Westinghouse Electric Corporation
Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

ET-NRC-93-3872
NSRA-APSL-93-0148
Docket No.: STN-52-003

April 29, 1993

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

ATTENTION: R. W. BORCHARDT

SUBJECT: WESTINGHOUSE RESPONSES TO NRC REQUESTS FOR ADDITIONAL INFORMATION ON THE AP600

Dear Mr. Borchardt:

Enclosed are three copies of the Westinghouse responses to NRC requests for additional information on the AP600 from your letters of January 26, 1993 and March 12, 1993. This transmittal is a partial response to these letters. A listing of the NRC requests for additional information responded to in this letter is contained in Attachment A. The Westinghouse responses to the remainder of the requests for additional information contained in your letter of January 26, 1993 will be provided prior to May 29, 1993.

If you have any questions on this material, please contact Mr. Brian A. McIntyre at 412-374-4334.

Brian A McIntyre / for
Nicholas J. Liparulo, Manager
Nuclear Safety & Regulatory Activities

/nja

Enclosure

cc: B. A. McIntyre - Westinghouse
F. Hasselberg - NRC

050014

0953A

E004
1/4

ET-NRC-93-3872
NSRA-APSL-93-0148

April 29, 1993

bcc:	M. D. Beaumont	Rockville, MD	1L
	R. A. Bruce	WEC 4-32 East	1L
	J. C. Butler	WEC 4-24 East	1L
	P. A. Chahoy	WEC 4-10 East	1L, 1A
	J. Cobian	Madrid	1L
	B. Z. Cowan	Eckert, Seamans, Cherin, Mellott	1L, 1A
	W. E. Cummins	WEC 4-28 East	1L, 1A
	A. B. de St. Maurice	WEC 5-28 East	1L, 1A
	H. J. Fix	WEC 529 East	1L
	S. M. Franks	DOE	1L
	J. M. Moore	Expo Mart 335	1L
	J. A. Peoples	WEC 4-7A East	1L, 1A
	F. A. Ross	DOE	1L, 1A
	R. Schene	Brussels	1L
	W. W. Travis, Jr.	WEC 4-27 East	1L, 1A

0953A

ET-NRC-93-3872
ATTACHMENT A
AP600 RAI RESPONSES
SUBMITTED APRIL 29 1993

RAI No.	Issue
100.009	ITAAC rationale and selection criteria
410.100	VCS & VFS conformance to SRP (WCAP-13053)
410.102	Turbine bldg ventilation (WCAP-13053)
420.012	On/off control of plant loads
420.013	IPS/ICS differences
420.017	Special monitoring system
420.018	Reference to IEEE Std 769-1983
420.020	EMI protection for digital I&C
420.021	RT group 1/ group2 inconsistencies
420.022	IEEE Std 796 bus function
420.023	Monitor bus design basis
420.028	ESFAC interfaces
420.030	Remote VO analog cabinet function
420.031	Reactor trip channel bypass logic
420.032	Fault tolerance design methods
420.033	ESFAC diagram clarification
420.034	Communication diagram clarification
420.035	Isolation devices
420.037	Interlocks to prevent simultaneous testing
420.041	GDC 21 with two channels bypassed
420.042	Reactor trip breaker bypass design
420.050	Video display unit qualification methods
420.051	Portable testers
420.054	DAC design V&V process
420.056	Standard EMI seismic cabinet
420.057	Different bits of resolution

ET-NRC-93-3872
ATTACHMENT A
AP600 RAI RESPONSES
SUBMITTED APRIL 29 1993

RAI No.	Issue
420.058	Criterion for use of EEPROMs
420.059	Max field parameter for EMI/RFI protection
420.060	Isolation transformer and EMI/RFI effects
420.061	Limits for shipping environment
420.062	Cabinet cooling assembly power supply
420.063	Automatic calibration feature
420.064	Communication subsystem single failure analysis
420.065	Automatic tester anaylsis
420.066	Scope of automatic surveillance testing
420.067	Portable tester software development
420.068	Data highway for protection & monitoring system
420.069	Number of microprocessor based subsystems
420.075	Remote shutdown workstation
420.076	Remote shutdown workstation security
420.083	Procedure for loss of alarm system
420.084	Impact of environment on alarm system
420.087	Multiplexer connection to each workstation
420.089	Trip-Normal-Bypass switch description
471.002R01	Radiation zone designations
471.003R01	ALARA concerns
620.050	Display/control/alarm matrix

Question 100.9

The staff has conducted an initial review of the inspections, tests, analyses, and acceptance criteria (ITAAC) submitted by letter dated December 15, 1992. 10 CFR 52.47(a)(1)(vi) requires that the applicant submit proposed ITAAC, which are necessary and sufficient to provide reasonable assurance that, if the ITAAC are performed and the acceptance criteria met, a plant that references the design will be built and operated in accordance with the design certification. Westinghouse has proposed that only 40 systems out of the total number of systems in the design require ITAAC and, therefore, treatment as certified design material. Provide the rationale and criteria for selection of these systems, and describe how this proposal meets the requirements of 10 CFR 52.47(a)(1)(vi).

Response:

A process was developed and implemented that utilized a screening criteria form, consensus measurement, technical review, and management team review to determine the scope of systems to be included in ITAAC. The first step in the process was to develop the screening criteria. To develop the criteria, the classifications of systems was used as a starting point in determining which systems would be included. The designers of each system were given a screening criteria check list and instructions that all systems containing a safety-related (Class A, B, or C) structure, system, or component be included in the initial pass. Also, any system containing a structure, system, or component classified as Class D because it provides a defense-in-depth function was also included in the initial screening. (A structure, system, or component is classified as Class D when it directly acts to prevent unnecessary actuation of the passive safety systems. Structures, systems, and components required to support those that directly act to prevent the actuation of passive safety systems are also Class D.) This initial phase screened the 96 AP600 systems.

The next step was to compile the completed screening criteria check lists and submit the package to a panel of technical reviewers to discuss and agree on the appropriateness of inclusion. The technical review team consisted of representatives from Westinghouse design groups and licensing, EPRI, NUMARC, and Westinghouse subcontractors. Each member reviewed the designer's screening criteria sheet and submitted his assessment of inclusion in ITAAC on each system. Any system not having complete agreement was discussed before the panel until a consensus was reached.

This panel further developed a rationale for logically grouping functions. For instance, all containment isolation features were handled in the containment system, thus eliminating from ITAAC any system whose only screened function was containment isolation. The protection and safety monitoring system addresses the safety-related portions of the operational and control centers system, and the plant control system and data display and processing system covered the defense-in-depth portion of the same system. Also, instrumentation for each system were covered in the instrumentation systems instead of the mechanical or fluid system it monitored.

Systems that were the design responsibility of the combined license applicant were also considered. These selected systems were reviewed, and the determination was that there are no anticipated safety-related or defense-in-depth structures, systems, or components within these systems. The technical review team produced a final list of 36 systems that would need ITAAC. Some features of other systems were handled within these 36.

The results of the technical review team meeting were presented to the management team. The management team consisted of representatives from utilities, INPO, EPRI, subcontractors, and Westinghouse management. The final review determined that 36 systems would require ITAAC. These were transmitted to the NRC on December 15, 1992, along with four non-system-based ITAAC. Information that was not conveniently covered through the system approach was covered in the four non-system-based ITAAC. This includes human factors design, nuclear island buildings, safety-related piping, and the interface requirements.

The ITAAC written on each of the 36 systems thoroughly covered both the safety-related and the defense-in-depth functions. The process ensured that the safety-related functions and important-to-safety defense-in-depth functions of the non-safety-related systems were covered by ITAAC. If the ITAAC are successfully completed, the functionality of each system with respect to the certified design and safety of the plant would be demonstrated. This provides reasonable assurance that a plant that references the design is built and will operate in accordance with the design certification.

ITAAC Revision: NONE

Question 410.100

For Q410.95-Q410.104, demonstrate how the AP600 design meets applicable GDCs by providing failure modes and effects analyses and other requested details, as identified in applicable SRP section(s) review methodology.

WCAP-13053 indicates that information on the ESF ventilation system will be provided later. Section 9.4.5 of the SSAR, "ESF Ventilation System," indicates that this section is not applicable to the AP600 design. Sections 9.4.6, "Containment Recirculation Cooling System (VCS)," and 9.4.7, "Containment Air Filtration System (VFS)," do not mention conformance with any particular SRP sections.

The staff concludes that these two HVAC systems should be evaluated as ESF ventilation systems as part of the design-in-depth concept. Therefore, these systems should conform with the guidance of Section 9.4.5 of the SRP. Demonstrate that these systems conform with the guidelines of (1) R.G. 1.29 (to show they meet GDC 2), (2) Position C.2 of R.G. 1.52 and Positions C.1 and C.2 of R.G. 1.140 (to show they meet GDC 60), and (3) NUREG/CR-0660 (to show they meet GDC 17). Also, demonstrate that these systems conform with GDC 4. The system P&IDs, flow diagrams, component data and system description should reflect corresponding details as identified in Section 9.4.5 of the SRP, i.e., Table 3.2-3 of the SSAR should reflect equipment information for HEPA filters, absorbers, single failure criteria design for equipment, isolation dampers, radiation detectors, etc.

Response:

The VCS and VFS are not engineered safety features ventilation systems (ESFVS). The VCS and VFS have no safety-related design functions, other than to isolate the VFS containment penetrations. Therefore, SRP 9.4.5 design criteria are not applicable to these systems.

Containment Recirculation Cooling System (VCS):

The VCS provides containment cooling during normal plant operation (SSAR Subsection 9.4.6). A containment isolation signal due to an anticipated transient or a design basis loss of coolant accident (LOCA) will isolate the cooling coils for the VCS recirculation coolers (SSAR Figure 9.4.6-1) from their source of cooling water provided by the central chilled water system (SSAR Figure 9.2.7-1, Sheet 2). Containment cooling after a design basis LOCA is provided by the passive containment cooling system (SSAR Subsection 6.2.2) and does not depend on VCS operability. Hence, the VCS is classified as a non-ESF ventilation system.

The VCS complies with the applicable regulatory criteria as discussed next:

Compliance with Position C.1 of R.G. 1.29 does not apply because the VCS is not designed to perform any safety-related functions.

Compliance with Position C.2 of R.G. 1.29 is satisfied because the VCS is evaluated for interaction with seismic Category I systems as described in SSAR Subsection 3.7.3.13 so that the VCS cannot reduce the functioning of any safety-related plant features.

Compliance with Position C.3 of R.G. 1.29 is satisfied because the VCS does not include any seismic Category I components, and the connection of VCS nonseismic Category I equipment and duct supports to seismic Category I structures will not reduce functioning of seismic Category I structures.

The guidance provided in R.G. 1.52 does not apply because the VCS is a non-ESF system and has no design function to provide atmospheric cleanup of airborne contamination following a design basis accident.

The guidance provided in R.G. 1.140 does not apply because the VCS has no design function to provide atmospheric cleanup of airborne contamination during normal plant operation.

Compliance with NUREG/CR-0660 does not apply to AP600 based on SSAR Table 8.1-1.

Compliance with GDC 4 does not apply to the non-safety-related VCS.

System single failure criteria does not apply because the VCS does not perform any safety-related functions. The principal codes for the VCS equipment and components are provided in SSAR Subsection 9.4.6.2.2. The VCS does not include any Class A, B, C, or D equipment, as defined in SSAR Subsection 3.2.2, and was not included in Table 3.2-3. Specific VCS equipment performance criteria are shown in SSAR Table 9.4.6-1.

Containment Air Filtration System (VFS):

The VFS provides radiological and pressure control inside containment during normal plant operation (SSAR Subsection 9.4.7.1.2). SRP 6.2.4 provides design criteria for containment purge systems specifically where the design affects the safety-related containment isolation system (SSAR Subsection 9.4.7.2.1). An isolation signal due to high airborne radioactivity inside containment or a design basis LOCA will isolate the VFS supply and exhaust units from the containment (SSAR Subsection 6.2.3.2.1 and Figure 9.4.7-1). There are no design basis accidents requiring VFS operability except for containment isolation. The VFS is classified as a non-ESF ventilation system.

The VFS complies with the applicable regulatory criteria as discussed next.

Compliance with the guidelines of R.G. 1.29 for the VFS, which provides filtered exhaust for the fuel handling area, is discussed in the response to Q410.99.

The guidance provided in R.G. 1.52 does not apply because the VFS is a non-ESF system and has no design function to provide atmospheric cleanup of airborne contamination following a design basis accident.

Compliance with Positions C.1 and C.2 of R.G. 1.140 for the VFS is discussed in the response to Q410.99.

Compliance with NUREG/CR-0660 does not apply to the AP600 based on SSAR Table 8.1-1.

Compliance with GDC 4 does not apply to the non-safety-related VFS. The VFS containment penetrations that form a portion of the containment isolation system meet GDC 4 based on SSAR Subsection 6.2.3.1.1.

System single failure criteria, based on SRP 9.4.5 guidelines, does not apply to the VFS except for the VFS containment penetrations that provide containment isolation. The containment isolation does meet single active failure criteria based on SSAR Subsection 6.2.3.1.1. The principal codes for the VFS equipment components are shown in Table 3.2-3, with specific equipment performance criteria shown in SSAR Table 9.4.7-1. The design of the radiation monitors that initiate operation of the VFS is described in SSAR Section 11.5.

WCAP-13053 has been replaced with WCAP-13054 and is consistent with the response to this RAI.

SSAR Revision: NONE

Question 410.102

For Q410.95-Q410.104, demonstrate how the AP600 design meets applicable GDCs by providing failure modes and effects analyses and other requested details, as identified in applicable SRP section(s) review methodology.

Section 9.4.9 of the SSAR addresses the turbine building ventilation system. WCAP-13053 indicates that the turbine area ventilation system conforms to Positions C.1 and C.2 of R.G. 1.29, Positions C.1 and C.2 of R.G. 1.140, and GDC 5.

Demonstrate that this system conforms with (1) the guidelines of Position C.1 of R.G. 1.29 for the safety-related portions of the system and Position C.2 for the non-safety-related portions of the system (to show that it meets GDC 2 with respect to the system being capable of withstanding the effects of earthquakes), (2) the guidelines of Positions C.1 and C.2 of R.G. 1.140 (to show that it meets GDC 60 with respect to the capability of the system to suitably control the release of gaseous radioactive effluents to the environment), and (3) the requirements of GDC 5. Also, provide (1) design temperatures inside the room(s) and areas of the turbine building, (2) a detailed system description, and (3) system component data.

Response:

The turbine building ventilation system neither serves nor supports the plant safety-related function. Therefore, the system need not be designed to withstand the effects of earthquakes, and the requirements of R.G. 1.29 and 1.140 as stated in the question do not apply.

Some areas in the turbine building have a potential for radioactive contamination. The turbine building is considered to be a nonradioactive area and leakage is expected to be low. Radiological monitors are provided to detect system leakage in the condenser air removal, steam generator blowdown (BDS), component cooling water (CCS), and main steam systems. (See the response to Q460.14). Turbine building areas having a potential for radioactive contamination include provisions to allow temporary barriers for radiological protection. Provisions for these temporary barriers are made around the BDS, CCS, and condensate polishing system areas.

As specified in GDC 5, structures are not shared between units for the AP600.

The turbine building ventilation system is designed for -10° to 110°F ambient conditions. The HVAC for specific rooms within the turbine building is designed for human heat stress limits and working comfort as well as for equipment operation (electrical and instrumentation).

WCAP 13053 has been replaced with WCAP-13054 and is consistent with the response to this RAI.

SSAR Revision: NONE

Question 420.12

Clarify the statement in Section 7.1.1 of the SSAR that "the protection logic cabinets provide the capability for on-off control of individual plant loads." Is the plant control system performing automatic load control? What is the interface between the protection logic and the plant control systems?

Response:

The protection logic cabinets provide the capability for on-off control of individual safety-related plant components such as valves. These components are not cycled by the safety system during normal plant operation. The plant control system provides automatic load (modulating) control and on-off control functions for the non-safety-related plant components. There is no interface between the protection logic cabinets and the plant control system. See the response to Q420.39 for a description of the interface between the protection and safety monitoring system and the plant control system. See also the response to Q420.13.

SSAR Subsection 7.1.1, fourth paragraph will be revised as follows:

SSAR Revision:

The protection logic cabinets provide the capability for on-off control of individual safety-related plant loads. They receive inputs from the engineered safety features actuation cabinets and the control room.

Question 420.13

Clarify the statement in Section 7.1.1 of the SSAR that "the integrated control cabinets and the control logic cabinets perform similar functions to the integrated protection cabinets and the protection logic cabinets." Identify the differences in design, qualification, channel separation, software priority, and physical arrangement between the integrated protection system and the integrated control system.

Response:

The integrated control cabinets and the control logic cabinets use the same modular hardware and software building blocks as the integrated protection cabinets and protection logic cabinets. The integrated control cabinets and control logic cabinets are non-safety related and no qualification is performed, nor is channel separation provided. The software used in the integrated control cabinets and control logic cabinets is verified and validated, but to less stringent requirements than software used for safety-related applications. The internal arrangements of the integrated control cabinets and control logic cabinets are the same as the internal arrangements of the integrated protection cabinets and protection logic cabinets.

SSAR Subsection 7.1.1, fifth paragraph, will be revised as follows:

SSAR Revision:

The integrated control cabinets and the control logic cabinets perform non-safety-related instrumentation and control functions that are similar ~~functions~~ to safety-related instrumentation and control functions performed by the integrated protection cabinets and the protection logic cabinets for the non-Class 1E instrumentation and control applications.

Question 420.17

Section 7.1.1 states that "there are six sets of systems enclosed by the dotted line boxes (of Figure 7.1-1)." However, there are only 5 systems described in Section 7.1.1. Provide a discussion on the Special Monitoring System.

Response:

The following description of the special monitoring system will be added to SSAR Subsection 7.1.1 following the Protection and Safety Monitoring System subsection:

SSAR Revision:

Special Monitoring System

The special monitoring system does not perform any safety-related or defense-in-depth functions. The special monitoring system consists of specialized subsystems that interface with the instrumentation and control architecture to provide diagnostic and long-term monitoring functions.

The special monitoring system includes the metal impact monitoring system. The metal impact monitoring system detects the presence of metallic debris in the reactor coolant system when the debris impacts against the internal parts of the reactor coolant system. The metal impact monitoring system comprises digital circuit boards and associated controls, indicators, and power supplies and up to 12 remotely located accelerometers and related signal processing devices. The accelerometers and their related signal processing devices are mounted in pairs to maintain the impact monitoring function if an accelerometer fails in service.

Question 420.18

Section 7.1.2 references the IEEE Standard 796-1983 "IEEE Microcomputer System Bus" for the design of the data highway system of the protection and safety monitoring system. IEEE Standard 796-1983 has not been referenced in the previously docketed nuclear plant instrumentation and control systems design. Identify the key features of this standard and describe these key features with respect to the requirements of IEEE Standards 279-1971 and 603-1980, which are the regulatory bases for the protection systems. The key features should include but not be limited to the following (Section 7.1.2):

- single failure criterion
- channel independence
- testability
- reliability
- quality of components and modules
- channel bypass or removal from operation
- system repair
- isolation devices
- single random failure
- multiple failures resulting from a credible single event
- information read-out

Response:

IEEE Standard 796-1983, "IEEE Microcomputer System Bus," applies to the circuit boards and the microprocessor card cage described in Section 3.2 of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6). This bus is not the data highway system of the protection and safety monitoring system, but is the internal communications means for the microprocessor subsystems inside the cabinets. The scope of IEEE 796-1983 is defined in Section 1.1 of the standard: "This standard deals only with the interface characteristics of microcomputer devices, not with design specifications, performance requirements, and safety requirements of modules...."

The requirements of IEEE Standards 279-1971 and 603-1980 apply to the collection of microprocessor subsystems, treated as a total architecture within the protection and safety monitoring system, not to a single card or communications protocol within one of these microprocessor subsystems. IEEE Standard 796-1983 was referenced for information, not regulatory approval.

SSAR Revision: NONE

Question 420.20

Describe the electromagnetic interference (EMI) protection for the digital instrumentation and control system throughout the plant. The description should not be limited only to the protection cabinets (Section 7.1.1).

Response:

The response to Q420.1 also addresses EMI/RFI protection.

Cabinet design features to protect against EMI/RFI are discussed in Section 4.0.6 of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6). Noise and surge filters (Section 4.0.9 of WCAP-13391) are provided at sensor and contact inputs to the cabinets to reject EMI/RFI picked up by incoming cables. Filters (Section 4.0.4.2 of WCAP-13391) are provided in the power distribution assembly to reject EMI/RFI picked up by the power cabling. The cabinet grounding scheme (Section 4.0.5 of WCAP-13391) also helps to reject EMI/RFI. These features are used for both safety-related and non-safety-related cabinets.

In the protection cabinets, the built-in self-tester reduces cabinet access, lowering the amount of time that the cabinet doors are open and more susceptible to EMI/RFI.

The AP600 instrumentation and control architecture contains features to minimize the reception of EMI/RFI by the instrumentation cables. The cables for nuclear instrumentation use triaxial cable, providing a second shield to protect the signal conductors from noise sources. Fiber optic data links and data highways for inter-cabinet communications significantly decrease the number of copper cables that could pick up EMI/RFI and significantly lowers the possibility of ground loops, which can amplify EMI/RFI problems. Multiplexing in the AP600 instrumentation and control architecture provides fewer opportunities for noise coupling. The wiring in the AP600 is segregated by voltage level as described in SSAR Subsection 8.3.1.3.4 to help prevent noise from high-voltage power cables from coupling to lower-voltage signal cables. Cables are routed to avoid noise sources, such as the pressurizer heater controller. The physical separation of the safety-related cables lowers the possibility of noise pickup by more than one division from a single source.

SSAR Revision: NONE

Question 420.21

Section 7.1.2.2.1 of the SSAR states that the reactor trip function is divided into two functionally diverse subsystems for accident protection. Is the Reactor Trip Group 1 Subsystem always backup to the Reactor Trip Group 2 subsystem or vice-versa? Are they sharing the same hardware within each cabinet? What is the significance of the diverse subsystems with respect to the "partial trip" and "global trip" arrangement. There appears to be discrepancies between Section 7.1.2.2.1 of the SSAR and Section 4.1.2 of WCAP-13382 on subsystem lists for group 1 and group 2. Is the pressurizer level in group 1 or group 2? Should the "low power range neutron flux" be "high power range flux low setpoint"? Correct these inconsistencies.

Response:

Table 7.2-5 of the SSAR, Conditions for Reactor Trip, lists the primary and backup functions that initiate reactor trip for the Chapter 15 design basis events. Functional diversity requires the following:

- a minimum of two functions is listed as initiating a reactor trip for an event and
- at least one of these functions must be in a different reactor trip group in the integrated protection cabinets

Functional diversity in the AP600 protection and safety monitoring system is addressed in the defense-in-depth and diversity report being prepared in response to Q420.5

The reactor trip subsystems are implemented in separate microprocessor subsystems as shown in Figure 4.1-1, Integrated Protection Cabinets Arrangement, of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6). The reactor trip subsystems are not diverse subsystems; they are similar microprocessor subsystems processing diverse signals, thus "functionally" diverse.

Partial trips and global trips are described in Section 4.1 of WCAP-13391. A partial trip is produced by one of the reactor trip group subsystems when a plant parameter exceeds a setpoint. Two or more partial trips in different divisions originating from the same plant parameter and setpoint are sufficient to produce a plant trip. A partial trip is combined with one or more partial trips from the same plant parameter in another integrated protection cabinet by the trip enable subsystem and a dynamic logic unit in the integrated protection cabinet originating the partial trip. A global trip is produced by the global trip subsystem in an integrated protection cabinet when two or more partial trips exist for the same plant parameter in the three other integrated protection cabinets. See Figure 4.1.5 of WCAP-13391.

The high pressurizer level trip is in group 1 as listed in SSAR Subsection 7.1.2.2.1. WCAP-13391 will be corrected for its next revision.

"Low power range neutron flux" should be "high power range flux low setpoint", similarly "high power range neutron flux" should be "high power range flux high setpoint."

SSAR Subsection 7.1.2.2.1 will be revised as follows:

SSAR Revision:

- Reactor Trip Group 2 Subsystem
  - High intermediate range neutron flux
  - ~~Low power range neutron flux~~
  - High power range flux low setpoint
  - ~~High power range neutron flux~~
  - High power range flux high setpoint
  - High positive rate power range neutron flux
  - Low pressurizer pressure
  - High pressurizer pressure
  - High-2 compensated steam generator narrow range level
  - Low compensated steam generator narrow range level.

Question 420.22

The definition of the "IEEE Standard 796 Bus" shown in the Chapter 7 figures is not clear. In accordance with IEEE Standard 796, signals transferred over the bus have 5 classes (Section 7.1.2):

- control lines
- address and inhibit lines
- data lines
- interrupt lines
- bus exchange lines

Figures 7.1-3, 7.1-4, 7.1-5, 7.1-7, 7.1-8, 7.1-9, 7.1-11, and 7.1-12 of the SSAR all have the IEEE Standard 796 bus interfacing with various components. How is the bus function determined?

Response:

The entire bus is available to the circuit boards installed in the card cage. The bus signals are utilized as required by the communications protocols, such as master/slave and direct memory access, which exchange commands and data between the various boards used in a subsystem.

See also the response to Q420.18.

SSAR Revision: NONE

Question 420.23

What is the design basis for the AP600 "monitor bus?" Provide a reference to an industrial standard that the AP600 monitor bus design will follow (Section 7.1.2).

Response:

The planned implementation of the monitor bus function is a dual-redundant, fault-tolerant fiber optic data highway based on standard FDDI (Fiber Distributed Data Interface) technology.

Because of the rapid advances in electronics technology, the actual implementation will be selected as late as possible in the design process to enable the latest technology to be incorporated into the plant. The industrial standards applicable to the monitor bus will be described in the combined license application.

SSAR Revision: NONE

Question 420.28

Clarify the interfaces between the engineered safety features actuation cabinets (ESFAC), the protection logic cabinets, the multiplexers, and the actuated devices. Identify the following (Section 7.1.2.9):

a. The total number of engineered safety features actuation cabinets in the plant.
b. The total number of protection logic cabinets in the plant.
c. The type of cable used from the logic cabinet to the actuated devices and to the multiplexers.
d. Are there isolators being used from the logic cabinet through the multiplexer to the control room operator workstation?
e. The approximate number of dedicated control circuits that will be used in the plant.
f. Is there any difference in the design of the "data highway" for the monitor bus and the "data highway" between the ESFAC and the logic cabinets?

Response:

a. There are four sets of engineered safety features actuation cabinets in the AP600. Each set consists of two cabinets, as shown in Figure 4.2.1 of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description", Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6).

b. There are eight protection logic cabinets in the AP600.

c. Multiconductor copper cable is used from the logic cabinets to the actuated devices. Fiber optic cable is used to implement the logic bus data highway that connects the multiplexers to the logic cabinets.

d. Isolators are not required between the logic cabinets, multiplexers, and soft control devices because these devices are located within the same electrical division. The fiber optic cable used to implement the logic bus and used for communication between the multiplexers and soft control stations does, however, provide inherent electrical isolation.

e. Each logic cabinet is capable of actuating up to 20 motor-operated valves or up to 40 solenoid valves.

f. The non-safety-related monitor bus is a general-purpose fiber optic data highway using an internally redundant ring topology. The safety-related logic bus is a specialized fiber optic data highway using a star topology that is both division redundant and internally redundant. The monitor bus and logic bus serve different purposes in the plant and consequently have different functional requirements and use different communications protocols.

SSAR Revision: NONE

Question 420.30

Describe the function of the "Remote VO Analog Cabinet" shown in the lower left corner of Figure 7.1-1 of the SSAR. (Section 7.1.2.9)

Response:

The cabinets are the remote I/O analog cabinets and are part of the qualified display processing system. Their function is to provide signal conditioning and data acquisition for the qualified data processing cabinets shown above them in Figure 7.1-1 of the SSAR.

SSAR Revision: NONE

Question 420.31

Describe the channel bypass provision in the reactor trip logic. The description should include the detailed design of hardware and software for reverting 2/4 logic to 2/3 logic, 2/4 logic to 1/2 logic, 2/4 logic to automatic trip, alarm provision, and the basis for permitting an indefinite period of time with one or two channels bypassed for testing maintenance. Is the "channel bypass" limited to the same function (for example: high pressurizer pressure) or can it be applied to different functions (for example: one high pressurizer pressure and one low SG level)? Describe the relationship between channel bypass and the "Global Trip" design. Describe the method of the bypass indication at the workstation in the main control room. (Section 7.1.2.10)

Response:

WCAP-8897, "Bypass Logic for the Westinghouse Integrated Protection System," describes the operation of the channel bypass and global trip used for the reactor trip. Figure 4.0.1 of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6), shows the operation of the 2/4 bypass logic for the possible combinations of partial trip and bypass states. One or two channels can be in bypass for test or maintenance for an indefinite period of time because the operation of the logic will allow a single failure without placing the plant in an unsafe state. However, with two channels bypassed, a single failure can cause a nuisance trip. See the response to Q420.37.

A channel bypass is limited to a single function within each of the four divisions. Each trip function has its own 2/4 bypass logic. In the example given in the RAI, one high pressurizer pressure bypass is not combined with one low SG level bypass.

The 2/4 bypass logic is implemented in each division by the global trip subsystem, the trip enable subsystem, and the dynamic trip bus in the integrated protection cabinets. These are described in Sections 4.1.4 through 4.1.6 of WCAP-13391.

Bypass indication at the workstation in the main control room is discussed in the response to Q420.43.

SSAR Subsections 7.1.6 and 7.1.2.10 will be revised as follows:

SSAR Revision:

(Subsection 7.1.6)

7. "WCAP-8897 (P), WCAP-8898(NP), "Bypass Logic for the Westinghouse Integrated Protection System."

(Subsection 7.1.2.10)

Number of Inputs Bypassed	Number of Remaining Inputs to Result in a Trip
0	two out of four (2/4)
1	two out of three (2/3) (alarmed)
2	one out of two (1/2) (alarmed)
3	automatic trip
4	automatic trip

(Reference 7)

Question 420.32

Does the "Fault Tolerance" described in Section 7.1.2.10 of the SSAR include both hardware and software? Describe the methods used to achieve a "Fault Tolerance" design.

Response:

Fault tolerance refers to architectural features (such as functional diversity, internal and external redundancy, physical separation, channel independence, segmentation, optical isolation between cabinets, fail-safe design, and 2/4 bypass logic) that enable the AP600 instrumentation and control architecture to limit the propagation and effects of a failure, if one occurs. These features are described in WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6).

SSAR Revision: NONE

Question 420.33

Figure 7.1-10 of the SSAR, "Engineered Safety Features Actuation Cabinet Block Diagram," does not provide sufficient detail to understand the system configuration. The information presented on Figure 7.1-10 is not consistent with Figure 7.1-1. Why does the signal from the IPC to the ESFAC need isolation? What is the optical distribution center? Are the ESFAC and the protection logic cabinet located in the same cabinet? Which signals use hardwire transmission? (Section 7.1.2.10)

Response:

The engineered safety features actuation cabinets (ESFACs) are described in Section 4.2 of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6). Figure 4.2.3 of this WCAP provides more detail on the internal architecture of the ESFACs.

Each ESFAC receives information from the integrated protection cabinet (IPC) set in the same division and the three IPCs in the other divisions. The signal from the IPC in the same division as the ESFAC does not require electrical isolation; however, electrical isolation is an inherent feature of the fiber optic data link used for this intercabinet communications path. The electrical isolation between the IPCs and ESFACs takes place within the fiber optic data links. Six inches of fiber optic cable constitutes an isolation device in accordance with Regulatory Guide 1.75. The isolation function was shown within the cabinet and has been changed.

The optical distribution center in Figure 7.1-10 is the same device as the signal distribution center shown in Figure 7.1-13. It is a passive star that distributes signals between the various fiber optic cables that form the logic bus data highway.

The ESFAC and protection logic cabinets are located in different cabinets. However, the automatic tester subsystem in the ESFAC is used to test both the ESFAC and the protection logic cabinets that are connected to it by the logic bus.

Hardwired signal transmission is used for signals from the dedicated system level controls in the main control room and remote shutdown area to the ESFACs.

SSAR Revision:

SSAR Figure 7.1-10 (proprietary) will be revised to show electrical isolation outside of the ESFACs.

Question 420.34

Figure 7.1-13 of the SSAR, "Protection Logic Cabinet Communication Diagram," indicates "2/3 voted outputs" at the bottom of the block diagram. Why is 2/3 voted instead of 2/4? Clarify the number of divisions, and number of trains in the system shown on Figure 7.1-13. Is there any signal from division A to train B? (Section 7.1.2.10)

Response:

A 2/3 voted logic is used in the logic cabinets because the internal architecture of both the protection and the control logic cabinets is triple redundant as shown in Figure 7.1-22 of the SSAR. Figure 7.1-22 applies equally to both the protection and the control logic cabinets. This should not be confused with the external redundancy, which is based on 2/4 logic. The logic cabinets are further described in Section 4.3 of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6).

Only one electrical division (Division A) of instrumentation is shown in Figure 7.1-13 of the SSAR. Figure 7.1-13 does not deal with fluid system trains. The term "TRAIN A" on this figure is incorrect and should read "DIVISION A."

The AP600 engineered safeguards systems are designed in accordance with single failure and Probabalistic Risk Assessment (PRA) objectives with the assignment of electrical divisions in accordance with the design objectives. The confimation of the design process is the failure mode and effects analysis and the PRA.

SSAR Subsections 7.1.2.10 and 7.1.3.5 and Figures 7.1-13 and 7.1-22 will be revised as follows:

SSAR Revision:

(Subsection 7.1.2.10, fifth bulleted paragraph)

- Component level logic, in the logic cabinets, is triple redundant, as shown in Figure ~~7.1-13~~ 7.1-22. The three redundant logic computers are contained ..

(Subsection 7.1.3.5, last sentence)

The functional architecture of the protection and control logic cabinets is shown in Figure 7.1-22.

SSAR Figure 7.1-3 (proprietary) will be revised as described in the above response.

The title of SSAR Figure 7.1-22 (proprietary) will be revised to read "~~Control~~ Logic Cabinet Architecture."

Question 420.35

Clarify whether the "optical coupling" is the only isolation device to be used in the AP600 I&C design. Identify and describe any other isolation devices to be used in the design. (Section 7.1.2.11)

Response:

Optical coupling is the preferred method for signal isolation in the AP600 instrumentation and control systems. Other methods of signal isolation may be used as the design progresses and technology choices are made. These methods will be in accordance with Regulatory Guide 1.75.

Other methods of electrical isolation in the instrumentation and control systems include the coil-to-contact isolation, which is used for the diverse actuation system isolation valves.

Isolation between the Class 1E and non-Class 1E plant electrical systems using regulating transformers and battery chargers is described in the responses to Q435.55 and Q435.68.

SSAR Revision: NONE

Question 420.37

Section 7.1.2.12 of the SSAR states that there are no built-in interlocks to prevent simultaneous testing of two integrated protection cabinets. It will rely on operation procedures. Since the reactor protection channel under test is bypassed, simultaneous bypass of more than one channel could place the plant in an unsafe condition. Modify the design with built-in interlocks to prevent simultaneous testing of more than one cabinet or justify the proposed design.

Response:

Please refer to Figure 4.0-1 of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6). With two channels in bypass, the 2/4 logic reverts to 1/2 operation. One of the two remaining channels is capable of tripping the plant. The single failure criterion is not violated and the plant is in a safe condition. Administrative procedures discourage more than one channel from being tested at the same time since this condition makes the plant susceptible to nuisance trips.

Should three channels be placed in bypass, a reactor trip is issued.

SSAR Revision: NONE

Question 420.41

Describe (supported by detailed schematic diagrams) how the design meets the requirements of GDC 21 with two channels bypassed. Discuss the periodic testing aspect of the design. How does the protective function initiate when the third channel fails? Describe the method for indication of bypasses to satisfy the IEEE Standard 279 requirements for continuous indication in the control room. (Section 7.1.4.2.11)

Response:

With two channels bypassed, the 2/4 logic reverts to a 1/2 logic as shown in Figure 4.0.1 of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6). In this state, a trip request from one of the two remaining channels is sufficient to trip the reactor, and a single failure will not prevent a valid trip from the remaining channel. Figure 4.1.5 of WCAP-13391(NP) shows the design of the dynamic trip bus inside an integrated protection cabinet and the manner in which the dynamic trip bus is bypassed for testing by the automatic tester. During the automatic test sequence, test signals are injected into the global trip and trip enable subsystems to simulate partial trip and bypass signals from the other divisions in order to test the 2/4 bypass logic in the integrated protection cabinet set under test. Testing of the ESF actuation logic is performed in a similar manner. Testing is done in an overlapping manner in order to test each element required to produce a reactor trip or an ESF actuation.

If, while two channels are in bypass, a third channel fails and produces a false partial trip, false partial ESF actuation, or false bypass signal, a plant trip or an ESF actuation occurs, as shown in Figure 4.0.1 of WCAP-13391(NP). If while two channels are in bypass, a third channel fails and fails to produce a required partial trip or partial ESF actuation, the fourth, unfailed channel is sufficient to satisfy the logic and cause the required plant trip or ESF actuation to occur.

The method of indication of bypasses in the main control room is described in the response to Q420.43.

SSAR Revision: NONE

Question 420.42

Describe (supported by detailed schematic diagrams) the capability of the reactor trip breaker bypass design. Can the shunt trip components be tested during power operation? How often are they tested? (Section 7.1.4.2.11)

Response:

Figure 7.1-14 of the SSAR shows the configuration of the reactor trip breakers. The breakers are arranged so that any single breaker can be tripped without interrupting power from the rod drive motor-generator set to the rod control cabinets. The configuration also permits tripping both reactor trip breakers in a division (for instance, breakers C1 and C2) without interrupting power from the rod drive motor-generator set to the rod control cabinets.

Figure 4.1.8 of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6), shows the test switch arrangement for the reactor trip circuit breakers. The shunt trip mechanism and the undervoltage trip mechanism of each reactor trip breaker can be tested individually. Because of the reactor trip breaker configuration discussed in the previous paragraph, this test can be performed during power operation.

AP600 Technical Specification 3.3.1, Rev. 0, 6/26/92, item 3.3.1.6, requires testing the reactor trip breakers once every 92 days.

SSAR Revision: NONE

Question 420.50

Describe the qualification methods and test results of the "qualified video display units". (Section 1.2.1 of WCAP-13382)

Response:

The qualification methods for the qualified video display units used in the AP600 will be similar to the qualification methods described in WCAP-8587 Supplements EQDP-ESE-63A, Rev. 1, 6/87, "Plant Safety Monitoring System (PSMS) Plasma Display and Keyboard," and EQDP-ESE-63B, Rev. 1, 6/87, "Plant Safety Monitoring System (PSMS) Modular Plasma Display." Equipment qualification test results are beyond the scope of design certification.

SSAR Revision: NONE

Question 420.51

The AP600 protection and safety monitoring system performs surveillance testing via a portable tester. How many portable testers will be provided for the plant? Is there any interlock to prevent testing more than one channel at the same time? During a channel test, the bistable output to the logic circuitry is interrupted and causes that portion of the logic to be actuated, accompanied by a channel trip alarm in the control room and the status lights indication on the cabinet test panel. Can the operator get the status indication at his workstation? What type of messages will the operator receive during a channel test, maintenance, or removal from service? (Section 2.4 of WCAP-13382)

Response:

The portable tester discussed in Section 2.4 of WCAP-13382 is an operator interface device that contains a computer terminal and printer. One is provided per plant; however, the owner may obtain additional units. The automatic surveillance test sequence does not require the portable tester. The automatic surveillance test sequence is initiated by use of controls on the automatic tester subsystem, which is mounted in the cabinets. The printer on the portable tester is normally used to print a permanent test record. The portable tester computer terminal is normally used to make setpoint changes or to initiate partial tests and is not required for normal testing.

Administrative procedures are used to prevent testing more than one channel at the same time. If more than one channel is tested at the same time, the 2/4 logic used for reactor trip and ESF actuation responds to maintain the plant in a safe state as described in the response to Q420.41. Because the automatic tester for the ESF actuation cabinet and associated logic cabinets tests one-half of the redundant subsystems at a time, the redundant subsystems in the same cabinets are available to respond to a plant event that occurs during the testing.

Signals will be issued to the communications system to report the status of the equipment under test. The design and presentation of error messages to the operator will be determined by the process described in SSAR Section 18.8.

SSAR Revision: NONE

Question 420.54

Describe the hardware and software design verification and validation process for the Diverse Actuation System. (Section 2.11 of WCAP-13382)

Response:

Because the diverse actuation system (DAS) is independent of the protection and safety monitoring system (PMS) and the plant control system (PLS), and the DAS is a non-safety-related system, the verification and validation processes for the DAS will be diverse from the verification and validation processes performed for the PMS and PLS, and will be performed by different people. The hardware and software verification and validation will be performed to the level appropriate for hardware and software used in defense-in-depth systems to accomplish defense-in-depth functions.

The design, verification, and validation process for the diverse actuation system consists of hardware verification, software verification, system verification, and system validation. The hardware verification consists of inspections and tests to verify that the hardware meets design specifications. The software verification consists of functional tests to verify that the software meets software design requirements at the module and subsystem levels. The system verification consists of integrated subsystem tests to verify that the integrated subsystems meet system design requirements. The system validation test consists of a factory acceptance test to verify that the integrated system meets system functional requirements.

SSAR Revision: NONE

Question 420.56

Provide test results to demonstrate that the "Standard EMI Seismic Cabinet" can provide shielding for electromagnetic interference and the seismic effect. The test plan should include the basis for the magnitude of the EMI and seismic forces. (Section 3.1.1 of WCAP-13382)

Response:

The standard EMI seismic cabinet was previously qualified for electromagnetic interference and the seismic effects for a different application. The seismic qualification was reported in WCAP-8587 Supplements EQDP-ESE-53, Rev. 1, 4/84, "Plant Safety Monitoring System," and EQDP-ESE-53B, Rev. 1, 6/87, "Plant Safety Monitoring System (PSMS) Components." The electromagnetic interference qualification was reported in WCAP-11341(NP), "Noise, Surge, and Radio Frequency Interference Test Report," 11/86.

SSAR Revision: NONE

Question 420.57

The Analog Input Process Board (M40) and the D/A Conversion Board (MDA) have different bits of resolution to achieve the required accuracy. Why are they different? How are these extra bits being handled in the signal process? The IEEE Standard 796 bus processes the least-significant byte first. How is the system operation affected when an 8-bit bus master reads 16-bit data in the lower eight data line? (Section 3.2.8 & 3.2.10 of WCAP-13382)

Response:

The D/A conversion board (MDA) is used to generate the analog signals that are injected into the analog inputs during automatic testing. Consequently, as a tester, it requires a greater resolution than the boards it is used to test, such as the analog input process board (M40).

Transfer of multi-byte data structures of arbitrary size across microprocessor buses is handled by transferring the data as slices that are either processed in a stream or reassembled, then processed by the software. The width of a microprocessor bus (8 bit, 16 bit, and so forth) limits the rate of data transfer, but does not limit or affect the size of data entities that can be transferred.

SSAR Revision: NONE

Question 420.58

There are two types of erasable programmable read only memory (EPROM and EEPROM) being used in the AP600 design. What is the criterion or guidance that permits using EEPROMs, which can be rewritten from the console without removing it from the board. (Section 3.2.9 of WCAP-13382)

Response:

EEPROMs, which can be rewritten while installed in the cabinets, contain the setpoints and tuning constants that may need to be periodically modified under the combined license holder's administrative control. These setpoints and tuning constants are entered in engineering units. EPROMs, which need to be removed from the locked cabinets to be modified, are used to contain program code and configuration data under the combined license holder's software change control program. An EPROM is programmed as an individual unit, outside the cabinets, in a special device, and is changed by removing a circuit board from the microprocessor subsystem and replacing the old EPROM.

To reprogram an EEPROM or to replace an EPROM requires access to the locked instrumentation and control cabinets. In addition, a password is required in order to change the contents of an EEPROM.

SSAR Revision: NONE

Question 420.59

Define the maximum field parameters considered for the electromagnetic interference (EMI) and radio frequency interference (RFI) protection for the I&C cabinets. How is the environment to be verified at the site where the cabinets will be located? (Section 4.0.6 of WCAP-13382)

Response:

EMI/RFI testing performed on instrumentation and control cabinets for previous nuclear plant projects has met the requirements of level 3 of IEC 801-3. See the response to Q420.56.

AP600 internal design document GW-J1R-003, Rev. 0, "AP600 Electromagnetic Interference (EMI), Radio Frequency Interference (RFI) Test Requirements Study," compares historical instrumentation and control cabinet testing performed by Westinghouse with national and international standards. This document demonstrates that the equipment has been tested to requirements equivalent to level 3 of IEC 801-3. The EMI/RFI test envelope for the AP600 prototype encompasses the frequency range and the signal strength and characteristics of both IEC 801-3, level 3, and ANSI/IEEE C37.90.2.

Compliance of the plant with the EMI/RFI environment requirements at a specific site for instrumentation and control cabinets will be the responsibility of the combined license holder.

SSAR Revision: NONE

Question 420.60

Describe the operating experience of the isolation transformer at the power feeders to minimize EMI/RFI effects. If this is effective for nuclear instrumentation inputs, why is it not used for other process parameter inputs in the integrated protection cabinets? (Section 4.0.6.2 of WCAP-13382)

Response:

The isolation transformers are provided for power feeders to the nuclear instrumentation. Operating experience has demonstrated that the low-signal energy levels of the nuclear instrumentation are more susceptible to EMI/RFI noise. The isolation transformers are used to provide an additional EMI/RFI barrier for the nuclear instrumentation. The other process input signals are at a higher energy level, and do not require EMI/RFI rejection beyond that provided by the input signal filtering and power supply filtering described in the response to Q420.20.

SSAR Revision: NONE

Question 420.61

Provide the results of the prototype cabinet temperature and humidity limit test when it is completed. Justify the temperature limits specified for the shipping environment which are larger than the normal operating environment. (Section 4.0.8.1 of WCAP-13382)

Response:

Please see the response to Q420.56 for results of a prototype cabinet temperature and humidity limit test.

During shipment the cabinets are not energized, thus the internal power supplies and electronic assemblies do not act as heat sources creating a temperature rise above ambient in the cabinet. Consequently, an ambient temperature above normal operating temperature is permitted for shipment.

SSAR Revision: NONE

Question 420.62

Describe the mechanism of the cabinet cooling assembly power supply arrangements. Section 4.0.8.2 of WCAP-13382 states that cabinet cooling is used after loss of on-site AC-power. How does the cooling assembly function after a power loss?

Response:

The cabinet cooling is powered from the same battery-backed, uninterruptable ac power sources as the power supplies used for the cabinet electronics.

SSAR Revision: NONE

Question 420.63

Describe the automatic calibration feature that detects a multiplexer failure. (Section 4.0.10.1 of WCAP-13382)

Response:

The automatic calibration feature is not a licensing basis test and does not replace the periodic functional testing. This built-in diagnostic test is provided to support diagnostic and maintenance functions.

The multiplexer discussed in Section 4.0.10.1 of WCAP-13382 resides on the M40 analog input processor card (Section 3.2.8 of WCAP-13382). The analog input processor is connected to a number of analog sensors by analog input boards or RTD input boards, and sequentially performs the analog-to-digital conversions for these sensors. One or more of these signals are known test signals. The multiplexer on the analog input processor is used to choose the individual inputs to convert. If this multiplexer fails, the correct test signal will not appear at the input to the analog-to-digital converter in sequence, and thus will provide a detectable error.

SSAR Revision: NONE

Question 420.64

The communication subsystem provides information to alarm and monitoring systems external to the integrated protection system, such as cabinet entry status, cabinet temperature, DC power supply voltage and subsystem diagnostic status. Provide an analysis to demonstrate that no single failure (including failures such as overheating due to loss of cabinet cooling) will prevent the diagnostic status from being provided. (Section 4.1.10 of WCAP-13382)

Response:

There is no requirement that the communication subsystem within a cabinet meet the single failure criterion. The diagnostic information provided by the communication system is for maintenance only. There is sufficient redundancy in the protection and safety monitoring system to meet the single failure criterion, even with a failed cabinet. A communication subsystem provides dynamic information to, as a minimum, alarm and monitoring systems. The cessation of signals from a failed communications subsystem will be detected. Any failure not indicated by the communication system will be detected by the periodic functional test. Therefore, the diagnostic status does not need to function following a single failure.

The communications subsystems in the cabinets in the protection and safety monitoring system are Class 1E subsystems.

SSAR Revision: NONE

Question 420.65

The automatic tester subsystem injects signals by disconnecting the normal input signals and replacing them with simulated test signals. During test injection for the nuclear instrumentation signals, the automatic tester subsystem will switch off the high voltage supplies of the nuclear instrument detectors. Describe the mechanism to restore the normal status once the test is completed. Provide an analysis to demonstrate that the automatic tester will neither cause inadvertent actuation nor prevent the trip capabilities. (Section 4.1.11 of WCAP-13382)

Response:

When the high voltage supplies to the nuclear instrument detectors are de-energized, the signal from these detectors disappears, which is detectable by the automatic tester. When the high-voltage supplies are re-energized, the nuclear detector signals reappear, which is also a detectable event. For the case in which the automatic test is performed during plant shutdown, the presence of the nuclear instrumentation signals is confirmed during plant startup.

When an instrument channel is tested by the automatic tester, the automatic tester applies a bypass to that channel to prevent inadvertent actuation. When the test is completed, the bypass is removed, and the removal of the bypass is confirmed by the automatic tester to confirm that the channel has been returned to service.

SSAR Revision: NONE

Question 420.66

Define the scope of the automatic surveillance testing of the integrated protection cabinets and the ESFAS cabinets. Identify the tasks tested by a portable tester and the tasks tested by the built-in circuit in the protection cabinets. Are the test circuits in the protection cabinet fully qualified as Class-IE components? (Section 4.2 of WCAP-13382)

Response:

Please see the response to Q420.51 for a discussion of the portable tester. The automatic surveillance testing of an ESFAC and associated logic cabinets is performed by injecting input signals into the input channels (data link receivers) of the ESFAC and observing the response of the logic processor subsystems in the logic cabinets. One half of the redundant subsystems in the ESFAC and logic cabinets are tested at a time, so the system is still able to respond to plant events. During the testing, the signals from the half under test are disabled and the actuated devices do not change state during testing. The I/O cards in the logic cabinets are capable of automatically checking circuit continuity at their outputs and reporting open circuits.

The actuated devices are tested individually by manual operation.

The automatic tester subsystems and test circuits in the protection system are classified as associated Class 1E and are seismic qualified.

SSAR Revision: NONE

Question 420.67

Describe the software development process of the portable tester. Is the verification and validation process for the portable tester the same as the protection and safety monitoring system? (Section 4.2 of WCAP-13382)

Response:

Please see the response to Q420.51 for a description of the portable tester. The portable tester is not required to initiate the automatic test sequence. Because the portable tester provides only a printer and a communications device, commercial software is used where required, and a verification and validation process is not required.

SSAR Revision: NONE

Question 420.68

Describe the physical protection of the data highway for the protection and monitoring system and the plant control system. Are the data highways routed inside electrical conduits?

Response:

The fiber optic cables that compose the safety-related data highways in the protection and safety monitoring system will be protected in the same manner as the equivalent safety-related electrical cables in the protection and safety monitoring system. These fiber optic cables will be physically separated from fiber optic or electrical cables in other electrical divisions and non-safety-related electrical cables. Redundant fiber optic cables within a division are separated to the extent possible, except inside the cabinets, where the cabinets provide physical protection.

The fiber optic cables that compose the non-safety-related data highways in the plant control system and the data display and processing system will be protected in the same manner as the electrical cables in the plant control system and the data display and processing system. These fiber optic cables are separated from safety-related fiber optic or electrical cables. Redundant fiber optic cables within the plant control system and the data display and processing system are also separated to the extent possible, except inside the cabinets, where the cabinet provides physical protection.

The fiber optic cables that compose the various data highways in the AP600 will be routed in cable trays or conduit as appropriate.

SSAR Revision: NONE

Question 420.69

There is a discrepancy between Section 7.1.2.2 of the SSAR and Section 4.1.1 of WCAP-13382. How many microprocessor-based subsystems are in the integrated protection cabinet. Are there 8 or 9?

Response:

Please see Figure 4.1-1 of WCAP-13382. The integrated protection cabinets contain 10 functional microprocessor subsystems mounted in eight card cages. The trip enable subsystem and global trip ubsystems and the two nuclear instrumentation signal and processing and control (NISPAC) subsystems are mounted on dual backplanes in single card cages. In the SSAR, the NISPAC subsystems are treated as part of the nuclear signal conditioning.

SSAR Subsection 7.1.2.2 will be revised as follows:

SSAR Revision:

To conform with the system criteria concerning separation and diversity, the functions of the protection and safety monitoring system are implemented in ~~eight~~ 10 ~~electrically and physically separated~~ microprocessor-based subsystems mounted in eight card cages. These subsystems are the following:

- Reactor trip group 1
- Reactor trip group 2
- Global trip
- Trip enable
- Engineered safety features group 1
- Engineered safety features group 2
- Communication
- Automatic tester.
- Nuclear instrumentation signal and processing and control (NISPAC) 1
- Nuclear instrumentation signal and processing and control (NISPAC) 2

Question 420.75

Describe the design of the remote shutdown workstation with respect to preventing inadvertent lockout or inadvertent actuation. (Section 7.4.3)

Response:

Inadvertent lockouts and inadvertent actuations from the remote shutdown workstation are prevented by administrative controls. The remote shutdown workstation is in a room that is kept locked when not in use. The door to this room is alarmed. The switches that transfer control between the main control room and the remote shutdown room are locked and alarmed. These transfer switches are described in the response to Q420.73.

SSAR Revision: NONE

Question 420.76

Discuss the accessibility of the remote shutdown station to the operator without the use of security devices, such as keys or key cards and without electrical power. (Reference: Section 4.9.1.2.3 of Chapter 10 of the EPRI ALWR Utilities Requirements Document) (Section 7.4.3 of the SSAR)

Response:

The AP600 remote shutdown panel is in the auxiliary building on elevation 100'-0" in a dedicated room. The normal access door from the elevation 100'-0" corridor is not locked, therefore it does not require the use of any security devices such as keys or key cards. Electrical power is not required to obtain access to the remote shutdown panel room.

SSAR Revision: NONE

Question 420.83

Section 18.9.2.3.8 of the SSAR states that the alarm system is not a contributor to plant unavailability. However, Section 18.9.2.4.1 states that the alarm system is a monitoring system required to be operating for normal and abnormal plant conditions. Clarify the discrepancy between these statements. Discuss the plant emergency procedures for a loss of the alarm system.

Response:

Attachment G to Westinghouse letter ET-NRC-92-3748, "Comments on Draft NRC Policy *Design Certification and Licensing Policy Issues Pertaining to Passive and Evolutionary Advanced Light Water Reactor Designs*," from N. J. Liparulo to Dr. Ivan Selin, September 17, 1992 discusses the Westinghouse position on the classification of the alarm system in the AP600. While the passive design of the AP600 generally requires no operator actions to remain safe, there are a limited number of transients that require operator action. These transients develop slowly and provide ample opportunity for the operators to intervene. There is no need for an alarm to alert the operators to these events since they will be discovered by the normal, routine surveillance of displays.

SSAR Subsection 18.9.2.4.1, second sentence, (Proprietary Volume) will be revised as follows:

SSAR Revision:

The alarm system is a monitoring system required to be operating for normal ~~and abnormal~~ plant conditions.

Question 420.84

Section 18.9.2.4.2 of the SSAR states that no special requirements exist for the protection of the alarm system. Provide a discussion on the effects on the alarm system from environmental conditions due to high temperature, high humidity, and smoke.

Response:

Please see the response to Q420.83, Section 18.9.2.4.1 of the SSAR, and Attachment G to Westinghouse letter ET-NRC-92-3748, "Comments on Draft NRC Policy *Design Certification and Licensing Policy Issues Pertaining to Passive and Evolutionary Advanced Light Water Reactor Designs*," from N. J. Liparulo to Dr. Ivan Selin, September 17, 1992. The AP600 alarm system is a non-safety-related system and is not designed to meet the requirements of Class 1E equipment. While the passive design of the AP600 generally requires no operator actions to remain safe, there are a limited number of transients that require operator action. These transients develop slowly and provide ample opportunity for the operators to intervene. There is no need for an alarm to alert the operators to these events since they will be discovered by the normal, routine surveillance of displays.

The plant alarm system is a non-safety-related system therefore, environmental conditions such as high temperature, high humidity, and smoke are not included in the design basis.

The alarm system is expected to operate within normal ranges of temperature (+10° to +40°C) and relative humidity (20 to 80% at 40 °C).

SSAR Revision: NONE

Question 420.87

Paragraph 4 of Section 4.4.1 of WCAP-13382 states that each multiplexer is connected to each workstation. Does this mean every workstation has 8 logic bus connections (i.e., Logic Bus 1 and Logic Bus 2 for each of the four divisions)? If so, is there a single failure or common-mode-failure potential that one workstation can prevent ESF actuation? For example, the workstation may fail in a mode such that it continually sends out "stop and close" signals to the ESF equipment. Since the workstations interface to the Logic Bus, which is downstream of the ESF system initiation signal coming from the Integrated Protection Cabinets (IPC), the workstation signal can override the IPC's ESF signals. Thus, the workstations may prevent initiation of the ESF system when needed.

Response:

The four safety-related divisions in the protection and safety monitoring system each contain two multiplexer cabinets, one for the main control room interface and one for the remote shutdown workstation interface.

Each workstation (operator, supervisor, and remote shutdown) in the AP600 instrumentation and control architecture is capable of sending out signals on each of the four dual redundant logic buses in the AP600 instrumentation and control architecture by means of the multiplexer cabinets in each of the four divisions. For a signal to be transmitted on a logic bus, two distinct signals are required, a command signal and a confirmation signal. If a workstation fails to a mode in which it continuously transmits a false signal without the required confirmation signal, the multiplexer cabinet will ignore these signals and will not transmit on the logic bus. It is considered beyond the design basis that a single failure in a workstation will produce a command signal and the confirmation signal in the proper sequence.

SSAR Revision: NONE

Question 420.89

Describe how the Trip-Normal-Bypass (TNB) switch, the Auto Bypass, the Global Bypass, and the Auto Global Bypass work. Provide a table that shows the inputs (i.e., partial trips, TNB switch, auto bypass, global bypass, auto global bypass, and all other inputs needed for a trip) versus the outputs (i.e., Partial Trip; A, B, C, or D Division Trip; Reactor Trip). (Section 7.1.2.2.3.3)

Response:

Please see the response to Q420.31. WCAP-8897 describes the operation of the reactor trip logic and includes tables showing the output versus the inputs to the logic network.

The Trip-Normal-Bypass (TNB) switch, located on the dynamic trip bus, allows each trip function to be placed in a manual partial trip state or a manual bypass state or to be returned to the normal state. The operation of the TNB switch is discussed in Section 3.7 of WCAP-13391(NP), "AP600 Instrumentation and Control Hardware Description," Rev. 0, May 15, 1992 (Reference 3 of SSAR Subsection 7.1.6). A TNB switch is provided for each reactor trip function in the integrated protection cabinet. In addition, a single TNB switch is provided that is capable of applying a manual partial trip or a manual partial bypass to each reactor trip channel in the integrated protection cabinets. These are called the global trip and global bypass.

The application of automatic bypasses is discussed in Section 4.2 of WCAP-8897. When an automatic bypass is applied to a single reactor trip channel, it is referred to as an auto bypass. When it is applied to each reactor trip channel in the integrated protection cabinets, it is referred to as an auto global bypass.

SSAR Revision: NONE

Question 471.2

Section 12.3 of the SRP specifies that the SSAR should contain radiation zone designations (including zone boundaries and normal traffic patterns) on the plant layout drawings. The zone maps are laid out very well, except that Very High Radiation Areas as defined in the revised 10 CFR Part 20 are not identified during normal and anticipated operational occurrences. Also, there are no traffic patterns identified for normal traffic flow or for access to vital areas during accident operations. This information is needed by the staff to ensure all areas having potentially lethal levels of radiation are identified and controlled. Provide this information.

Response (Revision 1):

The radiation zone maps have been revised to identify the traffic patterns for normal operation and shutdown. These radiation zone maps also identify the very high radiation areas in the plant as required by 10 CFR Part 20. Radiation zone maps during normal and post-accident operation for the nuclear island, annex I and II buildings, and radwaste building are provided via letter ET-NRC-93-3839 (N. J. Liparulo to R. W. Borchardt, dated March 18, 1993).

The applicable post-accident zone maps identify the traffic patterns for access to perform the following:

- Main control room access
- Post-accident sampling
- Spent fuel pool cooling make up
- Containment inventory make up
- Temporary water hookup to passive containment cooling system tank
- Temporary HVAC to main control room and PAMS cabinets
- Temporary power to Class 1E regulating transformers
- Temporary power to hydrogen recombiners

Descriptions of the access routes follow.

Main Control Room Access

The main control room and its supporting facilities are in the northeast corner of the auxiliary building at elevation 117'-6". From the plant entrance at elevation 100' in annex I building, proceed up the stairs to elevation 117'-6", and exit using the doors just outside the shift turnover room, across the hall from the technical support center. To access the MCR, proceed west through the doors into the controlled access hallway of the turbine building. Move down the hall to the door on the left, which leads d[illegible] the control room access foyer.

From the control room, egress is provided by the reverse of the entry path.

Post-Accident Sampling

Samples are taken for onsite analysis from the sample room. To access the sample room, proceed through the radwaste building at elevation 100'-0" to the auxiliary building, using the access doors to the rail bay. Note that other post-accident operations use this rail bay and obtain access through the large, overhead door in the southeast corner. If this door is already open, access through the radwaste building may be unnecessary. The overhead door route may be used. Directly north of this area, a door provides access to the auxiliary building stairs. Enter the stairs and proceed down to level 66'-6" and exit. The sample room is just north of this hallway. Exit by reversing the entry path.

Spent Fuel Pool Cooling Makeup

The AP600 provides a connection for providing makeup water to the spent fuel pool. The first activity is in the southeast corner rail bay. After manually opening the large, overhead door (in the southeast corner), emergency water sources would be positioned on the railroad tracks in the rail bay. The water source would then be connected using the plant hookup just inside the double doors to the north. Once this connection is established, further access is required in the pipe chase room just south of the radioactive chemistry lab on elevation 82'-6". Enter the stairs and proceed down to level 82'-6" and exit. Enter the door to the pipe chase room on the left and open a manual, locked-closed valve to establish a flow path. Exit by reversing the entry path. Once the flow path is complete, flow may be regulated by controlling the source, which is in the rail bay.

Containment Inventory Makeup

Similar to the general procedure for spent fuel pool cooling makeup, containment inventory makeup capability is provided using the normal residual heat removal system (RNS). Access requirements and physical hookup procedures for using the RNS piping are the same as described for the spent fuel pool cooling makeup, with one exception. Using the RNS piping requires that a containment isolation valve be opened. If control power is not available for control room remote operations, the valve must be aligned manually. This valve is in the RNS valve room just above the radioactive chemistry lab. To access this valve, one must proceed into the filter/demineralizer room. From this filter room, continue north and through the last door on the left into the annulus. Proceed left through the annulus, and enter the first door on the left. Use the ladder directly in front to proceed up to elevation 92'-0". Exit by reversing the entry path.

The task of valve alignment can be accomplished rapidly. This makeup is not necessary for approximately one month and the volume of water needed is small.

Temporary Water Hookup to the Passive Containment Cooling System Tank

Emergency firetruck-type equipment is used to provide makeup water to the PCS storage tank. The current design includes a makeup water connection located at the wall penetrations which lead to the valve/piping penetration room on elevation 100'-0" in the northwest corner of the auxiliary building. One valve must be aligned to accomplish this task. It is necessary to access the valve/piping penetration room to operate this valve. Access to this area is from the turbine building, using the door at the northwest corner of the auxiliary building. Exit by reversing the entry path.

Temporary HVAC to Main Control Room and PAMS Cabinets

Temporary HVAC is provided to the control room by using an air-cooled chiller package and a room cooler. The air-cooled chiller package is set up in the shift turnover room (STR) of the annex 1 building on elevation 117'-6". Using penetrations provided through the wall into the control room, this portable unit provides chilled water to a room cooler temporarily located in the control room. The heat generated by the air-cooled chiller package is rejected to the STR area.

For the PAMS cabinets, portable fans are located outside the main entrance to the annex 1 building, north of the security area at elevation 100'-0". The flexible hoses (elephant trunks) for this service will be routed past security and west through the doors into the north-most clean access corridor of the auxiliary building and into the B and C electrical rooms to provide airflow for once-through cooling with outside air. This equipment does not require chilled water.

Temporary Power to Class 1E Regulating Transformers

The portable emergency diesel-generators necessary for this temporary service are positioned outside the main entrance to the annex 1 building north of the security area at elevation 100'-0". The electrical cables for this service are routed past the security area west through the doors to the auxiliary building's north-most clean access corridor of the auxiliary building. The necessary electrical connections and breaker positioning can be accomplished at the regulating transformers in the B and C Class 1E equipment rooms (elevation 82'-6"). Access to this level is obtained using the stairs at the west end of the clean access corridor. Exit by reversing the entry path.

Temporary Power to Hydrogen Recombiners

The hydrogen recombiners are inside containment and can be connected to a temporary power hookup from the portable emergency diesel-generators described in the preceding paragraph. The hookups are in the non-1E electrical penetration rooms on elevations 100'-6" and 117'-6". One of the electrical cables for this service is routed past the security area, west, and then south, down the corridor to the auxiliary building access doors. This cable is then routed into the auxiliary building penetration room on elevation 100'-6". A second electrical cable is routed past the security area, west, and then up the annex 1 stairwell. After exiting the stairwell, route the cable past the STR and into the auxiliary building penetration room on elevation 117'-6", where the temporary hookups are made.

SSAR Section 12.3 will be revised as follows:

SSAR Revision:

(SSAR Figures 12.3-1 and 12.3-2 will be replaced with the drawings submitted to the NRC via letter ET-NRC-93-3839, dated March 18,1993.)

Question 471.3

Provide expected peak airborne radioactivity concentrations, estimated man-hours of occupancy, and estimated inhalation exposures for all areas of the plant accessed by plant personnel. This information is required by the Standard Review Plan and is needed by the staff to ensure that the plant's ventilation flow is sufficient to maintain airborne radioactivity levels ALARA.

Response (Revision 1):

The expected peak airborne radioactivity concentrations, estimated man-hour occupancy, and estimated inhalation exposures are provided in Table (1). A summary of the evaluations for the nuclear island, turbine building, annex buildings I and II, and radwaste buildings follows.

Nuclear Island

This section provides information on the models, design parameters, and sources of airborne radioactivity concentrations during normal plant operations. Areas of Zone II and lower in the nuclear island are not included since airborne radioactivity concentrations in these less-restricted and frequently occupied areas are a very small fraction of 10 CFR 20, §20.1001-2401, Appendix B concentrations. Pipeways and chases are also not included since these areas do not contain active components that are leak sources, and the access requirements for these areas are very infrequent.

Airborne radioactivity sources include the concentrations of radionuclides in the reactor coolant system (RCS), chemical and volume control system (CVS), normal residual heat removal system (RNS), spent fuel pool cooling system (SFS), liquid radwaste system (WLS), and gaseous radwaste system (WGS). For areas where the reactor coolant source is applicable, the realistic source values of SSAR Table 11.1-8 are used based on normal plant operation.

The assumptions and design parameters are provided in SSAR Section 12.4.

1. **Airborne Radioactivity Dose Estimates**

The total inhalation exposure dose for a room or an area is the sum of the inhalation exposure from individual activities in the subject room or area. Activities for the nuclear island include normal plant operation, routine surveillance, testing and maintenance, in-service inspection (ISI), refueling operations, and special maintenance. The inhalation dose exposure is proportional to the occupancy and the radioactivity concentration of the area.

The occupancy time for the activities in a room or an area is estimated based on the equipment and the data on typical equipment surveillance, ISI, maintenance, and repairs from operating experiences. Some of the occupancy data are used and presented in SSAR Subsection 12.4.1 for dose assessment from direct radiation. These data are also used to determine the airborne inhalation dose exposures of the corresponding rooms or areas. The estimated occupancy time for the activities is provided in Table (1).

The estimated airborne radioactivity in a room or an area is a function of the source and the removal of activity by the ventilation system. The source of airborne radioactivity in a room or an area is primarily from equipment leakage. The total leakage for a room or an area is estimated as the sum of leakage from the individual equipment within the room or area. The data for individual equipment leakage are historical data from operating plants. The data on the supply and exhaust air flow for the related room or area are based on the plant ventilation system design. The airborne radioactivity is determined by using the calculation model presented in SSAR Subsection 12.2.2.4. The estimated peak airborne concentration and the calculated inhalation dose exposure for each room or area in the nuclear island are provided in Table (1).

Airborne radioactivities for the containment and the fuel building presented in SSAR Tables 12.2-23 and 12.2-25 are based on overall plant design parameters and operating conditions. These airborne radioactivities are used to estimate the peak airborne radioactivity and inhalation dose exposures for the area.

2. Method for Calculating the Inhalation Dose

The inhalation thyroid, lung, and whole-body doses are calculated using:

$$D_t = \Sigma \ C_i \times DCF_i \times BR \times T_o$$

where:

D_t = thyroid, lung, or whole-body dose from all isotopes except H^3 (rem)

C_i = equilibrium concentration of each radioisotope (Ci/m^3)

DCF_i = inhalation dose conversion factor for isotope i (rem/Ci) (based on DCFs from Regulatory Guide 1.109)

BR = breathing rate (3.47×10^{-4} m^3/sec)

T_o = occupancy time

3. Method for Calculating the Tritium Dose

The tritium dose is calculated using:

$$D_{tritium} = C_{tritium} \times DCF_{tritium} \times BR \times T_o$$

where:

$D_{tritium}$ = dose caused by absorption of tritium by lungs and skin (Rem)

$C_{tritium}$ = equilibrium concentration of tritium isotope (Ci/m^3)

$DCF_{tritium}$ = inhalation dose conversion factor for tritium (rem/Ci) (based on DCFs from Regulatory Guide 1.109)

BR = breathing rate ($3.47x10^{-4}$ m^3/sec)

T_o = occupancy time

Note: Airborne H^3 dose is the sum of the skin dose and the lung dose, where skin dose is equal to lung dose.

This model is conservative since it is based on a continuous intake model. The individual is assumed to remain in a tritium environment for the entire time T_o with no credit taken for decay (radiological or biological) when the individual is out of the tritium environment.

The partition factors and the assumed equipment leak rates (airborne radioactivity model - SSAR Subsection 12.2.2.4) used to estimate the peak airborne radioactivity for rooms and areas are provided in Tables (2) and (3).

Turbine Building

Turbine building airborne radioisotope concentrations are calculated based on 1700 pounds of secondary-side steam leakage per day consistent with NUREG-0017. Steam activity is based on SSAR Table 11.1-8, and the turbine building is treated as a single volume with once-through HVAC. The resultant equilibrium concentrations are used for inhalation and submersion dose calculations, assuming 2000 hours per year exposure and an average of 75 persons in the building.

Radwaste Building and Annex II Building

The radwaste building does not have any sources of gaseous radioactivity. Gaseous krypton, xenon, and tritium activities are not present on the spent resins or in the detergent or chemical wastes, and iodine activity is tied up on the spent resins. The radwaste building HVAC system provides air flow from areas with lower to higher potential for airborne radioactive particulates. In addition, the following confined areas and components, where the potential exists to generate airborne particulates, are vented directly to the HVAC system exhaust fan and filtration units:

High activity filter storage tube module
High activity filter processing cask
Onsite storage casks
Spent resin container fill stations
Spent resin container fill heads via the vent overflow drum
Spent resin tanks via the tank room sump
Radwaste sumps

Detergent waste, monitor and chemical waste tanks
Filter dryer
Drum compactor
Low activity waste monitoring unit
Low activity waste dryer
Clean waste dryer
Sorting glove box and box compactor
Hazardous waste sample (fume) hoods
Hazardous/mixed waste accumulation drum hoods
Laundry sorting table hood
Laundry dryers
Respirator cleaning disassembly hood
Respirator cleaning dryer
Respirator cleaning decon glove box
Respirator cleaning filter decon hood
High pressure hot water decon booth
Abrasive decon booth

These exhausts remove airborne radioactivity before it enters normally occupied areas. Thus, the airborne radioactivity in normally occupied areas in the radwaste building is expected to be at background, and inhalation exposures are expected to be essentially zero.

A conservative estimate of the airborne dose to personnel in the radwaste building is made using historical data on radioactive particulate releases and methods used by the NRC to relate these releases to in-plant sources. NUREG/CR-2907, which documents the latest releases of radioactive materials from nuclear power plants, indicates that the release of particulate radioactivity between 1980 and 1988 for all operating nuclear power plants averaged 9×10^{-9} Ci/MWe-hr. Based on NUREG-0017, about 5 percent of this is expected to be from the "auxiliary building" source. For the AP600, the "auxiliary building" source includes the radwaste building, the non-fuel-pool areas of the auxiliary building, and the annex II building. Considering the systems and operations in these buildings, the distribution of this release from the AP600 auxiliary, radwaste, and annex II buildings is estimated to be 40 percent, 40 percent, and 20, percent respectively. The radwaste building release is therefore approximately 2 percent of the total plant particulate radioactivity release, and the release from the radwaste building is about 1.8×10^{-10} Ci/MWe-hr. At a capacity factor of 80 percent, the estimated release of particulate activity from the AP600 radwaste building is about 7.6×10^{-4} Ci/year. Based on an HEPA filter efficiency of 99 percent (NUREG-0017, page 1-28), the average airborne particulate release rate before filtration is about 7.6×10^{-2} Ci/year, or 1.4×10^{-10} μCi/cc in the exhaust flow of 36,000 cfm.

The dose estimates in Table (1) are calculated using methods and dose factors in Regulatory Guide 1.109. It is conservatively assumed that releases occur only during batch operations (for example, laundry sorting, filter storage drum loading) and that these batch operations are in progress 10 percent of the time (2.4 hours per day). This increases the particulate activity source concentration by a factor of 10 to 1.4×10^{-9} μCi/cc. The radwaste building occupancy is estimated to be 48,000 hours per year. However, because of general and local ventilation exhausts, exposure to airborne particulates should occur less than 1 percent of the time. Thus, the exposure duration of 480 hours per year is considered conservative.

As described for the radwaste building, the annex II building does not have any sources of gaseous radioactivity, and ventilation exhausts are employed to minimize airborne particulates. The airborne particulate activity dose estimates in Table (1) are conservatively derived using the same methods described for the radwaste building. The release rate is taken as 20 percent of the "auxiliary building" source, or 1 percent of the total plant particulate radioactivity release. The source concentration is estimated to be 1.04 x 10^{-8} μCi/cc based on a ventilation rate of 24,400 cfm and with releases occurring only 1 percent of the time. Occupancy for activities with potential for particulate release is estimated to be 9600 hours per year. The exposure duration is expected to be less than 1 percent of the time.

SSAR Revision: NONE

Table 1 Airborne Dose Estimate to Plant Operating Personnel

Location	Estimated Airborne Activity (μCi/cc)	Work/Activity Description	Total Occup. Time (hrs/no. of workers)	Inhalation Lung Dose (man-rem/yr)	Inhalation Thyroid Dose (man-rem/yr)	Airborne H^3 Dose (man-rem/yr)	Inhalation Whole-Body Dose (man-rem/yr)
SG Vaults (Rooms 11201, 11202)	NG = 1.09E-12 I = 1.33E-10 P = 1.94E-11 H = 7.42E-8 NG - Noble gases I - Iodine P - Particulates H - Tritium	RC pump inspection	2/2 (1.5 yrs)	7.0E-6	3.2E-5	3.9E-4	1.3E-6
		RC pump ISI	41/2 (10-yr interval)	2.1E-5	9.8E-5	1.2E-3	4.1E-6
		SG eddy current tube inspection & plugging	97/2 (1.5 yrs)	3.4E-4	1.6E-3	1.9E-2	6.5E-5
		Sludge lancing of SG	78/6 (1.5 yrs)	2.7E-4	1.2E-3	1.5E-2	5.2E-5
		Visual exam. of SG - secondary side	17/2 (1.5 yrs)	5.9E-5	2.7E-4	3.3E-3	1.1E-5
		SG secondary-side repair	44/-- (annual)	2.3E-4	1.1E-3	1.3E-2	4.4E-5

Table 1 Airborne Dose Estimate to Plant Operating Personnel

Location	Estimated Airborne Activity (μCi/cc)	Work/Activity Description	Total Occup. Time (hrs/no. of workers)	Inhalation Lung Dose (man-rem/yr)	Inhalation Thyroid Dose (man-rem/yr)	Airborne H^3 Dose (man-rem/yr)	Inhalation Whole-Body Dose (man-rem/yr)
		SG ISI	70/2 (10-yr interval)	3.6E-5	1.7E-4	2.1E-3	7.0E-6
Pressurizer (rooms 11303, 11403, 11503, 11603)	NG = 1.09E-12 I = 1.33E-10 P = 1.94E-11 H = 7.42E-8	Pressurizer shell ISI	12/--- (annual)	6.3E-5	2.9E-4	3.5E-3	1.2E-5
		Pressurizer repair	10/--- (annual)	5.2E-5	2.4E-4	2.9E-3	1.0E-5
Reactor cavity (Room 11205)	NG = 1.09E-12 I = 1.33E-10 P = 1.94E-11 H = 7.42E-8	RV & RV head ISI	26/--- (annual)	1.4E-4	6.2E-4	7.6E-3	2.6E-5
Primary containment	NG = 8.4E-7 I = 9.73E-9 P = 1.6E-9 H = 2.56E-6	At-power containment entries	100/--- (annual)	2.2E-2	3.53E-1	1.01E-1	5.83E-3
	NG = 1.09E-12 I = 1.33E-10 P = 1.94E-11 H = 7.42E-8	RC loop piping ISI	15/--- (annual)	7.8E-5	3.6E-4	4.4E-3	1.5E-5
		Refueling operation	645/--- (1.5 yrs)	2.2E-3	1.0E-2	1.3E-1	4.3E-4

Table 1 Airborne Dose Estimate to Plant Operating Personnel

Location	Estimated Airborne Activity (μCi/cc)	Work/Activity Description	Total Occup. Time (hrs/no. of workers)	Inhalation Lung Dose (man-rem/yr)	Inhalation Thyroid Dose (man-rem/yr)	Airborne H^3 Dose (man-rem/yr)	Inhalation Whole-Body Dose (man-rem/yr)
Fuel building refueling area	NG = 1.31E-9 I = 5.86E-10 P = 4.43E-10 H = 4.0E-6	Refueling operation	240/--- (1.5 yrs)	1.4E-2	7.1E-1	1.0E+0	1.7E-2
12151	I = 2.90E-10 P = 2.48E-12 H = 4.32E-8	Routine operation & maintenance in demin./filter room	333/--- (annual)	1.1E-3	1.1E-2	5.7E-3	4.3E-5
12152	NG = 7.9E-7 I = 8.75E-10 P = 7.53E-12 H = 1.31E-7	Routine operation & maintenance in primary sampling room	358/--- (annual)	4.8E-3	3.6E-2	1.9E-2	1.4E-4
12155, 12258	NG = 1.90E-6 I = 2.12E-9	Routine operation & maintenance in waste gas equipment room	443/--- (annual)	6.5E-3	1.1E-1	0	3.3E-4
12162, 12163	NG = 4.38E-7 I = 4.50E-10 P = 4.53E-9 H = 4.06E-8	Routine operation & maintenance in RNS pump rooms	145/--- (annual)	1.4E-1	2.2E-2	2.3E-3	7.8E-4

Table 1 Airborne Dose Estimate to Plant Operating Personnel

Location	Estimated Airborne Activity (μCi/cc)	Work/Activity Description	Total Occup. Time (hrs/no. of workers)	Inhalation Lung Dose (man-rem/yr)	Inhalation Thyroid Dose (man-rem/yr)	Airborne H^3 Dose (man-rem/yr)	Inhalation Whole-Body Dose (man-rem/yr)
12164, 12165	I = 4.3E-12 P = 3.58E-14 H = 6.24E-9	Routine operation & maintenance in waste monitor tank room	187/--- (annual)	8.5E-6	9.1E-5	4.6E-4	3.5E-7
12166, 12167	I = 3.94E-12 P = 3.29E-13 H = 5.73E-9	Routine operation & maintenance in waste holdup tank rooms	187/--- (annual)	7.8E-6	8.3E-5	4.2E-4	3.3E-7
12171	I = 2.65E-11 P = 2.21E-13 H = 3.85E-9	Routine operation & maintenance in effluent holdup tanks room	166/--- (annual)	4.7E-5	5.0E-4	2.5E-4	1.9E-6
12252	NG = 7.93E-8 I = 8.75E-11 P = 7.53E-13 H = 1.31E-8	Chemical sampling & analysis	1000/--- (annual)	1.3E-3	1.0E-2	5.2E-3	3.9E-5
12255	NG = 3.46E-7 I = 3.71E-10 P = 3.31E-12 H = 5.76E-8	Routine operation & maintenance in makeup pump room	202/--- (annual)	1.2E-3	9.0E-3	4.6E-3	3.5E-5

Table 1 Airborne Dose Estimate to Plant Operating Personnel

Location	Estimated Airborne Activity (μCi/cc)	Work/Activity Description	Total Occup. Time (hrs/no. of workers)	Inhalation Lung Dose (man-rem/yr)	Inhalation Thyroid Dose (man-rem/yr)	Airborne H^3 Dose (man-rem/yr)	Inhalation Whole-Body Dose (man-rem/yr)
12272, 12273	I = 1.66E-17 P = 5.38E-17 H = 1.43E-9	Routine operation & maintenance SFS equipment rooms	208/--- (annual)	2.5E-10	7.2E-9	1.2E-4	1.1E-9
12362, 12363	NG = 2.8E-7 I = 2.92E-10 P = 2.86E-9 H = 2.57E-8	Routine operation & maintenance in RNS heat exchanger rooms	111/--- (annual)	6.8E-2	1.1E-2	1.1E-3	3.8E-4
12364, 12365	I = 3.68E-12 P = 3.16E-14 H = 5.50E-9	Routine operation & maintenance in effluent monitor tank rooms	187/--- (annual)	7.5E-6	8.0E-5	4.1E-4	3.1E-7
12561	NG = 8.58E-11 I = 8.55E-16 P = 2.76E-15 H = 4.01E-6	Routine operation & maintenance in fuel handling area	1500/--- (annual)	4.3E-7	2.6E-6	2.4E+0	4.0E-7
Radwaste building	P = 1.4E-9	Radwaste processing, laundry & respirator cleaning	48,000/25 1% exposure 480 hours	0.12	---	---	0.026

Table 1 Airborne Dose Estimate to Plant Operating Personnel

Location	Estimated Airborne Activity (μCi/cc)	Work/Activity Description	Total Occup. Time (hrs/no. of workers)	Inhalation Lung Dose (man-rem/yr)	Inhalation Thyroid Dose (man-rem/yr)	Airborne H^3 Dose (man-rem/yr)	Inhalation Whole-Body Dose (man-rem/yr)
Annex II building	P = 1.04E-8	Hot machine shop operations & maintenance related activities on el. 135'-3"	9600/5 1% exposure 96 hours	0.18	---	---	0.039
Turbine building	NG = 5.40E-12 I = 9.27E-13 P = 4.09E-14 H = 2.45E-9	Maintenance and operation activities	150,000/75	0.053	0.074	0.053	0.0003

TABLE (2) PARTITION FACTORS (PF) FOR LEAK SOURCES

	PARTITION FACTORS			
Leak Source	Noble Gases	Halogen	Particulate	H-3
Steam/Gas Source	1.0	1.0	1.0	1.0
Containment(1) (Primary Coolant)	1.0	0.4	0.4	0.4
CVS(1)	1.0	0.4	0.4	0.4
Normal RHR System	1.0	0.01	0.001	0.1
Fuel Pool Cooling System	1.0	0.01	0.001	0.1
Liquid Leakage from the Secondary Side	1.0	0.01	0.001	0.1
Cold Leakage	1.0	0.01	0.001	0.1

(1) Based on flashing fraction (CVS regenerative heat exchanger inlet conditions)

TABLE (3) ASSUMED LEAKAGE RATES FOR VARIOUS EQUIPMENT

Equipment	Leakage Rate (cc/hr)	Equipment Size
Small Valve	3	≤ 2" dia. valve
Large Valve	30	≥ 2" dia. valve
Low -Head Pump	30	
High-Head Pump	60	
Heat Exchanger	240	
Flanges	30	In-line flange

(1) No leakage is assumed for component with leakoff connections.

Question 620.50

The emergency response guidelines (ERGs), in conjunction with additional safety-significant operator actions derived from the AP600 probabilistic risk assessment (PRA), should be used as the basis for developing a minimum inventory of fixed and continuous displays, controls, and alarms relied on by the operator for transient and accident mitigation. In addition to the ERGs requested in Q440.32, develop the minimum inventory of displays, controls, and alarms described above based on the AP600 ERGs and appropriate PRA operator action insights, and provide this information using the following matrix:

COLUMN ITEM

1 State whether the step is an ERG or PRA reference

2 State each high level ERG or PRA step (include each entry condition, caution, and note as a separate step).

3 Describe each primary operator action associated with the high level step separately (NOTE: Primary operator actions are substeps of ERGs and should include any pertinent operator actions referenced from ERGs to System Operating Procedures, Integrated Operating Procedures, or other procedures).

4 List all operator information and alarm requirements necessary to determine if each primary operator action is to be performed (e.g., RCS temperature, pressurizer pressure, containment pressure, and SG low level alarm).

5 List all operator control requirements necessary to perform each primary operator action (e.g., operator must select a pressurizer spray isolation valve and depress "open" switch).

NOTE: **For items 6-13, place an asterisk (*) next to each display, control, alarm, or operator aid which is not expected to be in the control room, and describe its intended location.**

6 List all displays required by the operator to perform each primary operator action (e.g., narrow range SG level indication, wide range RCS temperature indication, narrow range pressurizer pressure indication, etc.).

7 List all controls required by the operator to perform each primary operator action (e.g., RCP start switch).

8 List all alarms required by the operator to perform each primary operator action (e.g., SG low level alarm, pressurizer high pressure alarm).

9 List all operator aids required by the operator to perform each primary operator action (e.g., nomgraphs, steam tables, computer-based aids, etc.).

10-13 List all displays, controls, alarms, and operator aids used for feedback to operators to ensure that each primary operator action has been accomplished or initiated appropriately.

14 Determine if each display, control, or alarm required to perform operator actions or to be used for feedback purposes is Class 1E instrumentation and/or R.G. 1.97 instrumentation.

Response:

The RAI requests the development of the minimum inventory of fixed and continuous displays, controls, and alarms that the operator relies upon for transient and accident mitigation. Through research by the Westinghouse Science and Technology personnel in cognitive psychology and decision making and by studying other designs, Westinghouse has learned that fixed and continuous displays are often not the most effective. In terms of individual displays, there are many plant states and instances in time when fixed and continuous displays do not accurately represent the current plant state or conditions, do not provide information pertinent to current conditions, or do not efficiently present data regarding the current plant state or conditions. In terms of all fixed and continuous parallel presentation, like traditional control boards, only raw data is presented that then needs to be acquired, given a context, and synthesized by the operator into something meaningful. The cognitive task analysis will define the level of abstraction of the information required and the grouping and presentation context necessary to support the decision-making tasks. This will form the foundation for the display system design. Because of all these reasons, the AP600 control room design concept is that few or no displays will be "fixed or continuously displayed.

A display system of the AP600 scope and magnitude needs to retain flexibility to present the data differently under different plant conditions. Westinghouse does, however, recognize the benefits of spatial dedication and will employ it to some degree in the overview alarm displays and on the wall panel information system. The QDPS (qualified display processing system) used for post-accident monitoring has displays that are selectable by the operator. The QDPS presents alarms on every display page to alert the operator of a specific operating concern. The wall panel information system is a dynamic display that changes with the plant state. The wall panel information system is dynamic in order to make it useful not only during normal operations but also during other plant modes, including shutdown and refueling. The displays in the information system that are normally used with the computerized emergency operating or normal operating procedures also have multiple dynamic data displays that are selectable by the operator.

The PRA results are input to the ERG development process. Since this analysis is input to the process, there is no need to identify those steps that result from the PRA references as opposed to other inputs to the ERG process. Therefore, each step or substep will be an ERG step or substep.

Chapter 18 in the AP600 SSAR describes the detailed process that will be followed in order to develop the M-MIS information. As discussed with the NRC on January 22-23, 1992 and November 19, 1992, the process discussed in Chapter 18 of the SSAR is the basis for design certification. The Human Factors Engineering ITAAC (see ITAAC 4.1 in the AP600 Tier 1 Material Including Plant Description and ITAAC) specifies Tier 1 aspects of the process, supported by the details described in the SSAR (Tier 2). The Tier 2 documentation includes the process pertaining to the development of the plant procedures and completion of the function-based task analysis. The information in Chapter 18, along with that information to be provided in response to this question and to Q440.32, provides the basis for the staff to complete its safety evaluation. The final control room design details are developed by executing the described process and will be confirmed by the fulfillment of the Human Factors Engineering ITAAC.

A preliminary list of indications and controls needed to support the high-level operator action strategies (documented in SSAR Subsection 18.9.8.1.1.2) will be submitted to the NRC, in conjunction with the documentation supporting Q440.32, on June 30, 1993. In response to Q440.32, Westinghouse provides additional information concerning the development of high-level operator action strategies for the AP600, along with information pertaining to the use of the Westinghouse two-loop, low-pressure reference plant ERGs. Refer to the response to Q440.32 for additional details in these areas.

SSAR Revision: NONE