. The condensate collected from all FCUs in the upper and the lower drywell is piped to an LD&IS flow meter to measure the condensation rate of unidentified leakages.

#### 1.2.2.14.7 Flammability Control System

The Flammability Control System (FCS) is designed to limit the concentration of oxygen in a potentially hydrogen-rich post-accident containment atmosphere by controllably recombining ~~burning~~ hydrogen at low levels of oxygen inside the containment.

The FCS consists of passive autocatalytic recombiners (PARs) ~~divisionally assigned low power consumption igniter assemblies~~ strategically intermixed throughout the containment including the upper and lower drywell cavities, and wetwell air space. ~~and powered by Class 1E divisional power.~~

~~The FCS is controlled from the MCR. Prior to the postulated design basis LOCA, the containment is maintained inert at  $\leq 4\%$  oxygen volumetric concentration by the CACS. The FCS automatically initiates 24 hours after receipt of a LOCA signal for the controlled ignition of hydrogen with oxygen. Once initiated, igniters will continue to operate unless manually stopped by the operator. Manual FCS initiation is also possible from the MCR.~~

During normal plant operation, the CACS provides containment atmosphere oxygen level monitoring. During FCS operation, post-accident oxygen level monitoring is provided by the Containment Atmospheric Monitoring System (CAMS).

### 1A.2.10 Relief and Safety Valve Position Indication [II.D.3]

#### *NRC Position*

Reactor coolant system relief and safety valves shall be provided with a positive indication in the control room derived from a reliable valve-position detection device or a reliable indication of flow in the discharge pipe.

#### *Response*

SRV position is indicated in the control room in full compliance with this requirement.

### 1A.2.11 Systems Reliability [II.E.3.2]

This TMI action plan item is superseded by USI A-45, which is addressed in Appendix 19H.

### 1A.2.12 Coordinated Study of Shutdown Heat Removal Requirements [II.E.3.3]

This TMI action plan item is superseded by USI A-45, which is addressed in Appendix 19H.

### 1A.2.13 Containment Design-Dedicated Penetration [II.E.4.1]

#### *NRC Position*

For plant designs with external hydrogen recombiners, provide redundant dedicated containment penetrations so that, assuming a single failure, the recombiner systems can be connected to the containment atmosphere.

#### *Response*

The Flammability Control System (FCS) does not use external hydrogen recombiners that require redundant dedicated penetrations. Therefore, this TMI requirement is not applicable to the SBWR Standard Plant design. The SBWR FCS design utilizes inerting and ~~passive autocatalytic recombiners hydrogen igniters~~ for the purpose of ~~preventing the mitigating the potential~~ buildup of combustible gases generated from the radiolytic decomposition of water and from 100% metal-water reaction of the active fuel cladding during a LOCA.

### 1A.2.14 Containment Design-Isolation Dependability [II.E.4.2]

#### *NRC Position*

- Containment isolation system designs shall comply with the recommendations of Standard Review Plan Subsection 6.2.4 (i.e., that there be diversity in the parameters sensed for the initiation of containment isolation).
- All plant personnel shall give careful consideration to the definition of essential and non-essential systems, identify each system determined to be non-essential, describe

The design of the testing of containment heat removal system meets the requirements of Criterion 40. For further discussion, see the following sections:

Chapter/ Section	Title
6.2.2	Passive Containment Cooling System
7.3.2	Passive Containment Cooling System

### 3.1.4.12 Criterion 41 — Containment Atmosphere Cleanup

#### **Criterion 41 Statement**

Systems to control fission products, hydrogen, oxygen, and other substances which may be released into the reactor containment shall be provided as necessary to reduce, consistent with other associated systems, the concentration and quantity of fission products released to the environment following postulated accidents, and to control the concentration of hydrogen or oxygen and other substances in the containment atmosphere following postulated accidents to assure that containment integrity is maintained.

Each system shall have suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and containment capabilities to assure that for on-site electric power system operation (assuming off-site power is not available) and for off-site electric power system operation (assuming on-site power is not available) its safety function can be accomplished, assuming a single failure.

#### **Evaluation Against Criterion 41**

Fission products, hydrogen, oxygen, and other substances released from the reactor are contained within the low-leakage containment. Except for bypass leakage, leakage from the containment after an accident enters the safety envelope, which is isolated on an accident signal and which contains, dilutes, and holds up leakage from the containment such that the dose guidelines of 10CFR100 are not exceeded. Containment leakage that bypasses the safety envelope enters the reactor building.

The containment is inerted with nitrogen during normal operation. A Flammability Control System controls post-accident hydrogen and oxygen levels with passive autocatalytic recombiners ~~a series of~~ to prevent deflagration or detonation of hydrogen and oxygen, thus assuring that containment integrity is maintained.

These systems have sufficient redundancy to withstand a single failure, ~~and are operable from either off-site or on-site power sources.~~ Criterion 41 is satisfied.



## 6.2.5 Flammability Control System

### 6.2.5.1 Design Bases

The Flammability Control System (FCS) is designed to mitigate, without loss of containment structural integrity, the potential buildup of combustible gases generated from the radiolytic decomposition of water and up to 100% from 100% metal-water reaction of the active fuel cladding during a LOCA.

The FCS is designed with suitable redundancy to ensure that no single ~~active~~ component failure, ~~including power supply failures,~~ will prevent functioning of the system. The FCS is a safety-related system, and is designed for long-term continuous operation for the duration of post-accident oxygen generation. ~~FCS initiation is automatic, requiring no operator action for 72 hours following an accident. After 72 hours, operators are required to perform only simple actions to assure system functionality.~~

All required FCS components are designed and qualified to withstand adverse environmental conditions resulting from a design basis event (LOCA) for a duration of 100 days, and are designated Seismic Category I.

Prior to the design basis LOCA, the containment is maintained inert at 4% oxygen or less volumetric concentration by the Containment Atmospheric Control System (CACS) (See 9.4.8 for CACS description).

### 6.2.5.2 System Description

The FCS is an Engineered Safety Feature (ESF) system whose function is to mitigate oxygen buildup inside containment by controlled reaction ~~ignition~~ of hydrogen with oxygen. The FCS is designed to recombine ~~burn~~ hydrogen at low oxygen volumetric concentrations as ~~they~~ (oxygen and hydrogen) are generated, thereby maintaining oxygen levels below the hydrogen detonatable limit and preventing containment overpressure.

The FCS consists of passive autocatalytic recombiners (PARs) ~~44 igniter assemblies~~ strategically located throughout the containment, including the upper and lower drywell cavities, and inside the suppression chamber air space. ~~The igniters are grouped into 4 divisions. Each division is powered from a dedicated Class 1E battery physically and electrically independent from the other divisions.~~

#### 6.2.5.2.1 Major Component Description (New)

The PARs consist of catalyst cartridges fastened within a stainless steel box frame enclosure. The enclosure also guides flow through the PAR device. The spaces between the cartridges serve as ventilation channels, with gasses containing hydrogen and oxygen being sucked in at the bottom, recombination occurring throughout the height,

and heated gases containing combined hydrogen and oxygen in the form of water vapor leaving the top. A chimney funnels the exit flow through an outlet that has the same area of the flow channels. Testing showed that the chimney improves the efficiency and forced ventilation capability of the PAR device. The chimney can be eliminated for installation in tight spaces where mixing is not crucial. The chimney also can have different shapes to adapt to special locations. Some spaces, such as in crowded compartments or the free space at the upper portion of tanks, may not accommodate or need a standard full PAR device nor would they need a full device to control combustible gases. For this eventuality, a series of smaller size units would be designed, all utilizing the standard cartridges.

The hydrogen igniter (glow plug) is a thermal ignition device that when activated by electric current produces a resistance at the element (or tip) and a nominal temperature 927°C (1700°F). This tip temperature is sufficient to cause combustion of the surrounding gases at relatively low concentrations. The 44 igniters are glow plugs, commonly used in diesel engines.

The igniter is mounted in an igniter assembly or housing with only the tip (glow plug) exposed. The housing is constructed of stainless steel and contains a transformer to step down the voltage to the igniter from 120 Vac to 12 Vac, a terminal block for connection of internal wiring, and all the associated electrical wiring required to make the assembly functional. The housing (assembly) is designed with a spray shield which extends over the glow plug tip, to protect against a reduction in tip temperature caused by impingement of containment spray. Gasketing material and sealant are provided on the igniter enclosure to give protection against condensation and/or containment sprays.

#### 6.2.5.2.2 PAR Igniter Location Criteria

Hydrogen and oxygen can be released to the containment atmosphere by radiolysis and metal-water reaction, through the safety/relief valves, depressurization valves, or pipe breaks inside the drywell. Eventually, most non-condensables end up in the suppression chamber air space. Therefore, PAR igniter assemblies are located in a ring above the suppression pool, as well as at other strategic locations throughout the containment.

The location, distribution and number of PARs is are based on potential oxygen release location, regions where non-condensables will accumulate, appropriate spacing in open areas, redundancy, and potential for higher local concentration in enclosed regions. Details of the these criteria are described below:

- For enclosed areas within the containment, a minimum of 4 igniters (one from each division) are provided to ensure all areas that could be subjected to oxygen-pocketing are covered.

- For open areas in the containment, igniters are installed alternately with the other divisions at a maximum distance of 9 meters (30 ft) such that a maximum of 18 meters (59 ft) distance exists between operable igniters if one divisional power source is not available.
- Igniters are located at least 1 meter below compartment ceilings so as not to restrict convection.
- Igniters in the suppression chamber air space are located outside of the pool swell zone.
- Igniters are located in such a way that adequate coverage is maintained in the event of a postulated high energy line break for which leak before break criteria have not been demonstrated.
- Igniters located in high traffic areas (that could interfere with equipment maintenance or other activities during outages) are adequately protected against physical damage to the igniter or injury to the working personnel.
- Igniters are located such that maintenance and surveillance activities can be achieved with minimal difficulty and radiation exposure as low as reasonably achievable (ALARA).

Igniter distribution is shown in Figures 6.2-23 and 6.2-24, and tabulated below. Figure 6.2-23 shows area location of the igniters in the containment. Figure 6.2-24 igniter schematics and physical separation of the 4 divisional igniters. Igniters designated as "A" are division 1, "B" are division 2, "C" are division 3, and "D" are division 4.

Area- Location	Area Description	Number of Igniters
1	Drywell Head Area	4
2	Upper Drywell Cylinder	12
3	Upper Drywell Annulus	8
4	Lower Drywell Cavity	8
5	Suppression Chamber Air Space	12

### 6.2.6.2.3 System Operation

The FCS is automatically initiated 24 hours after detection of a LOCA condition. Since the containment is initially inert ( $\leq 4\%$  O<sub>2</sub>) and radiolysis is the only significant source

of O<sub>2</sub>, there can be no high energy combustion reaction before initiation. Once initiated, igniters will continue to operate unless manually stopped by the operator. Manual FCS initiation is also possible from the main control room.

#### 6.2.5.2.4 Power Supply

The 44 igniter assemblies are powered from 4 divisional Class 1E DC batteries (11 per division). Each divisional power is brought to its respective divisional distribution panel and junction box outside the containment which is inverted from 125 Vdc to 120 Vac, then penetrates containment where power is distributed to individual igniter transformers for voltage reduction to 12 VAC. Each of the 4 divisional batteries are sized to provide continuous igniter operation for 72 hours without recharging. Each division consists of 6 circuits with each circuit having a maximum of 2 igniters. Each circuit is protected by one circuit breaker and a fuse in series for protection of electrical penetration and to preclude multiple igniter failures if a short circuit develops in one of the circuits. Individual test switch is provided in each igniter for testing. Figure 21.7.3-9 provides hydrogen igniter power supply schematics.

#### 6.2.5.3 Safety Evaluation

A calculation was performed to determine hydrogen and oxygen generation (by radiolysis and metal-water reaction) under post LOCA events inside containment with no recovery or mitigation actions. This calculation is based on the methodology presented in SRP 6.2.5. In the SBWR there are no design basis events that result in core uncover or core heatup sufficient to cause metal-water reaction. Per Reg. Guide 1.7, the design basis metal-water reaction is that equivalent to the reaction of the active clad to a depth of 0.00023 inches. SBWR will be operated with an inert atmosphere which precludes short-term combustibility due to metal-water reactions. Therefore, the FCS function is for long-term combustible gas control due to slow buildup of oxygen from radiolysis. Hydrogen is also generated due to radiolysis, but due to pre-inerted containment, combustibility is precluded by limiting oxygen buildup regardless of hydrogen concentration. In the analysis the containment is initially inerted to 4% oxygen. ~~The hydrogen and oxygen concentration profile for a DBA event is shown in Figure 6.2.25. Based on the calculation results, the igniters will be energized 24 hours following the accident. The PAR system will be designed to prevent the oxygen volumetric concentration from exceeding 5%.~~

#### **Evaluation Against Regulatory Requirements**

Compliance to the regulatory requirements referenced in the Standard Review Plan 6.2.5 are discussed.

**General Design Criterion 41** — The FCS is designed to mitigate ~~buildup generation~~ of oxygen following an accident by ~~recombining slowly burning~~ hydrogen at low levels of oxygen to preclude combustible gases from reaching detonable limits that could

damage containment integrity. The system is designed with sufficient reliability, redundancy (~~4 divisions~~) and physical independence (separation) such that no single failure ~~or one channel removed from service~~ could result in a loss of FCS safety function.

**General Design Criterion 42** — The FCS components are ~~electrical components and are~~ designed to permit periodic visual inspection.

**General Design Criterion 43** — The FCS design permits ~~full~~ operability testing during a refueling outage. ~~Limited functional testing is also possible during plant normal operation.~~

**Regulatory Guide 1.7** — The FCS design basis calculation of the post-accident generation of combustible gases is based on the methodology depicted in Reg. Guide 1.7, ~~with the following modification:~~

- ~~Oxygen yield rate  $G(O_2)$  is 0.2 molecule/100eV.~~

#### **6.2.5.4 Testing and Inspection Requirements**

~~The FCS is preoperationally tested to ensure correct functioning of all controls, indications, alarms, wiring and igniter components providing baseline data for subsequent testing and maintenance. The test includes energizing each of the 4 divisional sets of igniters from the main control room and verifying that all igniters powered from associated panel are functional.~~

Functional testing of FCS includes, as a minimum, measuring and recording the following:

- ~~surface temperature of each igniter, to verify that it is operating at/or above 927°C (1700°F) with 12 Vac applied; and~~
- ~~voltage and current drawn by each circuit feeding the igniters in each of the 4 divisions.~~

#### **6.2.5.5 Instrumentation Requirements**

~~Instrumentation and controls requirements for the Flammability Control System are described in Subsection 7.3.6.~~

#### **6.2.6 Containment Leakage Testing**

This section describes the testing program for determining the containment integrated leakage rate (Type A tests), containment penetration leakage rates (Type B tests), and containment isolation valve leakage rates (Type C tests) that complies with Appendix J and General Design Criteria 52, 53, and 54 of Appendix A to 10CFR50. Type A, B, and

## 7.3.6 Flammability Control System

### 7.3.6.1 Design Bases

The Flammability Control System (FCS) design bases are discussed in Subsection 6.2.5.

### 7.3.6.2 System Description

The FCS system description is discussed in Subsection 6.2.5.

### 7.3.6.3 Safety Evaluation

Table 7.1-1 identifies specific general design criteria, codes and standards, and regulatory requirements referenced in Section 7.3 of the Standard Review Plan for Engineered Safety Features Systems. The following paragraphs discuss compliance and any exceptions or clarifications. Subsection 6.2.5 also discusses FCS compliance with other regulatory requirements, in accordance with Chapter 6 of the SRP.

#### **Specific Regulatory Requirements Conformance**

##### ~~10CFR50.55a (IEEE 279)~~

The requirements of IEEE 279 are enveloped by RG 1.153/IEEE 603.

#### **General Design Criteria**

**General Design Criterion 2** — The FCS igniter assemblies are installed inside the containment. Power supplies, distribution panels and junction boxes are located outside the containment (inside the reactor building). The containment both structures is are Seismic Category I and is are designed to withstand the effects of natural phenomena, including earthquakes, tornadoes, floods, hurricanes, etc.

**General Design Criterion 4** – The FCS components, including their supports, are designed to withstand, without loss of function, the dynamic effects, including effects of missiles, pipe whips, etc.

**General Design Criterion 13** – The Containment Atmospheric Control System (CACS) provides FCS oxygen level monitoring during normal plant operation. The FCS post-accident oxygen level monitoring is provided by the Containment Atmospheric Monitoring System (CAMS).

**General Design Criterion 19** – GDC 19 is a plant-wide requirement for provision of a control room. A main control room is provided in the SBWR plant design. The FCS has ~~no control~~ functions inside the main control room.

**General Design Criterion 20** – The FCS logic is automatically responds to the presence initiated upon receipt of a LOCA signal (low water level). Integrated to this logic is a 24-hour time delay for energizing the igniters of hydrogen and oxygen by recombining them to form water vapor.

**General Design Criteria 21, 22, 24, and 41** – The FCS is designed to mitigate generation of oxygen following an accident by ~~burning~~ recombining hydrogen at low levels of oxygen. The FCS design permits capability for periodic testing every refueling outage. The system is designed with sufficient reliability, redundancy (~~four divisions~~), and physical independence ~~independency~~ such that no single failure ~~or one channel removed from service~~ could result in loss of FCS safety-related function.

#### ***NRC Regulatory Guides***

**Regulatory Guides 1.22 and 1.118** – Periodic operability testing of the FCS is accomplished every refueling outage. ~~Limited functional testing during normal plant operation is also possible.~~

**Regulatory Guide 1.47** – The FCS ~~design provides control room alarm and indication if the system is out of service or in inoperative status.~~ is a passive system that is always operative and requires no control room alarms.

**Regulatory Guide 1.53** – The FCS ~~provision for four divisional systems meets the requirements of this regulatory guide.~~

**Regulatory Guide 1.62** – The FCS ~~design includes provision for manual initiation from the main control room for each of the four divisions.~~

**Regulatory Guide 1.75** – Each FCS division is physically and electrically independent. Each division is powered from a dedicated Class 1E source, each power source located in separated areas of the reactor building. The power, equipment, and control from each division are totally separate from the other. Five compartment regions have been defined within the containment. Multiple igniters (from each independent division) are located within the defined regions. Subsequently, if one or two igniters are inactive, operating igniters from other divisions are available to provide the flammability control function. Class 1E interfaces with non-Class 1E alarms and indicators are provided with fiber optic isolation devices.

**Regulatory Guide 1.105** – The FCS fully meets the requirements of RG 1.105. Instrument setpoint methodology is covered under a licensing topical report (Reference 7.3-1).

**Regulatory Guide 1.153** – The FCS is designed in accordance with the requirements of RG 1.153 and IEEE 603.

#### ***NRC Branch Technical Positions:***

- (1) BTP ICSB 21: The FCS fully meets the requirements of BTP ICSB 21 and RG 1.47.

- (2) BTP ICSB 22: The igniters are located inside the inerted containment, and therefore cannot be fully tested (i.e., ignition temperatures measured) during normal reactor operation. However, the igniters can be energized, and voltage and current can be measured from the distribution panel and/or junction box located outside the containment to assure connections are functioning and electrical loads are normal.

#### 7.3.6.4 Testing and Inspection Requirements

The FCS testing and inspection requirements are described in Subsection 6.2.5.

#### 7.3.6.5 Instrumentation Requirements

None.

##### ***Logic and Interlocks***

The FCS initiation is fully automatic. Upon receipt of a LOCA signal (Level 1), the 24-hour time delay starts. When the timer times out, FCS initiation is sealed in. Once initiated, the igniters heat up and reach their operating temperature. Recombination proceeds when oxygen and hydrogen concentrations are at or above ignition level. The FCS will continue to operate until manually terminated by the operator from the main control room.

The FCS manual initiation is also possible from the main control room. Manual FCS control consists of four remote manual control switches (one in each division). Each control switch is used to energize and terminate operation of the igniters in each respective division.

The FCS automatically trips on loss of power to the bus. The FCS operation may be restarted only after manual reinitiation by the remote manual control switches. The FCS system instrument and electrical diagram (IED) and logic diagram (LD) are depicted in Figures 21.7.3-9 and 21.7.3-10 respectively.

##### ***Indication and Alarms***

The following FCS status indications and alarms are provided in the main control room:

- "ON and "OFF" status lights
- "AUTO TRIP" status light
- "IGNITERS INITIATED" alarm
- "LOSS OF POWER" alarm
- "BUS UNDER VOLTAGE" alarm



- ~~"OUT-OF-SERVICE" alarm~~

~~During FCS operation, oxygen concentration indication is provided by the GAMS.~~

### **7.3.7 COL License Information**

None.

### **7.3.8 References**

None.

~~7.3.1 Instrument Setpoint Methodology, Licensing Topical Report NEDC-31336.~~

~~7.3.2 Military DOD Standard 2167, Defense System Software Development.~~

Table 9A.7-1a SBWR Safety-Related Equipment List (Continued)

MPL Number	Description	Elect Div	Bldg Loc	Fire Area Designation	Panel/Cabinet
T31-F015	AO GLOBE VALVE	4	S	F1B100	
T31-F023	AO GLOBE VALVE	1	S	F1A100	
T31-F024	AO GLOBE VALVE	2	S	F1A100	
T31-F025	AO GLOBE VALVE	1	S	F1A100	
T31-PIN012	PRESS INDICATION HVAC SUPPLY	N	S	F1B100	
T31-PIN019	PRESS INDICATION HVAC SUPPLY	N	S	F1B100	
T31-PTN011	PRESS TRANSMITTER HVAC SUPPLY	N	S	F1B100	
T31-PTN018	PRESS TRANSMITTER HVAC SUPPLY	N	S	F1B100	
T31-TEN008	TEMPERATURE ELEMENT	1	S	F1A100	
T31-TEN015	TEMPERATURE ELEMENT	1	S	F1A100	
T31-TEN038	TEMP ELEMENT (Typ of 12)	1	P	F1P100	
T31-TEN040	TEMP. ELEMENT (Typ of 6)	1	P	F1P100	
T49-B001A	HYDROGEN IGNITER	4	P	F1P100	
T49-B001B	HYDROGEN IGNITER	2	P	F1P100	
T49-B001C	HYDROGEN IGNITER	3	P	F1P100	
T49-B001D	HYDROGEN IGNITER	4	P	F1P100	
T49-B002A	HYDROGEN IGNITER	4	P	F1P100	
T49-B002B	HYDROGEN IGNITER	2	P	F1P100	
T49-B002C	HYDROGEN IGNITER	3	P	F1P100	
T49-B002D	HYDROGEN IGNITER	4	P	F1P100	
T49-B003A	HYDROGEN IGNITER	1	P	F1P100	
T49-B003B	HYDROGEN IGNITER	2	P	F1P100	
T49-B003C	HYDROGEN IGNITER	3	P	F1P100	
T49-B003D	HYDROGEN IGNITER	4	P	F1P100	
T49-B004A	HYDROGEN IGNITER	1	P	F1P100	
T49-B004B	HYDROGEN IGNITER	2	P	F1P100	

Table 9A.7-1a SBWR Safety-Related Equipment List (Continued)

MPL Number	Description	Elect Div	Bldg Loc	Fire Area Designation	Panel/ Cabinet
T49-B004C	HYDROGEN IGNITER	3	P	F1P100	
T49-B004D	HYDROGEN IGNITER	4	P	F1P100	
T49-B005A	HYDROGEN IGNITER	1	P	F1P100	
T49-B005B	HYDROGEN IGNITER	2	P	F1P100	
T49-B005C	HYDROGEN IGNITER	3	P	F1P100	
T49-B005D	HYDROGEN IGNITER	4	P	F1P100	
T49-B006A	HYDROGEN IGNITER	1	P	F1P100	
T49-B006B	HYDROGEN IGNITER	2	P	F1P100	
T49-B006C	HYDROGEN IGNITER	3	P	F1P100	
T49-B006D	HYDROGEN IGNITER	4	P	F1P100	
T49-B007A	HYDROGEN IGNITER	1	P	F1P100	
T49-B007B	HYDROGEN IGNITER	2	P	F1P100	
T49-B007C	HYDROGEN IGNITER	3	P	F1P100	
T49-B007D	HYDROGEN IGNITER	4	P	F1P100	
T49-B008A	HYDROGEN IGNITER	1	P	F1P100	
T49-B008B	HYDROGEN IGNITER	2	P	F1P100	
T49-B008C	HYDROGEN IGNITER	3	P	F1P100	
T49-B008D	HYDROGEN IGNITER	4	P	F1P100	
T49-B009A	HYDROGEN IGNITER	1	P	F1P100	
T49-B009B	HYDROGEN IGNITER	2	P	F1P100	
T49-B009C	HYDROGEN IGNITER	3	P	F1P100	
T49-B009D	HYDROGEN IGNITER	4	P	F1P100	
T49-B010A	HYDROGEN IGNITER	1	P	F1P100	
T49-B010B	HYDROGEN IGNITER	2	P	F1P100	
T49-B010C	HYDROGEN IGNITER	3	P	F1P100	
T49-B010D	HYDROGEN IGNITER	4	P	F1P100	
T49-B011A	HYDROGEN IGNITER	1	P	F1P100	
T49-B011B	HYDROGEN IGNITER	2	P	F1P100	

Table 9A.7-1a SBWR Safety-Related Equipment List (Continued)

MPL Number	Description	Elect Div	Bldg Loc	Fire Area Designation	Panel/Cabinet
T49-B011C	HYDROGEN IGNITER	3	P	F1P100	
T49-B011D	HYDROGEN IGNITER	4	P	F1P100	
T49-RMS001A?	REMOTE MANUAL SWITCH-IGNITERS	1	CR	F6N100	
T49-RMS001B?	REMOTE MANUAL SWITCH-IGNITERS	2	CR	F6N100	
T49-RMS001C?	REMOTE MANUAL SWITCH-IGNITERS	3	CR	F6N100	
T49-RMS001D?	REMOTE MANUAL SWITCH-IGNITERS	4	CR	F6N100	
T53-LMU???A*?	SPTMS LOCAL MULTIPLEXER UNIT	1	S	F1A100	
T53-LMU???B*?	SPTMS LOCAL MULTIPLEXER UNIT	2	S	F1B100	
T53-LMU???C*?	SPTMS LOCAL MULTIPLEXER UNIT	3	S	F1C100	
T53-LMU???D*?	SPTMS LOCAL MULTIPLEXER UNIT	4	S	F1D100	
T53-TE001A	TEMPERATURE ELEMENT	1	P	F1P100	
T53-TE001B	TEMPERATURE ELEMENT	2	P	F1P100	
T53-TE001C	TEMPERATURE ELEMENT	3	P	F1P100	
T53-TE001D	TEMPERATURE ELEMENT	4	P	F1P100	
T53-TE002A	TEMPERATURE ELEMENT	1	P	F1P100	
T53-TE002B	TEMPERATURE ELEMENT	2	P	F1P100	
T53-TE002C	TEMPERATURE ELEMENT	3	P	F1P100	
T53-TE002D	TEMPERATURE ELEMENT	4	P	F1P100	
T53-TE003A	TEMPERATURE ELEMENT	1	P	F1P100	
T53-TE003B	TEMPERATURE ELEMENT	2	P	F1P100	
T53-TE003C	TEMPERATURE ELEMENT	3	P	F1P100	
T53-TE003D	TEMPERATURE ELEMENT	4	P	F1P100	
T53-TE004A	TEMPERATURE ELEMENT	1	P	F1P100	
T53-TE004B	TEMPERATURE ELEMENT	2	P	F1P100	

Table 9A-1b SBWR Safety-Related Equipment List (Continued)

MPL Number	Description	Elect Div	Bldg Loc	Fire Area Designation	Panel/Cabinet
G31-RMC004A*7	REMOTE MANUAL CONTROL (F004A)	1	CR	F5N100	
G31-RMC004B*7	REMOTE MANUAL CONTROL (F004B)	2	CR	F5N100	
G31-RMS005A*7	REMOTE MANUAL SWITCH (F005A)	1	CR	F5N100	
G31-RMS005B*7	REMOTE MANUAL SWITCH (F005B)	2	CR	F5N100	
G31-RMS006A*7	REMOTE MANUAL SWITCH (F006A)	1	CR	F5N100	
G31-RMS006B*7	REMOTE MANUAL SWITCH (F006B)	2	CR	F5N100	
G31-RMS007A*7	REMOTE MANUAL SWITCH (F007A)	1	CR	F5N100	
G31-RMS007B*7	REMOTE MANUAL SWITCH (F007B)	2	CR	F5N100	
G31-RMS036A*7	REMOTE MANUAL SWITCH (F036A)	1	CR	F5N100	
G31-RMS036B*7	REMOTE MANUAL SWITCH (F036B)	2	CR	F5N100	
G31-RMSPSS1A	REMOTE MANUAL SWITCH (PSS1)	1	CR	F5N100	
G31-RMSPSS1B	REMOTE MANUAL SWITCH (PSS2)	2	CR	F5N100	
H10-P601	CONTROL ROOM PANEL	N	CR	F5N100	
<del>T49-RMS001A?</del>	<del>REMOTE MANUAL SWITCH-IGNITERS</del>	<del>4</del>	<del>CR</del>	<del>F5N100</del>	
<del>T49-RMS001B?</del>	<del>REMOTE MANUAL SWITCH-IGNITERS</del>	<del>2</del>	<del>CR</del>	<del>F5N100</del>	
<del>T49-RMS001C?</del>	<del>REMOTE MANUAL SWITCH-IGNITERS</del>	<del>3</del>	<del>CR</del>	<del>F5N100</del>	
<del>T49-RMS001D?</del>	<del>REMOTE MANUAL SWITCH-IGNITERS</del>	<del>4</del>	<del>CR</del>	<del>F5N100</del>	
G31-F035A	SWING CHECK VALVE	N	S	F7N100	
G31-F035B	SWING CHECK VALVE	N	S	F7N100	
G31-F036A	MO GLOBE VALVE	1	S	F7N100	
G31-F036B	MO GLOBE VALVE	2	S	F7N100	

**3.6 Containment Systems****3.6.3.1 Containment Flammability Control**

LCO 3.6.3.1 Four divisions of igniters shall be OPERABLE.

APPLICABILITY: MODES 1 and 2.

**ACTIONS**

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One division of igniters inoperable.	A.1 Restore inoperable division of igniters to OPERABLE status.	30 days
B. Two divisions of igniters inoperable.	B.1 Restore one inoperable division of igniters to OPERABLE status.	7 days
C. Required Action and associated Completion Time not met.	C.1 Be in MODE 3.	12 hours

**SURVEILLANCE REQUIREMENTS**

SURVEILLANCE	FREQUENCY
SR 3.6.3.1.1 Perform a system functional test for each division of igniters.	REFUELING INTERVAL
SR 3.6.3.1.2 Visually examine each <u>recombiner</u> igniter enclosure and ensure there is no evidence of abnormal conditions <u>or</u> <u>fouling</u> .	REFUELING INTERVAL
SR 3.6.3.1.3 <u>Test performance of PAR catalytic element with H<sub>2</sub>, O<sub>2</sub> mixture.</u> Perform a resistance to ground test for each igniter.	REFUELING INTERVAL

## B 3.6 Containment Systems

### B 3.6.3.1 Containment Flammability Control

#### BASES

---

---

#### BACKGROUND

The Flammability Control System (FCS) ensures containment integrity in post-accident environments by eliminating the potential breach of containment due to a hydrogen-oxygen reaction.

The FCS is required to control combustible gas (oxygen) concentration in the containment following a loss-of-coolant accident (LOCA). The containment FCS accomplishes this by using passive autocatalytic recombiners (PARs) igniters for recombining hydrogen and oxygen to form water vapor, which remains in the containment.

~~The FCS is an Engineered Safety Feature (ESF) system. It is single-failure proof and consists of four 33% capacity subsystems. The FCS is designed to recombine burn hydrogen at low oxygen volumetric concentrations as they (oxygen and hydrogen) are generated, thereby maintaining oxygen levels below the hydrogen detonable limit and preventing containment overpressure. The PARs igniters are designed to maintain the oxygen gas concentration within the containment below the flammability limit of 5.0 volume percent (v/o) following a postulated LOCA.~~

FCS consists of PAR 44 igniter assemblies strategically located throughout the containment, including the upper and lower drywell cavities, and inside the wetwell air space. ~~The igniters are grouped into 4 divisions with each division powered from a dedicated Class 1E battery physically and electrically independent from the other divisions.~~

~~The igniter (glow plug) is a thermal ignition device that when activated by electric current produces a resistance at the element (or tip) and an increase in temperature of at least 927°C (1700°F). This tip temperature is sufficient to cause combustion of the surrounding gases at relatively low concentrations.~~

~~The igniter is mounted in an igniter assembly or housing with only the tip (glow plug) exposed. The housing is constructed of stainless steel and contains a transformer to step down the voltage to each igniter from 125 Vac to 12 Vac, a terminal block for~~

connection of internal wiring, and all the associated electrical wiring required to make the assembly functional. The igniter assembly is designed with a spray shield which extends over the glow plug tip, to protect against a reduction in tip temperature caused by impingement of water spray. A junction box is attached to the exterior of the containment and contains the cable terminations. Gasketing material and sealant are provided to ensure leak tightness of the igniter enclosure.

The location, distribution, and number of igniters is based on potential oxygen release location, regions where non-condensibles are likely to accumulate, appropriate spacing in open areas, redundancy and potential for pocketing in enclosed regions.

FCS is automatically initiated on a RPV Level 1 signal (LOCA signal) plus a 24-hour time delay following a design basis accident. Since the containment is initially inert prior to the accident, oxygen level is not expected to reach detonable limit for approximately 72 hours. Once initiated igniters will continue to operate unless manually stopped by the operator. Manual initiation is also possible from the main control room.

The 44 igniter assemblies are powered from 4 divisional dedicated Class 1E DC batteries (11 per division). Each divisional power is brought to its respective divisional distribution panel outside the containment which is inverted from 125 VDC to 120 VAC, then penetrates containment where power is distributed to individual igniter transformers for voltage reduction to 12 VAC. Each of the 4 divisional batteries are sized to provide continuous igniter operation for 72 hours without recharging. Each division consists of 6 circuits with each circuit having a maximum of 2 igniters. Each circuit is protected by one circuit breaker and a fuse in series for protection of electrical penetration and to preclude multiple igniter failures if a short circuit develops in one of the circuits.

APPLICABLE  
SAFETY ANALYSES

The containment PARs igniters ensure containment integrity by providing the capability of controlling the bulk oxygen concentration in primary containment to less than the lower flammable concentration of 5.0 v/o following a Design Basis Accident (DEA). This control would prevent a containment wide hydrogen burn, thus ensuring containment



integrity and minimizing damage to safety-related equipment located in containment. The limiting DBA relative to hydrogen generation is a LOCA.

Hydrogen and oxygen may accumulate in containment following a LOCA as a result of:

- a. a metal-steam reaction between the zirconium fuel rod cladding and the reactor coolant results in release of hydrogen;
- b. radiolytic decomposition of water in the Reactor Coolant System (RCS) results in release of hydrogen and oxygen; and
- c. hydrogen dissolved in the RCS is released.

To evaluate the potential for hydrogen and oxygen accumulation in containment following a LOCA, the hydrogen and oxygen generation is calculated as a function of time following the initiation of the accident. The assumptions recommended by Reference B 3.6.3.1-1 are used to maximize the amount of hydrogen and oxygen calculated.

The FCS satisfies Criterion 3 of the NRC Interim Policy Statement, as passive components PARs will be operable at all times.

LCO

~~Four containment igniter subsystems must be OPERABLE with power from four independent, safety-related dc power supplies. This assures the operation of at least three containment igniter subsystems in the event of a worst case single active failure.~~

~~Operation with at least three containment igniter subsystems ensures that the post LOCA oxygen concentrations can be prevented from exceeding the flammability limit. Unavailability of all four containment igniter subsystems might lead to the generation of a sufficient amount of oxygen (the flammability limit exceeded) that could react with hydrogen following the LOCA. The reaction could take place fast enough to lead to high temperatures and overpressurization of containment and, as a result, breach containment or cause containment leakage rates above those assumed in the safety analyses. Damage to safety-related equipment located in containment could also occur.~~

## APPLICABILITY

Not Applicable

In MODES 1 and 2, the four containment igniter subsystems are required to control the oxygen concentration within containment below its flammability limit of 5.0 v/o following a LOCA, assuming a worst case single failure. This ensures containment integrity and prevents damage to safety-related equipment and instruments located within containment.

In MODE 3, both the hydrogen and oxygen production rate and the total hydrogen and oxygen produced after a LOCA would be less than that calculated for the DBA LOCA. Also, because of the limited time in this MODE, the probability of an accident requiring the containment igniters is low. Therefore, the containment igniters are not required in MODE 3.

In MODES 4 and 5, the probability and consequences of a LOCA are low due to the pressure and temperature limitations in these MODES. Therefore, the containment igniters are not required in these MODES to ensure containment integrity.

## ACTIONS

Not Applicable A.1

With one containment igniter division inoperable, the inoperable subsystem must be restored to OPERABLE status within 30 days. In this Condition, the remaining OPERABLE divisions are adequate to perform the oxygen and hydrogen control function. However, the overall reliability is reduced because a single failure in the OPERABLE divisions could result in reduced oxygen and hydrogen control capability. The 30-day Completion Time is based on the low probability of the occurrence of a LOCA that would generate oxygen and hydrogen in amounts capable of exceeding the flammability limit, the length of time after the event that operator action would be required to prevent this limit from being exceeded, and the low probability of failures of the OPERABLE containment igniter divisions.

Required Action A.1 has been modified by a Note which states the provisions of LCO 3.0.4 are not applicable. As a result, a MODE change is allowed when one division of igniters is inoperable. This allowance is provided because of: (1) the low probability of the

occurrence of a LOCA that would generate oxygen and hydrogen in amounts capable of exceeding the flammability limit, (2) the low probability of the failure of the OPERABLE divisions, (3) the length of time after a postulated LOCA before operator action would be required to prevent exceeding the flammability limit from being exceeded, and (4) the availability of other hydrogen-mitigating systems.

#### B.1

With two containment igniter divisions inoperable, one subsystem must be restored to OPERABLE status within seven days. The 7-day Completion Time is based on the low probability of the occurrence of a LOCA that would generate hydrogen and oxygen in the amounts capable of exceeding the oxygen flammability limit, the length of time after the event that operator action would be required to prevent exceeding this limit and the availability of the igniters and drywell-purge systems.

#### G.1

The plant must be placed in a MODE in which the LCO does not apply if the inoperable containment igniter subsystem cannot be restored to OPERABLE status in the associated Completion Time. This is done by placing the plant in at least MODE 3 within 12 hours. The allowed completion time of 12 hours is a reasonable time, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

## SURVEILLANCE REQUIREMENTS

### SR 3.6.3.1.1

Performance of a system functional test for each containment igniter subsystem ensures that the igniters are OPERABLE and can attain and sustain the temperature necessary for oxygen and hydrogen recombination. In particular, this SR verifies that the minimum igniter temperature increases to  $\geq 927^{\circ}\text{C}$  ( $1700^{\circ}\text{F}$ ) in  $\leq 15$  minutes, and that it is maintained at that temperature for at least four hours thereafter to check the ability of the igniter to function properly. The Frequency of every REFUELING

~~INTERVAL for this SR was developed considering such factors as the ruggedness of the equipment and containment access.~~

#### SR 3.6.3.1.2

Every outage PARs will be inspected to determine any external damage. Any debris that collects on the surface of the catalytic elements will be removed by vacuuming or other means. To ensure that the catalytic elements have not been fouled by foreign material that could reduce their efficiency selected catalytic elements will be tested for recombination effectiveness.

~~This SR ensures there are no physical problems that could affect igniter operation. Since the igniters are mechanically passive, they are subject only to minimal mechanical failure. The only credible failures involve loss of power, submergence under water, missile impact, etc.~~

~~A visual inspection is sufficient to determine abnormal conditions that could cause such failures. The Frequency of every REFUELING INTERVAL for this SR was developed considering such factors as the ruggedness of the equipment and containment access.~~

#### SR 3.6.3.1.3

~~This SR performs a resistance to ground test of each igniter to make sure that there are no detectable grounds. This is accomplished by verifying that the resistance to ground for any igniter is  $\geq 10,000$  ohms. The Frequency of every REFUELING INTERVAL for this SR was developed considering such factors as the ruggedness of the equipment and containment access.~~

## REFERENCES

- B 3.6.3.1-1 Regulatory Guide 1.7, "Control of Combustible Gas Concentrations in Containment Following a Loss-of-Coolant Accident, U.S. Nuclear Regulatory Commission."
- B 3.6.3.1-2 SBWR SSAR, Section 6.2.5.

**B 3.6 Containment Systems****B 3.6.3.2 Containment Oxygen Concentration****BASES****BACKGROUND**

All nuclear reactors must be designed to withstand events that generate hydrogen either due to the zirconium metal-water reaction in the core or due to radiolysis. The primary method to control hydrogen is to inert the containment. With the containment inert, that is, oxygen concentration less than 4.0 volume percent (v/o), a combustible mixture cannot be present in the containment for any hydrogen concentration. The capability to inert the containment and maintain oxygen below 4.0 v/o works together with the Flammability Control System (LCO 3.6.3.1) and the Containment Atmospheric Control System to provide redundant methods to mitigate events that produce hydrogen. For example, an event that rapidly generates hydrogen from zirconium metal-water reaction will result in excessive hydrogen in containment, but oxygen concentration will remain below 4.0 v/o and no combustion can occur. Long-term generation of both hydrogen and oxygen from radiolytic decomposition of water may eventually result in a combustible mixture in containment, except that the passive autocatalytic recombiners recombine ~~igniters (glow plugs) burn~~ hydrogen and oxygen gases faster than they can be produced from radiolysis and again no combustion can occur. This LCO is to ensure that oxygen concentration does not exceed 4.0 v/o during operation in the applicable conditions.

**APPLICABLE  
SAFETY ANALYSES**

The Reference B 3.6.3.2-1 calculations assume that the containment is inerted where a Design Basis Accident (DBA) loss-of-coolant accident (LOCA) occurs. Thus, the hydrogen assumed to be released to the containment as a result of metal-water reaction in the reactor core will not produce combustible gas mixtures in the containment. Oxygen, which is subsequently generated by radiolytic decomposition of water, is recombined ~~by the igniters~~ (LCO 3.6.3.1) more rapidly than it is produced.

Containment oxygen concentration satisfies Criterion 2 of the NRC Interim Policy Statement.

**LCO**

The containment oxygen concentration is maintained below 4.0 v/o to ensure that an event that produces any amount of hydrogen and oxygen does not result in a combustible mixture inside containment.

## APPLICABILITY

The containment oxygen concentration must be within the specified limit when containment is inerted, except as allowed by the relaxations during startup and shutdown addressed below. The containment must be inert in MODE 1, since this is the condition with the highest probability of an event that could produce hydrogen.

Inerting the containment is an operational problem because it prevents containment access without an appropriate breathing apparatus. Therefore, the containment is inerted as late as possible in the plant startup and de-inerted as soon as possible in the plant shutdown. As long as reactor power is below 15% RATED THERMAL POWER (RTP), the potential for an event that generates significant hydrogen is low and the containment need not be inert. Furthermore, the probability of an event that generates hydrogen occurring within the first 24 hours of a startup or within the last 24 hours before a shutdown is low enough that these "windows," when the containment is not inerted, are also justified. The 24-hour time is a reasonable amount of time to allow plant personnel to perform inerting or de-inerting.

## ACTIONS

A.1

If oxygen concentration exceeds 4.0 v/o at any time while operating in MODE 1, with the exception of the relaxations allowed during startup and shutdown, oxygen concentration must be restored to below 4.0 v/o within 24 hours. The 24-hour Completion Time is allowed when oxygen concentration is above 4.0 v/o because of the availability of other hydrogen-mitigating systems (recombiners) (~~e.g., igniters~~) and the low probability and long duration of an event that would generate significant amounts of hydrogen occurring during this period.

If equipment used to monitor oxygen concentration in containment is determined to be inoperable, the containment oxygen concentration is not considered to be within limits and Required Action A.1 applies to restore such equipment to OPERABLE status.

B.1

If oxygen concentration cannot be restored to within limits in the associated Completion Time, the plant must be placed in a MODE in which the LCO does not apply. This is done by reducing power to  $\leq 15\%$  RTP in 8 hours. The 8-hour Completion Time is reasonable, based on operating experience related to the amount of time required to reduce reactor power from full power in an orderly manner and without challenging plant systems.

regime since the oxygen is diluted with added hydrogen. Further details of the CACS can be found in Subsection 9.4.8.

The SBWR is also provided with hydrogen passive autocatalytic recombiners (PARs) igniter assemblies (as part of the Flammability Control System [FCS]) which mitigate the buildup of oxygen in the containment, due to radiolysis, from creating a potentially flammable mixture. Radiolysis is the only potential source of oxygen in the SBWR primary containment. Further details of the FCS can be found in Subsection 6.2.5.

#### **19G.2.13 Long-Term Training Upgrade [Item (2) (i)]**

##### ***NRC Position***

Provide simulator capability that correctly models the control room and includes the capability to simulate small-break LOCAs. (Applicable to construction permit applicants only.) [I.A.4.2]

##### ***Response***

This is a COL license information requirement (see Subsection 19G.3.1).

#### **19G.2.14 Long-Term Program of Upgrading of Procedures [Item (2) (ii)]**

##### ***NRC Position***

Establish a program, to begin during construction and follow into operation, for integrating and expanding current efforts to improve plant procedures. The scope of the program shall include emergency procedures, reliability analyses, human factors engineering, crisis management, operator training, and coordination with INPO and other industry efforts. (Applicable to construction permit applicants only.) [I.C.9]

##### ***Response***

This is a COL license information requirement (see Subsection 19G.3.2).

#### **19G.2.15 Control Room Design Reviews [Item (2) (iii)]**

##### ***NRC Position***

Provide, for Commission review, a control room design that reflects state-of-the-art human factor principles prior to committing to fabrication or revision of fabricated control room panels and layouts. [I.D.1]

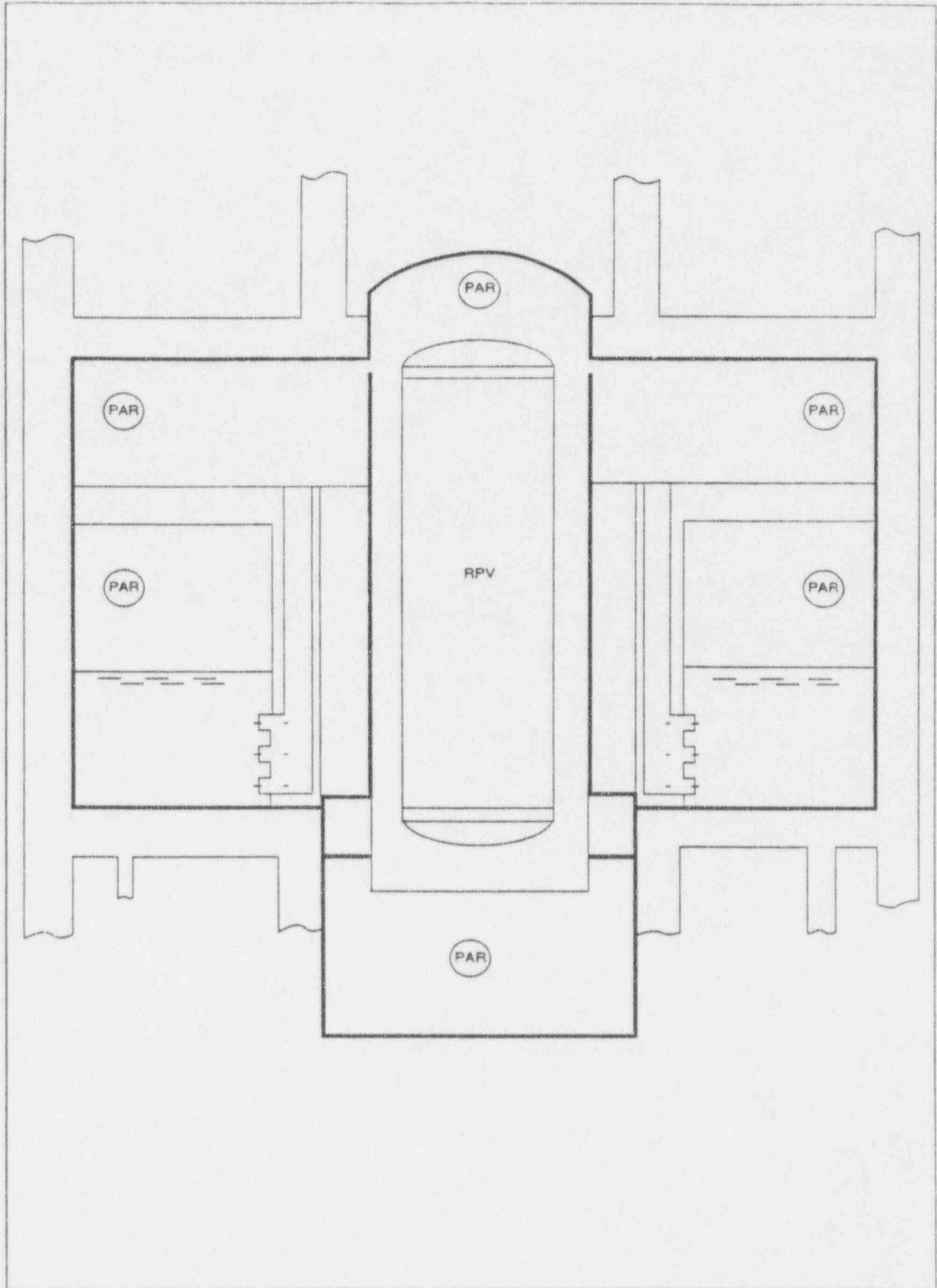
##### ***Response***

This item is addressed in Subsection 1A.2.2.

#### **19G.2.16 Plant Safety Parameter Display Console (SPDS) [Item (2) (iv)]**

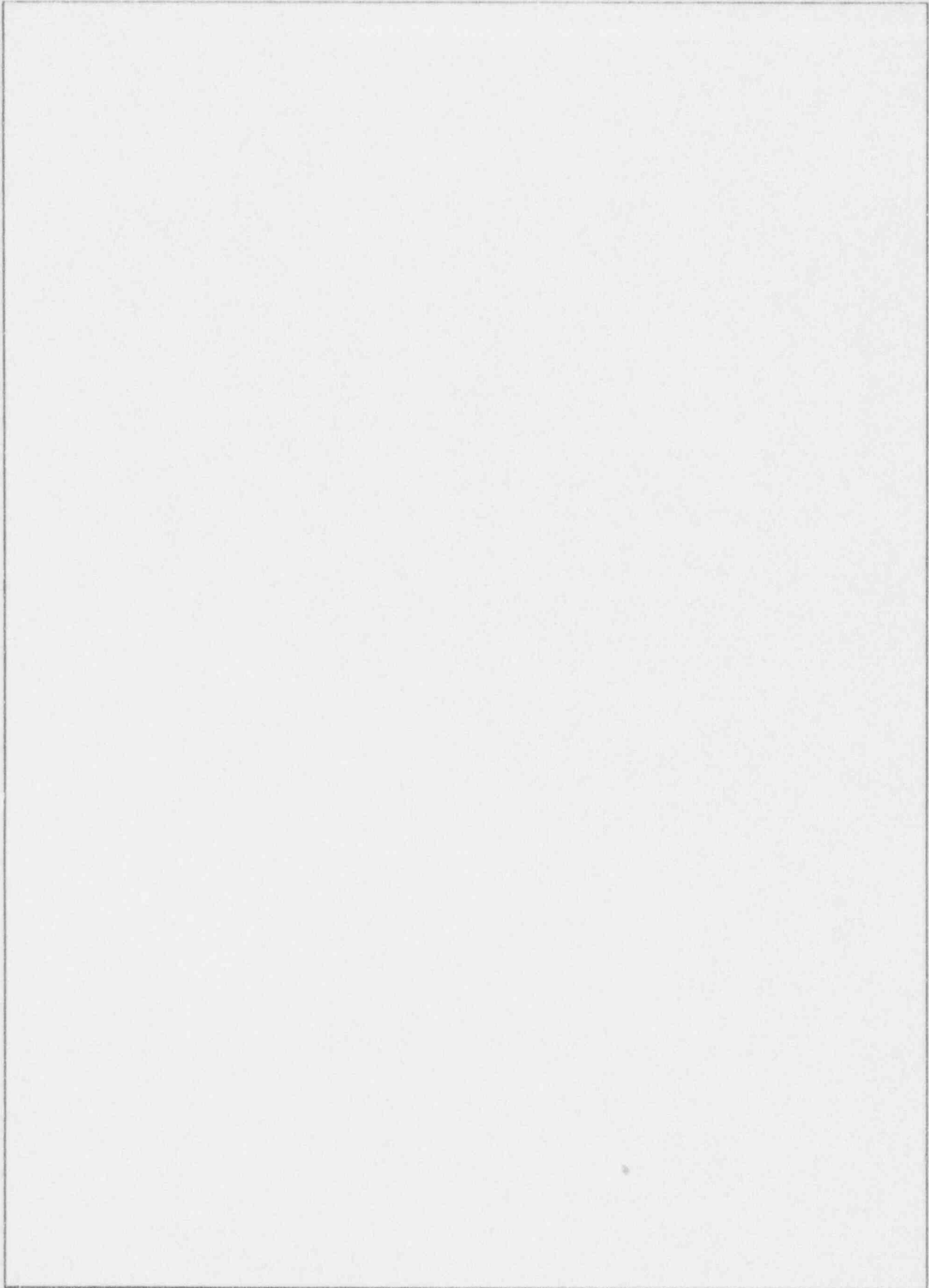
##### ***NRC Position***

Provide a plant safety parameter display console that will display to operators a minimum set of parameters defining the safety status of the plant, capable of displaying



**Figure 6.2-23 PAR Hydrogen Igniter Distribution in the Containment**





**Figure 6.2-24 Hydrogen Igniter System Schematics**



**Figure 6.2-25 SBWR Combustible Gas Concentration — DBA LOCA**

TABLE REV A  
DATE 10/1/84

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100

DELETED

11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

2

3

4

5

6

7

E

D

C

B

A

DELETED

2

3

4

5

6

7

E

D

C

B

A

DELETED

2

3

4

5

6

7

E

D

C

B

A

DELETED

2

3

4

5

6

7

E

D

C

B

A

DELETED

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

**RAI 420.5**

The last sentence on page 7.1-9 of the standard safety analysis report (SSAR) in the discussion of compliance with RG 1.47 states that those portions of the bypass indications that, when faulted, could reduce the independence between redundant safety-related systems are electrically isolated from the protection circuit. Identify which are the portions of the bypass indications that are referred to on SSAR page 7.1-9.

**GE Response:**

All bypass status indications of safety related systems are isolated using isolation devices. See attached revised SSAR subsection 7.1.2.2, page 7.1-9.



### **Conformance to Regulatory Guides**

The following compliance statements for Regulatory Guides apply to the I&C generally. Individual system application is addressed in Table 7.1-1, and possible clarifications or exceptions are discussed in the Safety Evaluation subsections within Sections 7.2 through 7.7.

#### **Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions —**

All safety-related systems have provision for periodic testing. Proper functioning of analog sensors can be verified by channel cross-comparison. Some actuators and digital sensors, because of their locations, cannot be fully tested during actual reactor operation. Such equipment is identified and provisions for meeting the requirements of Paragraph D.4 (per BTP ICSB 22) are discussed in the Safety Evaluation subsections within Sections 7.2 through 7.7.

**Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems —** Bypass indications are designed to satisfy the requirement of IEEE 279, Paragraph 4.13, Regulatory Guide 1.47, and BTP ICSB 21. The design of the bypass indications allows testing during normal operation and is used to supplement administrative procedures by providing indications of safety-related systems status.

~~Bypass indications are designed and installed using isolation devices to in a manner which precludes preclude the possibility of any adverse electrical effect that bypass indication circuits could have on the plant safety-related system. Those portions of the bypass indications which, when faulted, could reduce the independence between redundant safety-related systems are electrically isolated from the protection circuits.~~

**Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems —** The safety-related system designs conform to the single failure criterion. However, this guide is outdated in that it endorses an earlier version of IEEE 379 than that applied to the SBWR (Table 1.9-21). The augmentations of this guide are therefore assumed to be equally applicable to the later Institute of Electrical and Electronic Engineers (IEEE) version, although the section references in the guide may not correlate.

**Regulatory Guide 1.62 - Manual Initiation of Protective Actions —** Manual initiation of the protective action is provided at the system level for all safety-related systems.

**Regulatory Guide 1.75 - Physical Independence of Electric Systems —** This guide is outdated in that it endorses an earlier version of IEEE 384 than that applied to the SBWR (Table 1.9-21). The augmentations of this guide are therefore assumed to be equally applicable to the later IEEE version, although the section references in the guide may not correlate.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.7**

The application of high technology semiconductor electronics components has resulted in high current densities in some portions of equipment used in non-nuclear application. Identify how these higher current densities, which can result in localized hot-spots that can damage the electronic components, will be considered in the design. Is there provision in the design for monitoring hot-spots and high localized temperature? When designing the electronic equipment, will thermal analysis be performed of the electronic boards? What method of cooling is being considered in the design, forced or natural circulation?

**GE Response:**

Computing devices used for SBWR instrumentation are designed to utilize the lowest power components available for the task. Technologies such as CMOS and low power Schottky, including high speed and advanced versions, will be the standard device types used for all functions, including the microprocessor. The emphasis is on low stress design; when these components are operated within their voltage and current ratings and at their specified clock frequency, no unusual heat stresses will occur within the semiconductor materials. As much as possible, all components shall be of the high reliability type or adequately screened and burned-in to ensure high reliability.

The only likely areas of high current density will be in the power semiconductors of solid-state load drivers. The effects of these localized hot spots will be mitigated by proper heat sinking and ventilation of the local area, following the component vendor's recommendations. High power devices will be physically separated as much as possible from low power circuitry.

To ensure that adequate compensation for heat rise is incorporated into the design, a COL licensing information thermal analysis will be performed at the circuit board, instrument and panel design stages. The heat release by internal panel components shall not raise the internal temperature of a panel to great than 15°C above external ambient temperature of the equipment room for electronic components within a chassis or within any printed circuit file structure. Convective cooling is assumed; cooling fans, particularly for safety-related equipment, are not recommended for mounting within instruments or panels. However, if fans are used to increase reliability of equipment located in high density panels or high temperature areas, no credit shall be taken for forced-air cooling in the thermal analyses. since it is intended that all computerized

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.7 (continued)**

instrumentation will be installed in the Main Control Room or in other areas with similar environmental conditions, adequate HVAC will generally be available for proper heat transfer. In case of loss of HVAC, the instrumentation is designed for operation to an ambient temperature of 50°C. Environmental qualification testing of safety-related equipment shall include adequate margin to ensure that this condition can be met under extreme conditions. The minimum margin shall be stated in IEEE-323, Subsection 6.3.1.5. Additional margin will be determined by thermal analysis of the installed equipment areas.

All I&C designs shall meet the environmental criteria stated in the following SBWR requirements documents.

(1) General Electric Environmental Qualification Program, NEDE-24326-1P, Proprietary Document, January 1983.

At the component design level, the methods of MIL-HDBK-217E (or latest revision) shall be used to include environmental stress as part of overall reliability prediction. During the detailed design stage, the Part Stress Analysis Prediction method shall be applied to all parts, using an appropriate environmental factor such as Ground, Fixed (rack mounted, air-cooled, but uncontrolled environment) or Ground, Benign (control room-type conditions). Thermal analysis is an important part of this method; all analyses shall follow the methods described in MIL-HDBK-251, "Reliability/Design: Thermal Applications".

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.8

The SBWR design has active non-safety systems that perform important functions. These non-safety systems need to be operated reliably. To address the needed reliability, provide a discussion of the following:

- a. Overall design verification program for the non-safety equipment that are important to safety;
- b. Software development program, as described in Question 420.3;
- c. Self-test requirements and surveillance test requirements;
- d. Reliability/availability goals; and
- e. The applicable standards and RGs.

**GE Response:**

*(Note: complete responses to items a), b), c), and d) are provided herewith. Response to item e) may be supplemented as deemed necessary following resolution of the Regulatory Treatment of the Non-Safety Systems Issue).*

The non-safety systems control and instrumentation that perform important support functions, identified in the SSAR sections 7.7.2 through 7.7.9, are as follows:

- C11 - Rod Control & Information System (RC&IS)
- C31 - Feed Water Control System (FWCS)
- C82 - Automatic Power Regulator System (APRS)
- C85 - Steam Bypass & Pressure Control System (SB&PCS)
- C91 - Performance Monitoring & Control subsystem (PMCS) of the Process Computer System
- C91 - Power Generation Control Subsystem (PGCS) of the Process Computer System
- C62 - Non-essential Multiplexing System (NEMS)
- C51 - Automated Fixed In-core Probe Subsystem (AFIP) of the Neutron Monitoring System
- T31 - Containment Atmospheric Control System (CACCS) except for the containment isolation function

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.8 (continued)**

a. Design Verification Program

The design verification for the non-safety instrumentation and controls, that are important to safety, uses the same basic process as that applied to the design of the safety system instrumentation and controls.

A structured, engineered approach to the development of both hardware and software is implemented to assure that the design proceeds along the lines of the requirement specifications and documentation.

Verification and validation (V&V) includes the establishment of test and evaluation criteria, the development of the test and evaluation procedures, the testing of the integrated hardware and software, and the installation of the hardware and software in the field.

In accordance with the step-by-step verification process, design reviews are performed at;

- system functional and performance requirements level,
- specification/task analysis and allocation of functions level,
- hardware and software design level,
- test and evaluation criteria and procedures level,
- personnel requirements and operating/maintenance plan level.

Such reviews are conducted by knowledgeable and experienced system engineers, software engineers, hardware engineers, etc., who are not directly responsible for the design, but who may be from the same organization.

An illustration of a typical structure utilized for the controls and instrumentation design can be found in the ABWR SSAR 23A6100, Appendix 7A, Figure 7A-2.

b. Software Development Program

A discussion on the overall software development program (including verification and validation) can be found in the response provided for RAI 420.03.

c. Self-test Requirements and Surveillance Test Requirements

All support functions of the non-safety related systems which are taken credit for in the transient analysis are covered by the surveillance test requirements. These surveillance test requirements are provided in Chapter 16 of the SSAR. In particular the following functions of these systems are to be surveillance tested:

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.8 (continued)

- a) Pressure Isolation Valve functionality of the feedwater system,
- b) Low water level (level 8) trip instrumentation of the feedwater system,
- c) Turbine bypass valve functionality,
- d) Automated Thermal Limit Monitor functionality of the PMCS,
- e) Rod control and display functionality of the RC&IS,
- f) Containment isolation valve functionality of the CACS.

The surveillance test requirements will be supplemented by the plant operational reliability assurance activities (O-RAP) such as periodic surveillance inspections; monitoring of structures, systems and component performance; and/or periodic preventive maintenance. More discussion on O-RAP can be found in the SSAR Subsection 17.3.9.

- d. Reliability/availability goals  
These non-safety systems are designed and maintained with a high degree of reliability commensurate with the importance of the system's contribution to the overall plant reliability/availability. There are no specific quantitative reliability/availability goals for these systems. More discussion on the SBWR plant systems' reliability goals can be found in the response to RAI 420.12.
- e. Applicable Standards and Regulatory Guides  
These non-safety systems are not required to meet the exclusive safety criteria and standards applicable to the design of those systems which perform safety-related functions. However, as listed in Tables 3.2-1 and 7.1-1, the 10CFR50.55 General Design Criteria 13 and 19, ISA S67.02 and Regulatory Guide 1.151 have been used as a basis for design procedures established for these non-safety systems.

*(Note: More information on the applicable standards and Regulatory Guides can be provided later under the discussion and/or closure of Regulatory Treatment of the Non-Safety Systems).*

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.12

What are the reliability/availability goals for the reactor protection system and engineered safety features (ESFs) systems? In addition, what testing will be done to demonstrate reliability and what is the scope of each test? The discussion should also include the method used in determining the system reliability/availability.

**GE Response:**

SBWR System Reliability

Each SBWR system is designed to be as reliable as or more reliable than corresponding systems in currently operating BWRs. This is accomplished in the SBWR by having system design based on existing systems, in cases where current experience is acceptable, or by incorporating design improvements that will enhance system reliability. Examples of the latter are the use of fault-tolerant digital controls with automatic self-checking capability in some systems and the use of two-out-of-four logic instead of two-out-of-two or one-out-of-two twice logic in other systems, such as the instrumentation and control equipment.

The SBWR is designed to meet top level availability and reliability requirements specified by the ALWR URD. These requirements include a frequency of unplanned automatic scrams less than one per year, a core damage frequency (CDF) less than E-5, and an overall plant availability at least 87%. The SBWR Reliability, Availability and Maintainability (RAM) Program has the responsibility of allocating system contributions to plant unavailability so that total unavailability is no greater than 13%.

Instrumentation and control systems are designed with reliable components and configurations so that they will contribute positively to the systems to which they apply. By keeping mean time between failures (MTBFs) high and mean time to repair (MTTR) low, the designers are able to assure high system reliability.

For most systems there is not a specific reliability goal, but the system reliability is evaluated by the system's contribution to the plant core damage frequency, and the plant availability (or unavailability). As long as the overall plant goals for CDF, scram frequency and unavailability are met, and no one system is a predominant contributor to these major goals, individual systems are judged to have acceptable reliability.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.12 (continued)

Some systems' reliabilities are calculated for specific events or sequences. For example, the Reactor Protection System (RPS) reliability is calculated by fault tree for some of the ATWS sequences and entered into the event trees at the appropriate step. As mentioned above, as long as the CDF is less than its goal, and the RPS is not a conspicuous contributor to the CDF, the RPS reliability is judged to be acceptable. Calculated values for RPS reliability can be seen in the PRA event trees in Figures 19AD-25a, -26a, 17a, -28a and -29a.

In summary, as long as the overall plant goals are achieved and no one system is a dominant contributor to plant unreliability or unavailability, specific goals for individual systems are not specified.

Testing

The testing which will be used to demonstrate the RPS and ESF systems readiness/ availability to perform the intended system function(s) is same as that discussed in ABWR SSAR Subsection 7.1.2.1.6 "Protection System Inservice Testability", starting on Page 7.1-7.

The methodology which will be used in determining the system reliability/availability is based on ANSI/IEEE std. 352 and will comprise one or more of the following elements:

- 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)



**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.14**

Provide a list of the reactor protection system supporting equipment, such as air conditioning systems. If these supporting equipment are non-Class-1E equipment, what are the reliability requirements of the supporting equipment, and explain how they are isolated from the RPS. Would the failure of any of the supporting equipment reduce the reliability of the RPS? (Reference SSAR Section 7.2.1.)

**GE Response:**

RPS Supporting Equipment

- Control Room Area
  - Control room envelope HVAC
  - Class 1E 120 VAC for manual controls
  - Essential multiplexing system
  
- Reactor Building divisional "Clean Areas" (outside secondary containment)
  - Clean area ventilation system
  - Class 1E 125 VDC (4 divisions) for protection system logic
  - Safety System Logic and Control (SSLC) cabinets
  - Essential multiplexing system
  
- Reactor Building inside secondary containment
  - Controlled area ventilation system
  - Two divisions of class 1E 120 V vital AC (UPS) for scram pilot valve solenoids
  - Two divisions of class 1E 125 VDC for the backup scram valve solenoids.

RPS has a high probability of performing its safety-related reactor trip function on demand because of its redundant, 4-division, logic arrangement; physical and electrical independence; functional separation; fail-safe trip design; and in-service testability. As stated in SBWR SSAR Section 7.2.1.1(14): "The RPS will fail into a safe state if conditions such as disconnection of the system or portions of the system, loss of electrical power, or adverse environment are experienced." In addition, per Section 7.2.1.1(12): "...The RPS is capable of accomplishing its safety-related protection functions in the presence of any single failure within the RPS, all failures caused by the single failure, and all failures caused by any design basis event that requires RPS protective action."

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.14 (continued)**

All automatic safety functions of RPS are located within the reactor building safety envelope in four divisionally separated clean areas. These areas are cooled by the clean area ventilation system (CLAVS), which is a subsystem of the reactor building HVAC system. CLAVS is not safety-related, but has redundant exhaust fans for normal use and redundant smoke exhaust fans that are used only when necessary (see SSAR Section 9.4.6). CLAVS will maintain the areas where RPS equipment is located to within 29°C (85°F). However, RPS and its supporting SSLC logic do not depend upon HVAC for a safe-state response to abnormal conditions, since the equipment is operable in the long term to at least 50°C (122°F). Moreover, as discussed above, failure of multiple RPS channels results in a fail-safe trip output, de-energizing the scram pilot valve solenoids. Manual scram, which directly breaks the power source connections to the solenoids, is hardwired outside of the electronic trip logic.

Manual actuation functions of RPS are located within the Sealed Emergency Operating Area (SEOA). These functions are:

- Manual scram
- Reactor mode switch (causes scram in shutdown mode)
- CRD header charging pressure trip bypass
- NMS coincident/non-coincident trip selection switch
- Auto-scram test

The control room envelope HVAC (CREHVAC) system cools this area during normal operation. Although non-safety-related, CREHVAC has a redundant, qualified, safety-related function of automatically isolating the SEOA on detection of high airborne radioactivity, toxic gases, and smoke (see SSAR Sections 6.4 and 9.4.1). The habitability features within the SEOA will permit operating personnel to perform manual safety-related actions as necessary.

The loss of supporting equipment does not reduce the reliability of RPS to perform its trip function on demand, but can bring the system closer to an inadvertent trip (which is, however, a safe-state response). The most significant contributors to RPS reliability are the dual 2-out-of-4 trip configuration (2-out-of-4 sensor channels for a trip decision and 2-out-of-4 trip systems for an output scram decision); continuous, on-line self-diagnostics; rapid, on-line, replacement capability for failed parts; and fail-safe equipment design.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.14 (continued)

Loss of single divisions of vital AC electrical power will at most cause a half-scam (if Division II or Division III power is involved), but this would require loss of the divisional inverters which provide Class 1E DC support of vital AC. Loss of two or more divisions of power results in reactor scram.

As discussed above, the equipment that performs RPS functions, including the essential multiplexing system, is qualified to at least 50°C for continuous operation. Nevertheless, assuming component failures at high temperatures, the result will generally be a safe-state trip response because of the fail-safe trip design. However, assume a worst-case loss of all HVAC in the Reactor Building clean areas such that an *undetected* common-cause failure occurs on rising temperature that locks all four divisions of RPS in an *untripped* state concurrent with a demand for automatic trip. Even this unlikely condition is mitigated by the availability of diverse reactor vessel water level and pressure sensors hardwired directly to the control room displays. These displays enhance the operator's ability to perform the manual scram function, which is implemented outside of the RPS electronics and simply breaks the power source connection (placing the reactor mode switch in shutdown position causes the same action). In addition, anticipated transient without scram (ATWS) features are available (with diverse automatic and manual actuation), such as alternate rod insertion (ARI) capability, standby liquid control system initiation, and feedwater runback. These functions are implemented in logic that is diverse from RPS so that even if subjected to the same abnormal environment, will not fail common-mode at the same time.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.15**

Using a block diagram, describe the reactor protection system power distribution system. In addition, identify any non-Class 1E equipment connected to the Class 1E power supply. If any non-1E equipment is connected to the RPS power distribution system, explain how this non-1E equipment is isolated from the 1E power system, and explain the reasons for connecting non-1E equipment to 1E power supply. In addition, explain how the SBWR design complies with General Design Criteria 17 and 18, IEEE Standard 308-1974, and RG 1.32. (Reference SSAR Section 7.2.1.)

**GE Response:**

A block diagram showing power distribution for the reactor protection system (RPS) is provided in Figure 420.15-1. As shown in this diagram the 120 Vac divisional distribution panel is normally supplied from the plant normal preferred power source and is backed-up by four other sources, viz., plant alternate preferred, on-site standby diesel generator, 125 Vdc (2 hour) batteries and on-site transportable diesel generator sources. With multiple power sources and four separate and independent divisions of power distribution, a loss of any single power source will not cause sufficient instrument channel trips or solenoids de-energized to result in full reactor scram or insertion of control rods of any of the four scram groups. This arrangement provides a high degree of power supply availability and helps reduce the unplanned scrams.

A simplified schematic diagram showing power distribution for the RPS actuators can be found in the SSAR Figure 7.2-1 and an SSLC system interface diagram including RPS functions can be found in the SSAR Figure 7.3-3 (this figure is a GE proprietary information).

The Class 1E 120 Vac and 125 Vdc divisional power system shown on the block diagram 420.15-1 supplies power exclusively to safety loads and there are no non-Class 1E loads connected to these power supplies.

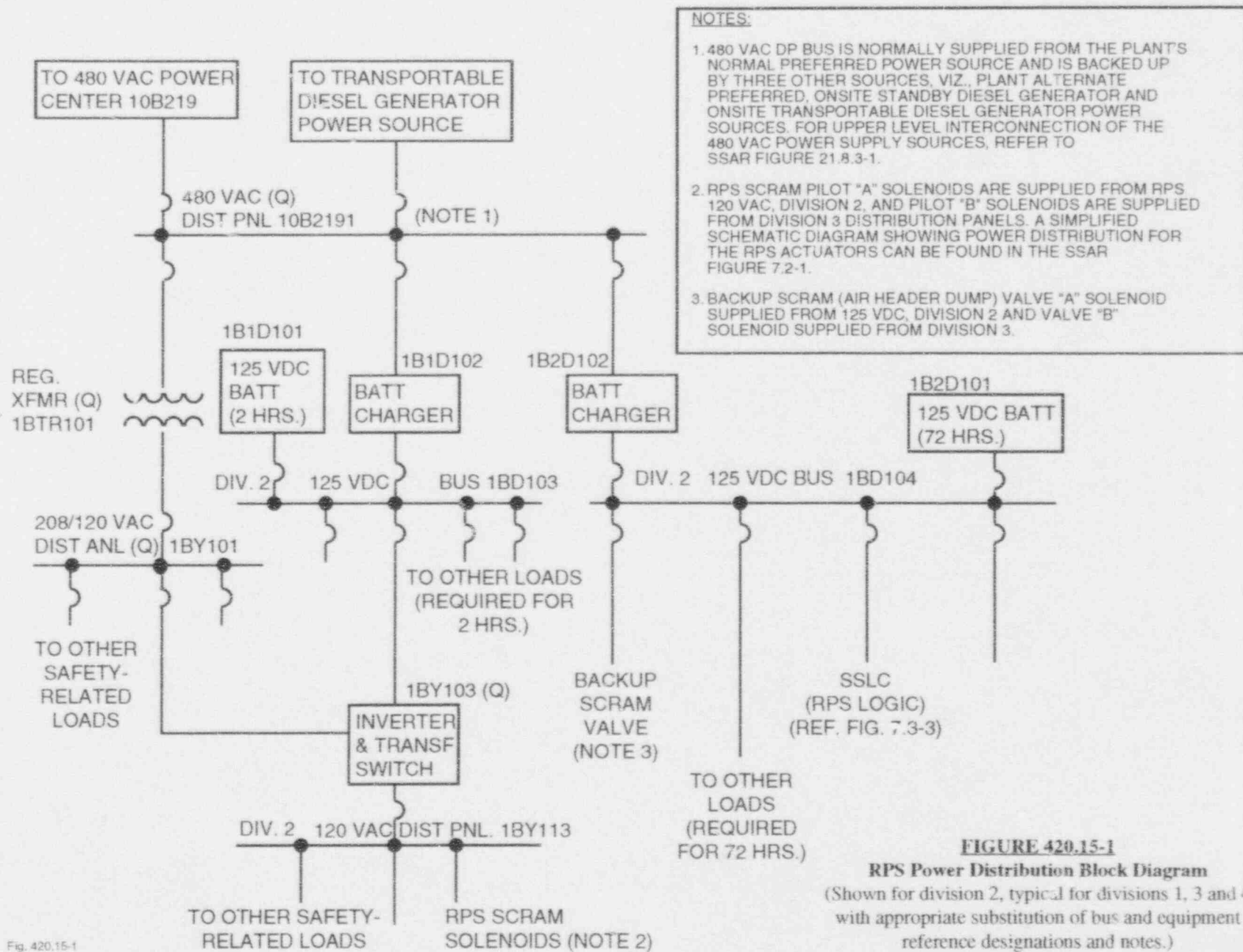
Discussion on compliance with the General Design Criteria 17 and 18 for the plant ac power supply systems including the RPS power distribution is provided in the SSAR subsections 3.1.2.8, 3.1.2.9 & 8.3.1.2.1. As far as the Regulatory Guide 1.32 and its associated IEEE Std. 308 (SBWR SSAR Table 1.9-3 lists 308-80 as opposed to 308-74 indicated in the RAI) are concerned they have a much broader scope than the RPS power distribution system. As for the conformance with the requirements of IEEE std 308-80 criteria 6.2.2 and 6.3.2, the Class 1E AC and DC start and operate all their required loads, each division of the distribution system is physically separate and

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.15 (continued)

electrically independent from other divisional equipment with no provision for automatic interconnection of redundant loads, and distribution equipment auxiliary devices supplied from the related bus or bus section. For a conformance statement on the RG 1.32 refer to the SSAR subsections 8.1.5.2.3, 8.1.6.3, 8.2.2 and 8.3.2.2.2.



- NOTES:**
1. 480 VAC DP BUS IS NORMALLY SUPPLIED FROM THE PLANT'S NORMAL PREFERRED POWER SOURCE AND IS BACKED UP BY THREE OTHER SOURCES, VIZ., PLANT ALTERNATE PREFERRED, ONSITE STANDBY DIESEL GENERATOR AND ONSITE TRANSPORTABLE DIESEL GENERATOR POWER SOURCES. FOR UPPER LEVEL INTERCONNECTION OF THE 480 VAC POWER SUPPLY SOURCES, REFER TO SSAR FIGURE 21.8.3-1.
  2. RPS SCRAM PILOT "A" SOLENOIDS ARE SUPPLIED FROM RPS 120 VAC, DIVISION 2, AND PILOT "B" SOLENOIDS ARE SUPPLIED FROM DIVISION 3 DISTRIBUTION PANELS. A SIMPLIFIED SCHEMATIC DIAGRAM SHOWING POWER DISTRIBUTION FOR THE RPS ACTUATORS CAN BE FOUND IN THE SSAR FIGURE 7.2-1.
  3. BACKUP SCRAM (AIR HEADER DUMP) VALVE "A" SOLENOID SUPPLIED FROM 125 VDC, DIVISION 2 AND VALVE "B" SOLENOID SUPPLIED FROM DIVISION 3.

Fig. 420.15-1

**FIGURE 420.15-1**  
**RPS Power Distribution Block Diagram**  
 (Shown for division 2, typical for divisions 1, 3 and 4 with appropriate substitution of bus and equipment reference designations and notes.)

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.16

The second sentence of the second paragraph of SSAR page 7.2-13 on bypass indication states that indicator lights indicate which part of a system is not operable. Clarify whether these indicator lights indicate the bypass or inoperability of portions of a system that performs a function important to safety. (Reference SSAR Section 7.2.1.2.1 and RG 1.47.)

GE Response:

Bypass Indicator Lights

The indicator lights do signify the bypassing of portions of systems important to safety, namely Reactor Protection System (RPS) and Engineered Safety Feature (ESF). The bypass functions and their alarm status are clearly identified in SSAR section 7.2.1.5.2. Operational bypasses are essentially interlocks that permit or inhibit specific functions under stated conditions, while maintenance bypasses remove larger portions of RPS from service for repair, calibration, or test.

All bypass functions are safety-related and are incorporated into the divisional circuitry. Interlocking of bypass status among divisions to prevent multiple bypasses is performed over isolated signal paths. Automatic indication of each bypass or inoperable condition is implemented in conformance to RG 1.47. These indication provisions serve to supplement administrative controls and aid the operator in assessing the availability of component and system level protective actions. This indication does not perform a safety-related function.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.18

Identify any on-line test equipment or circuits that are not part of the safety-related system. Also describe the interface between the safety-related system and the on-line test equipment. Show that faults in the test equipment will not challenge the system or equipment being tested. Explain how all four channels of reactor protection system are tested without violating independence/isolation criteria. Describe the process (configuration management) that will be incorporated at operating facilities when on-line diagnostics uncovers an error in the computer system. (Reference SSAR Section 7.2.1.4.)

**GE Response:**

On-line Test Equipment for RPS

All on-line test functions are safety-related. On-line testing of Reactor Protection System (RPS) is performed by:

- 1) Built-in self-test software and hardware contained in each microprocessor-based control unit,
- 2) Monitoring functions contained in non-microprocessor logic circuits,
- 3) Manual test switches,
- 4) Manual control switches, with portions of the logic channels bypassed and the remaining portions in a state of reduced, but safe, redundancy.

On-line testing never violates the independence and separation of the four RPS divisions because automatic cross-division tests are not performed. Instead, because of the digital multiplexed nature of RPS data communications, continuous diagnostics within the on-line self-test for each controller monitor each I/O communication path for operability and also monitor the logic for correct timing and general operability. However, the diagnostics do not insert trip signals or otherwise cause changes of state in the trip signal path. Trip testing within a division of sensor channels is performed only when divisional system level bypasses are applied, thus blocking the final output to the actuators; or off-line during a maintenance outage, when simultaneous 4-division testing is possible. Conventional half-scam actuator testing is also performed as specified in the plant technical specifications.



RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.18 (continued)

On-line detection of errors in any safety-related controller results in an inoperable indication to the operator. The operator then, as appropriate, places the affected division of sensors in bypass at the input to the TLU or takes the division out of service after the output of the TLU. Even on a second failure of a given sensor channel, the operator can place an individual sensor channel within a division in a trip condition. Thus, there is no need for automatic bypass because any single failure within one division results in a safe-state condition (i.e., either a 2-out-of-3 or 1-out-of-3 condition for trip output, depending upon the failure state). As described in the ABWR Technical Specifications (ABWR SSAR Chapter 16, LCO 3.3.3.1), the operator is given 6 hours to place the failed channel or division in trip or bypass, respectively. Repair of the failed equipment is facilitated by automatic identification of the failed equipment and its location to the lowest replaceable module level via the on-line diagnostic facilities.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.19

Discuss the reactor protection system automatic testing features' compliance with RG 1.22, RG 1.118, and IEEE Standard 338. (Reference SSAR Section 7.2.1.4.)

**GE Response:**

Reactor Protection System (RPS) Automatic Test Equipment Compliance with RG 1.22, RG 1.118, and IEEE Std 338

SBWR SSAR Section 7.2.1.3 states RPS compliance with RG 1.22, RG 1.118, and IEEE Std 338. Automatic testing, in conjunction with the 2-out-of-4 sensor channel and trip channel arrangement, augments conventional manual methods and eliminates the need for lifted leads and jumpers. The continuous self-diagnostics enhance the periodic testing requirements of RG 1.22 and RG 1.118 by quickly detecting logic and hardware failures. The bypassable 2-out-of-4 voting logic configuration permits temporary bypass of sensors or trip channels so that in-depth off-line testing (without final actuator trip) can be performed with the off-line self-tests built-in to the logic controllers or with the manual divisional trip controls, which permit half-scam testing of the scram pilot valve solenoids. In this way, complete system testing by means of overlap testing (per IEEE Std 338) is possible. Intervals for these tests are specified in the plant technical specifications (SSAR Chapter 16). The types of tests performed are given in SSAR Section 7.2.1.4. During a maintenance outage, external automatic self-test controllers are connected in each division for rapid end-to-end testing of all four divisions simultaneously.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.20

Provide a single failure analysis of the reactor protection system as part of the failure modes and effects analysis (FMEA) in response to Question 420.1.c. (Reference SSAR Section 7.2.1.)

GE Response:

Single Failure Analysis of Reactor Protection System (RPS)

A single failure analysis is provided within the documents referenced in the response to RAI 420.1(c), namely the SBWR PRA in SSAR Chapter 19 and the LLNL Diversity and Defense-in-Depth Study. However, a concise description of the single failure capability of RPS is provided in SSAR section 7.2.1.4, which is quoted below:

"The RPS is designed to provide reliable single-failure-proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. The RPS remains single-failure-proof even when one entire division of channel sensors is bypassed and/or when one of the four automatic RPS trip logic systems is out-of-service. This is accomplished through the combination of fail-safe equipment design, the redundant two-out-of-four sensor channel trip decision logic, and the redundant two-out-of-four trip systems output scram logic arrangement utilized in the SSLC/RPS design.

All equipment within the RPS and within the RPS-related portions of the SSLC System is designed to fail into a trip initiating state on loss of power, loss or disconnection of any input signal, or loss of any internal or external device-to-device connection signal. In conjunction with this fail-to-safe-state design, the trip initiating logic signals to and within the RPS are asserted low (i.e., "0" to scram) whereas trip bypass logic signals and trip bypass permissive logic signals are asserted high (i.e., "1" to bypass and "0" to release bypass)."

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.21**

RG 1.47 requires that manual capability exist in the control room to activate each system-level indicator provided in accordance with Regulatory Position C.1. This position states that administrative procedures should be supplemented by a system that automatically indicates at the system level the bypass or deliberately induced inoperability of the protection system and the systems actuated or controlled by the protection system. Explain how SBWR complies with this RG 1.47 position. (Reference SSAR Section 7.2.1.5.3.)

**GE Response:**

The reactor protection system (RPS) instrumentation and control design implements the Regulatory Guide 1.47.

Individual indicator lights are provided to indicate divisional sensor and division out of service bypasses and inoperabilities/out of service. The bypass capabilities are included within the safety system logic and control system and are provided by means of bypass switches for trip logic units and digital trip modules. More information on the RPS and ESF bypass capabilities is provided in response to RAI 420.43 and bypass status indication is provided in response to RAI 420.26.

Automatic indicators once activated remain illuminated and cannot be cleared until the function is restored to the operable condition. This automatic activation is provided over and above the manual administrative controls. More discussion on the conformance to Regulatory Guide 1.47 can be found in SSAR subsection 7.2.1.3. Information on the manual actuation of system level bypass indications is also provided in response to RAI 420.24.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.22

Explain how the reactor protection system complies with RG 1.62, Regulatory Positions C.2 and C.3. (Regulatory Position C.2 of RG 1.62 on manual initiation of protective actions requires that manual initiation of a protective action at the system level perform all actions performed by automatic initiation. Regulatory Position C.3 states that the switch for manual initiation of protective action at the system level should be located in the control room and be easily accessible to the operator so that action can be taken in an expeditious manner.) In addition, explain how the RPS complies with Regulatory Position C.5 of RG 1.62, which states that manual initiation of protective actions should depend on the operation of a minimum of equipment. (Reference SSAR Section 7.2.1.)

GE Response:

- **Compliance with RG 1.62, Position C.2:**  
Reactor scram in SBWR, like other BWRs, is accomplished by interruption of AC power to scram solenoids and supplying DC power to back-up scram solenoids. The scheme for controlling electrical power to scram and backup scram solenoids is graphically presented in Figure 7.2-1 of the SSAR. Load-drivers (contacts) designated by small letters are controlled by automatic scram logic of RPS; whereas, load-drivers designated by capital letters are controlled by manual scram logic of RPS. As can be seen, the end-result for either automatic or manual scram is interruption of divisional AC power to scram solenoids and supply of divisional DC power to back-up scram solenoids.
- **Compliance with RG 1.62, Position C.3:**  
On Page 7.2-14, first paragraph, the location for manual scram push-buttons is determined to be on the principal control room console which is easily accessible to the operator.
- **Compliance with RG 1.62, Position C.6:**  
As depicted in Figure 7.2-1 and Figure 21.7.2-2, sheets 47 and 48 of the SSAR, the manual scram equipment and devices are limited to manual scram push-buttons and relay logic associated with contacts designated by capital letters. In essence, this is the minimum equipment for implementation of manual scram. The details of manual scram logic is depicted on sheets 47, 48, and sheets 53 through 56 of Figure 21.7.2-2 of the SSAR.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.24

Do all system-level bypass indicators have the manual capability to be activated according to Regulatory Position C.4 of RG 1.47? List any bypass that does not have manual-activation capability and explain the reasons for not having it. (Reference SSAR Section 7.2.1.3.)

GE Response:

Manual Actuation of System Level Bypass Indicators per RG 1.47

Reactor Protection System (RPS) cannot be bypassed on an overall system level (which would inhibit automatic scram), but because of its 4-division, 2-out-of-4 trip configuration, up to an entire division of trip logic can be bypassed. No provided bypass can render the system inoperable; likewise, no single failure can render the system inoperable. However, each type of divisional bypass (division-of-sensors or division out-of-service), although manually induced, is automatically indicated in the main control room. All operational and maintenance bypasses, along with their automatic and manual activation capability, are described in SBWR SSAR Section 7.2.1.5.2. Note that automatic operational bypasses are actually normal responses to changes in plant operating modes and do not cause system inoperability, so do not need to conform to the manual bypass indicator activation requirement. All manual operational and maintenance bypasses have indication. This includes logic controllers being placed in an off-line condition or circuit cards being removed from their connectors (card-out-of-file indicator).

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.25

Describe the built-in interlocks that will prevent a simultaneous bypass of more than one channel. Provide a list of bypasses that do not have this interlock capability and provide justifications for not having it. (Reference SSAR Section 7.2.1.3.)

GE Response:

Bypass Interlocks

The division-of-sensors and division-out-of-service (trip logic unit bypass) bypasses can be applied independently because each reduces the system redundancy at its point of application to no worse than a 2-out-of-3 condition. However, each type of bypass is interlocked divisionally among its redundant channels such that a second bypass of that type cannot be activated if a previous bypass has not been removed. The interlock arrangement is illustrated in Figures 420.43-1 and 420.43-2, which are attached to the response for RAI 420.43. These figures are similar to those appearing in the ABWR SSLC Hardware/Software System Specification, 23A6915, Rev. 0, but have been revised to apply to the SBWR configuration. Bypass status transmitted across divisional boundaries is electrically and physically isolated among divisions.

All other bypasses are applied to specific operational functions, as indicated in SSAR Section 7.2.1.5.2, and are required to be applied in four divisional channels. Thus, interlocks are not required for these bypasses.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.26

Does all equipment have a bypass status indication local to the equipment to provide information to maintenance personnel. (Reference SSAR Section 7.2.1.3.)

GE Response:

Local Bypass Status Indication

Bypass status indication is displayed on each Safety System Logic and Control (SSLC) panel located in each reactor building divisional clean zone. These panels contain all Reactor Protection System (RPS) logic processing equipment. The local multiplexing unit (LMU) cabinets in each clean zone, which acquire sensor data for RPS, also indicate bypass status.



RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.27

Describe how the bypass indicators are grouped in the control room.  
(Reference SSAR Section 7.2.1.3.)

**GE Response:**

Individual indicator lights are arranged together in the control room to indicate which function of the system is out of service, or otherwise inoperable. Two types of channel bypasses are provided, division-of-sensors bypass and division-out-of-service (or division maintenance) bypass. All bypasses are alarmed (per division) in the main control room. At the operator display, bypass indications are grouped near the sensor trip alarms. More discussion on the RPS and ESF trip logic bypass arrangement and processing is provided in response to RAI 420.43.

A general discussion on the control room fixed-position alarms is provided in the SSAR Subsection 18.4.2.12 and discussion on alarm processing logic is provided in Subsection 18.4.2.13. A discussion on system level (conceptual) grouping philosophy for the RPS bypass indications can be found in Subsection 7.2.13.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.28

Identify the reports that will be provided to support any aspects of the neutron monitoring system design that are different relative to designs previously reviewed by the staff. (Reference SSAR Section 7.2.2.)

**GE Response:**

The report that supports the Automated Fixed In-Core Probe (AFIP) subsystem (addressed in Section 7.7.8) of the neutron monitoring system is included in the SBWR SSAR, Appendix 7A, "A Fixed In-Core Calibration System for the Neutron Monitoring System".

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

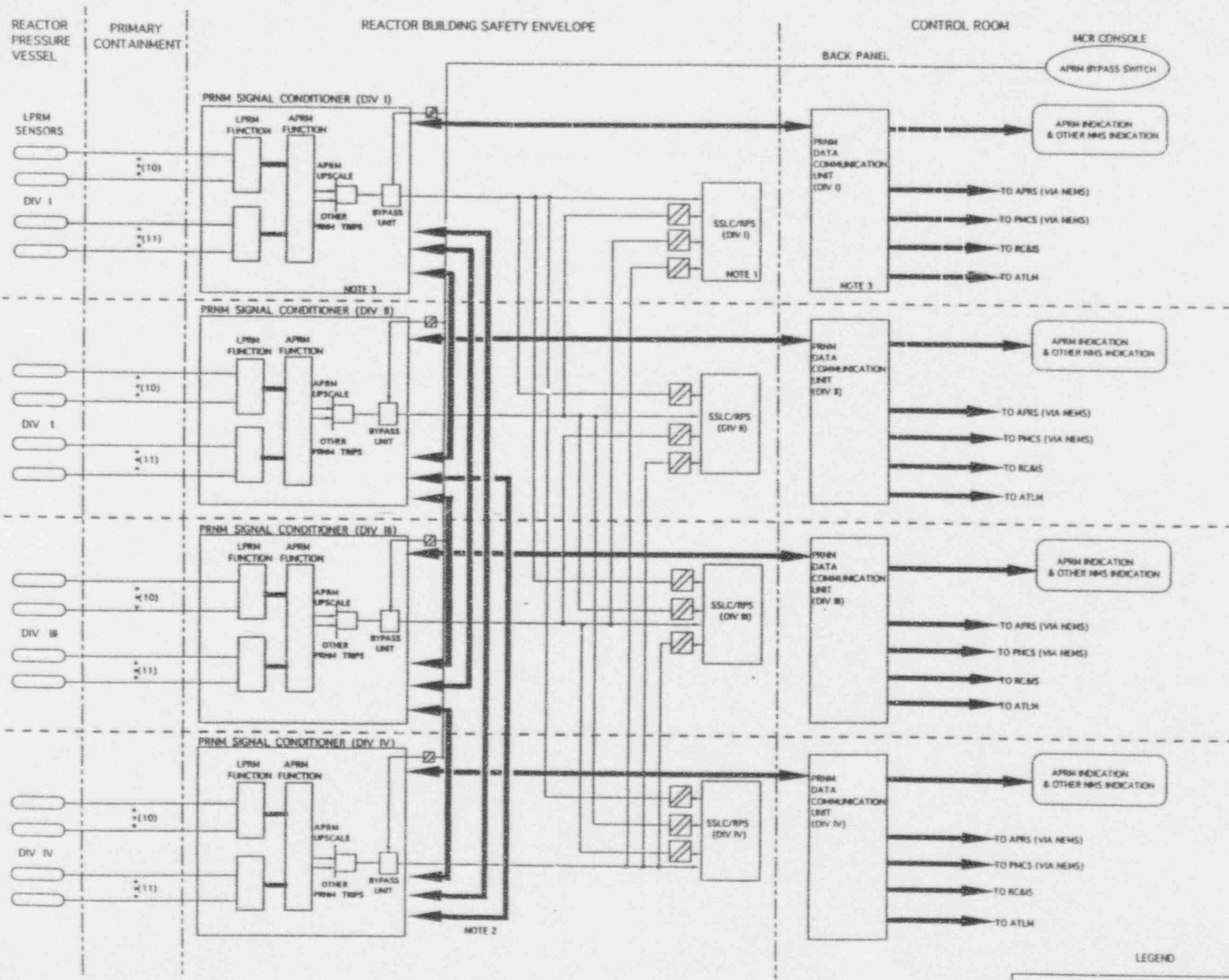
---

**RAI 420.29**

Using block diagrams, describe the operation of the reactor protection and safety monitoring system for a average power range monitor upscale trip. The description should trace the transmission of the initiating signals from the sensors through the integrated protection cabinets, the engineered safety features actuation cabinets, and the monitoring and controls at the control room work station to the actuated devices. The diagram should also include all the major components, such as the sensors, the signal conditioners, the isolation devices, the multiplexers, the data buses, the indicators, the protection cabinets, and control rod drive system. The diagram should show all channels and components and interfaces. (Reference SSAR Section 7.2.1.)

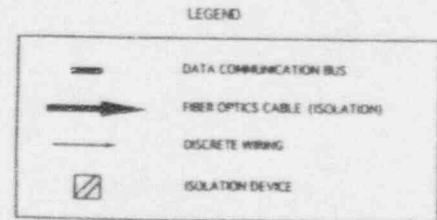
**GE Response:**

See attached Figure 420.29-1 of NMS block diagrams. Figure 420.29-1 shows the initiating signals from the sensors, through the signal conditioner, to the reactor protection system. Figure 7.3.2B of the SBWR SSAR shows the signals from the SSLC/RPS to the actuation devices. The neutron monitoring system safety related trip signals use a dedicated data transmission path to the safety system logic control (SSLC) and reactor protection system (RPS) and do not go through the essential multiplexing system (EMS). Other NMS signals going to the plant monitoring & control system (PMCS) and automated power regulation system (APRS) go through the non-essential multiplexing system (NEMS) first. This is illustrated in Figure 420.29-1. The NMS also has a dedicated data transmission pathway to the rod control & information system (RC&IS) and its subsystem, the automated thermal limit monitor (ATLM).



NOTE 1 FOR SIGNAL TRANSMISSION WITHIN SSLC/RPS & TO ACTUATOR DEVICES REFER TO FIG 7.3.2B OF THE SBWR SSAR.  
 2 CROSS-CHANNEL DATA COMMUNICATION OF THE PARTIALLY AVERAGED APRM SIGNAL FROM EACH CHANNEL.  
 3 FOR DETAILED DESCRIPTION OF LOCAL AND BACK PANEL INDICATORS REFER TO NMS I/O (FIG 21.7.2-3) AND I/O (FIG 21.7.2-4).

**Figure 420.29-1 Block Diagram  
 Neutron Monitoring System APRM Trip To SSLC**



REF. RAI 420.29

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.30

Describe a startup range neutron monitor (SRNM) signal and the connections between a SRNM detector and preamplifier in the reactor building. Explain how the SRNM detector signals transmitted to preamplifiers are protected from the noises and interferences in their environment. (Reference SSAR Section 7.2.2.2.)

**GE Response:**

The SRNM detector is a regenerative uranium coated fission chamber that upon receiving a neutron in the detector will generate a negative pulse (voltage signal) out of the detector. The SRNM detector is housed in a dry tube assembly, with the sensor located near the mid plane of the active fuel region in the core. The SRNM signal is transmitted via a triaxial cable from the bottom of the RPV, through the RPV pedestal, to a preamplifier located on the immediate outside of the primary containment boundary. The number of pulses generated is proportional to the neutron flux level and thus the reactor power level. The SRNM combines the function of both the source range monitor (SRM) and the intermediate range monitor (IRM) of conventional BWRs. The SRM uses the pulse counting method which covers from 0.1 counts per second (CPS) to about 1000,000 CPS. The IRM uses the mean square voltage (MSV) method when the counting pulses per second is greater than 100,000 CPS and the pulses can no longer be differentiated from each other. The SRNM thus cover the range from 0.1 CPS to about  $1.5 \times 10^{13}$  nv, which is approximately 15% of rated power and higher. The preamplifier can process both counting pulses and MSV signals, with adjustable gain and pulse shaping capability. One SRNM detector is connected to one preamplifier, with a triaxial cable (with the signal conductor insulated and shielded) in between. In order to reduce noise, the length of the triaxial cable is kept to a minimum, corresponding to the shortest distance from the RPV under vessel to the outside wall of the primary containment. The SRNM triaxial cable is Class 1E and environmentally qualified to operate under both normal operating conditions and design basis accident conditions. The preamplifier is housed in a metal case to shield from outside electromagnetic interference. As a result, noises are minimized through the triaxial cable design, the proper grounding method performed between the detector ground, cable ground and the preamplifier ground, as well as through the metal protection case of the preamplifier. More detailed description of the SRNM can be found in the licensing topical report, NEDO-31439-A, submitted to the NRC in Oct. 1990.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.31**

Provide a discussion of how the neutron monitoring system (NMS) instruments are tested. The discussion should also include the requirements with which NMS instruments must comply. (Reference SSAR Section 7.2.2.4.)

**GE Response:**

The neutron monitoring system testing is performed routinely as part of the surveillance test, after the instrument is installed and has successfully passed the validation test including the preoperational test and the startup test.

The NMS instrument surveillance tests include the following test items:

1. Channel Check: This is a qualitative assessment by observation of channel behavior during operation. It includes comparison of the channel indication to other indications derived from independent instrument channels measuring the same parameter.
2. Division Function Test: The injection of simulated or actual signals into a division as close to the sensors as practicable to verify operability of the sensor channel in that division.
3. Comprehensive Function Test: This is a set of tests that exercise RPS/ESF actuation functions, etc., by simulating accident events that exercise the inputs and outputs of the SSLC, NMS, RPS actuation logic, etc. It also simulates power failures, measures CPU and network performance, runs microprocessor-specific and application-specific diagnostics.
4. Sensor Channel Calibration: This is the adjustment of the sensor channel such that it responds within the specified range and accuracy to specified values of the parameter that the sensor channel monitors.
5. Self Test: For micro-processor based system the self test function is performed automatically within the instrument at a predefined time interval. This includes all critical failure tests of the instrument firmware including inoperative failure, etc. Most self tests are performed at a time interval similar to the computer data processing and calculation interval, e.g. 100 milli-seconds.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.31 (continued)**

**SRNM:**

In Startup mode, the SRNM performance including the neutron flux upscale trip and the short period trip functions shall be tested for 1) Channel Check (every 12 hr), 2) Divisional functional Test (every 7 days), 3) verifying the SRNM and the APRM channels overlap within at least half decade (when first changing mode between the Startup mode and the Run mode), 4) Channel Calibration (18 months), 5) Comprehensive functional test (18 months). The SRNM inoperative trip shall be tested as well in this mode using divisional functional test.

In Refueling Mode, the SRNM performance including the neutron flux upscale trip shall be tested for 1) Channel Check (every 12 hr), 2) Divisional functional Test (every 30 days), 3) Channel Calibration (18 months), 4) Comprehensive functional test (18 months). The SRNM inoperative trip shall be tested as well in this mode using divisional and comprehensive functional test.

In both the Run and Startup modes, the SRNM ATWS Permissive function shall be tested using divisional and comprehensive functional test.

**APRM:**

In Run mode, the APRM performance including the neutron flux upscale trip and the simulated thermal power trip functions shall be tested for 1) Channel Check (every 12 hr), 2) verifying the APRM is consistent with the calculated reactor power (every 7 days), 3) Division functional test (90 days), 4) calibrate the local power range monitor (LPRM) (every 1000 MWD/T core exposure), 5) comprehensive functional test (18 months), 6) verifying trip response time every refueling interval.

In Startup mode, the APRM performance including the neutron flux upscale trip function shall be tested for 1) Channel Check (every 12 hr), 2) divisional functional test (every 7 days), 3) calibrate the local power range monitor (LPRM) (every 1000 MWD/T core exposure), 4) verifying the SRNM and the APRM channels overlap within at least half decade (7 days).

In both the Run and Startup modes, the APRM ATWS Permissive function shall be tested using divisional and comprehensive functional test. In both modes, the APRM inoperative trip shall be tested using divisional and comprehensive functional test.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.31 (continued)

The above test requirements are summarized in the following table. The "SR" refers to the surveillance requirements which are same as those identified in ABWR SSAR 23A6100, Chapter 16, SR 3.3.1.1, Rev. 3. Detailed definition of the above test items and test interval, condition, and bases of the above items, is documented in the SBWR Technical Specification, Chapter 16 of the SBWR SSAR. The current version of the SBWR SSAR Chapter 16 is being revised to reflect the above requirements on the NMS portion which are similar to that of the latest ABWR Tech Spec. (Rev 33).



**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

RAI 420.31 (continued)

Table 1 (420.31) NMS Instrumentation Surveillance Test

<u>Function</u>	<u>Applicable Mode</u>	<u>Surveillance Requirements</u>	<u>Function</u>	<u>Applicable Mode</u>	<u>Surveillance Requirements</u>
<u>SRNM</u>			<u>APRM</u>		
SRNM	Startup Upscale	SR 3.3.1.1.1 SR 3.3.1.1.3 SR 3.3.1.1.8 SR 3.3.1.1.9 SR 3.3.1.1.10	APRM Upscale	Startup	SR 3.3.1.1.1 SR 3.3.1.1.3 SR 3.3.1.1.7 SR 3.3.1.1.8
	Refueling	SR 3.3.1.1.1 SR 3.3.1.1.4 SR 3.3.1.1.9 SR 3.3.1.1.10	TPM Upscale	Run	SR 3.3.1.1.1 SR 3.3.1.1.2 SR 3.3.1.1.5 SR 3.3.1.1.7 SR 3.3.1.1.9 SR 3.3.1.1.12
SRNM	Startup Short Period	SR 3.3.1.1.1 SR 3.3.1.1.3 SR 3.3.1.1.8	APRM Upscale	Run	SR 3.3.1.1.1 SR 3.3.1.1.2 SR 3.3.1.1.5 SR 3.3.1.1.7 SR 3.3.1.1.9 SR 3.3.1.1.12
	Refueling	SR 3.3.1.1.1 SR 3.3.1.1.4 SR 3.3.1.1.9 SR 3.3.1.1.10			
SRNM ATWS Permissive	Run/Startup	SR 3.3.1.1.5 SR 3.3.1.1.9	APRM ATWS Permissive	Run/Startup	SR 3.3.1.1.5 SR 3.3.1.1.9
SRNM	Run/Startup Inop Refueling	SR 3.3.1.1.3 SR 3.3.1.1.4 SR 3.3.1.1.9	APRM Inop	Run/Startup	SR 3.3.1.1.5 SR 3.3.1.1.9

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

**RAI 420.32**

Provide a description of how all four NMS channels are tested without violating independence/isolation criteria. (Reference SSAR Section 7.2.2.4.)

**GE Response:**

(Refer to Figure 420.29-1) As shown in Figure 420.29-1, all four PRNM channels are independent and isolated from one another except the inter-divisional communication through the fiber optics pathways. The fiber optics pathways serve as isolation devices. As a result, the isolation criteria between different divisions is satisfied. Testing of each NMS PRNM channel will not violate the isolation criteria.

The Average Power Range Monitor (APRM) channel is tested for channel check, for divisional functional test, for LPRM calibration, for APRM reading calibration, and for comprehensive functional test. For divisional functional test, the APRM tests the various trip functions and the associated trip setpoints. Such trip functions will be verified by the output of the APRM signal conditioner and the input to the Safety System Logic and Control/Reactor Protection System (SSLC/RPS). The APRM is tested one channel at a time. This test can be performed both with this channel bypassed through the APRM Bypass Switch and with this channel not bypassed. With this channel bypassed, the local trip indication light can be verified for proper trip output. With this channel not bypassed, the trip output at the SSLC/RPS cabinet can be verified for proper trip output. However, only one channel can be tested at any time. Whether this APRM channel is bypassed or not the test is not interfering with the cross channel (division) communication through the fiber optics pathway between divisions. The bypassing of any one APRM channel will not interfere with the data communication through the cross channel (division) communication pathway. The test is performed without violating any independence criteria. For Local Power Range Monitor (LPRM) calibration, the LPRM sensor being calibrated is first bypassed. This LPRM data will be temporarily excluded from the APRM averaging process. The LPRM count circuit will also reduce the LPRM number by one. This is only one LPRM bypassed out of a total of 84 LPRMs. As a result, the channel partial APRM and the total APRM reading is not affected noticeably. Consequently, the LPRM calibration test will not violate the independence criteria.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.32 (continued)**

For APRM reading calibration, the calibration procedure is first for each channel to calculate a partial APRM which is the sum & average of all the primary LPRMs in this channel (primary LPRMs refer to the LPRMs sent to this channel through coaxial cables from the LPRM sensors). The four partial APRMs are then sent to all four channels such that each channel will perform an identical calculation to obtain a total APRM which is the sum & average of the four partial APRMs. Finally, this total sum & average APRM will replace the partial APRM in each channel and become the new partial APRM of this channel, and at the same time this sum & average APRM will be multiplied by a gain adjustment factor such that the resulting value will be equal to the process computer-calculated reactor power (percent of rated). This resulting value is the final APRM value. The update of the partial APRM for each channel is performed one channel at a time with this channel bypassed. After the calibration, the updated partial APRMs from all four channels are all identical.

To summarize the procedure:

- 1) Bypass Division I APRM.
- 2) In division I APRM, verify the latest calculated four partial APRMs from the four divisions, three of them through the fiber optics pathways. Obtain the sum/average value of the four partial APRMs. This is the unadjusted-adjusted APRM. This value is to be used for the calibration of all four channels. That is, this value is locked for the use of all four channels during this calibration process.
- 3) Update the partial APRM in this channel by this unadjusted-adjusted APRM using a partial gain factor applied to the original partial APRM.
- 4) Calculate an APRM Gain Adjustment Factor which is the ratio of the process computer-calculated rated power value to the unadjusted-adjusted APRM. Multiply the unadjusted-adjusted APRM by this Gain Adjustment Factor. The resulted value is the final calibrated APRM.
- 5) Un-bypass Division I APRM.
- 6) Bypass Division II APRM. Repeat steps 2) to 5) for Division II APRM calibration, using the same unadjusted APRM obtained from 2) as the Division II unadjusted APRM.
- 7) Repeat 6) for Division III and Division IV APRMs.

The above APRM calibration test is thus performed without affecting the independence criteria.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.32 (continued)

For the comprehensive functional test, there is no additional concern of independence and isolation criteria compliance other than those discussed above for the neutron monitoring system test.

The SBWR SRNM subsystem design is similar to the ABWR NMS SRNM design, except with the slight reduction of the number of SRNM detectors in the core (from ten to eight). There is no cross division communication in the SRNM. The isolation and independence criteria are satisfied similar to the ABWR SRNM design.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.33**

Describe the methods and design criteria used to reduce the common mode failure vulnerabilities in the hardware and software of the NMS. (Reference SSAR Section 7.2.2.3.)

**GE Response:**

The issue of design consideration to reduce the common mode failure vulnerabilities in the SBWR Neutron Monitoring System (NMS) design can be addressed in the following categories:

1) General NMS System Design Consideration:

The SBWR NMS design generally follows the same design philosophy and general system structure as the ABWR and GESSAR design. The NMS includes safety related subsystems such as the Startup Range Neutron Monitor (SRNM) and the Power Range Neutron Monitoring (PRNM), each subsystem consisting of sensors, cables, signal conditioning electronics and monitoring equipment, etc. As part of the BWR proven design with many operating years of experiences, and as a result of rigorous quality control (QC) and quality assurance (QA) practices, the SBWR NMS has inherited a very good record of extremely low occurrence of any common mode failures. As shown by BWR operating experiences, any common failures of equipment are more or less on a random basis. The SBWR NMS design follows the similar strict reliability and availability requirements as well as QC and QA requirements similar to previous BWR NMS designs, and requirements specified in various regulatory guides and industry standards including RG 1.53, 1.152, IEEE 279, 379, 603, etc.

Compliance to such requirements effectively reduces the common mode failure vulnerabilities from a system design perspective, especially from a system hardware component point of view. Also, safety subsystems of the NMS are designed as single failure proof. Design criteria are established for any failures that should not disable the safety function of each subsystem. For example, the following failures shall not disable the safety function of any subsystem:

- a. A detectable failure from one failed component or circuit fault.
- b. Multiple detectable failures resulting from a single cause. This single cause is either external or internal to the system.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.33 (continued)**

- c. A failure that results from the accumulation of failures that are not detectable by periodic testing. (Such failures can be detected as either dependent or independent failures.)

In addition, a FMEA analysis was performed to evaluate and confirm that for the SBWR PRNM any component failure of the PRNM would not disable the system safety functions.

In summary, the key factors to reduce common mode failure vulnerabilities from system design level are the BWR NMS proven design with good operating records, strict reliability requirements, strict QC/QA requirements, failure detectability criteria, all tied with a step by step systematic design approach of the whole NMS system from the component level and up.

2) NMS Electronics Hardware & Software Design Consideration:

The SBWR NMS utilizes microprocessor based electronics equipment. As a result, additional design requirements are included to assure the reliability of both the hardware and software aspects of the design. In addition to the system level design requirements mentioned above, some hardware and software requirements must be implemented. These include: environmental requirements, reliability requirements, general hardware and software design requirements including component unit self test requirements. A list of important self test requirements are included in the NMS hardware/software specification 23A6301, Rev. 0.. Such self test functions can effectively reduce the common mode failure vulnerabilities.

3) NMS Software Verification & Validation:

Verification and Validation (V&V) is performed on all software contained in the NMS safety related equipment. The V&V procedure basically follows RG 1.152 requirements, which include design review, independent design verification, coding verification, validation test in the laboratory, and field startup test. The V&V can also effectively detect any potential common mode failure scenarios and reduce the common mode failure vulnerabilities. A NMS V&V Criteria Design Specification 23A6761, Rev. 0 (FMF K6/7) document is applicable to SBWR NMS.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.33 (continued)

4) NMS Surveillance Test:

i) Channel Check Requirement

This is a Tech Spec. required surveillance test item that involves qualitative assessment by visual observation of channel behavior during operation. It includes comparison of the channel indication to other indications derived from independent instrument channels measuring the same parameter. It is typically performed every 12 hours during plant normal operation. This check can effectively detect any common mode failure which causes instrument indication to be at fault condition.

ii) Electronics Self Test Requirements

The SBWR NMS uses microprocessor-based electronics units, which have the capabilities of performing automated self testing of routine hardware and software functions including some critical failures detection. For example, the instrument is designed to test itself automatically and continuously during operation to see that its hardware and software are functioning properly. Any faults detected will be traced to the replaceable module level and enunciated as well as displayed. A list of self test requirements is included in Specification 23A6301. The instrument self test will detect "critical" fault and issue inoperative trip. Critical fault includes such items as voltage supply abnormal, high voltage power supply output abnormal, module installation abnormal, microprocessor memory abnormal, etc. These periodical continuous self tests can effectively detect hardware and software failures and reduce the vulnerabilities of common mode failures of the instrument.

5) Safety Protection System Common Mode Failure Assessment:

i) NMS as One of many Inputs to SSLC/RPS

It is important to note that the NMS safety related trip output derived from the NMS safety related function is only one kind of many safety protection trip output signals sent to the SSLC/RPS. For common mode failure assessment of safety protection system, i.e., SSLC/RPS, failure of NMS trip output will not disable the protection function of the safety protection system.

ii) Defense-In-Depth and Diversity Assessment of the SBWR Protection System

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.33 (continued)

A defense in depth and diversity assessment of the SBWR Protection System including event analysis evaluation was performed which is similar to the NUREG-0493 analysis. This assessment was performed by Lawrence Livermore National Laboratory in Sept 1993. The objective of this assessment is to determine if postulated common mode failures could result in impairment of more than one echelon of defense, and thus compromising defense-in-depth. Design basis accident and transient events were used as the bases for analysis. This study concluded that for SBWR there are no system wide common mode failure vulnerabilities and there is no specific event vulnerabilities caused by neutron monitoring system inputs to the SSLC/RPS.



Table 7.1-1 Regulatory Requirements Applicability Matrix (Continued)

Applicable Criteria	Reg. Guide											BTP						II-D	II-E	II-F		II-K						
	1.22	1.47	1.53	1.62	1.75	1.97	1.105	1.118	1.151	1.152	1.153	3	12	20	21	22	26	3	4.2	1	3	1.23	3.13	3.15	3.18	3.21	3.22	3.23
Reference (RG) Standard (IEEE) (ISA)	279	279	379	279	384		887.04	338	887.02	7-4.3.2	803	279	279	279	1.47	1.22	279				1.97		*	*		*	*	
Reactor Protection Sys.	X	X	X	X	X		X	X		X		X		X	X	X												
Neutron Monitoring Sys.	X	X	X		X	X	X	X		X	X				X	X												
Supp. Pool Temp. Mon. Sys.	X	X	X		X	X	X	X		X					X	X				X	X							
Auto. Depress. Subsys.	X	X	X	X	X		X	X		X	X				X	X		X							X			
Gravity-Driven Cooling Sys.	X	X	X	X	X		X	X		X	X				X	X												
Leak Det. & Isol. Sys.	X	X	X	X	X	X	X	X		X	X				X	X			X		X							
Safety Sys. Logic and Cont.	X	X	X	X	X		X	X		X	X				X	X												
Essential Multiplexing Sys.	X	X	X	X	X		X	X		X	X				X	X												
Flammability Control Sys.	X	X	X	X	X		X	X		X	X				X	X												
SLC Sys.	X	X	X	X	X		X	X		X	X				X	X												
Remote Shutdown Sys.			X	X	X					X					X													
Reactor Wtr. Cleanup/Cool.	X	X	X	X	X		X	X		X	X			X	X													
Isolation Condenser Sys.	X	X	X	X	X		X	X		X	X				X	X												
Safety-Related Display	X	X	X		X	X	X	X	X	X					X	X		X		X	X	X						X
Cont. Atmos. Monitoring Sys.	X	X	X		X	X	X	X		X					X	X				X	X							
Control Systems (Non-1E)									X																			

\*Not applicable to SBWR - see Subsection 7.1.2.2, "Conformance to TMI Action Plan Requirements"

- RG 1.75 — Physical Independence of Electric Systems
- RG 1.97 — Instrumentation During and Following an Accident
- RG 1.105 — Instrument Setpoints for Safety-Related Systems
- RG 1.118 — Periodic Testing of Electric Power and Protection Systems
- RG 1.152 — Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants
- RG 1.153 — Criteria for Power, Instrumentation, and Control Portions of Safety Systems

The NMS conforms with all the above listed RGs.

**Branch Technical Positions (BTPs):**

In accordance with the Standard Review Plan for Chapter 7, and with Table 7.1-1, only BTPs 21 and 22 are considered applicable for the NMS. They are addressed as follows:

**BTP ICSB 21 - Guidance for Application of Regulatory Guide 1.47** — The SBWR design is a single unit. Therefore, Item B-2 of the BTP is not applicable. Otherwise, the NMS is in full compliance with this BTP.

**BTP ICSB 22 - Guidance for Application of Regulatory Guide 1.22** — The NMS is continuously operating during reactor operation. The accuracy of the sensors can be verified by cross-comparison of the various channels among the four redundant divisions. The bypass of any RPS division will cause the two-out-of-four trip voting logic to revert to two-out-of-three. Therefore, the NMS fully meets this BTP.

**TMI Action Plan Requirements (TMI)** — In accordance with the Standard Review Plan for Chapter 7, and with Table 7.1-1, there are no TMI action plan requirements applicable to the NMS.

#### 7.2.2.4 Testing and Inspection Requirements

##### 7.2.2.4.1 General Requirements

All NMS instruments (not including sensors) in the reactor building are designed such that they can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or scram, and with easy access to the service personnel.

NMS instrument modules, including SRNM and APRM, are designed with the capability of being tested for the normal performance, trip performance, and calibration function, either through automated process or through manual process. Routine

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.35

Describe the manual initiation features of the engineered safety features actuation system. The description should include how the manual features comply with (1) IEEE Standard 279 and RG 1.62 and (2) SECY-93-087, Position II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems." (Reference SSAR Section 7.3.1.1.2.)

GE Response:

Manual Initiation Features of Engineered Safety Features (ESF) Actuation System

Manual controls are provided for ESF as follows:

- Manual Automatic Depressurization System (ADS) actuation
  - Four dual-action switches (one per division), any two of which must be operated to cause an ADS trip (see SSAR Figure 21.7.3-1).
- Manual Depressurization Valve (DPV) actuation
  - Two key-locked switches, both of which must be operated to cause the timed sequential actuation of all DPVs (see SSAR Figure 19AE.14-11).
- Manual Safety/Relief Valve (SRV) initiation
  - Two switches for each SRV, either of which will open the valve (see SSAR Figure 19AE.14-14).
- Manual Gravity-Driven Cooling System (GDCCS) initiation
  - Two key-locked switches, both of which must be operated to cause the timed sequential actuation of all GDCCS squib valves (see SSAR Figure 19AE.14-11).
- Manual Leak Detection and Isolation System (LD&IS) initiation (see SSAR Figure 21.7.3-4)
  - Manual Main Steam Isolation Valve (MSIV) open/close function provided by four individual valve controls.
  - Manual MSIV test close function provided by four individual valve controls.
  - Manual main steam line (MSL) isolation function provided by four dual-action pushbutton switches, any two of which must be operated to close all four MSIVs.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.35 (continued)

- Containment isolation provided by two divisional control switches. The Division I switch activates the outboard isolation valves, while the Division II switch activates the inboard isolation valves (these valves are shown on sheet 1 of SSAR Figure 21.7.3-4).
- Two control switches provide actuation of the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) A and B loop inboard and outboard isolation valves, respectively.

These manual features are implemented outside of the software-based microprocessor equipment in simple discrete logic circuitry (except for the DPV portion of manual ADS, which is software-based, but diverse to the discrete-logic circuitry of SRV) and are also divisionally redundant. Thus, these features comply with IEEE 279, Section 4.17, in that they (a) are implemented with a minimum of equipment and (b) provide single failure protection, both from the standpoint of being a backup to the automatic isolation function and from having multiple actuation paths. Compliance with RG 1.62 is implemented by (a) providing system level manual initiation, (b) providing all system level functions including interlocks on the discrete logic cards, (c) having the system level switches in the main control room, (d) using a minimum of equipment common to the automatic and manual functions [generally, only the final actuation devices are common, where the manual and automatic signals are combined to give the final trip output; in the case of manual DPV, GDCS, and SRV actuation, the manual and automatic signals use completely independent actuation paths and devices out to the final actuators], (e) providing single failure protection via multiple channels and 2-out-of-4 configuration of output actuation devices, (f) using a minimum of equipment consistent with the preceding items, and (g) requiring that all protective actions at the system level go to completion after initiation [all final trips are sealed-in and must be manually reset].

The requirements of SECY-93-087, Position II.Q, are met by providing the manual functions in diverse, non-software-based logic as a backup to the automatic software-based trip logic. In addition, the required study to support implementation of these features has been performed [Lawrence Livermore National Laboratory (LLNL) SBWR Diversity and Defense-in-Depth Study (draft version 1.0, June 30, 1993)].

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

**RAI 420.36**

Unlike previous boiling water reactor ADS actuation sequencing, the SBWR ADS actuation sequencing initiates only on water level. Explain the change. Would this reduce the system reliability? (Reference SSAR Section 7.3.1.1.2.)

**GE Response:**

The Automatic Depressurization subsystem (ADS) is required to depressurize the RPV in sufficient time to allow the Gravity Driven Cooling system (GDCS) injection flow to replenish core coolant to maintain core temperature below design limits in the event of a loss-of-coolant accident. The ADS is required to initiate upon receipt of a Level 1 water level signal. This requirement is not dependent upon whether the Reactor Coolant pressure boundary break is inside or outside the containment.

Per SSAR Section 6.3.3.2:

The ADS automatically actuates on a reactor low-low level (Level 1) signal that persists for at least 10 seconds. A two-out-of-four Level 1 logic is used to activate the SRVs and DPVs. The 10 second persistence requirement for the Level 1 signal ensures that momentary system perturbations will not actuate the ADS when it is not required. The two-out-of-four logic assures that a single failure will not cause a spurious system actuation while also assuring that a single failure cannot prevent initiation.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.37**

Provide a discussion of how ADS channel integrity is maintained. This should include (1) the reliability of ADS and (2) environmental qualification of ADS. (Reference SSAR Section 7.3.1.1.2.)

**GE Response:**

Per SSAR Sections 7.3.1.1.2 & 7.3.1.1.4:

The ADS instrumentation and logic power is obtained from the Safety System Logic and Control divisions 1,2,3, and 4, 125 Vdc buses. The control power is from the divisions 1,2,3 and 4, 125 Vdc battery buses. The motive power for the electrically operated gas pilot solenoid valves on the Safety Relief Valves (SRVs) is from local accumulators supplied by the High Pressure Nitrogen Supply system. The ADS trip logic units are self-tested continually every 30 minutes. The continuity of the SRV pilot solenoids and the bridge wires within the DPV squib valve actuating circuitry are tested continuously by a low amperage current, causing an alarm if the circuit is interrupted.

System status during normal plant operation and ADS performance monitoring during an accident is based on the Main Control room indications specified in SSAR Section 7.3.1.1.5.

Per SSAR Section 7.3.1.1.5:

ADS electrical equipment (including instrumentation and controls) located in the drywell is designed and qualified to operate in an environment resulting from a loss-of-coolant accident. Safety-related electrical equipment located outside the containment is designed and qualified for the environment in which they perform their safety function.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.41

The leak detection and isolation system (LD&IS) isolates the sources of leaks from the containment. Are all LD&IS isolations backed up by manual actuation in the control room? If not, explain why. (Reference SSAR Section 7.3.3.1.)

GE Response:

Manual Backup of LD&IS Isolations

All isolations are backed up by manual actuation in the control room (see the response to RAI 420.35).

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.42

Using block diagram(s), describe the arrangement of the fiber-optic data links for inter-cabinet communications. Identify all the components (including power supply arrangements) to be used for inter-cabinet communications. List all the data links between the integrated protection cabinets, and explain how the data links in a cabinet are protected from faults in other cabinets. In addition, explain how the integrated protection cabinets communicate with other cabinets. (Reference SSAR Section 7.3.4.2.)

**GE Response:**

Inter-Cabinet Communications for Integrated Protection System

One Safety System Logic and Control (SSLC) cabinet resides in each of the four instrumentation divisions. The only inter-cabinet communication performed is the transfer of trip status data from the digital trip modules (DTMs) or analog trip modules (ATMs) in each division to the trip logic units (TLUs) or discrete logic units (DLUs) in the other divisions for 2-out-of-4 coincidence voting. Signal transmission is via fiber optic data links in one direction only. The optical isolation provides electrical independence, since power sources are not connected among divisions. Thus, electrical faults cannot propagate among divisions. A single failure of a component in a given division, therefore, only affects transmission or reception of channel trip signals, but cannot damage components in other divisions. Divisional redundancy of safety systems and fault tolerance resulting from the use of coincident voting to initiate safety-related actions preclude any single failure from inhibiting a safety function.

Data processing and signal transmission are asynchronous among divisions; i.e., no common timing signals are transmitted and the failure of a clock signal within a division cannot affect timing or signal transmission in other divisions. A standard, non-proprietary communications protocol is used (RS485 or equivalent at 10 Mbps).

The inter-cabinet data links are shown in SSAR Figures 7.3-2a and 7.3-2b. They are shown as trip outputs from the DTMs or ATMs to the TLUs or DLUs. Data is transferred only from a trip module to the associated logic units corresponding to the system data being processed.



RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

**RAI 420.42 (continued)**

The SSLC cabinets also transmit data to other system cabinets, either for control or alarm and display purposes. Safety-related data can only be transmitted to the non-safety-related side and not vice versa. Fiber optic data links are also used for this purpose. Signals for the main control room displays or process computer are transmitted to a network gateway device for routing to the high speed data network that connects the main control room console and process computer equipment to other plant equipment (see SSAR Figure 21.7.3-6).

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.43

Describe the channel bypass provision in the reactor trip logic. This should include a detailed description of the design of hardware and software for reverting the 2-out-of-4 logic to a 2-out-of-3 logic, 2-out-of-4 logic to automatic trip, other logic reverting, alarm provision, and the basis for permitting indefinite time bypass of one channel for testing or maintenance. Is the "channel bypass" limited to the same function (e.g., high containment pressure) or can it be applied to different functions (e.g., one high containment pressure and one low water level)? Describe the relationship between channel bypass and the trip design. Describe the method of the bypass indication at the work station in the main control room. (Reference SSAR Section 7.3.4.2.)

GE Response:

Channel Bypass Provisions for Reactor Trip Logic

The attached Figures 420.43-1 and 420.43-2 illustrate the Reactor Protection System (RPS) and Engineered Safety Feature (ESF) bypass circuitry, respectively. These figures have been revised from similar ones appearing in ABWR Safety System Logic and Control (SSLC) Hardware/Software System Specification 23A6915, Rev. 0. As described in SBWR SSAR Section 7.3.4.2, two types of channel bypass exist, division-of-sensors bypass and division-out-of-service (or division maintenance) bypass. For division-of-sensors bypass, all sensors in one division are bypassed simultaneously for both RPS and ESF channels; individual sensor channel bypass is not part of the SSLC design. However, individual channels can be placed in a trip condition by applying a simulated trip signal to the Trip Logic Unit (TLU) input for a given failed sensor channel. As shown in the figures, the four divisional bypass units are interlocked so that only one division-of-sensors bypass can be applied at a time.

When a division-of-sensors bypass is applied, all divisions revert to 2-out-of-3 for trip, since the bypass state in the bypassed division is transmitted to the remaining divisions and applied to those divisions' bypass inputs. The bypass units are implemented in simple hardware logic and use hardware switches. Bypass status and interlocking signal transmission between divisions is by means of isolated fiber optic data links. The bypass functions are fully integrated with the channel trips and are qualified with the trip functions as safety-related.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.43 (continued)**

The bypass state always goes high to bypass. For fail-safe RPS and Main Steam Isolation Valve (MSIV) logic, the trip state goes low to trip. Applying the bypass puts a permanent no-trip signal into each 2-out-of-4 voter, thus requiring two more inputs from any redundant set of sensor channels to go low to produce a trip output for that division. For fail-as-is ESF actuation logic, the trip state goes high to trip. Applying the bypass inhibits a tripped state from activating the 2-out-of-4 voter, thus requiring two more trip states to go high before a trip is produced in a particular ESF channel.

All bypasses are alarmed (per division) in the main control room, including the condition of sensors being in a tripped state in the bypassed division (see SSAR Figure 21.7.2-2 for RPS). At the operator display, bypass indications are grouped near the sensor trip alarms.

The other type of bypass, division-out-of-service (or division maintenance) bypass is applied at the output logic units of the divisional trip channels, after the trip logic unit. This bypass arrangement is similar to the division-of-sensors bypass, but is applied at the trip output to the load drivers, which are connected in a 2-out-of-4 configuration. In this way, all equipment in a bypassed division can be tested, calibrated, or serviced while the remaining divisions are operating in a 2-out-of-3 mode. As before, the bypass signal goes high to bypass. For RPS, the bypass signal effectively energizes that division's load drivers permanently, thus requiring two of the remaining three divisions to trip in order to cause a reactor trip. For ESF, the trip state goes high to trip. Applying the bypass inhibits the trip signal from reaching and energizing the load drivers, thus requiring two more high trip signals from other divisions before actuators are energized. Note that unlike division-of-sensors bypass, division-out-of-service bypass can be applied individually to the logic channels of the affected system.

Division-out-of-service bypass and division-of-sensors bypass are independent and can be applied together in any combination of divisions. Sensor voting logic and output trip voting logic are never reduced below 2-out-of-3.

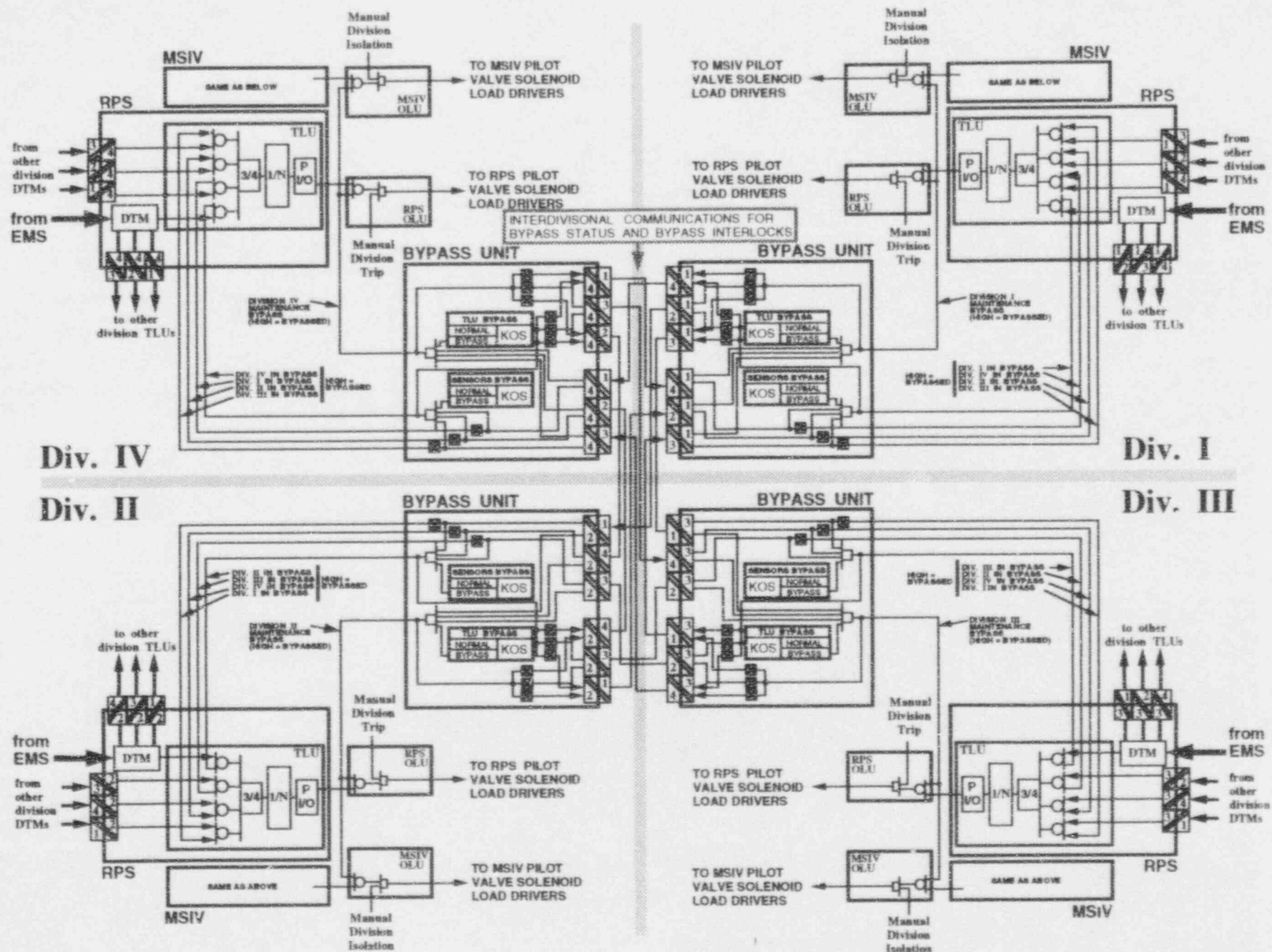
Manual divisional RPS trip, manual scram, manual Main Steam Line (MSL) isolation, manual containment isolation, and manual Depressurization Valve (DPV), Safety Relief Valve (SRV), and Gravity Driven Cooling System (GDCS) actuations are not bypassable.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

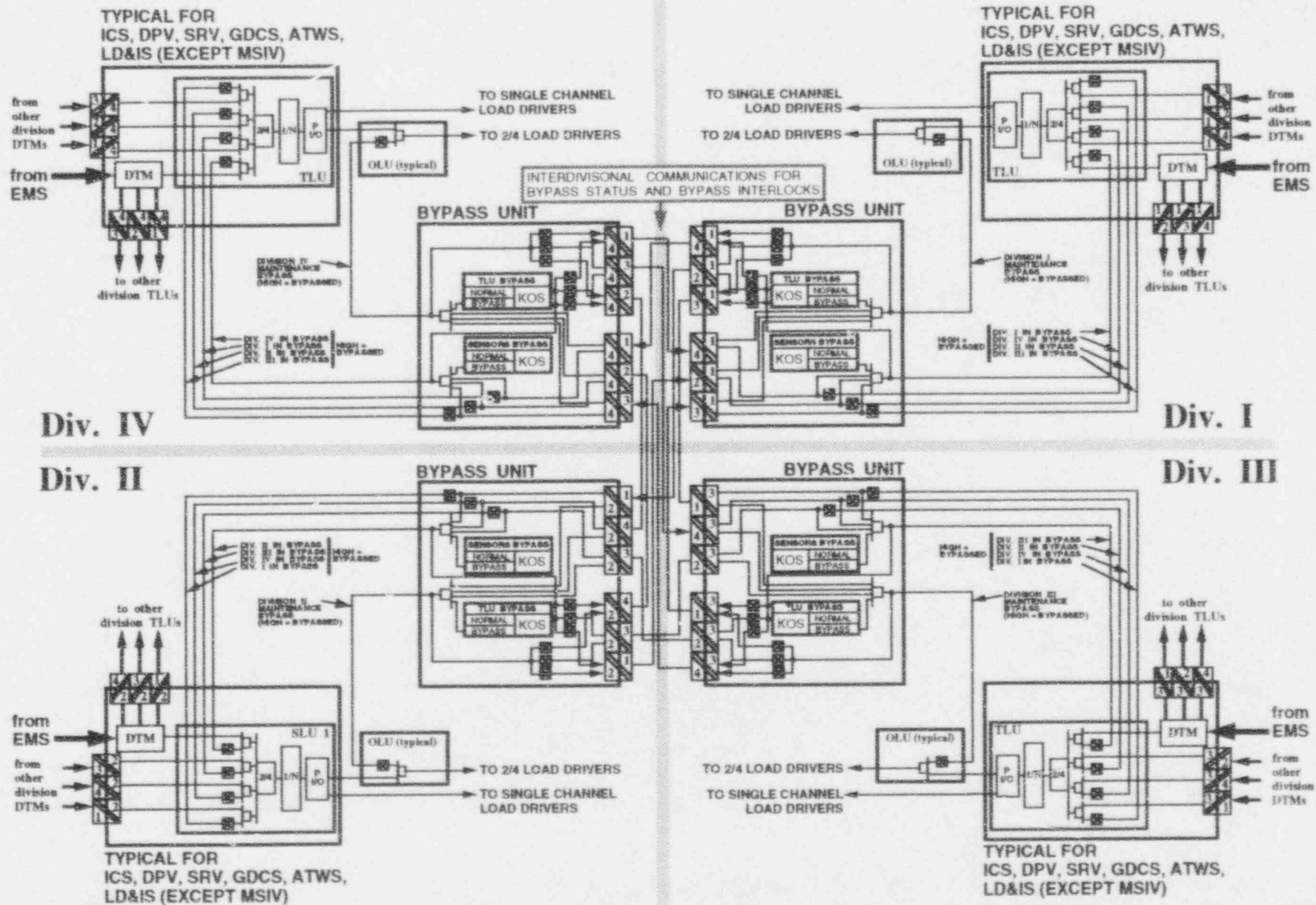
RAI 420.43 (continued)

Although indefinite time bypass of one division for testing or maintenance is feasible, GE does not take credit for this condition, since the SBWR PRA considers the protection system as having four operational divisions. This matter was resolved with the NRC staff in developing the ABWR technical specifications (SSAR Chapter 16), where a similar concern was raised. The ABWR Chapter 16 LCO completion times indicate the NRC/GE agreements for all combinations of bypass conditions. The SBWR completion times will be developed in a similar manner.



SSLC BYPASS SCHEME - RPS / MSiV  
Figure 420.43-1

REF. RAI 420.43



SSLC BYPASS SCHEME - ESF/ICS  
Figure 420.43-2

REF. RAI 420.43

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.44

Provide a list of manual actuation controls that are not independent of safety system logic and control or the essential multiplexing system. Provide a list of manual system-level and component-level actuation controls that are independent of the SSLC and EMS. (Reference SSAR Section 7.3.4.3.)

GE Response:

Independence of Manual Controls

- Manual actuation controls that are independent of the essential multiplexing system (EMS)
  - All manual actuation controls are independent of EMS. Multiplexing is used only for input data from plant sensors.
- Manual actuation controls that are independent of Safety System Logic and Control (SSLC)
  - Manual Scram
- Manual actuation controls that are not independent of SSLC
  - All other manual controls are within SSLC. However, if this question refers to whether the controls are within the software-based portion of SSLC or the hardware-based portion of SSLC, then the answer is as follows:
    - See the response to RAI 420.35 for the Engineered Safety Feature (ESF) manual controls. All these controls are outside of the software-based portion of SSLC except the manual Automatic Depressurization System (ADS) control that actuates the DPVs.
    - Manual divisional trip for Reactor Protection System (RPS) is outside of the software-based portion of SSLC.
    - Isolation Condenser System (ICS) controls are within the software-based portion of SSLC. However, a diverse Reactor Pressure Vessel (RPV) level2 actuation of ICS is performed in the hardware-based portion of SSLC. Note that ICS is not part of ESF.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.45

The second sentence of paragraph 2 on page 7.3-27 states that the testing shall not cause actuation of the driven equipment. Describe how this will be accomplished. (Reference SSAR Section 7.3.4.4.)

GE Response:

Testing

See the response to RAI 420.18. On-line self-test does not change the trip state of any logic; it checks for data errors in the communication path and monitors timing and program flow, status of registers, etc., in addition to checking power supply levels and circuit continuity. Off-line self-test, available when channels are bypassed, does change trip states, but because of the bypass, will not cause actuation of driven equipment.



RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.46

Describe the qualification of surveillance test equipment and diagnostic equipment. In addition, describe the interfaces between the test equipment and the safety equipment. Could the test equipment (1) compromise the separation between channels or (2) potentially degrade the safety-related equipment or system that they are testing? (Reference SSAR Section 7.3.4.4.)

**GE Response:**

Qualification Interfaces of Surveillance Test Equipment

The interfaces between the surveillance test equipment and Safety System Logic and Control/Essential Multiplex System (SSLC/EMS) are shown for one protection system division in attached Figure 420.46-1.

On-line self-diagnostics and conventional manual test methods are the main periodic test functions used for SSLC and EMS. Surveillance test equipment is only used for off-line testing and so cannot degrade the operational safety channels. The equipment is not connected to SSLC or EMS when the protection system is on-line. Connectors are provided on the protection system controllers for test equipment connection so normal system cabling is not disturbed. Portions of the protection system that are bypassed on-line can be surveillance tested without causing output trip.

Since automatic on-line testing is sufficient to check most logic and communication functions (including inter-divisional communications) without causing actuator trip, simultaneous four-division testing is only performed during a maintenance outage. Thus, channel separation is never degraded by test equipment during protection system operation. Because of the 2-out-of-4 voting configuration at both the sensor input and divisional trip output sides of the protection system, simulated sensor signals must be injected simultaneously into the redundant sensor channels. In this way all trip logic can be tested up to and including the actuators. Some driven equipment may have to be disconnected if actuation is not desired.

Since the surveillance test equipment is not an on-line interface to the safety systems, it is not qualified as Class 1E safety-related, but is, of course, calibrated to industrial standards for the appropriate accuracy required.

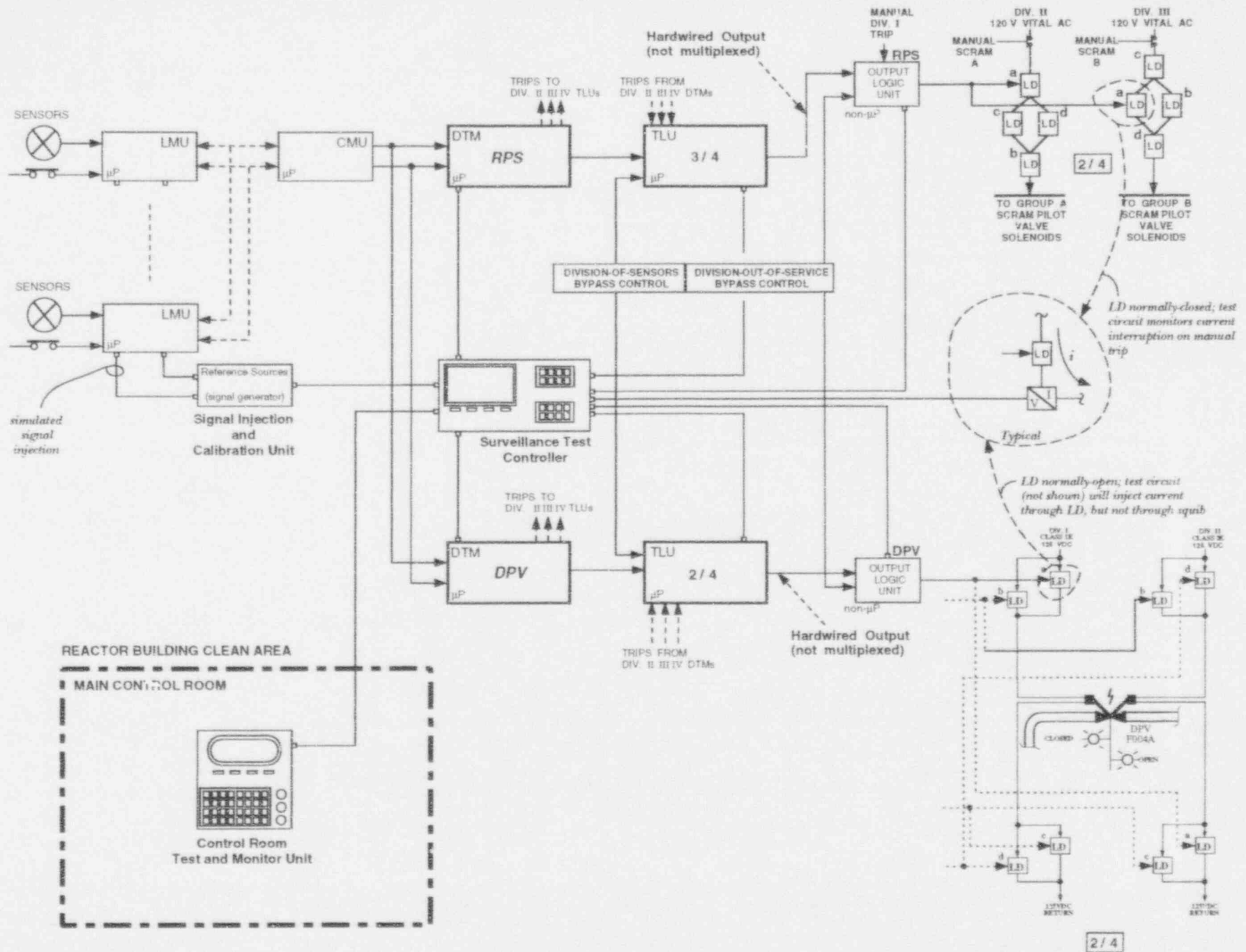


Figure 420.46-1  
**SAFETY SYSTEM LOGIC & CONTROL TEST SCHEME**  
*(typical end-to-end connection for RPS and part of ESF in one of four divisions)*

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.47

Describe how protection systems are tested end to end. If some portions of the systems are not tested, explain why. In addition, explain (1) how failures in on-line testing systems will not prevent the safety circuits from performing their safety functions and (2) how the test configuration does not violate the separation requirements. (Reference SSAR Section 7.3.4.4.)

GE Response:

End-to-End Testing of the Protection System

See the responses to RAI 420.17, 420.18, RAI 420.19, and RAI 420.46. Overall testing is performed through a series of overlapping functional tests, as permitted by IEEE Std. 338. As described in SBWR SSAR Section 7.2.1.4 for Reactor Protection System (RPS), these tests include the following:

- Channel Checks: Cross comparison of values of analog scram variables, permitting verification of operational availability of sensor instrument channel.
- Detector Actuation Tests: Simulated signals input to the individual detectors or sensor channels for all RPS-related instrumentation channels which are capable of initiating a reactor scram, permitting the trip channels to be tested or calibrated and setpoints to be verified.
- Trip System Logic Tests and Trip Actuator Tests: Simulated scram signals, permitting trip system logic to be tested. System outputs toggle, permitting operation of the trip actuators to be tested.
- Paired-Control-Rods Scram Tests: Switches are installed in the main control room to permit testing of the fast scram operation of the individual pairs of control rods and to confirm, when necessary, that the individual control rods have scrambled.
- Coincident Logic Tests: Testing of coincident two-out-of-four (or one-out-of-four, twice) trip logic will verify each combination of trip conditions for each set of input scram variables in an RPS trip channel. Testing will also verify each output logic combination of trip conditions in the four RPS trip systems. This testing will be performed in accordance with the Technical Specifications.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.47 (continued)**

Similar tests are performed for Engineered Safety Feature (ESF) functions (see SSAR Section 7.3.4.4, covering Safety System Logic and Control (SSLC) logic processors).

All portions of the protection system are testable on-line, but not all portions can be tested automatically. For RPS and Main Steam Isolation Valve (MSIV), the final output logic and load drivers are tested periodically with the divisional trip switches, resulting in a half-scam or half-isolation, respectively. For ESF, similar tests are possible for the 2-out-of-4-configured systems; for single-train-per-division systems such as LD&IS and ICS, with motor-operated or air-operated valves, on-line load driver actuation is not possible without actuating the driven equipment.

Suitable test intervals for performing in-service tests of the RPS and ESF sensor instrument channels and the RPS and ESF trip actuators (i.e., load drivers, relays, and motor control centers) are provided in the Technical Specifications (Chapter 16).

On-line diagnostics are monitoring functions that do not insert signals into the trip path or cause trips to change state. These diagnostics are qualified along with the safety-function software as part of the final software verification and validation (V&V) program. Within the real-time operating system, diagnostics are performed only during time intervals not used for safety function processing. In addition, since on-line diagnostics are confined to individual controllers, a random failure in one division will result only in a divisional failure that can be bypassed.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.48

Describe any design or testing requirements that deviate from Section 3.6.1, "Testability Requirements," of Chapter 10 of EPRI Advanced Light Water Reactor Utility Requirements Document, Volume III, Passive Plant. (Reference SSAR Section 7.3.4.4.)

GE Response:

Deviations of Testing from EPRI URD, Chapter 10, Section 3.6.1

As described in the responses to RAI 420.17, 420.18, RAI 420.19, RAI 420.46, and RAI 420.47, all testing requirements of Section 3.6 are met by the SBWR protection system design.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.49**

Provide a discussion of the use of commercial dedication software in safety systems. The discussion should also include the criteria for selecting commercial software, the accuracy of tools, and the process by which the developer notifies the end user of changes. (Reference SSAR Section 7.3.4.5.)

**GE Response:**

Use of Dedicated Commercial Software in Safety Systems

The use of commercial software in safety systems is covered in the SBWR Certified Design Material (CDM), Section 3.4(B) and the accompanying Inspection, Test, Analyses, and Acceptance Criteria (ITAAC) table and is endorsed in the SSAR through conformance to ANSI/IEEE ANS-7-4.3.2 (1993).

The issue of commercial dedication of software in safety systems is resolved in the ABWR SSAR in Appendix 7B (the Tier 2 material developed to support the I&C CDM) by a commitment to ANSI/IEEE ANS-7-4.3.2 (1993), "Standard Criteria for Digital Computers Used in Safety Systems of Nuclear Power Generation Stations". This standard includes commercial dedication of third-party software and the use of commercial software tools for safety-related applications. Appendix 7B and AMSO/IEEE ANS-7-4.3.2 (1993) both apply directly to SBWR, along with the following discussion.

As stated in the standard, the dedication process requires the inclusion of the requirements that the commercial software shall meet in the verification and validation (V&V) and configuration management plans. The requirements shall address the similarity of the nuclear and non-nuclear applications. Additionally, the requirements shall describe the aspects of the commercial software which demonstrated that the software has the high quality required. Both complete software designs and partial designs (operating systems) are covered by the dedication process.

Also as stated in the standard, commercial software development tools become part of the software configuration management process, and are controlled by, but are not formally certified through, the V&V program. These tools can include, but are not limited to, compilers, debuggers, software documentation programs, and testing tools. The software tools are not required to be verified and validated as safety software. A tool will be indirectly verified, first by prior knowledge of its extensive usage in

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.49 (continued)

operational industrial applications, and, second, through the formal verification process, where the results of code generation are checked by an independent team of reviewers against design requirements and performance specifications at each stage of software development. Eventually, testing of the integrated software and hardware combination is performed as part of the final validation process. The section of the standard covering tools reads as follows:

“5.3.4 Software Tools

A software tool is software which is used in the development of safety software but which is not installed and relied upon to perform a function. These tools can include, but are not limited to, compilers, debuggers, software documentation programs, and testing tools. The use of these tools is important to the development of quality software and therefore the tools are required to be identified in the V&V and configuration management plans. The software tools are not required to be verified and validated as safety software.”

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.50

Although there are some differences in the systems aspects of the advanced boiling water reactor (ABWR) and the SBWR design, the electronic components and modules used for the SBWR I&C are very similar to those of the ABWR. Therefore, the requirements met by the SBWR design also should be very similar to the ABWR requirements. Provide a list of the standards and RGs with which the ABWR design complies, but the SBWR design does not. Also provide a list of standards and RGs which are unique to the SBWR design. In addition, provide a justification for each difference. (Reference SSAR Section 7.3.4.5.)

**GE Response:**

Differences in Design Standards for ABWR and SBWR

There are no known reasons for standards to be different between the ABWR and SBWR I&C designs. While the system design and configuration differ between the two, in the areas of electronic components, software development, communications technology, operating environment, and setpoint methodology the same standards apply to both designs.



RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.51

Describe the methods used to program firmware. The discussion should address the programming process that is implemented to improve the reliability of the firmware. (Reference SSAR Section 7.3.4.3.)

**GE Response:**

Methods Used to Program Firmware

Firmware programming is controlled under the hardware and software development process described in Section 3.4, "Instrumentation and Control", of the SBWR Certified Design Material, 25A5354, Rev. A. This process establishes an overall software development plan, which includes a Software Management Plan, Configuration Management Plan (CMP), and Verification and Validation Plan (V&VP). The CMP defines methods to produce software design documentation, correct errors found in software design, and maintain the status of the developed software design. The V&VP ensures that validation is performed through controlled and documented testing of the developed software as installed in the target hardware (in the form of firmware) and that such testing demonstrates compliance of the software with the software requirements specifications and compliance of the devices under test with the system design specifications.

Actual programming methods for producing firmware are a design and manufacturing detail that will be established at the time of software coding to meet the requirements of the software development plan.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.52

Identify the reports that will be provided to support any aspects of the software development requirements that are different relative to software development requirements previously reviewed by the staff. (Reference SSAR Section 7.3.4.5.)

**GE Response:**

Differences in Software Development Requirements between SBWR and previously reviewed designs

Software development requirements are identical for the SBWR and ABWR instrumentation and control equipment.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.53

Describe how software errors are tracked during software development.  
(Reference SSAR Section 7.3.4.5.)

**GE Response:**

Methods for Tracking Software Errors

A commitment is made in Section 3.4, "Instrumentation and Control", of the SBWR Certified Design Material, 25A5354, Rev. A, to establish methods under the Configuration Management Plan for tracking software errors. The use of software metrics is mentioned as a method for consideration; however, under the Design Acceptance Criteria (DAC) process, the COL applicant will be able to evaluate and select the best methods at the time of software development.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.54

Paragraph 3 on page 7.3-27 states that the use of interrupts for processing safety-related functions is discouraged. What are the requirements for using interrupts when they are used? (Reference SSAR Section 7.3.4.5.)

GE Response:

Use of Interrupts for Processing Safety-Related Functions

The use of interrupts in the microprocessor-based logic processors of Safety System Logic and Control (SSLC) is discouraged in order to ensure that safety-related processes go to completion in the required time period without interference from competing tasks. In general, this applies to external interrupts, where, for example, the acquisition of data from a sensor that may be indicating a safety-related tripped state should not be interrupted to read other sensor data or perform other tasks that are not as critical. However, in real-time systems, the CPU's operating system may safely use interrupts when a high-priority task must interrupt a lower-priority task.

In the SBWR protection system design, each CPU uses a minimal operating system (kernel) optimized for the necessary functions. This provides more predictable performance than a full operating system for the few required safety system logic functions. The control program is structured in a modular, block fashion. The operating system controls the resource allocation to the various tasks which run under its control. The tasks call independent modules as needed and link them to perform their function. Safety-critical tasks have the highest priority and self-test has the lowest priority, running only when spare CPU time is available.

All real-time programs, including kernels, have "critical code" sections that must run to completion without being interrupted. At a "pre-emption point" in-between these sections, the kernel can safely interrupt its processing and turn its attention to other matters. Some kernels are fully pre-emptable at virtually any point.

If multitasking is used to minimize time delays, then the operating system periodically disables all interrupts and shuts itself off from the outside world to catch up on bookkeeping.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.55

Describe the local area networks and communication systems and provide a list of standards with which the SBWR will comply. In addition, provide the installation requirements for fiber optic lines. (Reference SSAR Section 7.3.5.2.)

GE Response:

Standards for Local Area Networks and Communication Systems

Since the stated reference in this RAI is to the SSAR system description section for the essential multiplexing system (EMS), the response will be limited to EMS.

A discussion of EMS has been provided in the response to RAI 420.9, with reference to the EMS IED in SSAR Figure 21.7.3-6, which shows the relationship of EMS to other plant data networks. In each division, EMS is a bi-directional, dual-redundant, reconfigurable Fiber Distributed Data Interface (FDDI) network, complying with the FDDI communications standard ANSI ASC X3T9.5 or equivalent. For compatibility in interfacing with other plant networks, microprocessor hardware and software for use in the EMS will be compatible with communication protocols developed under the International Standards Organization (ISO) open systems interconnect (OSI) specification, ISO 7498, as stated in SSAR Section 7.3.5.2. Additional information can be found in ABWR SSAR, 23A6100, Rev. 2, in Appendix 7A, Section 7A.2, Response 10.

*Installation Requirements for Fiber Optic Lines in SBWR*

Optical fiber cables are generally smaller and lighter than equivalent metallic conductor cables. However, they can be manufactured with sufficient ruggedness to permit installing these cables in cable trays and conduit along with metallic cables. Typically, the optical fibers are surrounded by support and fill materials, such as steel wire and elastomers, within the overall cable. This assembly may be wrapped with a non-metallic material such as Kevlar™ to improve tensile strength. In addition, the cable assembly may then be enclosed within an aluminum or copper tube and covered with an outer insulating jacket. This type of cable bundling allows optical cables to be handled like electrical coaxial cable when pulled through conduit. For SBWR use, the outer jacket would be fire resistant to meet the requirements of IEEE-383.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.55 (continued)**

Standard industrial grade fiber optic cable with insulation specified to meet local environmental conditions will be used for the EMS. After installation, all fibers used for the EMS will be checked for optical power loss in accordance with the manufacturer's data sheets. Any fiber not meeting the optical power loss criteria will be stripped away from the termination points so as not to be usable in the future.

The experience of the telecommunications industry has shown that it is possible to package optical fibers using combinations of the above techniques so that optical fiber cables can operate reliably even in hostile environments such as direct earth burial or under the ocean.

It is intended that optical communications for SBWR will be performed within the main control room (between protection divisions and to the operator control console or process computer) and between the main control room and local Safety System Logic and Control (SSLC) cabinets and local multiplexing units, which are located outside of the secondary containment in clean areas of the Reactor Building. These clean areas will have HVAC that will maintain a control room environment. Optical fiber cables will not be routed through high radiation areas. The quantity of cable will be minimized by using serial multiplexed data transmission as the main communication technique.

Although optical cables can be physically protected as described above, it should be noted that these cables do not need special protection from EMI/RFI sources (relays, switchgear, motors) and are not susceptible to crosstalk from adjacent metallic cables, including power cables, or other optical fiber cables.

Some skill and special care are required to install and align connectors on optical fiber cables so that the continuity of the light path is maintained from the transmitter to receiver with low losses. However, improved connectors and termination techniques are continually being developed by the industry. Since most cable breaks occur near the connectors, cables must also be properly supported to relieve strain on the terminations.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.56

The fiber optic line protects signals from the noises in the environment; however, the fiber optic line driver and receiver are susceptible to the noises in their environment. What are the environmental qualification criteria for these drivers and receivers? (Reference SSAR Section 7.3.5.2.)

**GE Response:**

Response to ABWR Question 420.84 (presented in the ABWR SSAR Section 20.3.8, page 20.3.8-46) and information presented in the ABWR Appendix 7A, Responses 7A.2(4), 7A.2(15), 7A.3(6) and 7A.3(8) provide detailed discussion on the criteria and standards that will be applied to the fiber optic equipment design and testing. These criteria and standards are also used for the SBWR design.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.57

Show how the independence criteria in accordance with IEEE Standard 603 and IEEE Standard 379 are satisfied with the proposed configuration of fiber optic links. (Reference SSAR Section 7.3.5.2)

**GE Response:**

Conformance of Fiber Optic Link Arrangement to Independence Criteria

*Conformance to Section 5.6.1 of IEEE 603-1991:*

Each of the four divisions of protection system equipment has a separate and independent essential multiplexing system (EMS) located within the reactor building safety envelope in the divisional clean areas. The fiber optic links of each EMS are connected only within each EMS division, either to the protection system equipment in that division or to the main control room displays and controls. No communications are performed between divisions of EMS (trip data is exchanged between divisions by fiber optic links of Safety System Logic and Control (SSLC) that are independent of EMS).

*Conformance to Section 5.6.2 of IEEE 603-1991:*

All protection system equipment, including EMS and SSLC, conforms to IEEE Std 603-1991 and is qualified as safety-related, Class 1E and Seismic Category I.

*Conformance to Section 5.6.3 of IEEE 603-1991:*

As stated in SBWR SSAR Section 7.2.1.3, RPS, which includes the fiber optic links of EMS and SSLC, complies with the criteria set forth in IEEE 603, Paragraph 5.6, and RG 1.75, which endorses IEEE 384. The fiber optic links themselves provide isolation, a physical barrier, and separation distance, but total protection of the four safety-related equipment divisions is afforded by the separation of the reactor building clean areas within the safety envelope. When software is involved in data transfer, software isolation is implemented through one-way broadcast of data without handshaking control and a prohibition on interrupt-driven requests for data from the non-safety side to the safety side. Further details on isolation of data transfer involving fiber optic links is given in ABWR SSAR Chapter 20, Response to RAI 420.128. This discussion also applies to SBWR.



RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.57 (continued)

*Conformance to Section 5.1 of IEEE 379-1977:*

Based on the above discussion of the independence of fiber optic links of EMS and SSLC, it can be seen that no single failure of a link or its associated signal processing equipment will interfere with the proper operation of redundant channels. An entire division of EMS can be removed from service by means of the division-of-sensors bypass provision without affecting protection system operation other than to place it in a 2-out-of-3 condition. Likewise, a single failure of an inter-divisional link can be resolved either by (1) placing the division from which the link is transmitting in division-of-sensors bypass, which will remove all of that division's signals from service in all other divisions; or (2) by placing the division to which the link is transmitting in Trip Logic Unit (TLU)-output-logic bypass, which removes that division from service and places the remaining divisions in a 2-out-of-3 condition.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.58

Describe the data highway system for the essential multiplexing system. This description should include error handling and error recovery of the system. Does the SBWR have sufficient error handling capability so that the discovery of an error would not cause a data highway traffic jam? In addition, describe the data handling capability of the EMS. Explain whether data traffic would increase during abnormal plant conditions? (Reference SSAR Section 7.3.5.2.)

**GE Response:**

Data Highway System for Essential Multiplexing System (EMS)

EMS is not a general purpose "data highway", but is a dedicated, deterministic network for providing safety-critical sensor signals to the digital protection system for possible trip action. The network must be deterministic because sensor signals must have guaranteed access to the network to ensure accurate, on-time trip determination. Sensor signals may be sent to the process computer, main control room complex, or other systems through isolated buffer devices (gateways), but no random communication is permitted.

Error handling is provided, as discussed in SBWR SSAR Section 7.3.5.2, by error detection software and hardware that monitor data I/O and internal processes of each EMS controller. If a fault is permanent and potentially unsafe, the system recovers (or fails) to a safe state and the operator is alerted on the interface unit in the main control room. The redundant multiplexing channels are repairable on-line if one channel fails. All processor memory not used for or by the operational program is initialized to a pattern that causes the system to revert to a safe state if executed. Errors will not cause a traffic jam on the network because the station management software of the network's Fiber Distributed Data Interface (FDDI) protocol handles error recovery and ensures automatic reconfiguration of the network on severe failures. A more detailed discussion of error handling and error recovery is found in the ABWR SSAR, 23A6100, Rev. 2, in Appendix 7A, Section 7A.2, Response 14. The ABWR EMS uses the same basic multiplexing equipment and communications protocols as SBWR EMS.

EMS operates at a constant data rate and with a constant number of sensors. All sensor data is periodically scanned at defined intervals; there are no interrupt-driven inputs. Thus, abnormal plant conditions will not affect the quantity or type of data on the network, just the data levels.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.59

Provide a safety and hazard analysis, sneak circuit analysis, and timing analysis for the protection systems. (Reference SSAR Section 7.3.5.2.)

GE Response:

Safety Analyses for the Protection System

Commitments for safety and hazard analyses, sneak circuit analyses, and timing analyses are COL action items since technology in these areas will change over time and must be specified by the final software vendor at the time of software design. A commitment to special analyses for safety-critical software is made under the software quality assurance program described in the SBWR Certified Design Material, 25A5354, Rev. A, Section 3.4(B).

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.60

Provide an explicit discussion of how the systems conform to IEEE Standard 279, paragraph 4.5 on channel integrity, as supplemented by RG 1.75 and IEEE Standard 384. (Reference SSAR Section 7.3.5.3.)

**GE Response:**

The reference SSAR Subsection 7.3.5.3 provides a summary of safety evaluation for the Essential Multiplexing System (EMS)

IEE Standard 297-71, paragraph 4.5 specifies the channel integrity criterion as follows:

*"4.5 Channel Integrity. All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions, and accidents."*

IEEE Standard 384-81, paragraph 7.2.1: specifies

*"7.2 Instrumentation and Control Circuits*

*7.2.1 General. Electrical isolation methods shall be used as required in instrumentation and control circuits to maintain the independence of redundant circuits and equipment such that safety functions required during and following any design basis event can be accomplished. This electrical isolation of instrumentation and control circuits shall be achieved through the use of Class 1E isolation devices applied to interconnections of (a) Class 1E and non-Class 1E circuits, (b) associated circuits and non-Class 1E circuits, or (c) Class 1E logic circuits of redundant divisions as shown in Fig. 8. Shielding and wiring techniques may also be necessary to achieve and maintain the independence of redundant circuits and equipment."*

Regulatory Guide 1.75 has no discussion on these criteria.

Layout of EMS configuration is depicted on Figure 7.3-2a and an interface block diagram for Safety System Logic and Control (SSLC) system including EMS is shown on Figure 7.3-3. The SBWR design includes considerations for the safety system channel divisionality and integrity such that necessary functional capability of protection system channels, within the EMS components, is maintained under the extremes of conditions relating to the environment, power supply, malfunctions (failure or misoperation of the mechanical or structural components) and accidents.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.60 (continued)

As shown on the above referenced guides, the EMS equipment is located in the reactor building clean area and thus not exposed to high level radiation hazard. Since the power supply provided for the EMS equipment operation is of the regulated (constant voltage, constant frequency) quality, there is no adverse effect of the power supply on the proper operation of the EMS equipment.

The EMS equipment is protected, either by barrier or by distance, from effects of failure or misoperation of mechanical and structural components in the vicinity of such equipment.

As discussed in the SSAR Subsection 3.11.1, the safety related equipment (including EMS components) shall be designed to perform its proper safety function in their localized environment during normal, abnormal, test, design basis accident and post accident conditions as applicable. As further discussed in Subsection 3.11.3, the 10CFR50.49(b) electrical equipment that is located in a harsh environment is qualified by test or other methods as described in IEEE 323 and permitted by 10CFR50.49(f).

Also as stated in Subsection 3.11.3, the procedures and results of qualification by tests, analyses or other methods for the safety-related equipment will be documented, maintained and reported as mentioned in the General Electric Environmental Qualification Program, NEDE-24326-1-P, Proprietary Document, January 1983.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.61**

Confirm whether system-level failures of any multiplexer system detected by automatic diagnostic systems are indicated to the operators consistent with the requirements of IEEE Standard 279 and IEEE Standard 603 regarding safety system status indication. (Reference SSAR Section 7.3.5.4.)

**GE Response:**

The Essential Multiplexing System (EMS) for the safety-related functions contains on-line self-diagnostics implemented in software and hardware that will continuously monitor system performance. Within each control station, the following typical parameters are monitored: (1) status of the CPU, (2) parity checks, (3) data plausibility checks, (4) watchdog timer status, (5) voltage levels in control unit circuitry, (6) memory (RAM and ROM) checks, and (7) data range and bounds checks. Self-test will indicate faults to the module board replacement level.

Each multiplexing system has dual channels for fault tolerance and is provided with automatic reconfiguration and restart capability. A detected fault is automatically enunciated to the operator at both the system and individual control station level. If one transmission loop is completely out of service, that will also be enunciated. Total shutdown of a multiplexing system is indicated by a separate alarm.

After repair, the system automatically re-initiates to normal status when power is restored to any unit and automatically resets any alarms. Power loss to any control station is separately monitored and enunciated to aid in troubleshooting and to alert the operator when power is deliberately removed from a unit when being serviced.

The above discussion indicates conformance to the requirements criterion 4.20, Information Read-Out, of IEEE Std. 279-71 and criterion 5.8.2, System Status Indication, of IEEE Std. 603.80.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.62

Describe how the essential multiplexing system interfaces with non-safety-related equipment. (Reference SSAR Section 7.3.5.2.)

**GE Response:**

The interconnection of Class 1E multiplexers to non-class 1E devices is done using fiber optic cable. The fiber optic cable will provide the necessary isolation.

The plant process computer is connected to a buffer module (memory storage module). Information is stored in this module by the Essential Multiplexing System (EMS) (Class 1E) units for access by the process computer, thus preventing any interruption by the Non-Class 1E process computer on the EMS (Class 1E) units.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.63**

Describe the equipment that are tested by the on-line testing and automatic testing, and describe how the essential multiplexing system is tested end to end. (Reference SSAR Section 7.3.4.5.)

**GE Response:**

Test Coverage for Essential Multiplexing System (EMS)

Since EMS transmits plant sensor data to Safety System Logic and Control (SSLC), coverage of the on-line and automatic testing features of EMS is included in previous RAI responses as part of the discussion of Reactor Protection System (RPS), Engineered Safety Feature (ESF), and SSLC testing. Please refer to the following RAIs:

- |          |          |
|----------|----------|
| • 420.10 | • 420.19 |
| • 420.13 | • 420.45 |
| • 420.17 | • 420.46 |
| • 420.18 | • 420.47 |

EMS is necessarily tested as part of SSLC testing or specific safety-related system testing (RPS or ESF) whenever sensor channel tests are performed from multiplexer input to trip channel output.

The automatic, on-line test features of EMS are summarized below:

- As in SSLC controllers, EMS multiplexing controllers (i.e., LMUs and CMUs) contain similar on-line self-diagnostics in firmware for the data acquisition portion of the equipment.
  - Error detection capability includes data I/O checks (plausibility, boundary, and rate limit checking), RAM and ROM checks, and program flow checks.
  - Basic system 'health' is monitored by both software and hardware watchdog timers.
  - In the data path, parity bits are appended to each data message and a cyclic redundancy check(CRC) is calculated. The data messages are then checked throughout the data channel for correct transmission and reception.
  - System hardware is also monitored for shorted, open, and oscillating inputs and outputs, and high or low power supply voltages.



**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.63 continued**

- Special multiplexing diagnostics in separate firmware Fiber Distributed Data Interface (FDDI) station management ROMs) monitor network activity and perform automatic reconfiguration of the usable portion of the network after failures are detected. Since EMS is dual redundant in each division, a single cable break or loss of a multiplexing device does not result in loss of all data.
- Additional details of EMS self-test can be found in Appendix 7A of the ABWR SSAR (Section 7A.2, Response 6).

For specialized pre-operational testing and specific testing for electromagnetic compatibility, see Responses 3 and 4, respectively, of Appendix 7A of the ABWR SSAR. These tests are directly applicable to SBWR.

End-to-end testing of EMS is essentially performed as part of sensor channel testing of SSLC, as mentioned above, since EMS serves primarily to digitize and transmit sensor data to RPS and ESF (manual actuation functions on EMS can readily be tested by toggling these functions). For the interfaces in the off-line mode between the surveillance test equipment and SSLC/EMS in one protection system division, see Figure 420.46-1 which is attached to the response for RAI 420.46.

True end-to-end testing of EMS alone is performed off-line using techniques described in Appendix 7A of the ABWR SSAR (Section 7A.3, Response 1). First, where practical, the condition of the fiber optic cables is checked with an optical power meter and light source. For long cable runs, optical time domain reflectometry is used to measure and display optical loss along any continuous optical fiber path. Secondly, transmission characteristics of EMS are tested by bit generation. A bit error rate tester generates random bit streams into the LMU end of the multiplexing system and verifies correct receipt of these streams at the receiving end (input to SSLC or output of control room CMUs).

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.64**

Unlike the ABWR design, the SBWR design has numerous non-safety systems that perform important functions. Provide a discussion of any precaution included in the SBWR design to prevent or minimize the inadvertent initiation of non-safety systems.

(Note: This RAI was further clarified by the NRC via telephone conversation with GE on January 12, 1994 as follows:

*The question is asking for a discussion of the reliability measures taken in the design of the important plant operating systems (feedwater, steam bypass & pressure control, automatic power regulator) such that these systems will not challenge the safety-related systems during plant disturbances or equipment failure. For example, discuss triplicated, fault-tolerant digital control and its effect on single point failure so that feedwater control will always operate reliably and not cause a low water level scram.*

**GE Response:**

The controls for non safety-related systems, that perform important plant operation/power generation functions, are designed such that the functional capabilities of the safety-related systems are not obviated. Such non safety-related systems include Feedwater Control System (FWCS), Automatic Power Regulator System (APRS) and Steam Bypass and Pressure Control System (SBPC). Control and instrumentation for these systems are described in the SSAR sections 7.7.3, 7.7.4 and 7.7.5.

Controls for FWCS consist of three-element fault tolerant digital controller and incorporates many provisions to protect against common-mode failure. More discussion on the FWCS can be found in the SSAR subsection 7.7.3.5, response to RAI 420.95 and RAI 420.96.

Controls for APRS and SBPC consist of redundant, triplicated master controllers and provide defense against common mode failures. More discussion on the APRS can be found in the SSAR subsection 7.7.4.5 and response to RAI 420.97. More discussion on the SBPC can be found in the SSAR subsection 7.7.5.5, and the response to RAI 420.98.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.66**

Explain how the SBWR design complies with 10 CFR 50.62 (requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants). (Reference SSAR Section 7.4.1.)

**GE Response:**

The SBWR design incorporates the following specific features for Anticipated Transient Without Scram(ATWS) prevention/mitigation:

- an Alternate Rod Insertion (ARI) system that utilizes sensors and logic which are diverse and independent of the Reactor Protection System (RPS),
- electrical insertion of Fine Motion Control Rod Drives that utilizes sensors and logic which are diverse and independent of the RPS,
- automatic feedwater runback under conditions indicative of an ATWS event, and
- automatic initiation of Standby Liquid Control System under conditions indicative of an ATWS event.

Detailed discussion on each of these features and conformance with the ATWS rule of 10CFR50.62 is provided in the SSAR Section 15.8. Discussion on compliance with 10CFR50.62 and independence between ARI and RPS is also provided in response to SBWR RAI 420.76.

A block diagram depiction of input sensors, logic interface and output interface to FMCRD, ARI, and SLCS equipment for ATWS is shown in the SSAR figures 7.3-4a and 7.3-4b. ( These figures are GE proprietary information and are furnished under separate cover).

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.71**

Explain how standby liquid control system or leak detection and isolation system actuation signals prevent the containment isolation valves from opening, or close them when they are open. In addition, provide a discussion of how reactor water cleanup (RWCU)/shutdown cooling (SDC) system actuation signals are isolated from SLCS and LD&IS actuation signals. (Reference SSAR Section 7.4.3.)

**GE Response:**

The Reactor Water Clean-Up/ Shutdown Cooling (RWCU/SDC) system functions are non safety-related except for the containment isolation by signals from the Leak Detection & Isolation System (LD & IS) and for the reactor vessel isolation by signals from the Standby Liquid Control System (SLCS). The SSAR Subsection 6.2.4.3.2.2 provides discussion on the RWCU/SDC system containment penetration lines isolation function and Table 6.2-26 shows the pertinent data for the RWCU/SDC system isolation valves G31-F005A/B, F006A/B and F007A/B. The SSAR figure 21.5.4 shows the Piping and Instrumentation Diagram (P & ID) and figure 21.7.4-4 shows the Logic Diagram (LD) for RWCU/SDC system. Figure 21.7.3-3, (sheet 6) shows the Instrument and Electrical Diagram (IED) and figure 21.7.3-4 (sheets 52 and 53) shows the LD specifically for RWCU/SDC isolation function signals within LD & IS.

As shown on the RWCU/SDC logic diagram figure 21.7.4-4 (sheets 3 & 4) isolation valves G31-F005A/B F006A/B and F007A/B are signaled to close if they are open and the valve open signal (including manual open) is blocked as long as the LD & IS isolation signal is present or not reset. As shown on the IED figure 21.7.3-3, and the LD figure 21.7.3-4 the LD & IS signals for the RWCU/SDC isolation includes Standby Liquid Control System (SLCS) initiation signals.

RWCU/SDC system non safety-related functions control signals are non-Class 1E and are processed via Non Essential Multiplexing System (NEMS), while the isolation valves controls are treated as safety-related and the LD & IS inputs(including SLCS initiation) are processed via Essential Multiplexing System (EMS). Thus the RWCU/SDC system controls are kept separate and isolated from the isolation valves controls.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

**RAI 420.73**

Provide a discussion of (1) the reactor water cleanup system/shutdown cooling system parameters monitored, and (2) how monitored data are processed. (Reference SSAR Section 7.4.3.)

**GE Response:**

The Reactor Water Cleanup/ Shutdown Cooling (RWCU/SDC) system parameters monitored for system safety function (isolation of the process lines penetrating containment) are part of the Leak Detection & Isolation System (LD & IS). These process parameters consist of RWCU/SDC flow in each loop, main steamline tunnel area ambient temperature and reactor vessel water level. Discussion on monitoring each of these parameters can be found in the SSAR Subsections 5.2.5.2.1 and 5.2.5.2.2. A summary of LD & IS control and isolation functions vs. monitored process variables is presented in Table 5.2-8. Discussion on how variables for LD & IS control and alarm functions are processed is provided in Subsection 7.3.3.2. Other RWCU/SDC process variables, such as conductivity, radioisotopic concentrations, temperature, pressure and flow, used for the system non safety-related functions are discussed in Subsection 7.4.3.2

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.74**

Describe which isolation condenser (IC) parameters are monitored to ensure that (1) the isolation condenser system is ready to accomplish its safety function, and (2) the IC pool has sufficient water. (Reference SSAR Section 7.4.4.)

**GE Response:**

The Isolation Condenser (IC) system's readiness to accomplish its safety function is demonstrated by means of continuous monitoring of the process valve positions, power supply and the nitrogen supply pressure availability and the IC pool levels. The functional operability of the IC system components also is verified by periodic testing of the logic and valves.

Specifically, the following parameters are monitored:

- Steam line to IC supply valves B32-F001 and F002 position
- Condensate to RPV valves B32-F003, F004, F005 and F006 position
- Power supply for valves B32-F001, F004 and F006 solenoids
- Power supply for valves B32-F002, F0093 and F005 motors
- Nitrogen supply pressure to valves B32-F001, F004 and F006
- Condensate return line temperature downstream of valve B32-F004
- Differential pressure on condensate return line
- Water level in the IC/Passive Containment Cooling (PCC) pool

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.85**

Provide a discussion of the equipment classification of the nuclear boiler system (NBS). In addition, provide a discussion of how the NBS achieves its reliability (i.e., single failure criteria, defense against failures, etc.). (Reference SSAR Section 7.7.1.1.)

**GE Response:**

NBS equipment is classified as safety-related except for the non-safety-related part of the Main Steam Line (MSL) drains and Feedwater lines upstream of the motor operated gate valve outside containment. (Equipment classification details are provided in Table 3.2-1 and the NBS Process and Instrument Diagram, Figure 21.5.1-1 of the SSAR.)

Mechanical systems and equipment are designed with redundancy to provide backup capability for safety functions in the event of a single failure. The mechanical portion of each safety-related division is physically separated from the other division by sufficient distance or structural barriers.

Each Main Steam line includes one inboard and one outboard isolation valve, located as close as possible to the primary containment boundary. Each Feedwater line has one check valve inside containment, two check valves and one motor operated gate valve outside containment. Four Safety Relief Valve (SRV)s are installed on each MSL to provide Reactor Pressure Vessel (RPV) overpressure protection and depressurization capability following a Loss of Collant Accident (LOCA). Two redundant vacuum breakers are mounted on each SRV discharge line inside the drywell. Six Depressurization valves are installed to depressurize the RPV rapidly following a LOCA signal. (Additional details are provided in Figure 21.5.1-1 of the SSAR.)

The mechanical portion of each division of the safety-related NBS instrumentation located in the Reactor Building is physically separated from the other divisions by structural and/or fire barriers.

Physical separation or electrical isolation exists between Class 1E divisions. Physical separation or electrical isolation exists between Class 1E divisions and non-Class 1E equipment.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.85 (continued)

MSIV's are spring loaded, pneumatically operated globe valves designed to close on loss of gas pressure or loss of power to the solenoid operated pilot valves. The separate and independent action of either gas pressure or spring force is capable of closing the MSIV. Per SSAR Section 6.2.4.2.5:

Electrical redundancy is provided for MSIV's, eliminating the dependency on one power source to attain isolation. Electrical cables for MSIV's in the same line are routed separately. (For additional information on MSIV's, refer to SSAR Section 5.4.5.)

Each Safety Relief valve is equipped with a pneumatic accumulator and check valve for the Automatic Depressurization System, (ADS) and overpressure relief operation (power actuated mode) opening functions. The accumulators assure that the valves can be opened following loss of gas supply. Depressurization valves are squib actuated non-reclosing valves. Though each valve has two squibs, only one is required to actuate the shearing plunger. Squibs are initiated by two battery-powered independent firing circuits. (For additional information see SSAR Sections 5.2.2 and 6.3.3.2.)



**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.86**

Describe how the nuclear boiler system is tested. Provide a list of the RGs and standards with which it will comply. (Reference SSAR Section 7.7.1.4.)

**GE Response:**

The testing of the various parts of the Nuclear Boiler System (NBS) is given in various sections of the SAR as follows:

The calibration and testing of the NBS instrumentation is performed during preoperational testing as well as during plant operation as described in section 7.7.1.4 of the SAR. The testing requirements and applicable Regulatory Guides for the Automatic Depressurization Subsystem (ADS) instrumentation and control which is a part of the NBS, are given in section 7.3.1.1. The applicable Regulatory Guides are listed in Table 7.1-1 against "auto depressurization subsystem" and out of these the particular ones applicable for testing are 1.22, 1.105, 1.118, & 1.153.

The testing and inspection requirements for the SRV's are given in section 5.2.2.4.

The preservice and inservice testing of the reactor coolant pressure boundary (which includes portions of the NBS) and the related standards are given in section 5.2.4.

The testing and inspection requirements for the ADS are briefly described in section 6.3.3.4.

The NBS preoperational testing is described in section 14.2.8.1.1.

**RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS**

---

**RAI 420.90**

Describe the power supplies of the non-safety systems that perform important functions described in SSAR Section 7.7. The description should also include the sources of power. Are these power supplies redundant and uninterruptable?

**GE Response:**

The non-safety systems that perform important functions described in the SBWR SSAR Section 7.2 are:

- C11 - Rod Control and Information System (RC & IS)
- C31 - Feed Water Control System (FWCS)
- C82 - Automatic Power regulator System (APRS)
- C85 - Steam Bypass & Pressure Control System (SB & PCS)
- C91 - Performance Monitoring & Control Subsystem (PMCS) of the Process Computer System
- C91 - Power Generation Control Subsystem (PGCS) of the Process Computer System
- C62 - Non-essential Multiplexing System (NEMS)
- C51 - Automated Fixed In-core Probe Subsystem (AFIP) of the Neutron Monitoring System
- T31 - Containment Atmosphere Control System (CACCS) except for the containment isolation function

Power supply for each of these systems is provided based on the system functional requirements.

C11 - RC & IS

Discussion on the power supplies for the fine motion driver cabinets (FMDC) and rod brake controller cabinets (RBCC) is provided in response to RAI 420.89. Power supply for the rod action control cabinets is provided from the regulated, 120 Vac, non-class 1E, uninterruptible power sources which are backed by the diesel generator plant investment protection (PIP) buses and 125 Vdc normal battery and a standby battery.

RESPONSES TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)  
SIMPLIFIED BOILING WATER REACTOR (SBWR)  
SSAR CHAPTER 7, INSTRUMENTATION AND CONTROLS

---

RAI 420.90 (continued)

C31 - FWCS, C82 - APRS and C85 - SB & PC

The control and instrumentation power for these systems is provided from the regulated, 120 Vac, non-class 1E, uninterruptable power sources which are backed by the diesel generator PIP buses and 125 Vdc normal battery and a standby battery. These systems are also supplied with non-class 1E, 125 Vdc from station (8 hour) batteries with chargers backed by the diesel generator PIP buses.

C91 - PMCS & PGCS

The plant process computer is supplied from the regulated, 208/120 Vac, non-class 1E, uninterruptable power sources which are backed by the diesel generator PIP buses and 250 Vdc normal battery and a standby battery.

C62 - NEMS

The NEMS is supplied from the regulated, 120 Vac, non-class 1E, uninterruptable power sources which are backed by the diesel generator PIP buses and 125 Vdc normal battery and a standby battery.

C51 - AFIP

The AFIP instrumentation is powered by the regulated 120 Vac non-class 1E instrument bus which is backed by the diesel generator PIP bus.

T31 - CACS

The CACS instrumentation is powered by 125 Vdc non-class 1E instrument bus supplied from the normal battery and a standby battery with chargers which are backed by the diesel generator PIP bus.