Westinghouse Electric Corporation
Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

ET-NRC-93-3824
NSRA-APSL-93-0045
Docket No.: STN-52-003

February 25, 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 October 28, 1992 and November 16, 1992. This transmittal completes the responses to the October 28, 1992 letter. A listing of the NRC requests for additional information responded to in this letter is contained in Attachment A. Attachment B is a complete listing of the questions associated with the October 28, 1992 letter and the corresponding Westinghouse letters that provided our response.

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

Nicholas J. Liparulo

Nicholas J. Liparulo, Manager
Nuclear Safety & Regulatory Activities

/nja

Enclosure

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

020102

E004
1/1

ET-NRC-93-3824
ATTACHMENT A
AP600 RAI RESPONSES
SUBMITTED FEBRUARY 25, 1993

RAI No.	Issue
100.006	Emergency response facilities
410.021	PZR safety valve discharge
410.022	Reference for PZR relief discharge system
410.024	Instrumentation for PZR relief discharge system
410.026	Flooding
410.029	External flooding
410.032	Equipment protection
410.035	Ground water seepage
410.036	Flood protection
410.038	External flooding
410.039	Design criteria
410.041	Waterproofing
410.045	Flooding monitors
410.058	Valve and bonnet design
410.060	Hydrogen bottle explosion
410.082	Line restrictions
420.007	I&C assessment
470.001	Source terms
470.002	Consequence analysis

ATTACHMENT B
AP600 SSAR/PRA REQUESTS FOR ADDITIONAL INFORMATION
STATUS SUMMARY FOR RAI's RETURNED TO NRC

Question No.	Issue	NRC Letter	Westinghouse Transmittal Date
100.006	Emergency response facilities	10/28/92	02/25/93
420.007	I&C assessment	10/28/92	02/25/93
470.001	Source terms	10/28/92	02/25/93
470.002	Consequence analysis	10/28/92	02/25/93
720.057	PRA	10/28/92	12/22/92
720.058	Data files	10/28/92	12/22/92

Question 100.6

Section 13.3 of the SSAR indicates that emergency planning is not within the scope of the AP600 design certification application. Additionally, the SSAR states that communication interfaces between the plant control room and the emergency planning centers discussed in NUREG-0696 are outside the scope of the AP600 design certification application. The staff agrees that emergency planning will be addressed by the utility applicant referencing the AP600 standard design and will significantly depend on plant and site-specific characteristics.

However, the SSAR further states that there are design features, facilities, functions, and equipment necessary for emergency planning that interface with the AP600 design scope. Section 7.5 of the SSAR identifies plant variables that are provided for interface to the emergency planning areas. The staff cannot identify any other references to features, facilities, functions, and equipment necessary for emergency planning in the SSAR.

The Technical Support Center (TSC) is identified in Figure 1.2-25 of the Annex I and II Building General Arrangement Plan (elevation 117' 6") as the Main TSC Operations Area (40406). The TSC is designated as an onsite facility located adjacent to and within two-minutes walking time of the control room. The design provides for a TSC; however, no information is provided regarding the availability of specific plant data, plant records, or size.

The staff concludes that the design considerations for emergency planning specified in the AP600 SSAR are not sufficient because the facilities and equipment necessary to support operations in the TSC are not specified as recommended in Supplement 1 to NUREG-0737 and NUREG-0696. In addition, the design should include an Operations Support Center (OSC) that should be located onsite with communication links to the control room.

Therefore, provide a description of design considerations for onsite emergency response facilities (such as the Emergency Operations Facility, TSC, OSC, and Onsite Decontamination Facility) as part of the AP600 design. The emergency preparedness regulations and supporting documents identified below contain the requirements and guidance for these facilities and functions. Address in detail the design of the facilities listed below by (1) providing a description of the pertinent design considerations that would enable these facilities to meet the referenced requirements or guidance, (2) citing the location of these descriptions in current or projected design documents, or (3) describing or identifying how the equivalent function is contained in the design considerations of another facility.

Facility	References
Emergency Operations Facility	10 CFR 50.47(b)(8) 10 CFR 50, Appendix E, IV.E.8 NUREG-0654, Paragraph II.H.2 NUREG-0696, Paragraph 1.3 NUREG-0737, Supplement 1, Paragraph 8.4
Technical Support Center	10 CFR 50.47(b)(8) 10 CFR 50, Appendix E, IV.E.8

	NUREG-0654, Paragraph II.H.1 NUREG-0696, Paragraph 1.3.1 NUREG-0737, Supplement 1, Paragraph 8.2
Operations Support Center	NUREG-0654, Paragraph II.H.9 NUREG-0696, Paragraph 1.3.2 NUREG-0737, Supplement 1, Paragraph 8.3
Onsite Decontamination Facility	10 CFR 50, Appendix E, Paragraph IV.E.3 10 CFR 50.46(b)(8)

Response:

The mission and major tasks of the TSC and the OSC are provided in SSAR Subsections 18.8.2.1.1.2.5 and 18.8.2.1.1.2.6, respectively. The crisis management Information system description and scope are described in SSAR Subsection 18.9.6. A discussion of the TSC design criteria is provided in SSAR Subsection 18.11.2. The exact plant data needed in the TSC and the communications and the plant records will be determined by performing the function-based task analysis for the TSC and by developing the decision sets model for the AP600 emergency management function.

Regulatory conformance with NUREG-0737 and NUREG-0696 is described in SSAR Appendix 1A. The operations support center location, described in the response to Q620.1, has communication links to the main control room. Plant information available to the MCR staff will be accessible to the TSC staff. Necessary plant records will be accessible from the TSC.

Communications needs between each of the emergency management functions, onsite and offsite, will be accommodated. Communications and shared data with the EOF will be determined using the Chapter 18 design process. The remainder of the EOF design is the responsibility of the combined license applicant. The onsite decontamination facility is located in the health physics area on elevation 100' in the annex II building.

SSAR Revision: NONE

Question 410.21

Section 5.4.11 of the SSAR states that the safety valves connected to the top of the pressurizer provide for overpressure protection of the reactor coolant system. The discharge of the safety valves is connected through a rupture disk to containment atmosphere. The discharge is directed away from any safety related equipment, structures, or supports that could be damaged to the extent that emergency plant shutdown is prevented by such a discharge.

Identify the worse case steam/water discharge and provide an analysis to determine the distance that the discharge jet may cause impingement damage. Provide a diagram of the proximity of the safety valves to show all the equipment, components, structures, or supports within this distance.

Response:

The discharge of the safety valves is connected through a rupture disk to containment atmosphere. The discharge is hard piped away from the safety-related ADS valves on the pressurizer in such a way that no safety-related equipment, structures, or supports are within the distance of the jet spray that would result from the maximum safety valve discharge. The effective distance for the jet loading is 10 pipe diameters. This is the same as the effective distance for jets that result from postulated pipe ruptures as described in SSAR Subsection 3.6.1.1., paragraph O.

SSAR Revision: NONE

Question 410.22

Section 5.4.11.2 of the SSAR states that the piping and instrumentation diagram (P&ID) for the connection between the automatic depressurization system valves and the in-containment refueling water storage tank is shown in Figure 6.3-1. Figure 6.3.1 is the P&ID for the passive core cooling system. It does not appear to contain the above mentioned information. Provide the appropriate reference for the pressurizer relief discharge system.

Response:

Portions of the pressurizer relief discharge system are shown in the reactor coolant system P&ID (Figure 5.1-5, sheet 2) and the passive core cooling system P&ID (Figure 6.3-1, sheet 2).

Section 5.4.11.2 , second paragraph, will be revised as follows:

SSAR Revision:

The discharge from each of two groups of automatic depressurization system valves, including a first-stage valve in each group, is connected to a separate sparger below the water level in the in-containment refueling water storage tank. The piping and instrumentation diagram for the connection between the automatic depressurization system valves and the in-containment refueling water storage tank is shown in Figures 5.1-5 and -6. ~~The piping and instrumentation diagram for the connection between the automatic depressurization system valves and the in-containment refueling water storage tank is shown in Figure 6.3-1.~~

Question 410.24

Section 5.4.11.4 of the SSAR, entitled "Instrumentation Requirements", states that the instrumentation for the safety valve discharge pipe, containment, and in-containment refueling water storage tank are discussed in Sections 5.4.9, 6.2, and 6.3, respectively. It is not clear where the specific information regarding the instrumentation requirements in the pressurizer relief discharge system is located in the referenced sections. Provide this specific information or provide a more specific reference for the information in the SSAR.

Response:

The temperature instrumentation in the safety valve discharge pipe is discussed in the last paragraph in SSAR Subsection 5.4.9.2.

SSAR Revision: NONE

Question 410.26

Section 3.4.1.2.2.1 of the SSAR states that reverse flow from the containment sump to the two PXS compartments and the CVCS compartment is prevented by redundant "backflow preventers" in each of the three compartment drain lines. Provide design information on these components, including leakage characteristics. Discuss the likelihood of failure of these components and the subsequent flooding effect.

Response:

See the response to Q410.1.

SSAR Revision: NONE

Question 410.29

Identify potential sources of external flooding from components which are within the AP600 design scope (Section 3.4.1).

Response:

This Request for Additional Information is identical to Q410.2. Please see the response to Q410.2.

SSAR Revision: NONE

Question 410.32

How will safety-related equipment and equipment important-to-safety be protected from failures of structures, systems, and components that are not within the AP600 design scope (Section 3.4.1)?

Response:

See the response to Q410.4.

SSAR Revision: NONE

Question 410.35

Identify safety-related equipment and equipment important-to-safety that are subject to groundwater seepage, and discuss how this will be controlled (Section 3.4.1).

Response:

The AP600 achieves and maintains safe shutdown following a flooding event using only safety-related equipment. There is no safety-related equipment subject to groundwater seepage because such equipment, if located below the groundwater level, is located in seismic Category I structures, which are protected against flooding by waterproofing membranes and waterstops as described in SSAR Subsection 3.4.1.1.

SSAR Response: NONE

Question 410.36

Identify whether flood protection depends upon the use of a dewatering and drainage system. If so, provide details on the system (Section 3.4.1).

Response:

Flood protection of the AP600 does not depend upon the use of a dewatering and drainage system. The AP600 site interface specifies that flooding shall not exceed grade. Certain features of the flood protection are site-specific. As stated in SSAR Subsection 3.4.1.3, the need for a permanent dewatering system is site-specific and is defined by the combined license applicant. A drainage system is, likewise, site-specific.

SSAR Revision: NONE

Question 410.38

How are external penetrations that are below plant grade protected from external flooding (Section 3.4.1)?

Response:

The AP600 minimizes the number of penetrations through the exterior wall below grade. Those few penetrations located below the maximum flood level (elevation 100') will be watertight. Any process piping penetrating through the exterior wall below grade either will be embedded in the wall or will be welded to a steel sleeve embedded in the wall.

SSAR Revision: NONE

Question 410.39

Discuss design criteria for doors, walls, and penetrations used to provide internal and external flood protection (Section 3.4.1).

Response:

There are no watertight doors in the AP600 used for internal or external flood protection.

Exterior walls are designed for hydrostatic loads up to grade (elevation 100') as discussed in SSAR Subsection 3.4.1.2.1. Penetrations through these walls are discussed in the response to Q410.38.

Interior walls are designed for hydrostatic loads up to the maximum flood level in a given area. The AP600 minimizes the number of penetrations through these walls below the flood level. Those few penetrations through flood protection walls that are below the maximum flood level are watertight. Any process piping penetrating below the maximum flood level either will be embedded in the wall or will be welded to a steel sleeve embedded in the wall.

SSAR Revision: NONE

Question 410.41

Provide design information on waterproofing membranes, waterstops, watertight doors, and other protective features (Section 3.4.1).

Response:

Specific vendor materials for waterproofing membranes and waterstops have not been selected. Performance criteria for waterproofing membranes and waterstops are described in SSAR Subsection 3.4.1.1. There are no watertight doors. The response to Q410.39 provides information on the interior walls and penetrations therein. Curbs are also provided, as discussed in SSAR Subsection 3.4.1.2.2.1.

SSAR Revision: NONE

Question 410.45

Are monitors which detect flooding in areas containing safety-related equipment and equipment important-to-safety related (Section 3.4.1)?

Response:

AP600 relies only on safety-related equipment for safe shutdown following a flooding event. As noted in SSAR Subsection 3.4.1.2.2.1, containment flooding is detected by the containment sump level monitoring system and the containment flood-up level instrumentation. Both of these level detection systems are safety-related.

Potential flooding in the auxiliary building is detected by non-safety-related sump level sensors. There is a sensor for each of the four sumps on level 1 of the auxiliary building. Each sensor produces an alarm in the main control room when the sump water level reaches the setpoint for starting the standby pump. The alarm alerts the operator to a possible malfunction of the lead pump or an unusually high sump influent rate, which indicates a potential for flooding. Safety-related instrumentation is not required because postulated flooding is controlled so that it cannot affect safe shutdown equipment. Also see SSAR Subsection 3.4.1.2.2.2. Outside the containment the flooding detection instrumentation is not important to safety.

SSAR Revision: NONE

Question 410.58

Provide design information regarding the retaining ring and yoke used in the valve bonnets of pressure seal, bonnet-type valves (Section 3.5.1.1).

Response:

As discussed in SSAR Subsection 3.5.1.1.2.1, the bonnets of pressure seal bonnet-type valves are constructed in accordance with ASME Code, Section III (1989 Edition with 1989 Addenda). Although specific hardware or a valve vendor has not been selected, valve design shall comply with the general design requirements of the appropriate Articles NB/NC/ND-3000 and NB/NC/ND-3500 of Section III. Specific design information regarding the retaining ring and yoke used in the valve is vendor-specific and proprietary.

The bonnet retaining ring holds the bonnet in place and effects a seal by compressing the bonnet gasket between the retaining ring and the bonnet. Typically, the bonnet retaining ring that holds the pressure seal bonnet in the valve body is considered as a pressure-retaining part (like the valve body, bonnet, and disk) and therefore is designed to meet the Code allowable stresses.

The yoke is attached to the valve body by either a clamp or by bolts. The yoke and the yoke attachment are not considered as a pressure-retaining part. The design of the yoke and the attachment are governed by the design specification requirements and are required to meet the maximum allowable stresses (for each service limit) allowed by the Code for the material used.

SSAR Revision: NONE

Question 410.60

Provide analysis to demonstrate that the contents of one hydrogen bottle will not lead to an explosion. Show how hydrogen release is limited to one bottle should a supply line fail (Section 3.5.1.1).

Response:

Hydrogen is supplied to the AP600 chemical and volume control system (CVS) inside containment from a single 550 scf hydrogen bottle located in the plant gases storage tank area. The quantity that could be released inside containment in the event of a failure of the hydrogen supply line is limited to the contents of a single bottle. The concentration of hydrogen within the CVS compartment, as a result of a failure of the hydrogen supply line, was evaluated based on the calculated free volume of the CVS compartment. The CVS compartment is well vented to the 107-foot level of the containment.

Based on the free volume of the CVS compartment (12712.33 ft^3) and the contents of a hydrogen bottle, the volume percent of hydrogen that could build up as a result of failure of the hydrogen supply (in the CVS compartment) is approximately 4.3 percent, assuming uniform mixing. Therefore, a release of hydrogen from the CVS would not lead to an explosion since the volume percent of hydrogen is less than the detonation limits in NUREG/CR-2017.

The concentration of hydrogen in building areas outside containment was also considered. Based on a preliminary routing of the hydrogen supply line from the hydrogen storage area to the CVS, the maximum volume percent of hydrogen that could build up as a result of a break in the hydrogen supply line outside containment is approximately 4.4 percent. This was evaluated assuming the break occurs within the most limiting building area and also assuming uniform mixing. The area with the most limiting building volume is the valve / piping penetration room in the auxiliary building on elevation 100'-0". The volume of this room is approximately 12420 ft^3 (See SSAR Figure 1.2-7).

Since the volume percent of hydrogen is less than the detonation limits outlined in NUREG/CR-2017, a failure of the CVS hydrogen supply outside containment would not lead to an explosion.

SSAR Revision: NONE

Question 410.82

Identify all line restrictions in high-energy lines that impact on the calculations of thrust and jet impingement forces, and provide a sample calculation to demonstrate how these restrictions were addressed in these calculations (Section 3.6.1).

Response:

SSAR Appendix 3E, included in the response to Q210.6, identifies the high-energy lines in the nuclear island with a diameter larger than one inch that do not satisfy the leak-before-break criteria. These lines will be evaluated to the pipe rupture criteria provided in SSAR Subsection 3.6.2. None of the high-energy lines outside the containment contain line restrictions that would affect the calculations of jet thrust and jet impingement forces.

SSAR Revision: NONE

Question 420.7

The AP600 I&C system uses a microprocessor-based distributed digital system to perform plant protection and safety monitoring as well as for plant control functions. The use of digital computer technology in protection and control systems raises a concern that the software and hardware for these computer systems could be vulnerable to design and programming errors that could lead to safety-significant common-mode failures. Provide detailed information to address the following concerns regarding the quality and diversity of the I&C system design.

a. Assessment Of Diversity

(1) Assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed. The staff considers software design errors to be credible common-mode failures that must be specifically included in the evaluation. An acceptable method of performing analyses is described in NUREG-0493. Other methods proposed will be reviewed on a case-by-case basis.

(2) In performing the assessment of defense-in-depth and diversity of the I&C system requested in (1) above, each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report should be analyzed. Demonstrate adequate diversity within the design for each of these events.

(3) If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subjected to the same common-mode failure, should be required to perform either the same function or a different safety function that provides adequate protection. The diverse or different safety function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. Diverse digital or non-digital systems are considered to be acceptable means. Manual actions from the control room are acceptable if time and information are available to the operators. The amount and types of diversity may vary among designs and will be evaluated on a case-by-case basis. How does the AP600 design address this position?

(4) In the draft Commission paper, "Design Certification and Licensing Policy Issues Pertaining to Passive and Evolutionary Advanced Light Water Reactors," dated July 6, 1992, the staff concluded that a set of safety-grade displays and controls, independent of the computer system(s) and located in the main control room, should be provided for system-level actuation and monitoring of criteria safety functions and parameters. The staff further stated that the displays and controls should be provided for those system-level actuations for critical safety functions and parameters that are required by control room operators to place the reactor plant in a hot shutdown condition. The displays and controls should be conventionally hardwired in the system architecture to the lowest level practicable. The staff stated that each set of equipment required will be evaluated individually.

The hardwired system-level controls and displays provide the plant operators with unambiguous information and control capabilities. These hardwired controls and displays are required to be in the

main control room to enable the operators to expeditiously mitigate the effects of the postulated common-mode failure of the digital I&C system. The control room would be the center of activities to safely cope with the event which could also involve the initiation and implementation of the plant emergency plan.

After a review of the comments received from the ACRS, EPRI, and the industry, the staff has modified its position on this matter. The staff is considering allowing more flexibility in implementing the independent set of displays and controls. The amount of flexibility would depend on the specific equipment and design features of the I&C system and would be evaluated individually with each vendor. This would permit using digital equipment that is not affected by the identified common-mode failures and reduce the complexity of the design. The staff is considering allowing simple digital equipment in lieu of only analog equipment in such a system. Safety parameter displays may include dedicated digital components. The system-level actuation controls that are "hardwired" to the lowest level practicable in the I&C architecture may use dedicated and diverse digital equipment.

The staff is aware that Westinghouse has proposed a diverse actuation system (DAS) which is a non-safety-related digital system to protect against common-mode failures in the protection system. However, Westinghouse has not provided detailed information to demonstrate the quality of the DAS design that includes the hardware and software verification and validation process. Provide information to justify the safety qualification of this design.

(5) Westinghouse submitted fault tree analyses for the protection system in Section C-20 of the PRA submittal. Section 3.5.4.3 of the EPRI Requirements Document for passive plants states that a failure mode and effects analysis (FMEA) can also assist in the identification and elimination of common-mode failures and may suggest areas where improvements in reliability can be achieved. RG 1.70, "Standard Format and Content of Safety Analysis Report for Nuclear Power Plants," states that an applicant should submit failure mode and effects analyses for the protection systems and components. Supplement the fault tree analyses with additional FMEA, as specified in IEEE 352, which is required by IEEE 603, or provide a method for obtaining FMEA-type information from the PRA and other sources of information.

b. Engineering Activities in Software and Hardware Development

Because the hardware and software design of the AP600 I&C systems have not been finalized, the staff will use the two-part approach stated in SECY-92-053, "Use of Design Acceptance Criteria (DAC). During 10 CFR Part 52 Design Certification Reviews," in the review of the AP600 I&C system. The first part of this approach involves a detailed functional review at the level of design provided in the safety analysis report to ensure that the design meets the Commission's requirements related to postulated single failures, appropriate signal isolation, and other aspects of the staff's review that are typical of a corresponding analog system review. This review will establish the detailed functional requirements for the I&C system. The second part of this approach (the DAC) will address the adequacy of the digital control system implementation with respect to the functional system requirements. This will rely upon a formal design implementation process with phased inspection, test, analysis and acceptance criteria (ITAAC) for design development.

Westinghouse submitted a pilot ITAAC program for the man-machine interface system, but it does not contain computer hardware and software development aspects. Address the engineering activities throughout the software life-cycle ITAAC. A software life-cycle ITAAC should include the following stages:

- planning
- requirements
- design
- implementation
- integration
- validation
- installation
- operation and maintenance

Also, provide information regarding the previous development activities related to the nuclear plant protection system hardware and software.

c. Design Implementation

The staff's consideration of the design acceptance criteria (DAC) also includes the design implementation phase of the advanced light water reactor. Westinghouse's DAC and ITAAC program should include steps that will allow the NRC to verify conformance with the requirement through the life-cycle phases of design, manufacture, installation, operation, maintenance, and modification of the I&C system. Provide such information in the DAC and ITAAC program for the AP600 I&C system.

d. Classification of the I&C System

As discussed in SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors," the staff is continuing to develop safety classification criteria for the I&C systems in the ALWR designs. The staff will consider the positions being developed by the international technical community in the draft International Electrotechnical Commission standard and EPRI's position paper for passive system classification, as well as the information provided in the AP600 SSAR in the consideration of the necessary classification criteria.

The AP600 submittal includes probabilistic risk assessments for the protection and safety monitoring system, the plant control system, the diverse actuation system, and many other plant systems (total - 21 systems). The traditional Class IE I&C and non-Class IE I&C classifications used to describe systems important-to-safety is too limited to properly account for the significant contribution to safety from traditional non-IE systems, as evidenced in the PRA results. The staff is considering a graded approach based on system importance-to-safety to establish specific requirements of active non-safety systems to ensure their capability and availability. This graded approach will require an applicant to submit the evaluations and analyses of those non-safety systems to help verify that the capability and availability of each system is commensurate with its safety importance.

How does the AP600 I&C design address this issue? The staff will evaluate Westinghouse's methodology and criteria used to establish the relative importance of those non-safety systems, and will evaluate the applicant's proposed system requirements during its review of the AP600 design.

Response:

a. 1. A defense-in-depth analysis of the AP600 instrumentation and control systems, as described in NUREG-0493, is being performed. (See the response to Q420.5)

2. Common-mode failures, including mechanical and software related, are beyond design basis events and, as such, are evaluated using a probabilistic rather than a deterministic method. Consistent with this basis, the AP600 SSAR does not address common-mode failures as a "single failure assumption" for each of the design basis events analyzed and reported in Chapter 15 of the SSAR.

The AP600 protection and safety monitoring system (PMS) includes design features to avoid occurrence of common-mode failures such as equipment qualification, the application of fail-safe design principles, maintenance capabilities, the system functional tester, and the verification and validation program. The diverse actuation system (DAS) provides diverse protection for low-probability common-mode failures of the protection and safety monitoring system.

3. The AP600 design includes a diverse actuation system. The DAS is a non-safety-related system that provides a diverse backup to the protection and safety monitoring system. The DAS includes diverse automatic and manual actuations along with a set of diverse indications. The specific functions performed by the DAS are selected based on the PRA evaluation. The DAS functional requirements are based on an assessment of the protection system instrumentation common-mode failure probabilities combined with the event probability. A description of the DAS, including identification of the automatic and manual functions and the indications provided by the DAS, is included in Subsection 7.7.1.11 of the Proprietary Volumes of the AP600 Standard Safety Analysis Report.

4. Safety-related, qualified displays and dedicated system-level controls are provided in the protection and safety monitoring system, which are independent of the digital subsystems that perform the automatic reactor trip and engineered safeguards features actuations.

The dedicated manual reactor trip controls are wired directly to the reactor trip switchgear, bypassing the integrated protection cabinets. Control devices that provide dedicated manual system-level safeguards actuations are hardwired directly to the engineered safeguards features actuation cabinets, which is the lowest appropriate level in the PMS architecture for systems-level actuations. Because these controls are wired directly to the engineered safeguards features actuation cabinets, the integrated protection cabinets are bypassed. Manual control of individual engineered safeguards features components, such as valves, is provided by using the safety-related soft control devices and associated multiplexer cabinets, which bypass the engineered safeguards features actuation cabinets and the integrated protection cabinets.

The safety-related displays, provided by the qualified display processing system within the AP600 protection and safety monitoring system, obtain signals from both independent sensors and sensors that are shared with the reactor trip and engineered safeguards features actuation functions. For the sensors that are shared, independent signal conditioners and independent subsystems within the integrated protection cabinets, dedicated to communications tasks, are used so that signals for the safety-related displays bypass the digital subsystems used to perform reactor trip and engineered safeguards features actuation calculations. The display devices used for the safety-related displays are qualified.

The diverse actuation system is a non-safety-related, class D system. This is consistent with the reliability level assigned to this system in the probabilistic risk assessment. - see the response to Q440.20.

The diverse actuation system displays and controls are in the main control room. The DAS manual actuations use dedicated, hard-wired control devices. The diverse actuation system is described in SSAR Subsection 7.7.11 and in Figure 7.2-1, Sheet 29.

The diverse actuation system will be included in the hardware and software verification and validation process to the same level as other defense-in-depth instrumentation and control systems, such as portions of the plant control system and data display and processing system. The PRA demonstrates that the reliability of a nonredundant diverse actuation system is adequate to meet the reliability goals of the AP600. The diverse actuation system is designed with two identical subsystems, with 2 out of 2 voting logic used to actuate reactor trip and safeguards actuations.

5. This item is addressed by the response to Q420.2. Per Regulatory Guide 1.70 and IEEE 352, an FMEA for the AP600 protection system will be provided.

b. The AP600 hardware and software design, verification, and validation program, which addresses software development activities throughout the software life cycle, is described in WCAP-13383 (Reference 420.7-1) which was submitted to the NRC as a supporting document for the AP600 SSAR. Under this program, Westinghouse is responsible for implementing the planning, requirements, design, implementation, integration, validation, and installation stages of the software life cycle. The combined license holder is responsible for implementing the operation and maintenance stages based on information generated in the preceding stages.

   WCAP-9739 (Reference 470.7-2) reports on the verification and validation program performed on the prototype integrated protection system design. WCAP-9153 (Reference 470.7-3) describes the design principles for the hardware and software and the verification and validation program for the prototype integrated protection system. This verification and validation program covers the hardware and software and the integrated system. The AP600 instrumentation and control architecture is based on the hardware and software verified and validated by this program.

   WCAP-10170 (Reference 470.7-4) reports on the verification and validation process used for the hardware, software, systems integration, and human factors aspects of the Westinghouse safety parameter display system.

Seven supplements to this WCAP were issued through 1989 to report on the results of the process for several currently operating plants.

c. Westinghouse submitted the "AP600 Tier 1 Material, Plant Description and Inspections, Tests, Analysis, and Acceptance Criteria" (Reference 470.7-5) on December 15, 1992. Reference 470.7-5 includes system ITAAC for the following instrumentation and control systems:

- Protection and Safety Monitoring System
- Diverse Actuation System
- Data Display and Processing System
- Incore Instrumentation System
- Plant Control System
- Radiation Monitoring System

Reference 470.7-5 also includes a design ITAAC for human factors engineering.

SSAR Chapter 7 and WCAP-13383 (Reference 470.7-1) address software development activities throughout the life-cycle phases of design, manufacture, installation, operation, maintenance, and modification of the instrumentation and control systems.

d. The following non-safety instrumentation and control systems perform defense-in-depth functions:

- Diverse Actuation System
- Data Display and Processing System
- Plant Control System
- Radiation Monitoring System

Section H of Reference 470.7-6 (attached) defines an approach for the design, construction, and operability of equipment that provides the defense-in-depth functions.

Westinghouse is also participating in the industry effort to develop a graded approach for software development.

References:

470.7-1 Birsa, J. J., "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report," WCAP-13383 (Proprietary), WCAP-13392 (Non-proprietary), May 1992.

470.7-2 Cook, B. M., et. al., "Summary of Integrated Protection System Validation and Verification Program," WCAP-9739 (Proprietary), July 1980.

470.7-3 Donnelly, J. A., et. al., "414 Integrated Protection System Prototype Verification Program," WCAP-9153 (Proprietary), August 1977.

470.7-4 Gallagher, J. M., "Emergency Response Facilities Design and Verification and Validation Process," WCAP-10170, April 1982.

470.7-5 Westinghouse letter ET-NRC-92-3779, "AP600 Tier 1 Material, Plant Description and Inspections, Tests Analysis, and Acceptance Criteria," from N. J. Liparulo to Dr. Thomas Murley, December 15, 1992.

470.7-6 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.

SSAR Revision: NONE

H. REGULATORY TREATMENT OF NON-SAFETY SYSTEMS

AP600 POSITION

The basic design approach that Westinghouse and the Utilities (through the URD) have selected for the passive safety features of the AP600 is to meet the existing NRC Regulations and Safety Policy without relying on active systems. The AP600 nonsafety-related active systems are designed to provide reliable support for normal plant operations and to provide defense-in-depth to minimize unnecessary challenges to the safety-related passive systems. These active systems are designed for more probable component and system failures. The systems include reliable, proven equipment and component designs. These active systems are capable of being powered by the nonsafety-related diesel-generators. The active nonsafety-related systems have automatic actuation and controls that are separate from those of the safety-related systems. The active nonsafety-related systems are not required to mitigate accidents.

The capability of the AP600 passive safety-related systems will be demonstrated through extensive safety analysis and testing to satisfy the NRC and the utilities/investors. The design of these systems is carried out in a systematic manner including the use of system specification documents which contain the system design criteria, system and equipment design requirements, and operation and in-service testing requirements. The reliability and availability of the passive safety-related systems is assured through a systematic design process, a conservative design (including redundancy, diversity, and separation), quality assurance, the ITAAC program, pre-operational and in-service testing, Technical Specifications, and the AP600 and Owner Reliability Assurance Programs (DRAP & ORAP).

The reliability and availability of the nonsafety-related systems will be controlled in a manner consistent with their safety importance. The design process for these systems is similar to that used for the passive safety-related systems although there are no safety-related requirements. The equipment used to perform these defense in depth functions are assigned to a quality level that is equivalent to the Reg Guide 1.26 Group D. The reliability and availability of these nonsafety-related systems is controlled through a systematic design process, quality assurance, the ITAAC program, redundancy, pre-operational and in-service testing, the DRAP and the ORAP.

We strongly disagree with the proposed NRC position because it presumes a design with reliance on nonsafety-related systems to meet NRC Regulations and Safety Policy. The AP600 / URD design approach represents an significant improvement in both public safety and in commercial attractiveness. Accordingly we recommend that the proposed NRC position be revised to accommodate the AP600 / URD approach.

RESPONSE TO SPECIFIC NRC STAFF CONCERNS

In its draft position paper, the NRC staff has identified several specific issues regarding the use of passive systems. Each of these should be resolvable during the detailed review of the AP600 design described in the SSAR and the PRA.

1) Reliability of Passive Safety Systems

The NRC staff has expressed concerns about the reliability of the passive safety-related systems including effects of low driving heads on the operability of the CMTs / IRWSTs / PRHR HXs. They also have concerns about the basic thermal-hydraulic performance of the gravity injection systems and the ADS.

Westinghouse is committed to demonstrating the passive systems are both capable and reliable. We have developed an extensive test program such that, along with the SSAR and PRA, we will demonstrate to both the NRC and the utilities that these passive systems meet the NRC Regulations and Safety Policy. Some of the original tests have been expanded and others have been added to better address NRC concerns, including the addition of a full height/full pressure integral systems test. The remaining tests and analyses provide the basis for confirming the capability and reliability of the passive safety-related systems.

2) Safe Shutdown Condition

The NRC staff expresses their belief that, by their nature, the passive systems cannot achieve cold shutdown conditions by themselves and therefore, the nonsafety-related systems may be required to achieve safe shutdown.

The AP600 design can achieve a safe shutdown condition using only passive systems that are automatically initiated and can be maintained indefinitely without operator actions. This provides a capability which improves upon current LWR long-term residual heat removal capabilities. These improvements include the automatic actuation of a closed loop, full pressure RHR system that only requires the opening of one of two fail-open air operated valves. As the passive RHR HX removes heat the RCS temperature will be automatically reduced, reaching 420 F in 36 hours and 400 F in 72 hours. The RCS pressure will correspondingly decrease to about 310 psia at 36 hours and 250 psia in 72 hours. These reduced pressures significantly reduce the RCS pipe stresses and therefore the chance of a leak or LOCA developing during such a shutdown condition. This shutdown condition can be maintained for an indefinite time by the passive safety-related systems without the operation of the nonsafety-related systems.

Because of the AP600 safe shutdown capability, there should be no concern over achieving and maintaining a safe shutdown condition even though it is not a "cold" shutdown. This capability does not rely on the nonsafety-related systems. See SSAR section 7.4 for additional discussion of the AP600 safe shutdown condition.

3) Long Term Shutdown Operation

The NRC Staff has expressed concern that after 72 hours the licensee may need to rely on active systems to mitigate an accident, thereby increasing the need to rely on nonsafety-related systems.

The AP600 is designed so that the passive safety-related systems are capable of protecting the public without operator action for 72 hours. (Note that existing plants often require operator action within 1/2 hour or less). By providing this capability the AP600 has achieved a major improvement in safety. It is essential to note that beyond 72 hours, the AP600 passive safety-related systems continue to maintain safe shutdown conditions, providing core cooling and containment cooling without any additional actions. The AP600 passive safety-related systems are also designed to maintain reduced containment pressures and to provide control room habitability and plant monitoring capability beyond 72 hours with some limited operator actions. These operator actions can be performed using readily available, pre-identified, offsite equipment and designed in, safety-related connections in the plant. Hence it is not necessary to rely on the nonsafety-related systems to maintain a safe shutdown. The specific operator actions required after 72 hours are outlined in SSAR section 1.9.5.4.

4) Passive Safety System Capabilities During Shutdown

The NRC Staff notes that the passive safety-related systems will likely be isolated during shutdown and, therefore, active systems may be the only available means of removing heat and making up core coolant. They consider, therefore, that the nonsafety-related systems are particularly important in plant shutdown.

With regard to shutdown cooling capability, the AP600 SSAR contains Technical Specifications (SSAR section 16.1) that require passive safety-related core cooling availability during all shutdown conditions. The safety-related systems are required by Technical Specifications to be available down to mid-loop conditions. Containment integrity is required by Technical Specification down to and including mid-loop operation. During mid-loop conditions the IRWST and ADS are required to be available. As an example, attachment 1 is the Technical Specification for the PRHR HX from the AP600 SSAR.

During flooded refueling conditions, the inventory of water in the refueling cavity provides the passive core cooling capability. This water inventory is sufficient to prevent core uncovery and damage for at least 72 hours without operator action even with the containment open. Beyond 72 hours, the AP600 has provisions for readily connecting portable equipment to continue operation of the passive safety-related features for an indefinite time. When containment integrity can be reestablished in several hours, then the passive systems would be able to cool the core indefinitely without water makeup. See SSAR section 6.3.3.4 for additional discussion of passive system capability during plant shutdown conditions.

The AP600 PRA also provides insights to the importance of shutdown events to risk. The calculated core damage frequency for shutdown events is 8.9 E-8/yr which is lower than the frequency for at-power events, (3.3 E-7/yr).

The leading causes of core damage during shutdown are for events occurring at mid-loop. The frequency of mid-loop initiating events is on the order of 1 E-4/yr including the frequency of being in mid-loop and the probability of failure of the normal RHR pumps, CCW pumps, or the SW pumps. The protection for these events is provided solely by the passive safety-related systems, in particular the IRWST injection to the RCS. The only impact that the nonsafety-related systems have on these events is the probability of their failure which could initiate such an event. As such, this is similar to being at power with the nonsafety-related main feedwater providing heat removal, except that mid-loop only occurs for a very limited period of time. Also refer to item 5 for additional discussion on the measures that have been incorporated into the AP600 to control the reliability of the nonsafety-related systems.

5) Use of Nonsafety-Related Systems as the First Level of Defense

The NRC staff notes that some systems which have been traditionally safety grade, e.g., emergency ac power and auxiliary feedwater, are nonsafety-related systems in the passive plants. The NRC staff expresses concern that certain transients, such as total loss of feedwater or loss of ac which are very demanding events for operators in existing plants may, therefore, be more likely and there will be a greater burden on the plant operators.

Several traditional safety-related systems are nonsafety-related in the AP600 design; however, this does not result in greater operator burden or a less safe design. On the contrary, the AP600 design should significantly reduce the operator burden and stress during these events.

The AP600 passive systems automatically accommodate these events without requiring operator action. Further, the AP600 has a reliable startup feedwater system (SFWS) and ac emergency power system to minimize the probability of such events occurring. The AP600 specifies the SFWS pumps to be AP600 quality level D, which is equivalent to NRC Regulatory Guide 1.26 quality group D. The availability of these pumps is controlled by the ORAP. The AP600 SSAR spells out the DRAP requirements which include the functions required, the modes of plant operation where the system should be available and when planned maintenance should be performed, the test frequency (via reference to the AP600 PRA), and the remedial actions in case of equipment unavailability. As an example, Attachment 2 (Table 16.2-2 from the AP600 SSAR) shows the DRAP requirements for the AP600 SFWS. Attachment 3, from the AP600 PRA section C8, shows the PRA test frequency for the SFWS.

The AP600 also includes multiple levels of defense provided by the passive safety-related systems themselves. The PRA was used to determine whether there were sufficient levels of defense because it accounts for initiating event frequency and the reliability of the protection features. For more probable events, the PRA indicates the need for more reliable protection. The PRA also quantifies the passive systems reliabilities including their vulnerability to common mode failures. The AP600 PRA shows that the multiple levels of defense provided by the passive safety-related systems support the NRC safety goal without the use of the nonsafety-related active systems. The nonsafety-related systems provide additional margin to core damage.

An example of the multiple levels of defense within the passive systems is the PRHR HX and passive feed and bleed cooling. The passive residual heat removal heat exchanger is the safety-related feature that removes decay heat during a transient. In case of multiple failures in the PRHR HX, defense in depth is provided by passive safety injection and automatic depressurization (passive feed and bleed). Therefore, since the passive systems provide automatic safety-related protection for such events and since they also provide defense in depth themselves, there is no need to apply additional regulatory requirements or oversight to the nonsafety-related systems.

6) Reliance on Nonsafety-Related Systems in PRA

The NRC staff notes that nonsafety-related equipment may contribute significantly to preventing and mitigating severe accident core damage and to recover the plant after a severe accident. We agree that the AP600 nonsafety-related systems reduce the potential for events leading to core damage. The AP600 PRA sensitivity studies show the contribution of the nonsafety-related systems.

	Core Damage Frequency (per year)	
	AP600	Typical Current Plant
- Base case, all systems	3.3 E -7	~ 1 E -5 to 1 E-4
- Safety systems and DAS	2.6 E -6	~ 1 E -4 to 1 E-3
- Only safety systems	9.0 E -6	~ 1 E -4 to 1 E-3

The AP600 core damage frequencies are taken from the AP600 PRA for internal events at power found in PRA section 8.0. The core damage frequencies for shutdown events and external events are even smaller. In current plants, there are several risk significant nonsafety-related features, including normal pressurizer spray, CVCS auxiliary spray, pressurizer PORV and diverse I&C actuation for ATWT. The RCS depressurization equipment is most important for the CDF since this function must be performed to be able to mitigate a SGTR. Also note that in current plants such nonsafety-related features credited in the PRA do not typically have availability controls such as those proposed for the AP600.

The AP600 is less sensitive to the availability of the nonsafety-related systems than for current plants. The AP600 fully complies with the NRC requirement that equipment which is important to prevent and mitigate severe accidents need not be safety grade but should be designed for the service and environment under which it is desired to function. As a result there is not a need to impose additional design requirements or to extend formal regulatory oversight to such systems and equipment. Additionally, the AP600 has an extremely robust containment which along with the associated passive containment cooling systems, provides a markedly increased level of public safety even in the event of severe accident.

The AP600 is designed to achieve low risk of severe accidents, well within the NRC Safety Policy goals, without relying on nonsafety-related systems. Therefore, it is appropriate to treat these systems as nonsafety-related and to not require additional licensing requirements.

7) Verification of Nonsafety-Related System Performance

The staff suggests that the SSAR should contain safety analysis that verifies that the nonsafety-related active systems can not prevent the operation of the passive safety-related systems.

The previous items have pointed out the nonsafety-related active systems are not required; to mitigate accidents, to maintain safe shutdown in the short or long term, or to meet the NRC safety goals. Therefore their ability to prevent the passive safety-related systems from actuating should be performed in design calculations, not in safety analysis contained in the SSAR. We disagree with the approach set forth by the staff in their draft policy paper.

RECOMMENDATIONS

We recommend that the draft NRC position on the treatment of nonsafety-related systems in passive plants be modified to accommodate the AP600 / ALWR design approach. This design approach is to design and verify the passive safety-related systems to meet the NRC Regulation and Safety Policy without reliance on the nonsafety-related active systems.

This design approach is an essential element behind the advantages of the AP600, providing significant improvements in public safety and at the same time providing significant improvements in plant operations and economics. The specific methods of treating the AP600 nonsafety-related systems are identified in the AP600 SSAR. We recommend that the NRC staff review these methods in conjunction with the ALWR URD requirements, as an example of implementing the URD, to establish agreement on both the AP600 design and on the URD requirements.

Question 470.1

Westinghouse has proposed a new reactor accident source term in the SSAR to be used in evaluating the radiological consequences of design basis accidents for the AP600 design. The SSAR references EPRI's "Passive ALWR Source Term" paper, dated February 1991, that was submitted on the EPRI docket (Project No. 669) to provide technical justification for EPRI's physically-based source term proposed in Chapter 5 of Volume III of the EPRI ALWR Utility Requirements Document. In addition to the EPRI document, review NUREG-1465, "Accident Source Terms for Light-Water Nuclear Power Plants," that was issued for public comment in June 1992, and provide the following information:

a. List any deviations from the source term guidelines provided in NUREG-1465. Each deviation should be supported by appropriate technical justification.

b. Describe the assumptions and parameters used in the assessment of the offsite and control room radiological consequences due to design basis accidents (DBAs) and corresponding technical justification for each assumption and parameter used.

c. Describe the fission product transport models and fission product removal mechanisms within the containment.

d. Describe how the post-LOCA pH of the water in the in-containment refueling water storage tank will be controlled.

e. Provide the computer input and output sheets showing computed offsite and control room doses.

f. Provide sample dose calculations for primary nuclides in each chemical species nuclide group to verify the computer outputs.

g. Provide the accident dose calculation code(s), along with the user's manual, on IBM PS-2 compatible 3.5" computer disks.

Response:

a. The justification for the source term model used for the AP600 LOCA dose analysis is provided in DOE/ID-10321, "Passive ALWR Source Term," prepared by EPRI's Advanced Reactor Severe Accident Program Source Term Group, February 1991.

b. The assumptions and parameters used in the LOCA dose analysis (SSAR Subsection 15.6.5.3) are defined in Table 15.6.5-2. Many of the assumptions and parameters require no justification for use on the AP600 application since they are accepted values that have been used in the analyses for many previous plant licensing applications or are simply AP600 design values, such as containment volume and main control room pressurization air flow. A small number of parameters from Table 15.6.5-2 fall outside these two

categories. These are listed below, together with a statement of the basis used for the selection of each parameter.

Time to isolate purge line: This is set at 15 seconds to accommodate a valve closure time of 10 seconds plus 5 seconds for signal generation and margin.

Reactor coolant flow out of 3 inch break: The 2900 lb/sec value was calculated to be the limiting flow that could occur for the postulated 3-inch break, which is the size of the largest line not qualified for leak before break.

Fraction of reactor coolant iodine that becomes airborne: The 50 percent value bounds the calculated flashing fraction for hot reactor coolant. It conservatively assumes that all iodine in the flashed coolant becomes airborne.

Elemental iodine deposition removal coefficient: The value of 1.6 hr^{-1} was calculated using the methodology defined in Section 6.5.2 of the SRP. This is discussed in Subsection 15.6.5.3.2.1.

DF limit for elemental iodine removal: The value of 200 is selected to be consistent with Section 6.5.2 of the SRP.

Removal coefficient for particulates: See the response to Q450.8.

DF limit for particulates removal: The value of 1000 is conservatively selected to reflect the potential for resuspension of particulates in the containment.

Unfiltered air in-leakage from control room ingress and egress: See the response to Q450.2.

The remaining assumptions and parameters in Table 15.6.5-2 are either AP600 design parameters or typical values that have been accepted for the LOCA analyses on many previous plants.

Consistent with past practice, the calculation of site boundary doses is based on the first two hours of the accident. The activity available for release to the environment during the first hour of this two-hour period is the activity from the primary coolant. The release of activity from the core to the containment begins at one hour into the accident.

c. The fission product transport model used for the design basis LOCA analysis is that the activity released to the containment atmosphere is assumed to be uniformly mixed. The airborne elemental iodine activity is subject to deposition removal. The particulate activity is subject to removal processes including agglomeration, diffusiophoresis, thermophoresis, and sedimentation; these different processes are combined to form the overall particulate removal coefficients. The airborne activity is released to the environment at the design basis containment leak rate (After 24 hours, it is assumed that the leak rate is reduced to half of the design basis containment leak rate.) Activity released from the containment is assumed to be released at ground level. No credit is taken for elevated release of any activity that enters the annulus between the

Question 470.2

The reactor accidents selected in Chapter 15 of the SSAR are generally consistent with the postulated design basis accidents described in Chapter 15 of the SRP. The reactor accidents that are unique to the AP600 design are included in Appendix L, "Severe Accident and Fission Product Source Term Analysis," and Appendix M, "Dose Evaluation Methodology," of Volume 3 of the probabilistic risk assessment for the AP600 submitted on June 26, 1992. The offsite radiological consequences due to these reactor accidents unique to the AP600 design were analyzed using the MELCOR Accident Consequence Code System (MACCS). Reanalyze these unique reactor accidents using the source term guidelines provided in NUREG-1465 for the assessment of the offsite radiological consequences for the AP600. The results of these analyses should be included in Chapter 15 of the SSAR.

Response:

The accidents addressed in the AP600 PRA are not design basis accidents and are not appropriate for inclusion in Chapter 15 of the SSAR. Additionally, the use of the source term from draft NUREG-1465 is not appropriate to the analysis of the spectrum of severe accidents addressed in the AP600 PRA. The severe accident analysis methodology includes generation of source terms specific to each class of events, whereas the source term presented in draft NUREG-1465 is "representative of the mean or average release fractions associated with a group of accident sequences typifying a complete core melt."

The offsite consequences from a severe accident event can vary widely, depending on many factors such as the extent of core damage, whether there is core-concrete interaction or loss of containment function. Therefore, the offsite consequences should be viewed in conjunction with their probability of occurrence. In the AP600 PRA, the fission product releases from severe accidents are binned into several release categories based on the similarities in the timing, magnitude, and type of fission products released to the environment. The characteristics of the fission products associated with the various release categories, also called source terms, are established by analyzing the severe accident progression in a realistic manner, without introducing additional conservatism. The offsite consequences are evaluated using the calculated source terms. This approach is consistent with the past PRA approach to severe accident radiological consequences.

PRA/SSAR Revision: NONE

containment shell and the shield building. Also, no credit is taken for delay of releases during passage through the auxiliary building or for removal processes during that passage.

The fission product removal mechanisms are addressed in the response to Q450.8.

d. The passive core cooling system provides the required pH control for the emergency core cooling water inventory in containment to support radionuclide retention during conditions with high radioactivity in containment and to prevent corrosion of equipment in containment during long-term floodup conditions.

The safety-related pH adjustment tank provides sodium hydroxide solution to the floodup volumes adjacent to the two containment recirculation screens and maintains the pH of the containment recirculation inventory from 7.0 to 9.5, as described in SSAR Section 6.3. See the responses to Q281.3 and Q281.5 for additional information on pH control for the emergency core cooling water inventory.

The addition of sodium hydroxide to the emergency core cooling water inventory is not required for iodine removal except in severe accident conditions with significant core damage. Core damage is not expected during the range of design basis LOCA events analyzed for the AP600. High radioactivity in containment would occur only following significant core damage.

As discussed in the response to Q720.21, during severe accident conditions the IRWST is manually drained to the reactor vessel cavity, where it mixes with the emergency core cooling water in the containment recirculation screen areas. Therefore, for iodine radionuclide retention, pH control of the makeup water in the IRWST is automatically controlled by the pH adjustment tank after the IRWST is drained to containment during severe accidents.

Control of the emergency core cooling water pH is also required to help prevent corrosion of equipment in containment during long-term floodup conditions. In general, following events where the containment floods up without high containment radiation levels, the pH adjustment tank is manually actuated only if the plant recovery from floodup is extended.

e,f,g. These requests go beyond the level of material to be provided as part of the AP600 design certification application. In accordance with past practice, this type of material is available for review by the NRC at the applicant's offices.