Question 032.27

With regard to remote shutdown panels, describe the criteria for the installation and routing of instrumentation and control circuitries between these panels and the main control room control boards.

Response

The main control panels are located at El. 35 ft in the Electrical Auxiliary Building (EAB). The auxiliary shutdown panel (ASP) is located at El. 10 ft in the same building. Control circuits for equipment required for safe shutdown are isolated by transfer switches, located in each of the Train A, B, and C Engineered Safety Feature (ESF) switchgear rooms. These transfer switches select between control room and auxiliary shutdown panel (ASP) control. Instrumentation circuits required for safe shutdown are routed from signal processing cabinets (located in five separate areas adjacent to the ASP) to the control room and the ASP. Isolation is provided to protect control room instrumentation from possible faults in the ASP instrumentation and to protect ASP instrumentation from possible faults in the control room instrumentation. Safe shutdown equipment cables are routed through separate fire areas to the control room and ASP; in addition train-to-train separation is maintained.

Cables of different trains are separated in accordance with Regulatory Guide 1.75 and IEEE 384-1974. Except where they converge at control panel locations, the cables are routed through different floor levels and different fire areas to provide maximum separation possible.

Where minimum separation distance between train and non-Class 1E raceways cannot be maintained, cable tray covers or conduit are utilized as barriers in accordance with the criteria referenced.

HISTORICAL INFORMATION

HISTORICAL INFORMATION

Question 032.9

The discussion of the solid state logic testing does not address several problems which have been experienced with the testing of the solid state protection system in operating nuclear power plants. For each of the following problems, describe how the implementation of the solid state equipment in the STPEGS has been modified to prevent the stated problem:

1. Integrated circuit ZlC (a NAND gate in the scram breaker undervoltage card) is not tested by the automatic test equipment.

2. An isolation problem was identified in the general warning circuit.

3. BFD-31 (sic) relays were not qualified for the equalizing voltage.

4. Previously qualified components were modified during production by their vendors and the modified components could not satisfy their original functional requirements.

5. Diodes with insufficient voltage ratings have been used in some circuits.

Response

Items 1, 2, and 5 are related to the same problem. This problem was an undetectable failure which occurred in the General Warning Alarm Circuit during testing of the Solid-State Protection System (SSPS). The consequence of this failure was reported by an operating plant. Westinghouse assessed the incident, reported the generic impact to the NRC, and submitted for approval modifications necessary to resolve the deficiency. After NRC acceptance was received (Letter June 21, 1976, R. Heineman to C. Eicheldinger) NRC Inspection and Enforcement witnessed verification tests which Westinghouse conducted. The modifications have been implemented in the SSPS for the South Texas Project Units 1 and 2, and are confirmed and documented in accordance with established Westinghouse PWR Quality Assurance procedures.

Item 3

BFD relays are not used in the instrumentation and control systems for STPEGS Units 1 & 2.

Item 4

Modifications to Westinghouse-supplied AR relays with latch assembly used in the protection system equipment for STPEGS Units 1 and 2 were completed prior to shipment of the equipment to the site. Confirmation and documentation are in accordance with established Westinghouse PWR Quality Assurance procedures. These changes resolve a tolerance problem discovered and reported to the NRC by Westinghouse.

Question 032.10

According to Regulatory Guide 1.70 "Standard format and content" Sections 7.2 and 7.3 the applicant should provide in the FSAR electrical schematic diagrams for all RTS and ESF circuits and supporting systems, and final logic diagrams, P&I diagrams, and location layout drawings.

Provide this information in your FSAR and describe any significant differences there may be between the logic diagrams and schematics which you previously submitted in the PSAR and the effects on safety-related systems.

Response

Electrical schematic diagrams and logic diagrams are provided in reference in Section 1.7. The piping and instrument diagrams (P&IDs) are provided in the appropriate sections of the UFSAR, with the system discussion. Tables 7.3-5 through 7.3-12, and Table 7.3-14 and 7.3-15 give the equipment actuated by the various Engineered Safety Features Actuation System (ESFAS) signals, and the P&ID number and UFSAR figure number on which each component may be found. Differences between logic diagrams and schematics previously submitted in the PSAR and those in the UFSAR is a result of the deletion of the Emergency Boration System (EBS), incorporation of new regulatory requirements (TMI), and continued system design.

Question 032.31
Describe the design basis, and separation and isolation for:

(a) Reactor Trip on Turbine Trip circuitry. Also, provide detailed cable routing diagrams for this trip circuitry from the sensor in the turbine building to the final actuation located in the Reactor Trip System.

(b) The circuitries from Reactor Trip System to the BOP devices in the Turbine/Auxiliary Building.

Response

Part (a)

The reactor trip on turbine trip is an "anticipatory trip".

The reactor trip on turbine trip provides additional protection and conservatism beyond that required for the health and safety of the public.

The signal is derived from redundant limit switches on each turbine steam stop valve and from redundant controls on three pressure switches that monitor the turbine emergency trip fluid pressure. Figure 7.2-17 shows the functional diagram and Section 7.2.1.1.3, item 6, describes the design basis for this reactor trip. The limit switches and pressure switches identified above are purchased as Class lE qualified equipment.

These limit switches and pressure switches are located in the nonseismically qualified Turbine Generator Building (TGB). Seismic qualification is limited to the mounting of the components at their respective localities, the mounting supports for the rigid steel conduits, and to the components themselves.

Wiring from these devices, located in the TGB, to the Solid-State Protection System (SSPS) cabinets, located in the Mechanical Electrical Auxiliary Building is routed in accordance with the same separation criteria applicable to Protection Channels, I, II, III and IV (as discussed in Sections 7.1.2.2 and 8.3.1.4), and is in rigid steel conduit dedicated exclusively for these signals within the TGB. Detailed cable routing diagrams for this trip circuitry was sent under separate cover, by letter ST-HL-AE-1486, dated October 29, 1985.

Part (b)

The circuitry from the Reactor Trip System to balance-of-plant (BOP) devices in the TGB is limited to the turbine trip on reactor trip.

The turbine trip on reactor trip circuitry is implemented in accordance with IEEE 279 with the following exceptions:

1. The circuitry is routed through a nonseismic structure.

Response (Continued)

2. The turbine trip equipment supplied by the turbine manufacturer, although of appropriate high quality, is not seismically or environmentally qualified to nuclear qualification standards.

3. The turbine solenoids are non-Class 1E and are powered by highly reliable non-Class 1E power sources.

The circuit design, up to and including the turbine trip solenoids, conforms to those sections of IEEE 279 concerning single failure (Section 4.2), quality (Section 4.3), channel integrity (Section 4.5, excluding seismic), channel independence (Section 4.6), and testability (Section 4.10), so as to assure adequate reliability.

The turbine trip solenoids are implemented so that the turbine is tripped on loss of control power. Wiring from the SSPS cabinet (located in the Mechanical-Electrical Auxiliary Building (MEAB)) to the turbine trip solenoids (located in the TGB) is routed in accordance with the same separation criteria applicable to Class lE circuits (Sections 7.1.2.2 and 8.3.1.4) and are in rigid steel conduit dedicated exclusively for these signals to maintain the integrity of the individual redundant trains.

Question 032.41

We deduce from Figures 7.2-3 and 7.2-4 that a single failure of the P-6 signal generation circuitry so that P-6 is energized at a power level lower than the P-6 setpoint places the reactor system in jeopardy. The operator can block out the source range trip at power levels at which it was intended for protection. In addition, the trip circuitry will not reset as the power level decreases below the P-6 setpoint during a power reduction. This appears to violate the single failure criterion. Bring your system in compliance with the single failure criterion or justify not so doing.

Response

The Chapter 15 analysis does not currently take credit for the source range reactor trip, which is provided as a backup trip.

Question 032.43

Engineering Safety Features (ESF) Reset Controls (IE Bulletin 80-06)

If safety equipment does not remain in its emergency mode upon reset of an engineered safeguards actuation signal, system modification, design change or other corrective action should be planned to assure that protection action of the affected equipment is not compromised once the associated actuation signal is reset. This issue was addressed in IE Bulletin 80-06. For facilities with operating licenses (OL) as of March 13, 1980, IE Bulletin 80-06 required that reviews be conducted by the licensees to determine which, if any, safety functions might be unavailable after reset, and what changes could be implemented to correct the problem.

For facilities with a construction permit including OL applicants, Bulletin 80-06 was issued for information only.

The NRC staff has determined that all construction permit holders, as part of the OL review process, are to be requested to address this issue. Accordingly, you are requested to take the actions called for in Bulletin 80-06 Actions 1 thru 4 under "Actions to be taken by Licensees". Complete the review verification and descriptions of corrective actions taken or planned as stated in Action 1 thru 3 and submit the report called for in Action Item 4.

Response

The STPEGS Engineered Safety Features (ESF) systems were reviewed against requirements in IE Bulletin 80-06, as requested by Action 1. The STPEGS position including exceptions is stated in Sections 7.3.1.2.4, 7.3.2.1.1(3), and 7.3.3.1.1(3).

Actions 2 through 4 of IE Bulletin 80-06 were completed prior to fuel load. The testing required by Action 2 is included in the interlocks and controls testing for the various systems, as discussed in Section 14.2.12.

Question 032.42

If reactor controls and vital instruments derive power from common electrical distributions system, the failure of such electrical distribution systems may result in an event requiring operator action concurrent with failure of important instrumentation upon which these operator actions should be based. This concern was addressed in IE Bulletin 79-27 (enclosed). On November 30, 1979, IE Bulletin 79-27 was sent to operating license (OL) holders, the near term OL applicants (North Anna 2, Diablo Canyon, McGuire, Salem 2, Sequoyah, and Zimmer), and other holders of construction permits (CP), including South Texas Project. Of these recipients, the CP holders were not given explicit direction for making a submittal as part of the licensing review. However, they were informed that the issue would be addressed later.

You are requested to address these issues by taking IE Bulletin 79-27 Actions 1 through 3 under "Actions to be Taken by Licensees". Within the response time called for in the attached transmittal letter, complete the review and evaluation required by Actions 1 thru 3 and provide a written response describing your reviews and actions.

Response

The responses to each action item of IE Bulletin 79-27 are given below by action item number.

1. A review of the instrumentation and control systems which could affect the ability to achieve a hot standby condition (see Section 7.4) and a cold shutdown condition (Appendix 5.4.A) has been performed. Each of these systems is supplied power from one of the redundant Class 1E 120 vac or 125 vdc busses. Refer to Figure 8.3-3 (sheet 1).

   The Class 1E 120 vac power is provided from one of the six 120 V vital AC channel distribution panels. Each panel is supplied power either through manual transfer circuit breakers or a static transfer switch from an individual inverter. There are two panels each for Channels I and IV and one panel each for Channels II and III. See also Section 8.3.1.1.4.5.

   The Class IE 125 vdc power is provided from one of the four 125 vdc distribution switchboards. Each switchboard is connected to a separate battery and two battery chargers. See also Section 8.3.2.1.1.

   Turbine, nonsafety-related reactor and other nonsafety-related instrumentation and control systems are provided power from non-Class 1E panels and switchboards. Refer to Figure 8.3-3 (sheet 1). The non-Class 1E 120 vac power for the Electrical Auxiliary Building (EAB) is provided from one of two 120 V vital AC distribution panels, each connected to an automatic transfer switch and an individual inverter. Another 120 V vital AC distribution panel is provided in the Turbine Generator Building (TGB); this panel is connected to an inverter package with an internal static transfer switch. Two 120 vac regulated power distribution panels are also provided for non-Class 1E instrumentation and control systems.

Response (Continued)

The non-Class 1E 125 vdc power is provided from two 125 vdc distribution switchboards, each connected to one battery and two battery chargers. A 48 vdc distribution switchboard supplying power only to the plant annunciator system is connected to one battery and two battery chargers. A non-Class 1E 250 vdc distribution switchboard is provided in the TGB, serving motors and the main generator control panels; it is connected to one battery and two battery chargers.

A separate non-Class 1E uninterruptible power supply system (120 vac) is provided for the plant computer. The Emergency Response Facilities (ERF) computer is powered from non-Class 1E 480 vac and has an uninterruptible power supply system to support its functions during a loss of power. Refer to Figure 8.3-3 (sheet 2).

The Radiation Monitoring System (RMS) computer is powered from non-Class 1E 480 vac and has uninterruptible power supply systems to supports its functions during a loss of power.

Non-Class 1E power is not required to support the ability to achieve hot standby or cold shutdown conditions. However, the non-Class 1E power supports indications to the operator (such as computer alarms and annunciation) of abnormal conditions and control systems normally used during plant operating modes.

1a. Loss of power to each of the six Class 1E 120V vital AC distribution panel busses is alarmed individually in the control room on a window of the Engineered Safety Features (ESF) status monitoring system. A ground fault on any of these panel busses is alarmed individually on a window of the plant annunciator as Panel Trouble. The ERF computer also indicates that a loss of power or a ground fault has occurred. Alarms are provided for each inverter through the ERF computer and the ESF status monitoring system.

Loss of power to each of the four Class 1E 125 vdc distribution switchboard busses is alarmed individually in the control room on a reflash window of the plant annunciator, along with other bus and battery charger alarms, as System Trouble. The ERF computer indicates whether bus or charger trouble has occurred. The ESF status monitoring system provides other battery and charger alarms.

Loss of power or a ground fault to the two EAB non-Class 1E 120V vital AC distribution panel busses is alarmed individually in the control room through the plant computer. Alarms are provided for each inverter through the annunciator and the plant computer.

Loss of power or a ground fault to the TGB non-Class 1E 120V vital AC distribution panel bus is alarmed in the control room through the plant computer. Inverter/rectifier alarms are provided through the plant computer and the annunciator.

Response (Continued)

Loss of power or a ground fault to either of the two non-Class 1E 120 vac regulated power distribution panel busses is alarmed in the control room through the plant computer.

Loss of power to either of the two non-Class 1E 125 vdc switchboard busses is alarmed individually in the control room on a reflash window of the plant annunciator, along with other bus and battery charger alarms, as System Trouble. The plant computer indicates whether bus or charger trouble has occurred.

Loss of power to the non-Class 1E 48 vdc switchboard bus, along with other bus alarms, is alarmed in the control room via the plant computer. Other bus and battery charger alarms are provided on a reflash window of the plant annunciator as System Trouble. The plant computer indicated whether bus or charger trouble has occurred.

Loss of power to the non-Class 1E 250 vdc switchboard bus is alarmed in the control room on a reflash window of the plant annunciator, along with other bus and battery charger alarms, as System Trouble. The plant computer indicated whether bus or charger trouble has occurred.

Loss of power or a ground fault to the non-Class 1E 120 vac distribution panel bus for the plant computer is alarmed in the control room. Various battery, charger, and inverter alarms for the computer uninterruptible power supply (UPS) are given in the control room on two reflash windows of the plant annunciator, one for Battery/Charger Trouble and one for Inverter Failure. The ERF computer indicated which signal caused the annunciator alarm.

Power to the ERF data acquisition, computer and display equipment is provided by an uninterruptible power supply (UPS) through two distribution panels, as shown on Figure 8.3-3 (sheet 2). Loss of power to these distribution panels is not alarmed specifically to the control room operator. However, should power to either panel be lost, the six monitors (CRTs) in the control room would not be updated, providing unambiguous indication of the power loss.

Various alarms are available to the operator through the ERF computer concerning the functioning of the UPS. These alarms include improper breaker positions (of power supply to the rectifier/charger, battery output, inverter input, inverter output, bypass power main supply and bypass power to static switch breakers), inverter problems (out of sync, low DC volts, fan failure), static switch not in normal position, and manual bypass switch not in normal position.

Responses (Continued)

Power to the Radiation Monitoring System computer (RM-11) is also supplied by UPS systems, as shown on Figure 8.3-3 (sheet 2). Since alarm output contacts are held in the non-alarm condition by energized relays, should power be lost to either computer, all annunciator windows associated with that computer would be lit and an audible alarm sounded. Three annunciator windows are associated with the Radiation Monitoring System computer. Also the associated CRT screen in the control room would be blank.

The RM-21A Dose Assessment computer has been replaced with a new Dose Assessment and Report Generation computer system with new software application. The new computer system runs in an ORACLE database environment with current technology servers and workstations. It can be accessible anywhere on site through the plant Local Area Network (LAN); it has been designed to be highly reliable utilizing hardware redundancy and backup power sources using uninterruptible power supply (UPS) and diesel generator.

1b. The review and evaluation of the Class 1E and non-Class 1E busses described above indicate that loss of power to any one instrumentation and control bus will not inhibit the ability to achieve a cold shutdown condition.

1c. The review and evaluation indicate that design modifications are not required.

2. The operating procedures used by control room operators will be reviewed with respect to loss of power to each Class 1E and non-Class 1E bus supplying power to instrumentation and control systems.

2a. The procedures will define symptoms and specify actions to be taken by the operators upon loss of power to Class 1E or non-Class 1E instrumentation and control systems.

2b. Where necessary, the procedures will specify alternate instrumentation and control circuits for use by operators.

2c. The procedures will include methods and precautions for restoring power to each Class 1E and non-Class 1E bus supplying power to instrumentation and control systems.

Should any design modifications or administrative controls be required as a result of the development of these procedures, descriptions of these will be provided.

3. 1E Circular No. 79-02 has been reviewed in relation to the safety-related power supply inverters. All safety-related power supply inverters are Class 1E. For these inverters, relative to the Circular requirements:

3a. Class 1E inverters do not use time delay circuitry.

3b. The AC input to each Class 1E inverter is to a transformer/rectifier section. The

Response (Continued)

transformer has taps that will be set according to the recommendations of the manufacturer. A relay trips the transformer/rectifier supply circuit breaker if overvoltage occurs.

3c. The alternate 120 V source is supplied either by manual operation of interlocked circuit breakers or through a static transfer switch. Manual operation of interlocked bypass switches will be used during testing or if the static transfer switch fails.

3d. Administrative controls will confirm the position of transformer taps and manual bypass circuit breakers when maintenance or testing have been completed.

No design modifications or additional administrative controls are required.

Question 032.22

General design criteria 20 and 25 require that the protection system be designed to assure that specified fuel design limits are not exceeded from an accidental withdrawal of a single rod control cluster assembly (not ejection). In the accident analysis, presented in Section 15.4 of the FSAR, it is assumed that no electrical or mechanical failure in the rod control system could cause the accidental withdrawal of a single rod control system could cause the accidental withdrawal of a single rod control cluster assembly. However, FSAR Chapter 7.7.1 does not describe how the design prevents such an occurrence. Provide a detailed description of the control circuitry and discuss how the design meets the requirements of criteria 20 and 25. Also, demonstrate conformance with Branch Technical Position 14 as stated in Appendix 7A of the standard review plant or identify and justify the alternative designs. In particular, demonstrate that no single failure in the rod control system can result in a violation of the specified fuel design limits while retrieving a rod which is out of alignment.

Response

For the discussion of design features that prevent an inadvertent single rod withdrawal, see Section 7.7.2.2. The capability of withdrawing a single rod cluster control assembly (RCCA) in a control bank is necessary in order to allow the reactor operator to retrieve an RCCA should one be accidentally dropped or misaligned.

In order to retrieve the RCCA, the Rod Control System is manually aligned to permit withdrawal of the dropped RCCA. The operator then manually withdraws the affected RCCA, with appropriate manual turbine load or boron concentration control to maintain the programmed value of Reactor Coolant System average temperature. Withdrawal is terminated when the RCCA reaches its recorded group step counter position. The Technical Specifications define the time period in which the dropped RCCA must be restored to operable status, within specified alignment requirements in order to continue power operation.

After the Rod Control System is manually aligned to permit withdrawal of the single RCCA, a single RCCA withdrawal accident could occur only with a subsequent single failure of the Rod Control System or an operator error during the recovery procedure. If the withdrawal is to be caused by a single failure, the failure would have to occur within the Technical Specification time limit for recovery from the failure which caused the RCCA to drop. In order for the single RCCA withdrawal event to occur due to operator error, the operator would have to:

1. Withdraw the RCCA all the way out of the core, ignoring the recorded step counter position of the remainder of the group. The group position is recorded by the operator before the retrieval process proceeds.

Response (Continued)

2. Ignore operating instructions which specify that the programmed Reactor Coolant System average temperature be maintained by manually controlling turbine load or born concentration.

3. Disregard most or all of the following event indications:

   a. Rod position indicators

   b. Rod deviation alarm

   c. T_{avg} deviation alarm

   d. High neutron flux alarm and rod stop

   e. High Delta T rod stop

   f. Control bank D Rod withdrawal limit alarm

   g. Continuous recorder indication of increasing nuclear power and T_{avg}

   h. T_{avg} - T_{ref} deviation alarm

CN-3096

Even if the operator were to withdraw the RCCA completely out of the core, there is no DNB problem unless the operator also ignores items b and c, above. The case of a fully withdrawn single bank D rod at full power is covered by the static rod misalignment analysis presented in Section 15.4.3.

A dropped or misaligned RCCA is itself an American Nuclear Society (ANS) Condition II event caused by some single failure in the Rod Control System. There no "planned adjustments" affecting a single RCCA which are otherwise required for Westinghouse plants.

Retrieval of the RCCA is therefore not a normal operational occurrence, and is under strict administrative control. The operator is expected to be fully cognizant of all actions and plant indications associated with the retrieval process. The combined probability of dropping or misaligning a single RCCA and either (1) a single failure which causes undesired RCCA withdrawal or (2) a series of operator errors as outlined above, plus failure or operator disregard of event indication, is so low that classification of the single RCCA withdrawal event as a Condition III fault is justified. For example, from experience the expected frequency of any RCCA drop while operating in the power range is expected to be about 0.6 per year. This probability should be multiplied by 0.17 to give the total probability per year of a Bank D RCCA drop, since full withdrawal of a single RCCA leads to an adverse power distribution only if the RCCA is a member of a partially inserted bank, and only control bank D is inserted in the core above about 50 percent power.

Response (Continued)

The probability of either a single failure or a series of operator errors during the recovery period which could lead to subsequent withdrawal of the RCCA is estimated to be no worse that 0.01 based on WASH-1400 Appendix III. This gives a combined probability of 0.001 per year which is well within the expected frequency of ANS Condition III events. A survey of data obtained from Westinghouse reactors operating between 1972 and 1974 supports this probability assessment, and also shows that for all single dropped RCCA events reported in the approximately 30 reactor years of operation between 1972 and 1974, the dropped RCCA was in all cases retrieved without incident.

Since the single RCCA withdrawal accident can only occur as a result of multiple faults or failures, and the probability of occurrence of these failures is within the expected frequency of Condition III events, it is concluded that the single RCCA withdrawal accident should continue to be classified as a Condition III event. As a Condition III event, the consequences presented in Section 15.4.3 are acceptable, not in violation of general design criterion 20 or 25 and, therefore, are in conformance with Branch Technical Position (BTP) Instrumentation and Controls System Branch (ICSB) 14.

Question 032.44

Operating reactor licensees were informed by IE Information Notice 79-22, issued September 19, 1979, that certain nonsafety-grade or control equipment, if subjected to the adverse environment of a high energy line break, could impact the safety analyses and the adequacy of the protection functions performed by the safety grade equipment. Enclose is a copy of IE Information Notice 79-22, and reprinted copies of an August 20, 1979, Westinghouse letter and a September 10, 1979, Public Service Electric and Gas Company letter which address this matter. Operating Reactor licensees conducted reviews to determine whether such problems could exist at operating facilities.

We are concerned that a similar potential may exist at light water facilities now under construction. You are, therefore, requested to perform a review to determine what, if any, design changes or operator actions would be necessary to assure that high energy line breaks will not cause control system failures to complicate the event beyond your FSAR analysis. Provide the results of your reviews including all identified problems and the manner in which you have resolved them to NRR.

The specific "scenarios" discussed in the above referenced Westinghouse letter are to be considered as examples of the kinds of interactions which might occur. Your review should include those scenarios, where applicable, but should not necessarily be limited to them. Applicants with other LWR designs should consider analogous interactions as relevant to their designs.

Response

IE Information Notice 79-22 specifically identified four potential interaction scenarios between nonsafety-grade and safety-grade equipment which could occur because of the effect of an adverse environment following a high energy line break. The four systems identified are:

- Steam Generator Power-Operated Relief Valve (PORV) Control System
- Pressurizer PORV Control System
- Main Feedwater Control System
- Automatic Rod Control System

A discussion of each scenario and affected system and its applicability to STPEGS follows.

Response (Continued)

It has been postulated that a failure of the steam generator (SG) PORV control system, due to adverse environment following a feedline rupture, could cause a depressurization of the unaffected SGs. The STPEGS SG PORV system is a Class 1E system. In addition, all portions of the SG PORV system that could be exposed to an adverse environment are isolated in the Isolation Valve Cubicle (IVC) structure on a loop-by-loop basis. Only one PORV could be affected by adverse conditions and that PORV would be in the affected SG loop. For these reasons, the scenario concerning the SG PORV control system is not applicable to STPEGS.

The second scenario assumes that the pressurizer PORVs fail in the open position, due to an adverse environment following a feedline rupture. This would cause a depressurization of the Reactor Coolant System (RCS), which may result in a voiding of the RCS and potentially uncovering the core. However, all portions of the pressurizer PORV control system located inside Containment have been environmentally qualified for the adverse environment. For this reason, the scenario involving the pressurizer PORV control system is not applicable to STPEGS.

The third scenario assumes a failure of the main feedwater control system, due to adverse environment following a small feedline rupture which occurs between the main feedline check valve and the Containment penetration. Such a failure could cause the liquid mass in the intact SGs at the time of reactor trip to be less than was assumed in the UFSAR analysis. The STPEGS SG water level transmitters are located within the Containment and are environmentally qualified for the adverse environment. The steam flow transmitters are also located in containment but are not environmentally qualified because the special treatment exemption has been applied. The feedwater flow transmitters are located inside the Turbine Generator Building (TGB) and the feedwater process controls are located in the Mechanical and Electrical Auxiliary Building (MEAB). Because of their respective locations, the transmitters and the feedwater controls would not be exposed to an adverse environment following a feedline rupture between the main feedline check valve and the Containment penetration. In addition, the feedwater isolation valves and associated instrumentation are compartmentalized by loop within the IVC, thus restricting exposure to the harsh environment to the loop with the break. For these reasons, the scenario involving a failure of the main feedwater control system is not applicable to STPEGS.

The fourth scenario assumes that the automatic rod control system fails, due to adverse environment following a small steamline rupture, in such a way that the control rods begin stepping out prior to receipt of a reactor trip signal on overpower ΔT. This could result in a departure from nucleate boiling ratio (DNBR) less than the limiting value. For a steam line rupture, the excore detectors which supply input to the rod control system could be exposed to the adverse environment and initiate rod withdrawal. In STPEGS, these excore detectors (and associated safety-related equipment) are part of the reactor trip system and have been environmentally qualified for a limited period of time (5 minutes) after a main steam line break (MSLB). Analysis has shown that steam line breaks which are too small to cause a reactor trip in less than five minutes will result in adequate DNB margin for the duration of the event. Control rod withdrawal will eventually bring the reactor into a condition from which an overpower ΔT reactor trip signal will be generated. For this reason, the scenario involving the automatic rod control system for a steam line rupture is not applicable to STPEGS.

Question 620.2N

Provide the following information and clarification regarding your summary report for the Detailed Control Room Design Review (DCRDR) submitted April 12, 1984:

a. Your systems function and task analysis (SFTA) was performed through document reviews, briefings, and walk-throughs on the mock-up and updated using the revised mock-up as reported in the SFTA Validation Report. Because the SFTA was not based on upgraded emergency operating procedures (EOPs) required by Supplement 1 to NUREG-0737, and because EOPs are not typically available at early stages of design and construction, but should be available prior to licensing, please confirm, after EOPs are finalized, that information and control function needs have been adequately identified and are satisfied by available instrumentation and controls.

b. Verify that an objective comparison of independently determined display and control requirements, as determined by function and task analyses has been made with the control room inventory to identify missing controls and displays as required in Supplement 1 to NUREG-0737, and summarize the results of this comparison.

c. Substantiate that an objective, independent determination of the operator information and control needs for each operator task has been made before instrument and control specifications are developed.

d. Describe the specific process for using generic guidelines and background documentation to identify the characteristics of needed instrumentation and controls. For the information of this type that is not available from the Emergency Response Guidelines and background documentation, described the process used to generate this information to derive required instrumentation and control characteristics.

e. Verify an auditable record is maintained regarding how the needed characteristics of required instruments and controls were determined for each instrument and control used to implement the emergency operating procedures.

f. Discuss the present status of the design of the sit-down control stations.

g. Provide a summary discussion and conclusions regarding the supplementary assessment to accommodate smaller (i.e., 5th-20th percentile) female operators and to use extended functional reach criteria for lower percentile subjects.

Question 620.2N (Continued)

h. Discuss the resolution of the three category "A" human engineering deficiencies regarding:

(1) The green Rotobellite indicator lights which cannot be distinguished when illuminated;

(2) The bypass and inoperable status light legend which are unreadable due to narrow stroke width and inadequate character separation and line spacing; and

(3) The legend messages containing more than three lines of text.

i. Discuss the results of the resolution of all unresolved human engineering deficiencies in categories "B", "C", "D", and "E".

j. Provide justification and rationale for using random checks rather than 100 percent checks of items which cannot be completed until the control room and/or simulator is operational.

k. Your present schedule is stated in general terms for completion of all planned DCRDR work. Provide a more specific schedule for implementation of corrective actions for human engineering deficiencies.

Response

STPEGS performed the Control Room Design Review (CRDR) as part of an overall integrated effort to address the requirements and guidance of Supplement 1 to NUREG-0737. CRDR activities were and continue to be integrated with the following STPEGS activities:

- Development of the Safety Parameter Display System (SPDS) which is implemented via the Emergency Response Facilities Data Acquisition and Display System (ERFDADS).

- Determination of instrumentation requirement for post-accident monitoring to address Regulatory Guide (RG) 1.97.

- Development of STPEGS Emergency Operating Procedures (EOPs) that are human factored, function oriented, and well integrated with the plant design.

The CRDR System Function and Task Analysis (SFTA) was independently performed by Torrey Pines Technology to comply with NUREG-0700 as defined in the STPEGS CRDR Program Plan submitted to the NRC by letter ST-HL-AE-899, Mr. J. H. Goldberg of Houston Lighting and Power to Mr. Thomas M. Novak, U.S. Nuclear Regulatory Commission dated October 20, 1982, and resubmitted with the CRDR Executive Summary Report by letter ST-HL-AE-1080, Mr. J. H. Goldberg of Houston Lighting and Power to Mr. Darrell G. Eisenhut, U.S. Nuclear Regulatory

Response (Continued)

Commission, dated April 12, 1984. A flow chart of the STPEGS CRDR SFTA process is shown in Figure Q620.2N-1. This SFTA was based on the Westinghouse Owners Group (WOG) Emergency Response Guidelines (ERGs) as well as the STPEGS Plant design. The STPEGS design was integrated with the WOG ERGs utilizing STPEGS design documentation and input from STPEGS plant operators to develop functional flow diagrams specific to STPEGS. These diagrams formed the basis for the SFTA tabulation of the operator tasks and required equipment (i.e., instrumentation or controls) associated with each task. This process for performing the STPEGS CRDR SFTA and the SFTA results are documented in the STPEGS CRDR System Function and Task Analysis Report submitted to the NRC with the CRDR Executive Summary. Following the revision to the STPEGS main control panel layout, the SFTA tabulations of operator tasks and required equipment were revised to reflect the new panel equipment and locations. This update formed the basis of the SFTA validation of the panel design. A procedure walk-through/talk-through was also conducted using draft plant specific procedures in the control room mock-up. These draft plant specific procedures were based on the WOG ERGs, STPEGS process design, and the STPEGS SFTA functional flow diagrams. This SFTA validation process and the results are documented in the STPEGS CRDR System Function and Task Analysis Validation Report submitted to the NRC with the CRDR Executive Summary.

In parallel with the STPEGS CRDR SFTA efforts, STPEGS performed an analysis to address post-accident monitoring requirements to respond to Regulatory Guide 1.97. A flow chart of the STPEGS RG 1.97 implementation process is shown in Figure Q620.2N-2. This was accomplished by performing a task analysis based on the WOG ERGs to identify variables necessary for implementation of the guidelines. This analysis was applied to the STPEGS specific design through a plant survey of the STPEGS design documents. The STPEGS specific analysis is summarized in STPEGS UFSAR, Appendix 7B. The analysis itself identified, in addition to the variables necessary for implementation of the ERGs, variable display requirements including range, accuracy, qualification, redundancy, recording needs, and operator task utilization. These requirements were compared to existing STPEGS instrumentation to determine required design changes. These changes were incorporated in the revised main control panel mock-up and were utilized in the CRDR SFTA validation. This instrumentation is summarized in UFSAR Table 7.5-1.

Also in parallel with the STPEGS CRDR SFTA and with the STPEGS RG 1.97 implementation, STPEGS began development of the EOPs based on the WOG ERGs, the identified RG 1.97 variables, and the revised panel layouts.

The RG 1.97 variable list developed during the RG 1.97 implementation process was then utilized to determine the ERFDADS/SPDS data base. This system is described in UFSAR Section 7.5.7. A subset of this data base, those Category I Type A and Type B variables determined from the Optimal Recovery Guidelines (ORGs) and the Critical Safety Function (CSF) Status Trees/Functional Recovery Guidelines (FRGs), respectively, is the data base for the Qualified Display Processing System (QDPS) described in UFSAR Section 7.5.6. The ERFDADS/SPDS display development process is shown in Figure Q620.2N-3.

Response (Continued)

a. The development of the South Texas Project Electric Generating Station (STPEGS) EOPs is based on Revision 1 of the Westinghouse Owners Group (WOG) Emergency Response Guidelines (ERGs). During the conversion process the instrumentation and control requirements of the ERGs are compared with the RG 1.97 equipment to develop both the normal and alternate indications available to the operators. Prior to final approval of the STPEGS EOPs, they were placed through a verification and validation program as specified by Supplement 1 to NUREG-0737. This program was described in detail in the Procedure Generation Package in letter ST-HL-AE-1266, dated June 14, 1985, from Mr. J.G. Dewease of Houston Lighting and Power Company to Mr. Hugh L. Thompson, Jr. of NRC. This program confirmed that the instrumentation and control function needs have been adequately identified and are satisfied. The validation of the STPEGS Emergency Operating Procedures was conducted during May 1986. This validation process was performed in the STPEGS simulator, using scenarios chosen to test the principal safety actions and branching into the steps of as many procedures as possible. This EDP validation process and the results are discussed in the Emergency Operating Procedures Validation Report, which was provided to the NRC by letter ST-HL-AE-1860, Mr. M.R. Wisenburg of Houston Lighting and Power Company to Mr. Vincent S. Noonan, U.S. Nuclear Regulatory Commission, dated December 23, 1986.

b. The CRDR SFTA process included a comparison of the display or control requirement, as defined by a task objective, to the main control panel equipment. The task objectives are stated in specific terms relating to plant equipment, for status or control requirements. This comparison was performed by Torrey Pines Technology personnel during the SFTA. The task objectives defining a display or control requirement were developed from functional flow diagrams. These functional flow diagrams were developed by Torrey Pines Technology utilizing the WOG ERGs, plant process design documentation, and input from plant design and operations personnel relative to plant system function.

   The RG 1.97 implementation process included a comparison of the display or monitoring requirements, as defined by the STPEGS design basis to respond to RG 1.97, to the main control panel equipment. The monitoring requirements are stated in terms of range, accuracy, and RG 1.97 category which in turn defines instrumentation qualification, redundancy, and display and/or recording requirements. This comparison was performed and documented in an STPEGS RG 1.97 plant survey.

   As a result of the CRDR SFTA, it was determined that the existing panel layout contained the required instrumentation and control equipment with the exception of essential cooling water (ECW) flow indication. This was documented as HED S-875 in the CRDR Executive Summary. The adequacy of the existing equipment was not specifically addressed as part of the SFTA. This was addressed as

Response (Continued)

part of the control room survey and as part of the RG 1.97 review. The CRDR SFTA identified significant concerns relative to panel layout and functional grouping of panel equipment. These results were a primary input to the decision to perform extensive panel redesign.

The RG 1.97 task analysis identified numerous changes required to panel display instrumentation (including ECW flow monitoring). The changes were in the form of additional or revised ranges, instrument qualification, or new display or recording devices. Approximately 100 changes were identified and were summarized in the STPEGS CRDR Implementation Plan Report initially submitted to the NRC by letter ST-HL-AE-946, from Mr. J. H. Goldberg to Mr. Thomas M. Novak, April 7, 1983.

The RG 1.97 results are also documented in Table 7.5-1.

c. The CRDR SFTA functional flow diagrams and task objectives were developed by Torrey Pines Technology utilizing the WOG ERGs, plant process design documentation, and input from plant design and operations personnel relative to plant system function. The task objectives defining a display or control requirement are stated in specific terms relating to plant equipment for status information or control needs, or plant process variable, for monitoring information or control needs. These task objectives determining operator information and control needs were developed prior to the comparison to the main control panel equipment as documented on the SFTA operator task identification and analysis forms.

   The RG 1.97 variable requirements were defined based on the Westinghouse generic design basis to respond to RG 1.97. These generic design bases were applied to the STPEGS specific process designs through reviews utilizing plant process flow diagrams and single lines, and the plant accident analyses. These variable requirements were developed prior to the comparison to the existing plant instrumentation.

   Numerous control and instrumentation specifications existed prior to the inception of the STPEGS CRDR or the STPEGS RG 1.97 implementation. As a result of both of these efforts, the majority of these specifications were revised to replace, upgrade, or enhance the existing controls and instrumentation. In addition many new specifications were developed after the needs were determined through either the CRDR or the RG 1.97 review.

d. The CRDR SFTA and the RG 1.97 review utilized the WOG ERGs and numerous plant specific documents. From these Torrey Pines Technology, as part of the CRDR SFTA, developed an extensive STPEGS "systems" background employing where necessary interviews with plant design and operations personnel. This "systems" knowledge is documented in the CRDR SFTA report and formed the basis for the SFTA.

Response (Continued)

The RG 1.97 reviews also employed the WOG ERGs and plant specific documents including the plant accident analyses for plant specific design data required to derive operator informational needs. As the STPEGS EOPs are developed, a continuing dialogue exists between the HL&P Operations staff and the system designers to ensure that operational information needed is identified and addressed by the control room instrumentation. The design basis for the operational information needs is documented in Appendix 7B and the instrument requirements are documented in Table 7.5-1.

e. An auditable record is maintained documenting the design basis for determining the instrumentation requirements (operator informational needs) based on the WOG ERGs and STPEGS plant specific documentation. This design basis, provided in Appendix 7B, and the detailed instrumentation listing provided in Table 7.5-1, are maintained through the development and validation of the EOPs.

f. There are six consoles within the control room: ZCC-025, ZCC-026, ZCC-027, ZCC-028, ZCC-029 and ZCC-030. The design has been completed on the consoles and the design has been reviewed for compliance to the STPEGS CRDR Criteria. The consoles have been fabricated and installed.

g. Houston Lighting and Power (HL&P) has developed a functional reach test to be administered to all Reactor Operator candidates. The development of the test included the identification of all controls that are critical in emergency situations. Two types of critical controls that are located at the greatest height on the vertical panels were identified. A mock-up test panel has been constructed to simulate the locations of the critical controls. Simultaneous with the functional reach test, a job-relevant preliminary visual acuity screen is conducted using control and annunciator labels identical to those used on the main control board. Procedures for the administration of the tests are detailed and provide clear pass/fail criteria. Personnel not passing the tests are not allowed to perform in the Reactor Operator position.

h. Dispositions of the Category "A" human engineering discrepancies (HEDs) have been updated and are included in the CRDR Human Engineering Discrepancy Resolution Report (see HL&P letter ST-HL-AE-1228, April 15, 1985). The three Category "A" HEDs questioned here are addressed on pages A-4 and A-5 of Appendix A.

i. Dispositions of the Category "B", "C", and "D" human engineering deficiencies (HEDs) have been updated and are included in the CRDR Human Engineering Discrepancy Resolution Report. Category "E" criteria are those checklist items that could not be reviewed prior to the control room completion. These include items such as lighting, sound, and communications. The schedule for completion

Response (Continued)

of review of Category "E" criteria is provided in response to item k below. HEDs resulting from review of Category "E" criteria are addressed in the Executive Summary Addenda and in the Human Engineering Discrepancy Resolution Report Addenda.

j. All of the following items have been or are in the process of being implemented through engineering drawings, data sheets, and specifications.

- Labels
- Annunciator tiles
- Demarcation painting
- Meter scales
- Legend light engravings and "closed corner" markings
- Recorder charts
- Vertical meter pointed color

Each of these are designed and controlled using documents which undergo 100 percent review for compliance to the STPEGS CRDR Criteria prior to issue for purchase, fabrication, and/or installation. This is a controlled design process and the purchase, fabrication, and/or installation of these items are governed by the STPEGS Quality Assurance Program. Sample checks are performed as identified in the CRDR Executive Summary Report as an additional assurance measure.

k. The STPEGS schedule for ongoing CRDR activities is located in the addenda to the CRDR Executive Summary Report, Section 5.0, schedule. The latest addendum provides a schedule for implementation of corrective actions and resolution of HEDs, which was subsequently modified in letter ST-HL-AE-3074, dated May 11, 1989, from Mr. M.A. McBurnett of the Houston Lighting & Power Company to the NRC.

Section 7A.S.5 provides a detailed list of all STPEGS CRDR reports, including addenda, which have been provided to NRC.