Westinghouse Electric Corporation
Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

ET-NRC-93-3815
NSRA-APSL-93-0030
Docket No.: STN-52-003

February 9, 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 9, 1992, October 14, 1992 and November 16, 1992. This transmittal completes the responses to the October 9, 1992 and October 14, 1992 letters. 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 9, 1992 and October 14, 1992 letters 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, Manager
Nuclear Safety & Regulatory Activities

/nja

Enclosure

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

120015

0781A

E004 1/3

ET-NRC-93-3815
ATTACHMENT A
AP600 RAI RESPONSES
SUBMITTED FEBRUARY 9, 1993

RAI No.	Issue
100.005	SRP compliance
100.007	Pre-application RAI's
410.055	Missiles from rotating equipment
410.056	Missile prevention
410.057	Missile generation from non-high-energy systems
410.077	Containment penetrations
410.078	Leak cracks in pipes
410.079	Section 3.6.1.1.J of SSAR
410.085	Subcompartments
410.090	Protection for RC loop
410.092	Pipe failure protection
420.008	ITAAC - safety monitoring system
435.001	Regulatory Guide conformance
435.003	Second offsite power source
435.010	Indications of diesel readiness
435.013	72-hr/post 72-hr equipment qualification
435.016	Adequacy of diesel start, loading..
435.030	Single failure design
435.031	UPS failure, plant trip, forced outage
435.034	nonsafety loads feed from Class 1E dc
435.046	Prevention of harmonic distortion in UPS
435.048	Battery room temperature for 72-hr loss of ac
435.052	dc cable size basis
435.053	dc surge protection for inductive load spikes
435.054	dc motors in dc short circuit calculations
435.055	Isolation of Class 1E loads from non-1E supply

ET-NRC-93-3815
ATTACHMENT A
AP600 RAI RESPONSES
SUBMITTED FEBRUARY 9, 1993

RAI No.	Issue
435.056	Class 1E equip submergence/wetting evaluation
435.057	Use of jumpers
435.058	dc/ac MOVs power off to meet single failure
435.059	Physical separation/electrical independence
435.062	Post 72-hr connection of portable diesel generator
435.066	Isolation devices
435.067	Setpoint selection/relay trip setpoint drift
435.073	Lightning protection/grounding
460.012	Exhaust monitoring
630.001	Risk significant SSCs
630.002	RAP Objective
630.003	D-RAP Design Organization
630.004	Priority of safety goals
630.005	RAP example

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
100.005	SRP compliance	10/09/92	02/09/93
435.001	Regulatory Guide conformance	10/09/92	02/09/93
435.002	Three-tier ac system	10/09/92	11/30/92
435.003	Second offsite power source	10/09/92	02/09/93
435.004	Spare unit auxiliary transformer	10/09/92	11/30/92
435.005	Post-72 hour portable diesels	10/09/92	12/22/92
435.006	Periodic inspection/testing offsite power system	10/09/92	11/30/92
435.007	Reg Guide 1.75 separation of nonsafety ac division	10/09/92	12/22/92
435.008	Diesel generator control	10/09/92	01/14/93
435.009	Diesel generator maintenance/testing program	10/09/92	12/22/92
435.010	Indications of diesel readiness	10/09/92	02/09/93
435.011	RCP trip safety function basis	10/09/92	11/30/92
435.012	Load sizing	10/09/92	12/22/92
435.013	72-hr/post 72-hr equipment qualification	10/09/92	02/09/93
435.014	Grid stability analysis	10/09/92	11/30/92
435.015	Plant operating limits	10/09/92	11/30/92
435.016	Adequacy of diesel start, loading	10/09/92	02/09/93
435.017	Lightning protection of main setup transformers	10/09/92	12/22/92
435.018	Cable derating based on passing thru fire barriers	10/09/92	11/30/92
435.019	Load sizing Class 1E batteries	10/09/92	11/30/92
435.020	Load sizing Class 1E batteries	10/09/92	11/30/92
435.021	Class 1E battery load definition	10/09/92	11/30/92
435.022	Class 1E battery load definition	10/09/92	11/30/92
435.023	Battery charger capabilities	10/09/92	11/30/92
435.024	Overvoltage protection of batteries	10/09/92	12/22/92
435.025	Ground detection of Class 1E dc system	10/09/92	12/22/92
435.026	Class 1E dc system control room alarms/indications	10/09/92	01/14/93
435.027	dc interrupting rating of molded case breakers	10/09/92	01/14/93
435.028	Reg Gudie 1.47 indication for dc system	10/09/92	01/14/93
435.029	Battery charger capacity	10/09/92	01/14/93
435.030	Single failure design	10/09/92	02/09/93
435.031	UPS failure, plant trip, forced outage	10/09/92	02/09/93
435.032	Reg Guide 1.75 compliance	10/09/92	12/22/92
435.033	dc power system transient response	10/09/92	12/22/92
435.034	nonsafety loads feed from Class 1E dc	10/09/92	02/09/93
435.035	Class 1E battery load sizing	10/09/92	01/22/93
435.036	battery charger capacity	10/09/92	01/22/93
435.037	Overcurrent protection for batteries	10/09/92	01/22/93
435.038	Battery condition monitor	10/09/92	01/14/93
435.039	Battery charger cooling	10/09/92	01/22/93
435.040	Battery charger/inverter surge suppression devices	10/09/92	01/22/93
435.041	Battery capacity margin basis	10/09/92	01/22/93
435.042	Battery common mode failures	10/09/92	01/22/93
435.043	Isolation of ac power from Class 1E batteries	10/09/92	01/22/93
435.044	Gas accumulation during charging	10/09/92	01/22/93
435.045	Battery cell vent caps	10/09/92	01/22/93
435.046	Prevention of harmonic distortion in UPS	10/09/92	02/09/93
435.047	Unavailability of UPS instrument buses/inverters	10/09/92	01/22/93
435.048	Battery room temperature for 72-hr loss of ac	10/09/92	02/09/93
435.049	Thermal overload protection for dc MOVs	10/09/92	01/22/93
435.050	Battery instantaneous loads	10/09/92	01/22/93
435.051	Elect/physical separation of spare battery/charger	10/09/92	01/14/93
435.052	dc cable size basis	10/09/92	02/09/93
435.053	dc surge protection for inductive load spikes	10/09/92	02/09/93
435.054	ac motors in dc short circuit calculations	10/09/92	02/09/93
435.055	Isolation of Class 1E loads from non-1E supply	10/09/92	02/09/93
435.056	Class 1E equip submergence/wetting evaluation	10/09/92	02/09/93
435.057	Use of jumpers	10/09/92	02/09/93
435.058	dc/ac MOVs power off to meet single failure	10/09/92	02/09/93
435.059	Physical separation/electrical independence	10/09/92	02/09/93
435.060	Containment electrical penetrations	10/09/92	11/30/92
435.061	Containment electrical penetration protection	10/09/92	01/14/93
435.062	Post 72-hr connection of portable diesel generator	10/09/92	02/09/93
435.063	dc system reliability/testability	10/09/92	01/22/93
435.064	Protection from lightning-initiated fires	10/09/92	01/22/93
435.065	Circuit breakers used for electrical isolation	10/09/92	12/22/92
435.066	Isolation devices	10/09/92	02/09/93
435.067	Setpoint selection/relay trip setpoint drift	10/09/92	02/09/93
435.068	1E/non1E boundary ac power source/120 Vac bus	10/09/92	12/22/92
435.069	Emergency lighting requirements	10/09/92	12/22/92
435.070	Lighting system failure during earthquake	10/09/92	01/14/93
435.071	Emergency lighting basis	10/09/92	01/14/93
435.072	Emergency lighting levels	10/09/92	01/22/93
435.073	Lightning protection/grounding	10/09/92	02/09/93

Question No.	Issue	NRC Letter	Westinghouse Transmittal Date
630.001	Risk significant SSCs	10/14/92	02/09/93
630.002	RAP Objective	10/14/92	02/09/93
630.003	D-RAP Design Organization	10/14/92	02/09/93
630.004	Priority of safety goals	10/14/92	02/09/93
630.005	RAP example	10/14/92	02/09/93

Question 100.5

WCAP-13053, "AP600 Compliance with SRP Acceptance Criteria," Revision 0, is dated August 1991. The design certification application was submitted in June 1992. Update the topical report to reflect the changes made since August 1991.

Response:

WCAP-13054, "AP600 Compliance with SRP Acceptance Criteria," (non-proprietary) is being updated. The revised document will be submitted to the NRC by March 1, 1993.

SSAR Subsection 1.9.2 will be revised as follows:

SSAR Revision:

1.9.2 Compliance With Standard Review Plan (NUREG-0800)

WCAP-13054, Revision 1, "AP600 Compliance with SRP Acceptance Criteria," provides the results of a review of the AP600 compliance with the acceptance criteria for each section of the Standard Review Plan, NUREG-0800.

Question 100.7

Provide written responses to the pre-application requests for additional information that were requested in letters dated January 30, 1992, June 22, 1992, July 21, 1992, and September 1, 1992, or provide a cross-reference to any responses that may have already been formally addressed.

Response:

Written responses to the above requests for additional information were provided in the following letters:

1. Response to Request Dated January 30, 1992
   Westinghouse letter ET-NRC-92-3663, S. R. Tritch to Mr. D. Crutchfield, "Responses to AP600 Design-Issues to be Resolved by High-Pressure Full-Height Integral Testing," dated February 14, 1992.

2. Response to Request Dated June 22, 1992
   Westinghouse letter ET-NRC-93-3797, N. J. Liparulo to Dr. T. Murley, "NRC Request for Additional Information Related to AP600 Design," Dated January 19, 1993.

3. Response to Request Dated July 21, 1992
   Westinghouse letter ET-NRC-93-3799, N. J. Liparulo to Dr. T. Murley, "NRC Requests for Additional Information on the AP600 Testing Program Dated July 21, 1992," dated January 19, 1993.

4. Response to Request Dated September 1, 1992
   Westinghouse letter ET-NRC-93-3798, N. J. Liparulo to Dr. T. Murley, "NRC Requests for Additional Information on the AP600 Testing Program Dated September 1, 1992," dated January 19, 1993.

SSAR Revision: NONE

Question 410.55

Provide sample analyses to demonstrate that housings of rotating equipment can contain missiles generated by the rotating equipment (Section 3.5.1.1).

Response:

The criteria in SSAR Subsection 3.5.1.1 to which this question apparently refers consider the generation of missiles outside containment by safety-related rotating equipment. By reference in other subsections and criteria, it also applies to equipment inside containment and may apply to non-safety-related equipment.

The safety-related systems and components needed to bring the plant to a safe shutdown are inside the containment shield building and auxiliary building, both of which have thick structural concrete exterior walls that provide protection from missiles generated in other portions of the plant. These walls are evaluated for tornado missiles that bound the energy available in internally generated missiles (except perhaps postulated turbine-generator missiles, which are evaluated separately).

Motor-driven pumps and fans are the rotating equipment considered for internal missile generation. See Q410.61 for a discussion of credible sources of internally generated missiles. Potential missiles from the turbine-generator are discussed separately; see SSAR Subsection 3.5.1.3 and the response to Q410.52. The AP600 has no turbine-driven pumps. The diesel-generator and motor-generators are outside the nuclear island (containment shield building and auxiliary building). See the response to Q410.61 for a tabulation of the rotating equipment assessed for potential missile generation within the containment shield building and the auxiliary building. See the response to Q410.65 for a discussion of the potential for missiles from the reactor coolant pump. The safety-related function of the normal RHR pumps is the maintenance of the pressure boundary. The rotating portions do not have to operate to provide a safety-related function. Missiles generated from the rotating parts of non-safety rotating equipment are assessed on a case-by-case basis.

Evaluation of potential missiles may include the determination by analysis, test, or experience that a pump or fan design would contain such a missile. The maximum no-load speed for a motor-driven pump or fan is equivalent to the operating speed of the motor. There is no combination expected of pipe break and single failure in the subject pumps that could result in significant overspeed. These factors minimize the potential for conditions that could lead to generation of a missile. Non-safety-related canned motor pumps have a housing designed to retain pressure and are expected to contain any fragments from a postulated fracture of the rotating elements. When analysis is used to demonstrate containment of postulated fragments, the energy absorption methods found in Reference 1 may be used.

Motors in motor-operated valve operators and mechanical handling equipment operate less than 2 percent of the time and are not considered to be credible sources of missiles.

AP600

Reference:

1. Hagg, A. C., and Sankey, G. O., "The Containment of Disk Burst and Fragments by Cylindrical Shells," ASME Journal for Power, April 1974, pp. 114-123.

The following paragraph will be added to SSAR Subsection 3.5.1.1.2.1, Missiles Not Considered Credible.

SSAR Revision:

3.5.1.1.2.1 Missiles not Considered Credible

- Rotating components that operate less than 2 percent of the time are not considered credible sources of missiles.

Question 410.56

Provide examples of equipment features used to prevent missile generation in the "special situations" referred to in Section 3.5.1.1.2.1 of the SSAR.

Response.

The criteria in SSAR Subsection 3.5.1.1.2.1 apply to components outside containment and by reference, to components inside containment. The specific use of the term *special situations* is included in a criterion related to non-safety-related rotating equipment. See the responses to Q410.61 and Q410.67 for a discussion of the credible sources of internally generated missiles from rotating equipment. As discussed in the response to Q410.55, only rotating equipment inside the containment shield building and auxiliary building is assessed for potential missile generation. Potential turbine-generator missile generation is treated separately. See the response to Q410.52 for information on the evaluation of turbine-generator missiles. Situations in which equipment features on non-safety-related rotating equipment are used to prevent missile generation to protect safety-related structures, systems, or components are evaluated on a case-by-case basis.

The non-safety-related pumps and fans inside containment and the auxiliary building are rugged industrial equipment that would not be expected to fail catastrophically. Equipment features used to prevent missile generation include a housing or an enclosure strong enough that a blade from the impeller would not penetrate the housing. For example, because of the pressure-retaining function of the outside shell, canned motor pumps provide sufficient thickness to contain fragments from the postulated failure of the rotating elements. An additional feature used in special situations is the control of design, construction, and application sufficient to provide for an impeller that has a low probability of fracture.

SSAR Revision: NONE

Question 410.57

Provide sample analyses to demonstrate that credible missiles cannot be generated from non-high-energy fluid systems. Are high energy systems that meet the 2% and 1% rules defined in Section 3.6.1.1 of the SSAR considered high-energy systems from the standpoint of missile generation (Section 3.5.1.1)?

Response:

Moderate-energy systems do not contain water with a temperature above the boiling point of water. Such low-temperature systems do not have the stored energy represented by the flashing of water to steam that higher-temperature systems do. In a water-solid system below 212°F a small increase in system volume results in a substantial decrease in pressure. This characteristic results in minimal energy available to propel a part in the event of a rupture or break.

Components of nonhigh-energy compressed gas systems inside the auxiliary and containment buildings are limited to air motors for reciprocating pumps, pneumatic valve operators, and a small number of accumulators for safety-related, pneumatically operated valves required to operate following the loss of the compressed and instrument air system. The operating pressure for these components ranges from 80 to 120 psi, which provides minimal energy to propel a part in the event of a rupture or break. The accumulators for safety-related valves are safety-related and are constructed to appropriate standards to provide pressure boundary integrity and high reliability. Missile generation due to the failure of a safety-related compressed air accumulator is not considered credible. The amount of compressed air contained within the air motors and the pneumatic valve operators is a limited volume and would not have the energy available required to generate a missile in the event of a break. Additionally, the safety-related pneumatic valve operators and air motors as well as those required for defense-in-depth functions are selected and constructed for their high reliability and functional integrity. Based on these facts, analysis of the potential for the generation of missiles from nonhigh-energy compressed gas systems is not required.

Systems that exceed 200°F or 275 psig for 2 percent or less of the time during which the system is in operation or that experience high-energy pressures or temperatures for less than 1 percent of the plant operation time are considered moderate-energy for the purposes of missile generation. These systems are not considered to be sources of missiles.

The exclusion of nonhigh-energy systems from sources of missiles has been found to be acceptable by the NRC in previous applications.

SSAR Revision: NONE

AP600

Question 410.77

Will containment penetration areas meet the break exclusion provisions of B.1.b of Branch Technical Position MEB 3-1 (Section 3.6.1)?

Response:

As noted in SSAR Subsection 1.9.2, the compliance with branch technical positions is provided in WCAP-13054, Revision 1, "AP600 Compliance with SRP Acceptance Criteria." The provisions of B.1.b of MEB 3-1 are met, except that there is no OBE event for the AP600 plant. See the response to Q252.6 for a description of the break exclusion zone boundaries for the main steam and main feedwater piping. Other portions of the break exclusion zone are described in SSAR Subsection 3.6.2.1.1.4.

SSAR Revision: NONE

Question 410.78

Section 3.6.1.1.F of the SSAR identifies the initiating events for the pipe failure effects analysis. Clarify if leakage cracks in moderate energy pipes are considered as initiating events.

Response:

Leakage cracks are postulated in high-energy piping as described in SSAR Subsection 3.6.2.1.2.3. Leakage cracks are not postulated in moderate-energy piping. Through-wall cracks are postulated in moderate-energy piping systems as described in SSAR Subsection 3.6.2.1.2.2.

SSAR Revision: NONE

Question 410.79

Clarify what is meant in Section 3.6.1.1.J of the SSAR.

Response:

SSAR Subsection 3.6.1.1.J describes the components that are used to mitigate the effects of pipe rupture. See the response to Q410.92 for additional details.

SSAR Revision: NONE

Question 410.85

Do any subcompartments inside the containment contain high-energy lines between 3 - 4 inches? If so, are breaks from lines of this size considered in the subcompartment pressurization analysis (Section 3.6.1)?

Response:

There are no high-energy lines inside containment with diameters larger than 3 inches and smaller than 4 inches. Subcompartment pressurization analysis is performed to cover the high-energy piping that does not satisfy the leak-before-break criteria described in SSAR Subsection 3.6.3.

SSAR Revision: NONE

Question 410.90

Provide additional detailed information regarding the methods used to protect the reactor coolant loops from the effects of failures of the main steam and feedwater lines and vice versa (Section 3.6.1).

Response:

The reactor coolant loop piping and the steam lines and feedwater lines are evaluated using the criteria for mechanistic pipe break (leak before break). See the responses to Q210.6, Q252.5, and Q252.10 for additional discussion of candidate systems for leak-before-break analyses and the evaluation of reactor coolant loop piping and the steam line and feedwater piping for leak-before-break criteria. Dynamic effects of pipe failures are not considered for piping systems that satisfy the criteria for mechanistic pipe break. Other nondynamic effects of pipe break such as spray wetting and flooding would not have an adverse effect on the safety-related functions of these piping systems.

The steam generator and supports are analyzed for loads due to pipe breaks in the reactor coolant system and the steam lines and feedwater lines. The size of the break analyzed is determined by the largest connected pipe that does not satisfy mechanistic pipe break criteria. The analysis includes evaluation of primary nozzle loads for breaks in the steam generator system (steam and feedwater lines) and secondary nozzle loads for breaks in the reactor coolant system. The motions of the steam generator due to postulated pipe ruptures in primary-side piping that does not satisfy leak-before-break criteria are calculated using dynamic structural analysis. These motions are evaluated as static anchor motions on the piping. The results are combined with normal operating condition loadings (100 percent power). These evaluations are sufficient to demonstrate that the systems connected to the steam generator are not adversely affected by loads transmitted through the steam generators.

If leak-before-break criteria are met for main steam line or feedwater line, then there is no effect on the primary loop piping since the closest pipe rupture in the main steam line or feedwater line is in the turbine building outside the anchor in the auxiliary building. If leak-before-break criteria are not demonstrated for the main steam line or feedwater line, then a dynamic analysis of the steam generator coupled to the primary loop piping will be performed to determine the loads in the loop piping. These loads are combined by the square root of the sum of the squares method with the safe shutdown earthquake loads and added to the normal 100 percent power loads.

The steam and feedwater lines are separated from the reactor coolant loop piping by reinforced concrete walls and floors, except for a small portion of the feedwater line inside of the steam generator cubicles.

SSAR Revision: NONE

Question 410.92

Identify systems important-to-safety that require protection from pipe failures and their effects (Section 3.6.1).

Response:

The term *important to safety* is taken to be as stated in Q410.51, that is, non-safety-related equipment whose failure could adversely affect the ability of safety-related equipment to perform its safety function.

The non-safety-related structure, system, or component in the plant that is relied on to mitigate a design basis accident is the portion including the turbine stop valves, moisture separator rehcater stop valve, feedwater control valves, and the piping connecting these valves to the safety-related portion of the main steam line and feedwater line. See the response to Q440.31 for a discussion of the use of non-safety-related systems and components to mitigate design basis accidents. The postulated pipe rupture for that this portion is used to demonstrate single failure protection is a break of the steam line inside containment. The single failures which are protected against in this case are failure of the steam line or feedwater line isolation valves to close. Closure of steam line valves is required in order to prevent bypass of containment atmosphere to the atmosphere outside containment. Closure of a feedwater line valve is required in order to terminate the supply of water to the break. Since the condition for which the important-to-safety segment provides protection is on the opposite side of the containment boundary, no additional protection from a steam line pipe rupture is required.

Non-safety-related systems in which a pipe rupture could adversely affect a safety-related system relied on for plant shutdown and accident mitigation subsequent to postulated pipe rupture are evaluated for pipe whip protection as part of the evaluation of the system affected.

SSAR Subsection 3.6.1.1, paragraph J, will be revised as follows:

SSAR Revision:

J. Safety-related systems and components are used to mitigate the effects of postulated pipe ruptures. In addition, the turbine stop, moisture separator reheater stop, and feedwater control valves (which are not safety-related) are credited in single failure analyses to mitigate postulated steam line ruptures.

Question 420.8

The instrumentation and control system of the AP600 uses microprocessor based distributed digital equipment to perform plant protection and safety monitoring functions. The software design quality is a major issue which must be adequately addressed by Westinghouse for the staff to make a safety determination. Because microprocessor and digital control technology is rapidly evolving it is important that the certified design description and the ITAAC do not "lock in" a design that would be obsolete at the time of construction. The staff's approach in this area is to certify a design process and "lock in" the specific design acceptance criteria (DAC). The degree to which a particular aspect of design is "locked-in" (Tier 1 or Tier 2) will be described in the certification rule.

The ITAAC submittal for the Protection and Safety Monitoring System of the AP600 only addresses functional requirements and does not provide design details or the design process commitment. The Certified Design Commitment for the microprocessor-based digital protection system or digital control system should address the software design process commitment and describe a formal design implementation process with a phased inspections, tests, analyses, and acceptance criteria. The ITAAC will be inspected by the NRC to verify conformance with the requirements at several phases or stages during the design process. At each phase of the ITAAC, implementation of the design development must be verified to be in accordance with the certified design process. Upon completion of each phase of the ITAAC, the COL holder will certify to the NRC that the stage has been completed and the design and construction completed up through that stage is in compliance with the certified design. The COL holder will also provide a description of the next phase of design development and associated testing, analysis and acceptance criteria in enough detail that the NRC staff can determine whether or not the proposed design development and testing is consistent with the certified design process and next ITAAC. This phased process will continue until all ITAAC stages for all the safety related software are completed.

In addition to the design process commitment, the ITAAC for the Protection and Safety Monitoring System should also address the following elements:

- Common mode failure prevention
- Human factors aspect of the design
- Communications (data link)
- Bypass capability (operation & maintenance modes)
- Setpoint methodology
- Safety action seal-in provision
- Physical separation of channels
- On-line testing and surveillance testing
- EMI/RFI protection
- Equipment qualification
- Safety and control systems interactions
- Cross reference to SSAR drawings

Response:

Design details are considered to be Tier 2 and are provided in Chapter 7.1 of the SSAR and in WCAP-13382. The design process for hardware and software is also considered to be Tier 2 and is described in WCAP-13383.

The elements listed in the question are considered to be Tier 2 and are addressed elsewhere as noted below:

- Common mode failure prevention

  The prevention of common mode failures in the protection and safety monitoring system is addressed by the following:

  - The verification and validation program (WCAP-13383)
  - The use of fail safe design principles
  - Functional diversity within the system design
  - Equipment qualification
  - The built-in functional tester
  - Equipment designed for maintenance

  To further address the issue of common mode failures in the protection and safety monitoring system, a diverse actuation system is provided (Reference Section 2.11 of WCAP-13382, SSAR Subsection 7.7.11, SSAR Figure 7.2-1; sheet 29, and the response to Q420.7a).

- Human factors aspect of the design

  The human factors considered in the design of the protection and safety monitoring system are addressed as part of the overall AP600 human factors design process described in Chapter 18 of the SSAR.

- Communications (data link)

  Communications within the protection and safety monitoring system are addressed by Sections 4.0.7 and 4.6 of WCAP-13382.

- Bypass capability (operation and maintenance modes)

  Bypass capability within the protection and safety monitoring system for operation and maintenance is described in SSAR Subsections 7.1.4.2.11 through 7.1.4.2.14 and Section 2.6 of WCAP-13382.

- Setpoint methodology

  The issue of setpoint methodology is a generic issue and is being addressed on an industry-wide basis.

- Safety action seal-in provision

  The sealing in of safety actions within the protection and safety monitoring system is described by SSAR Subsection 7.1.4.2.15.

- Physical separation of channels

  Physical separation of channels within the protection and safety monitoring system is described by SSAR Subsection 7.1.4.2.6 and Section 2.2 of WCAP-13382.

- On-line testing and surveillance testing

  SSAR Subsection 7.1.4.2.10 and Sections 2.4 and 2.10 of WCAP-13382 describe the on-line testing and surveillance testing provisions of the protection and safety monitoring system.

- EMI/RFI protection

  The EMI/RFI design of the protection and safety monitoring system is described in Section 4.0.6 of WCAP-13382. See also the response to Q420.1.

- Equipment qualification

  Equipment qualification is described in SSAR Subsection 7.1.4.2.4 of the SSAR.

- Safety and control systems interactions

  Design features of the protection and safety monitoring system to prevent safety and control systems interactions are described in SSAR Subsection 7.1.4.2.7 and Section 2.8 of WCAP-13382.

- Cross-reference to SSAR drawings

  SSAR drawings are considered to be Tier 2 and need not be referenced in Tier 1 design descriptions of ITAACs.

SSAR Revision: NONE

Question 435.1

Appendix 1A, "Conformance With Regulatory Guides, of the SSAR lists the applicable guides with referenced IEEE Standards. The column, "Clarification/Summary Description of Exceptions," states that, for several IEEE Standards, the AP600 uses the latest version of the industry standards (as of 1/90). These versions of IEEE Standards are not endorsed by a regulatory guide, but Westinghouse states that their use should not result in deviation from the design philosophy otherwise stated in the associated regulatory guide(s). For each of these IEEE standards, discuss (1) the difference between the latest version of the industry standard used in the design of the AP600 and the standard endorsed by the regulatory guide, and (2) the conformance of the AP600 to the standard. This discussion should use the new terminology/definitions introduced by IEEE 603/308 - 1980.

Response:

Appendix 1A of the SSAR lists eight regulatory guides that endorse the following IEEE standards. The endorsed standards are superseded by the latest version (publication as of 1/90) that the AP600 design uses.

Regulatory Guide	Endorsed IEEE Standard	Superseded by IEEE Latest Version
1.32, Rev.2, 2/77	308 - 1974	308 - 1980
	450 - 1975	450 - 1987
1.53, Rev.0, 6/73	379 - 1972	379 - 1988
1.63, Rev.3, 2/87	741 - 1986	741 - 1990
1.75, Rev.2, 9/78	384 - 1974	384 - 1981
1.89, Rev.1, 6/84	323 - 1974	323 - 1983
1.106, Rev.1, 3/77	279 - 1971	603 - 1980
1.118, Rev.1, 4/78	338 - 1977	338 - 1987
1.128, Rev.1, 10/78	484 - 1975	484 - 1987

Although the latest versions are not endorsed by the regulatory guide, they do not deviate from the regulatory guide design philosophy. A comparison table between the endorsed IEEE standard and the latest version follows.

Number & Section of R.G. 1.89, Rev. 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
1.89 Rev. 1	323-1974	323-1983		
C.1 App. A App. B	Not Applicable (N/A)	N/A	N/A	Fully conforms to R.G.
C.2	Section 6.2 Service Condition, Item (7)	6.1.5 Service Condition.	No major difference, except Section 6.1.5 of IEEE 323-1983 covers "submergence".	Fully conforms to R.G.
C.2.a App. C	N/A	N/A	N/A	Fully conforms to R.G.
C.2.a(4)	Appendix "A" Test Profile	7.0 Simulated Test Profile	App. A is deleted in IEEE 323-1983. Instead, Figures 1 and 2 are added for simulated condition test profile, which adequately clarifies NRC's position.	Fully conforms to R.G.
C.2.b	N/A	N/A	N/A	Fully conforms to R.G.
C.2.c App. "D"	N/A	N/A	N/A	Fully conforms to R.G.

Number & Section of R.G. 1.89, Rev. 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.2.c.1 C.2.c.2	N/A N/A	N/A N/A	N/A N/A	For exception see Appendix "1A" of SSAR
C.2.c.3 Through C.2.c.8	N/A	N/A	N/A	Fully conforms to R.G.
C.2.d	N/A	N/A	N/A	Fully conforms to R.G.
C.3	6.3 Type Test Procedure"	6.3 Type Testing		
C.3	6.3.1 General	6.3.1 General	None	Fully conforms to R.G.
C.3	6.3.1.1 Test Plan	6.3.1.1 Test Plan	IEEE 323-1983 covers the requirement of IEEE 323-1974 plus additional requirements, such as equipment safety function, acceptance criteria, margin, test sequence, maintenance/replacement during aging, and control of modification during test.	Fully conforms to R.G.
C.3	6.3.1.2 Mounting	6.3.1.2 Mounting	None	Fully conforms to R.G.

Number & Section of R.G. 1.89, Rev. 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.3	6.3.1.3 Connections	6.3.1.3 Connections	None	Fully conforms to R.G.
C.3	6.3.1.4 Monitoring	6.3.1.4 Monitoring	IEEE 323-1983 covers necessary monitoring requirements without classification of general categories from I through VII, as shown in IEEE 323-1974.	Fully conforms to R.G.
C.3	6.3.1.5 Margin	6.3.1.5 Margin	Suggested factors for margin are the same in both versions of IEEE 323, except IEEE 323-1983 covers environmental transients in more detail, with two methods that may be used to apply margin. IEEE 323-1983 also suggests not to use margin for natural aging.	Fully conforms to R.G.
C.3	6.3.2 Test Sequence	6.3.2 Test Sequence	The test sequence stipulated in IEEE 323-1983 is more refined compared to that shown in IEEE 323-1974, and it covers the requirements of IEEE 323-1974. IEEE 323-1983 recommends post-test-inspection instead of disassembly as stated in IEEE 323-1974.	Fully conforms to R.G.

Number & Section of R.G. 1.89, Rev. 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.3	6.3.2(5)	6.3.2(6)	IEEE 323-1974 references IEEE 344-1971 and IEEE 334-1971 for seismic vibration. IEEE 323-1983 References OBE and SSE seismic vibration per IEEE 344-1975 (R 1980). IEEE 334-1971 is obsolete and is therefore not referenced in IEEE 323-1983.	Fully conforms to R.G.

Number & Section of R.G. 1.89, Rev. 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.3	6.3.3 Aging	6.3.3 Aging	IEEE 323-1983 covers natural aging and age conditioning. It does not reference IEEE 101-1972 for statistical analysis of thermal life test data as addressed in IEEE 323-1974. Sample aging time of less than 100 hours is not permitted per IEEE 323-1974. IEEE 323-1983 has no specific time limit for aging. However, it recommends using the accelerated cycle rate for the number required during the design life, provided the rate is not accelerated to any value that results in effects not present at normal rates. IEEE 323-1983 also states that age conditioning involves applying simulated in-service stresses (thermal, radiation, wear, and vibration) at magnitude or rate that are greater than expected in-service levels but less than the material property limitations.	Fully conforms to R.G.

Number & Section of R.G. 1.89, Rev. 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.3	6.3.4 Radiation	6.3.4 Radiation	IEEE 323-1974 refers IEEE 278-1967 and ASTM D 2953-71 for dose equivalent to service for electrical insulating material and classification system for polymeric material for service in ionizing radiation. IEEE 323-1983 does not refer to these standards. However, it recommends use of a gamma radiation source to simulate the expected effects of the radiation environment. IEEE 323-1983 suggests that radiation testing may be excluded if it can be shown that the combined normal and accident radiation dose and dose rate do not affect the safety function(s) and that there are no adverse affects if radiation is done sequentially, either before or after thermal or wear cycling. IEEE 323-1983 suggests "if it can be shown that the radiation effect is restricted to the heating effects of energy absorption, the effect may be taken into account during accelerated thermal aging."	Fully conforms to R.G.

Number & Section of R.G. 1.89, Rev. 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.3	6.3.5 Vibration	6.3.5 Seismic and Non-seismic Vibration	Use of IEEE 344-1971 referenced in IEEE 323-1974 is changed to IEEE 344-1975 (R 1980) in IEEE 323-1983 for seismic vibration.	Fully conforms to R.G.
C.3	6.3.6 Operation Under Normal and Accident Condition	6.3.6 Operation Under Normal and DBE Condition	None	Fully conforms to R.G.
C.3	6.3.7 Inspection	6.3.7 Inspection	IEEE 323-1983 does not address dismantling the assembly after type testing and inspecting individual components as stated in IEEE 323-1974. Instead, it recommends visual inspection to document the physical condition of the equipment.	Fully conforms to R.G.
C.4-6	IEEE 323-1974	IEEE 323-1983	See IEEE Section 6.3.1.5, "Margin" and Section 6.3.3 ,"Aging" in R.G. Section C.3.	Fully conforms to R.G.
C.7 App. "E"	N/A	N/A	N/A	Fully conforms to R.G.

Number & Section of R.G. 1.89, Rev. 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.7	8.0 Documentation	8.0 Documentation	IEEE 323-1983 has been reformatted to include: • Identification of equipment qualified, specific safety function, identification of scheduled surveillance/maintenance, periodic testing, and parts replacement to maintain qualification • Summary and conclusions, including limitations and qualified life or periodic surveillance/maintenance interval determination	

Number & Section of R.G. 1.63, Rev 3	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
1.63 Rev. 3	741-1986, 5.4 - Primary Containment Electrical Penetration Assemblies	741-1990, 5.4 - Primary Containment Electrical Penetration Assemblies	None	Fully conforms to R.G.

Number & Section of R.G. 1.118, Rev. 2	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
1.118 Rev. 2	338-1977	338-1987		
C.1	General	2 Definitions	No major difference; definition of safety system is incorporated in the latest standard as required by the R.G.	Fully conforms to R.G.
C.2	5 - Design, Item (6), and 6.1 - Testing Program General Consideration, Item (2)	5 Design Requirements, Item 5, and 6.1 Testing Program Requirements General Consideration, Item (2)	None	Fully conforms to R.G.
C.3	5 Design, Item (11)	5 Design Requirements, Item (10)	The supplement required by the R.G. has been incorporated in Item (10) of Section 5 of the latest standard.	Fully conforms to R.G.
C.4	5 Design, Item (4)	5 Design Requirements, Item (13) and Item (14)	The latest standard incorporates the supplements required by R.G. Supplement (13) is incorporated partially and Supplement (14) completely. Item (4) of Section 5 of IEEE 338-1977 is deleted in the later version of the Standard (338-1987).	Fully conforms to R.G.

Number & Section of R.G. 1.118, Rev 2	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.5	6.3.4 Response Time Verification Tests	6.3.4 Response Time Verification Tests	None (Note: Nuclear sensors are exempt from response time testing since their worst case response time is not a significant fraction of the total overall system response).	Fully conforms to R.G.
C.6	6.4 Test Methods, Item (5)	6.4 Test Methods, Item (5)	The supplements (a) and (b) noted on the R.G. have been incorporated in the latest standard.	Fully conforms to R.G.
C.7	6.5.1 Initial Test Intervals	6.5.1 Initial Test Intervals	The supplement noted on the R.G. has been incorporated in the latest IEEE standard.	Fully conforms to R.G.
C.8	4 Basis, eighth paragraph, 5 Design, Items (2) & (3) 6.6.2 Procedure, Item (8)			N/A as these items are still under consideration by NRC.

Number & Section of R.G. 1.32, Rev 2	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
R.G. 1.32 Rev. 2	308-1974 (IEEE Std. 450-1975 is referenced for Battery Testing Criteria)	308-1980		
C.1a	5.2.3(4) Preferred power supply.	6.2.3 Preferred power supply	The revised text includes the time period to be "within few seconds."	Fully conforms to R.G.
C.1b	5.3.4 Battery charger.	3.3.4 Battery charger.	The revised text defines the sizing requirements in conformance with the Regulatory position.	Fully conforms to R.G.
C.1c	Battery Performance Discharge Test.	6.3.5 Test Provisions.	The revised text deletes the Table 2 and refers to IEEE Std. 450-1975 for the battery capacity test criteria. IEEE Std. 450-1987 Section 5.0 retains the same test schedule.	Fully conforms to R.G.
C.1d	5.2.1, 5.2.2 (3), and 5.2.4. Independence of redundant standby sources to be per R.G. 1.6 and 1.75.	6.2.1, 6.2.2 (3) and 6.2.4. Independence of redundant standby sources to be per R.G. 1.6 and 1.75.	The revised text invokes IEEE 384-1977 and IEEE 387-1977 which addresses the requirements of R.G. 1.75 and R.G. 1.6.	Fully conforms to R.G.
C.1e	4.9. Connections of non-Class 1E equipment to Class 1E system should be per R.G. 1.75.	5.11. Connections of non-Class 1E equipment to Class 1E system should be per R.G. 1.75.	The revised text invokes IEEE 384-1977 which addresses R.G. 1.75 requirements.	Fully conforms to R.G.

Number & Section of R.G. 1.32, Rev 2	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	C
C.1f	5.2.4 Selection of Diesel Generator Capacity.	6.2.4 Selection of Diesel Generator Capacity	The revised text invokes IEEE 387-1977 which addresses R.G. 1.9 requirements on standby power source capacity selection.	Fully conforms to R.G.
2.a	8.2 and 8.3 Shared electric systems for multi-unit nuclear power plants shall follow R.G. 1.81.	8.2 and 8.3 Shared electric systems for multi-unit nuclear power plants shall follow R.G. 1.81.	The IEEE standard text is essentially the same. The current standard does not invoke R.G. 1.81.	The current standard text does not conform to R.G. position 2.a. However, the present AP600 design basis is addressing only a single-unit plant. Hence, the multi-unit design considerations are not applicable.
2.b	7, Table 3 Suggested Alternatives with Degraded Class 1E Power Systems Conditions	No corresponding section in the current standard.	Section 7 and Table 3 have been deleted from the current standard. Hence, there are no more requirements on the topic.	Fully conforms to R.G.

Number & Section of R.G. 1.53, Rev 0	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
R.G. 1.53 Rev. 0	379-1972	IEEE Std. 379-1988		
C-2	5.2 Undetectable Failures	5.2 Undetectable Failures.	The current version of the standard defines the undetectable failures and clarifies the analysis requirements.	Fully conforms to R.G.
C-3	6.2 Channels	6.1 and 6.2 Procedures and System Portion Analysis	The current version of the standard Sections 6.1 and 6.2 have been updated to include specific statements that conform to the regulatory position.	Fully conforms to R.G.
C-4	6.3 and 6.4. Protection System Logic and Actuator Circuit	6.2.2, 6.2.3, and 6.2.4 System Logic, Actuation Devices, & Elect. Power Supplies	The current version of the standard addresses the Regulatory position by eliminating potentially ambiguous interpretation.	Fully conforms to R.G.

Number & Section of R.G. 1.75, Rev 2	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
R.G. 1.75 Rev. 2	384-1974	384-1981		
C-1	3 Definition - Isolation device.	Definition - Isolation device.	None.	Fully conforms to R.G.
C-2	3 Definition - Raceway	3 Definition - Raceway has been revised to delete "interlocked armor enclosing cable" to be construed as a raceway	None.	Fully conforms to R.G.
C-3	4.3 Methods of Separation	5.2. Methods of Achieving Independence	The revised text defines additional methods to achieve independence.	Conforms to R.G. by alternate means.
C-4	4.5 (1). Associated Circuits.	5.5.1 and 5.5.2. Associated Circuits	None	Fully conforms to R.G.
C-5	4.5. Associated Circuits - concluding "Note."	5.5.2 concluding Note	None	The R.G. supplement clarifies the application of the "Note." The current standard does not categorically deviate from the R.G. position.

Number & Section of R.G. 1.75, Rev 2	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C-6	4.5 (3), 4.6.2, and 5.1.1.2 Analysis Document Submission	5.5 and 5.6. Analysis document submission.	None.	Fully conforms to R.G.
C-7	4.6.2 No Blanket Exemption for the Non-Class 1E Instrumentation and Controls Circuits	4.6.2. No Blanket Exemption for the Non-Class 1E Instrumentation and Controls Circuits.	None.	Fully conforms to R.G.
C-8	5.1.1.1 Separation of Redundant Circuits in a Confined Space	6.1 Separation of Redundant Circuits in a Confined Space	The revised text elaborates on the minimum separation distances for various routing conditions and identifies testing/analysis requirements for special cases.	Fully conforms to R.G.
C-9	6.1.1.3 Cable Splices in the Raceways Prohibited	6.1.1.2 Cable Splices in the Raceways Prohibited	The revised section imposes cable qualifications requirements in accordance with IEEE 383-1974. This requirement addresses both the cables and the field splices to withstand fire hazards.	The current Standard conforms to the R.G. position by alternate means.
C-10 & C-11	5.1.2. Method of Identification of Circuits.	6.1.2 Method of identification of circuit.	The revised text complies with the intent of the R.G. position.	Full conformance.

Number & Section of R.G. 1.75, Rev 2	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C-12	5.1.3 Cable Spreading Area.	6.1.3. Non-Hazard Area	The revised text defines the requirements for non-hazard areas, and routing of the power circuit cables in enclosed raceways, which address the underlying reasons of the R.G. position.	The current standard conforms to the R.G. position by alternate means.
C-13	Figure 2	Figures 4, 5, 6 and 7	The revised figures clarify the text requirements. There is no significance attached to the tray width by virtue of the fact that tray dimensions are not included.	Fully conforms to R.G.
C-14	5.2.1 Standby Power Generator Redundancy	Sections 6.2, 5.7 and 5.9. Standby Power Generator Redundancy	The revised text imposes sufficient requirements to ensure that the independence of the redundant standby generating unit is maintained.	Fully conforms to R.G.
C-15	5.3.1 Independent Ventilation Needs to Preserve Redundant Class 1E Battery Operation.	6.3, 5.7 and 5.9 Independent Ventilation Needs to Preserve Redundant Class 1E Battery Operation	None	Fully conforms to R.G.
C-16	5.7 Instrumentation Cabinets	6.6 and 6.7. Control Switchboard & Instrumentation Cabinets	None	Fully conforms to R.G.

Number & Section of R.G. 1.106, Rev 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
1.106, Rev. 1	279-1971	603-1980		
C.1	4.0 through 4.5, 4.10, and 4.13 Bypass Initiation Circuitry.	5.1 through 5.5, 5.7, and 5.8.3 Bypass Initiation Circuitry.	None	Fully conforms to R.G. See also response to Q485.49

Number & Section of R.G. 1.128, Rev 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.1	4.1.4 Ventilation	5.1.4 Ventilation	None	Fully conforms to R.G.
C.2	4.2.21 Location	5.2.1 Location	Separation by IEEE 384-1974 for the endorsed IEEE and IEEE 384-1981 for the latest IEEE, both of which are identical.	Fully conforms to R.G.
C.3	4.2.2 Mounting, Items (1) through (5)	5.2.2 Mounting, Items (1) through (5)	None	Fully conforms to R.G.
C.4	5.3.2 Acceptance Test.	6.3.2: Acceptance Test.	Acceptance test by IEEE 450-1975 for endorsed IEEE and IEEE 450-1987 for the latest IEEE, both of which are identical.	Fully conforms to R.G.
C.5	7: References.	3: References.	The latest IEEE standard added two references, i.e., IEEE 946-1985 and IEEE 494-1974 (R 1983). IEEE 535-1986 provides specific reference to qualification of Class 1E lead storage battery, which replaces IEEE 323-1974.	Fully conforms to R.G.
C.6	Sections containing verb "should" to be treated the same as requirements of the standard.	Sections containing verb "should" to be treated the same as requirements of the standard.	None	Fully conforms to R.G.

Number & Section of R.G. 1.128, Rev 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.6.2	4.1.1 Location, Item (2)	5.1.1 Location, Item (3)	None	Fully conforms to R.G.
C.6.b	4.1.1 Location, Item (3)	5.1.1 Location, Item (4)	None	Fully conforms to R.G.
C.6.c	4.1.1 Location, Item (5)	5.1.1 Location, Item (6)	None	Fully conforms to R.G.
C.6.d	4.1.2 Mounting, Item (2)	5.1.2 Mounting, Item (2)	For the latest IEEE version, three-tier rack is acceptable provided the requirements of 5.1.1 (5) are met. The AP600 has a two-step rack battery configuration.	Fully conforms to R.G.
C.6.e	4.1.5 Instrumentation and Alarms.	5.1.5 Instrumentation and Alarms.	The latest version added instrumentation to measure current through the battery.	Fully conforms to R.G.
C.6.f	5.1.2 Unpacking.	6.1.3 Unpacking.	None	Fully conforms to R.G.
C.6.g	5.1.3 Storage.	6.1.3 Storage.	None	Fully conforms to R.G.
C.6.h	5.2.3 Preoperational Case.	6.2.3 Preoperstional Case.	Preoperational case by IEEE 450-1972 for the endorsed IEEE and IEEE 450-1987 for the latest IEEE, both of which are identical.	Fully conforms to R.G.

Number & Section of R.G. 1.128, Rev 1	IEEE Standard Endorsed by R.G., Section and Title	Latest IEEE Standard, Section and Title	Major Difference	Conformance
C.6.i	5 3.1 Freshening Charge	6.3.1 Freshening Charge	The latest IEEE version on freshening charge criteria for cell specific gravity corrected to 77°F (25°C) applies to nominal 1.215 specific gravity. The endorsed version applies to any cell.	Fully conforms to R.G.
C.6.j	6 Records	7 Records	None	Fully conforms to R.G.

SSAR Appendix 1A will be revised as follows:

SSAR Revision:

Reg. Guide 1.106, Rev. 1, 3/77 - Thermal Overload Protection for Electric Motors on Motor-Operated Valves

C.1	IEEE 279-1971, Sections 4.1, 4.2, 4.3, 4.4, 4.5, 4.10, and 4.13	Exception	Regulatory Guide 1.106 endorses IEEE Std. 279-1971 (Reference 27), which has been ~~superseded by Reference 16~~ replaced by IEEE Std. 603-1980 (Reference 51). The AP600 uses the ~~latest~~ superceded version ~~of the industry standards (as of 1/90)~~. This version is not endorsed by a regulatory guide. The only safety-related electric motor-operated valves are dc.

(Refences)

50. ANSI/ANS 18.1-1984, Radioactive Source Term for Normal Operation of Light Water Reactors, 1984.

51. IEEE Std. 603-1980, IEEE Standard Criteria for Power Generating Stations, 1980.

Question 435.3

Section 8.3.1.1 of the SSAR states that, during plant startup, shutdown, and maintenance, the main ac power (normal) is provided by the preferred power supply from the switchyard through the main step-up transformer and two unit auxiliary transformers. In addition, an offsite maintenance power supply circuit is provided which is "site specific." Therefore, a second offsite power supply circuit should be provided as an interface.

A failure of the normal offsite power circuit in the passive plant designs will result in a loss of offsite power and the operation of the standby power sources or the operation of the passive safety systems if the standby power sources also fail. The staff recognizes that the loss of offsite power as well as standby sources (i.e. station blackout) may not degrade the passive safety systems, but it does challenge those safety systems. With a second offsite circuit also available, these challenges to the safety systems could be reduced.

The lack of a second offsite power source could also impact shutdown risk. If the configuration of the AP600 during shutdown is such that the passive make-up and decay heat removal systems are not available, then an increased importance is placed on the ac systems. The staff, therefore, concludes that a second offsite power circuit should be provided during power operation as well as during maintenance. This is consistent with the principle of defense-in-depth and the philosophy that the safety systems should not be unnecessarily challenged. Provide such a second offsite power circuit, or provide additional justification for not doing so.

Response:

The AP600 configuration during shutdown provides availability of RCS makeup and decay heat removal. The AP600 has been designed with a defense-in-depth philosophy. Operation of either of the two onsite standby ac sources provides power to essential defense-in-depth equipment and avoids challenges to safety systems. Additional levels of defense have a negligible effect on PRA results and are not warranted.

Westinghouse supports the Electric Power Research Institute (EPRI) position that a second offsite power source is not required for the AP600. This issue is identified in the April 24, 1992 Draft Safety Evaluation Report (DSER) of Volume III of the Utility Requirements Document (URD) as ALWR/NRC Open Issue P.11.O-4 which has not been resolved between EPRI and the NRC.

SSAR Revision: NONE

Question 435.10

Review and evaluate the alarm and control circuitry for the diesel generators to determine how each condition that renders a diesel generator unable to respond to an automatic start signal is alarmed in the control room. These conditions include not only the trips that lock out the diesel generator start and require manual reset, but also control switch or mode switch positions that block signals such as automatic start, loss of control voltage, insufficient starting air pressure or loss of battery voltage, etc. This review should consider all aspects of possible diesel generator operational conditions, for example, test conditions, and operation from the local control stations. One area of particular concern is the failure to reset the diesel generator controls for subsequent automatic operation following a manual stop at the local station which terminates a diesel generator test.

Provide the details of this evaluation and specifically address the following information:

a. all conditions that render the diesel generator incapable of responding to an automatic start signal for each operating mode as discussed above; and

b. any condition that renders the diesel generator incapable of responding to an automatic start signal which is not alarmed in the control room.

Response:

The diesel generators are automatically started and connected to the associated medium-voltage buses in the event of a loss of voltage on these buses as a result of a loss of preferred power source concurrent with the turbine-generator trip (SSAR Subsection 8.3.1.1.1, paragraph 8).

The following conditions are prerequisites for the diesel generator automatic start:

- Starting air pressure within acceptable limits
- DC control power availability for fuel oil valve solenoid operation/and the starting air motor solenoid
- Fuel supply availability
- Diesel generator controls in the automatic mode
- Diesel generator breaker lockout trip permissive not activated by any of the trouble conditions
- Engine prelubrication provided

Satisfactory status of these "prestart" conditions is continuously monitored, and any failure is annunciated in the main control room. The diesel generator-related remote annunciation points are shown in SSAR Table 8.3.1-1. The DC control power availability is also monitored in the main control room.

A detailed discussion of the required design features follows:

The starting air system has an accumulator that stores the pressurized air required for the diesel engine cranking power. The starting air compressor, one per diesel generator, keeps the accumulators pressurized. An alarm in the control room detects the low starting air pressure.

DC control power for the starting air valve and fuel oil valve solenoid operation is provided from the dc buses that are fed from the battery chargers and backed by the stationary battery bank. DC control power availability at the diesel generator control panel is continuously monitored, and loss of control power is annunciated in the control room. The standby generators have permanent magnet excitation, thus eliminating dc power requirements for the field flashing circuit.

Each diesel generator has a fuel day tank located in such a way that fuel to the engine is gravity-fed. The day tank fuel level is continuously monitored and annunciated for low level indication in the control room.

The diesel generators are normally maintained in the standby mode ready to accept the starting signal for auto start. The standby mode status is provided in the control room that monitors the diesel generator control switch AUTO position, and the MCR/local transfer switch MCR position.

If the diesel generator control switch (located in MCR) is not in the AUTO position, annunciation is provided to the control room operator. The MCR transfer switch is placed in the LOCAL position to allow local start for testing purposes. After test completion, if the MCR transfer switch is not repositioned to the MCR position, annunciation is provided in the control room (SSAR Figure 8.3.1-3).

The diesel generator breaker controls are provided with a lockout relay that would trip and lock out the breaker for selected electrical faults and the engine trouble conditions that may be detrimental to the unit operation. The lockout relay operation is annunciated in the control room.

Prior to automatic start, the engine must be prelubricated. The diesel engine prelubrication is continuously provided while in standby mode by a normal ac motor-driven lubrication pump backed by a dc motor. Should the ac motor pump fail, transfer to the dc-driven motor is automatic. A minimum level of oil in the cylinder block is required in order to fulfill the starting system interlock. Low oil level is annunciated in the control room.

A provision for jacket water and lube oil heating ensures engine-ready condition. A jacket water temperature signal is available for operator use.

The conditions that may render the diesel generator incapable of automatic start are monitored or alarmed in the control room.

SSAR Revision: NONE

Question 435.13

Non-safety related equipment necessary for plant recovery subsequent to the assumed 72-hour period should be designed for the expected environment during the 72-hour period. In addition, the electrical equipment should be designed for the expected environment for the period immediately following the 72-hour period during which the recovery operations must be performed. Provide the qualification provisions for this equipment.

Response:

The electrical equipment required to be operational following the 72-hour coping period is classified as Class 1E. This equipment will be qualified for the expected environment. For further clarification, see the responses to Q435.5 and Q435.62.

No non-safety-related equipment is needed for plant recovery from an accident condition to the safe shutdown condition. Therefore, the non-Class 1E electrical equipment is not required to be qualified for the expected environment during the 72-hour coping period.

SSAR Revision: NONE

Question 435.16

Section 8.3.1.1.2.3 of the SSAR states that each diesel generator unit is ready to start, accelerate to the rated speed, reach the rated voltage, and connect to the associated 4160 volt switchgear bus to accept the design load within 20 seconds on receipt of the start signal. Is this fast enough to preclude actuation of the passive systems following system transients or small LOCAs?

Response:

The start time for the diesel generators and actuation times for the non-safety-related defense-in-depth systems are fast enough to prevent actuation of the safety-related passive systems following transients or reactor coolant system leaks.

The non-safety-related defense-in-depth systems automatically actuate to prevent unnecessary actuation of the safety-related passive systems. The actuation timing of the safety-related passive systems is delayed to allow actuation of the non-safety-related defense-in-depth systems. The time delay includes actuation of the non-safety-related diesel generators and loading of the appropriate components on the diesel generators for events in which the preferred power source is lost. Table 8.3.1-2 lists the loads that automatically load on the diesel generators following generator startup and the associated time sequencing for loading.

For example, the startup feedwater system is used to maintain a heat sink with the steam generators following a transient with a loss of main feedwater. In this event, a delay is incorporated into the actuation logic for the safety-related heat sink, the passive residual heat removal heat exchangers, to allow time for the startup feedwater system to initiate recovery of the steam generator inventory. The time delay is sufficient for the non-safety-related diesel generators and the startup feedwater pumps to start. The time delay can be seen in the actuation logic for the passive residual heat removal heat exchangers as shown in SSAR Figure 7.3.1-1. For this specific case with a loss of preferred power, the diesel generators start within 20 seconds and the startup feedwater pumps are sequenced on 5 seconds later. The total time delay for passive residual heat removal heat exchanger initiation used in the AP600 safety analyses for this event is 45 seconds. This allows about 20 seconds for the pumps to come up to speed and the flow control valves to establish a minimum flow to the steam generators. The passive residual heat removal actuation logic does not initiate heat exchanger flow if either startup feedwater pump maintains sufficient flow to both steam generators.

The AP600 safety analyses do not credit accident mitigation benefits from the non-safety-related defense-in-depth active systems since they are not required in order to protect the plant during design basis events. However, the safety analyses include appropriate startup time delays for the safety-related passive systems and equipment based on actuation time delays for the associated non-safety-related defense-in-depth systems.

SSAR Revision: NONE

Question 435.30

Section 7.2.1 of the EPRI ALWR Utility Requirements Document states that, "the dc power supply system shall be designed with sufficient redundancy to ensure that, in the case of a loss of offsite power concurrent with a turbine trip, the loss of any plant battery or dc bus concurrent with a single independent failure in any other system required for shutdown cooling will not result in a total loss of reactor coolant capability." State whether the AP600 design conforms to this guidance, and, if not, justify the deviation.

Response:

Draft Safety Evaluation Report (DSER) Industry Position (ALWR/NRC OPEN ISSUES P.11.0.13) provides additional information related to the question asked in this RAI.

To address the NRC concern about the loss of a Class 1E dc or vital ac bus and industry concerns about plant availability, revision 4 of URD Section 7.2.1 is as follows:

> The Class 1E dc and vital ac power supply system shall be designed with sufficient redundancy to ensure that the loss of either a dc or a vital ac bus will not result in a plant transient and simultaneous loss of single failure protection in the system needed to respond to the event.
>
> Rationale:
>
> This requirement is a particular case of the generic statement of the single failure criterion, endorsed by the URD for the passive plants (see Chapter 1B, Subsection 3.11.1.4.2).

The Class 1E dc and uninterruptible power supply system is designed to accommodate component failures -- such as the loss of a battery charger, a battery, or an inverter -- without the loss of power to either the dc bus or the ac instrumentation and control power bus. As discussed in the response to Q435.31, a single failure of a battery, a battery charger, or an inverter will not de-energize the associated dc or ac buses; therefore, plant operation is unaffected.

The AP600 design satisfies the requirements of the proposed revision to Subsection 7.2.1 of the EPRI ALWR Utility Requirements Document since the loss of a Class 1E dc bus or ac instrumentation and control power bus will not result in a plant transient and the simultaneous loss of single failure protection for safety-related systems needed to respond to the event.

SSAR Revision: NONE.

Question 435.31

Failures of the uninterruptible power supply (UPS) system have been shown to constitute one of the main causes of forced plant outages. Verify that the failure or unavailability of a single battery, battery charger, or inverter will not result in a plant trip or a forced outage.

Response:

A failure or the unavailability of a single safety-related battery, battery charger, or inverter will not result in a plant trip or a forced plant outage of the AP600.

SSAR Subsection 8.3.2 provides a description of the dc power systems. The dc power systems include a spare Class 1E battery bank with a spare battery, battery charger, and permanently installed cable connections that allow the spare bank to be connected to the affected bus by a plug-in, twist-lock disconnect. The spare bank can be aligned to either the Class 1E or the non-Class 1E dc power system, if component failures occur.

Following a loss of either a Class 1E or non-Class 1E battery charger, which is normally providing power to the associated dc bus, the battery would immediately supply the bus, maintaining continuity of power to the affected dc bus. Following a loss of either a Class 1E or a non-Class 1E battery, the battery charger would continue to supply power to the dc bus. With the loss of either a battery charger or a battery, continuity of power to the associated dc bus is maintained. Therefore, there is no effect on plant operation since the spare battery bank can be aligned while the faulty component is repaired.

Following the loss of either a Class 1E or a non-Class 1E inverter, the associated dc bus remains energized and the dc loads are not affected. The 208Y/120-Vac instrumentation and control power bus associated with the failed inverter remains continuously energized. Each uninterruptible power supply (UPS) includes an inverter and a backup regulating transformer that can supply the associated instrumentation and control bus if the inverter fails. The UPS includes a static transfer switch that automatically transfers the bus to the regulated power source if power is unavailable from the inverter. A manual mechanical bypass switch is also included in the UPS to provide a second connection for the bus to the backup regulated power source when the inverter is removed from service for maintenance.

Therefore, with a failure of a single battery charger or a single battery, power is continuously maintained to the dc buses. With a failure of an inverter, power to the instrumentation and control power bus is automatically transferred to a regulated backup power source. With a single failure or the unavailability of these components, the associated buses remain energized, thereby preventing a plant trip or forced outage.

SSAR Revision: NONE

AP600

Question 435.34

Verify that non-safety loads will not be fed from the Class 1E dc systems. Describe the non-Class 1E dc systems.

Response:

The Class 1E dc distribution system design is in compliance with IEEE Standard 384 and NRC Regulatory Guide 1.75. There are no non-safety-related loads fed from the Class 1E dc systems. See SSAR Subsection 8.3.2.1.2 for the non-Class 1E dc and UPS system description.

SSAR Revision: NONE

Question 435.46

Most of the UPS vendors comply with specification requirements for total harmonic distortion (THD) with the provision that these requirements are met for linear loads. The loads used for digital control power supplies and computers in the AP600 are inherently non-linear in nature. Also, variable speed drive systems and fluorescent lighting blasts introduce harmonics into the plant distribution system. Indicate the protective measures taken so that the THD due to non-linear loads on power system will not affect the current and voltage waveform of the UPS system.

Response:

The problem of total harmonic distortion (THD) due to the nonlinear loads inherently present in the AP600 has been recognized. The UPS inverters have harmonic filters designed specifically to reduce the effects of large third, fifth, seventh and higher-order harmonics that may result from anticipated 100 percent nonlinear loads. To provide high-quality power from the UPS system, the inverters will be specified to power nonlinear loads with a crest factor of 2 or higher (ratio of peak to rms value).

The variable speed drives used for the steam generator feedwater pumps will have special filters to eliminate the introduction of harmonics into the distribution system. Also, the battery chargers will be furnished with output filtering to limit ripple currents feeding into the dc power supply for the inverters.

SSAR Revision: NONE

Question 435.48

IEEE Standard 485 states that the standard temperature for stating cell capacity is 25 °C (77 °F), and the temperature variations in the battery room should not result in an unacceptable degradation of battery performance. Show that the temperatures expected to occur during a loss of ac power of 72 hours will not exceed values compatible with the required performance of the batteries during such an event.

Response:

Battery sizing for the AP600 Class 1E dc and uninterruptable power supply system is based on the requirements established by IEEE Standard 485, "Recommended Practice for Sizing Large Lead Storage Batteries for Generating Stations and Substations," with appropriate margins accounting for aging, temperature effects, and design margin. With the loss of ac power conditions, the battery room temperatures are not expected to change significantly since the heat load in the room is very low (estimated to be less than 100 watts) and the room walls (2 to 3 feet thick and approximately 20 feet below ground) are initially at the battery room operating temperature of 70°F, providing substantial thermal inertia. Based on the limited thermal sources and sinks and the extremely large heat capacity of the battery room walls, ceiling, and floor, the temperature change in the battery rooms will be well within the capacity margins.

SSAR Revision: NONE

Question 435.52

Discuss whether the supply cables for dc powered components are sized to provide adequate voltage for proper operation during the individual component's worst-case operating condition. Worst-case conditions for a constant power load (such as an inverter) may occur at a reduced battery terminal voltage, in which case there will be an increase in load current. In addition, discuss whether the voltage drop for twice the length of feeder cables (from starter to motor) for compound wound motors was considered in the total voltage drop calculation (due to the necessity of switching the series field when reversing the valve motor).

Response:

The dc power cables for the AP600 will be selected to continuously carry 1.25 times the full-load current of the dc equipment. In calculating the full-load current of the dc equipment (such as an inverter), the worst-case operating condition occurring at a minimum battery terminal voltage of 105 Vdc will be considered.

In calculating the dc voltage drop in the motor circuits, twice the length of feeder cables (from starter to motor) will be considered for nonreversing dc motors and four times the length of feeder cables for reversing motors. The cable size of dc motor-operated valve circuits will be analyzed considering worst-case voltage drop and required starting torque.

SSAR Revision: NONE

Question 435.53

Highly inductive loads may generate surges when de-energized that, if not suppressed, may impress voltage spikes on the dc system. Describe the protection provided to suppress these surges.

Response:

The dc system will be protected from surges generated on the ac system by the isolation provided by the battery chargers and regulating transformers, which are power-regulating devices. To further ensure protection, this equipment will employ surge suppressors on its input as described in the response to Q435.40.

On the dc system, inductive loads are limited to relay and motor starter coils. Surge suppression devices will be installed across the coils to limit voltage spikes when the coils de-energize.

SSAR Revision: NONE

Question 435.54

DC motors, if operating, will contribute to the total fault current. The maximum current that a dc motor will deliver to a short circuit at its terminals is limited by the effective transient armature resistance (rd') of the motor. For dc motors of the type, speed, voltage, and size typically used in the nuclear power plants, rd' is in the range of 0.1 to 0.15 per unit. Thus, the maximum fault current for a short at the motor terminals will typically range from 7 to 10 times the motor's rated armature current. Therefore, it is conservative to estimate the maximum current that a motor will contribute to a fault as 10 times the motor full load current. When a more accurate value is required, the short circuit contribution should be calculated, using specific rd' data for the specific motor, or actual test data should be obtained from the motor manufacturer. For additional accuracy, the calculation should account for the resistance of the cables between the motor and the fault.

In the dc short circuit calculations for the AP600, have the contributions made by the dc motors been considered?

Response:

The AP600 design will consider the effective transient armature resistance (rd') data obtained from the motor manufacturer. In cases for which the specific rd' data is not available, 10 times the motor full-load current will be considered for the motor short-circuit current contribution.

Because of the large capacity of the AP600 Class 1E battery (4800 ampere-hour), the short-circuit current contribution to a fault from the battery is predominant over the contribution from the dc motors. There are only a few small motors (MOVs) connected to the Class 1E dc buses. As such, the short-circuit duty of the Class 1E dc distribution system is primarily dictated by the contribution from the battery. The AP600 Class 1E dc system utilizes fusible disconnect switches rated for 100,000A interrupting.

SSAR Revision: NONE

Question 435.55

In cases where the non-Class 1E power supply circuits are connected to the input terminals of the Class 1E distribution system, discuss whether the AP600 design includes Class 1E power regulating devices or Class 1E protective devices so as to isolate the Class 1E loads from out-of-tolerance power outputs from the non-Class 1E sources that exceed the rated values of the Class 1E loads.

Response:

The cases in which non-Class 1E power supply circuits are connected to Class 1E equipment are limited to the four regulating transformers and four battery chargers at the 480-Vac level.

These Class 1E battery chargers and regulating transformers are power regulating devices that isolate (through isolation transformers) their loads from variations in their input. This equipment will be supplied with output surge suppressors to limit feeder-induced voltage spikes and includes control circuits that will open the input circuit breaker if the source is outside the range of rated input values. Also, this equipment will be provided with shunt trips for the input breakers (see the response to Q435.65).

SSAR Revision: NONE

Question 435.56

Identify all Class 1E electrical equipment that may become submerged or wetted as a result of a pipe break. For all such equipment that is not qualified for service in such an environment, provide an analysis to determine the following:

a. The safety significance of the failure of this electrical equipment (e.g. both spurious actuation and loss of actuation function) as a result of flooding/wetting.

b. The effects on Class 1E electrical power sources serving this equipment as a result of such flooding/wetting, and

c. Any proposed design changes resulting from this analysis.

Response:

SSAR Section 3.11 of the SSAR discusses the environmental qualification of electrical and mechanical equipment. The environmental zones (equipment room locations) and the list of safety-related electrical and mechanical equipment are provided in SSAR Table 3.11-1.

In the event of potential flooding/wetting, one of the following criteria is applied for protection of equipment for service in such an environment:

- Equipment will be qualified for submergence due to flooding/wetting.
- Equipment will be protected from wetting due to spray.
- Equipment will be evaluated to show that failure of the equipment due to flooding/wetting is acceptable since its safety-related function is not required or has otherwise been accomplished.

See also the response to Q410.5.

SSAR Revision: NONE

Question 435.57

Provide the results of a review of the operating, maintenance, and testing procedures for the AP600 to determine the extent of usage of jumpers or other temporary forms of bypassing functions for operating, testing, or maintaining safety related electric power systems. Identify and justify any cases where the use of the above methods cannot be avoided. Provide the criteria for any use of jumpers for testing.

Response:

No jumpers or temporary forms of bypassing functions are required for normal operation of the safety-related electric power systems. There is a design objective to minimize the need for jumpers or temporary bypasses in the AP600.

The maintenance and testing procedures will be developed by the combined license applicant. The extent of usage of jumpers or other temporary forms of bypassing functions for testing or maintaining safety-related electric power systems will be addressed by the combined license applicant.

SSAR Revision: NONE

Question 435.58

Provide a listing of all dc or ac motor-operated valves in the AP600 design that require removing powe· in order to meet the single failure criterion. Provide the details of the design to accomplish this requirement (See E P ICSB-18).

Response:

The following valves require removal of power consistent with the requirements of BTP ICSB-18:

- Accumulator Motor-Operated Valves (PXS PL V027A&B): Isolation valves in the PXS accumulator discharge lines have power removed in the open position during normal operation, as discussed in SSAR Subsection 6.3.2.2.7.5. Power is removed from the valves at the motor control center.

- IRWST Gravity Injection Line MOV (PXS PL V121A&B): The isolation valves for gravity injection of the IRWST have power removed in the open position during normal operation. The removal of power ensures IRWST injection following reactor coolant system depressurization to provide long-term cooling. Power is removed from the valves at the motor control center.

- PRHR Heat Exchanger Inlet Isolation Valve (V101): The inlet isolation valve to the PRHR heat exchanger provides emergency core decay heat removal for non-LOCA events. The removal of power from the isolation valve ensures the capability of heat removal under high pressure and temperature conditions in the reactor coolant system. Power is removed from the valve at the motor control center.

Although not required for single-failure purposes, power is removed from the normal RHR suction isolation valves (V001A&B and V002A&B) to minimize the potential for an intersystem LOCA. The reactor coolant system inner and outer isolation valves in the normal residual heat removal path (RNS) have power removed during normal operation, as discussed in SSAR Subsections 5.4.7.3.3.1 and 5.4.7.2.2. Power is removed from these valves at the motor control center.

SSAR Revision: NONE

AP600

Question 435.59

With regard to the safety-related electrical and control drawings and diagrams, provide the physical layout and cable interconnecting drawings to assist the staff's evaluation of the AP600 design with respect to the physical separation criteria for Class 1E systems, components and penetrations in the plant. Include how physical separation and electrical independence of the channels/divisions are maintained in distributed logic systems using multiplexing techniques.

Response:

The physical separation and electrical independence of the Class 1E power system are described in SSAR Subsections 8.3.2.3 and 8.3.2.4. The physical layout of the Class 1E batteries, electrical equipment room, electrical penetrations, and I&C cabinets is shown in SSAR Figures 1.2-4 th ugh 1.2-8. The interconnections of Class 1E power equipment are shown in Figures 8.3.2-1 and 8.3.2-2.

SSAR Subsection 7.1.2 describes the general protection subsystem configuration of the instrumentation and control systems and discusses how the electrical independence of the channels and divisions is maintained. WCAP-13382 Section 4.0.7 describes the electrical isolation features utilizing fiber optics. SSAR Figures 7.1-2 throug 1-22 provide I&C subsystems architecture and block diagrams illustrating the electrical independence of the channels/divisions and subsystem interconnections.

SSAR Revision: NONE

Question 435.62

The SSAR states that the low voltage ac distribution system provides power to the Class 1E battery chargers and the UPS. It also provides the capability to connect a portable diesel generator to supply power to dc safety-related loads and vital ac loads via the Class 1E battery charger and inverter after a 72-hour coping period upon a complete loss of all ac power. Discuss the provisions for connection of the diesel generator, the provisions for its availability, and the provisions made to ensure that the on-site distribution systems are not damaged due to events such as earthquakes or fires.

Response:

The AP600 design does not require Class 1E dc power sources after the 72-hour coping period. After the 72-hour coping period, 120-Vac power allows operation of the postaccident monitoring system, emergency lighting system, hydrogen recombiners, and ventilation equipment. The 120 Vac power is supplied from the transportable generators through the Class 1E regulating transformers, as discussed in SSAR Subsection 8.3.1.1.1. The Class 1E battery chargers and inverters are not connected to the portable generators.

Each portable generator is provided with a distribution panel mounted on its skid. This panel includes circuit breakers and plug-type, twist-lock connectors for connecting the required loads, utilizing prefabricated cables.

The portable generators will be stored offsite in a location from which they can be retrieved within 72 hours.

The ventilation equipment to be connected to the portable generator is also portable and is stored offsite with the generators and prefabricated cables. No onsite distribution systems are required to support the portable loads. Connections to these loads are made with plug connectors mounted on the equipment.

The post accident monitoring system and the main control room emergency lighting are fed from a regulating transformer. The regulating transformer and the hydrogen recombiner containment penetration electrical connections are the safety-related connection points for the portable generators. The essential Class 1E systems are designed to withstand the design basis earthquake and are protected against unacceptable damages due to fires. Connection to the regulating transformer is made with a plug connector mounted in the regulating transformer enclosure. A plug connector mounted in a seismically qualified terminal box designed to provide power through a containment electrical penetration is used to make the connection to the containment hydrogen recombiner. The associated cables will be routed in seismically supported raceways.

SSAR Revision: NONE

AP600

Question 435.66

Section 8.3.2.4.2 of the SSAR states that non-Class 1E circuits are electrically isolated from Class 1E circuits, and Class 1E circuits from different separation groups are electrically isolated by isolation devices. Describe the types of the isolation devices used in the AP600 design for this application.

Response:

Electrical isolation between the non-Class 1E and Class 1E system power circuits is provided by the Class 1E battery charger and the Class 1E regulating transformer, as discussed in the response to Q435.65. For control and low-energy signal circuits, a fiber optic coupler is generally used as an isolation device. WCAP-13382, Section 4.0.7, discusses electrical isolation features utilizing fiber optic isolation for outputs used for communication between safety divisions and from safety-grade to non-safety-grade cabinets. SSAR Subsections 7.1.2.11, 7.1.4.2.6, and 7.1.4.2.7 discuss isolation devices and their application in the AP600 I&C architecture.

SSAR Revision: NONE

Question 435.67

Recent experience with electrical system equipment protective relay applications has established that relay trip setpoints can drift and result in premature trips of the equipment. Provide a description of the provisions that avoid incorrect initial setpoint selection and protective relay trip setpoint drift.

Response:

The only Class 1E electrical system in the AP600 is the 125-Vdc and UPS system, which uses fuses and molded-case circuit breakers for the protective trip functions. Electromechanical type auxiliary relays are used for alarm functions only. Fuses and molded-case circuit breakers do not present setpoint drift problems.

For the non-Class 1E ac power system, solid-state relays typically are used for the protective trip functions. The solid-state relay trip setpoint stays within the manufacturer's tolerance limit. Electromechanical relays are used only where suitable solid-state relays are not available. Design calculations will be performed to determine initial relay trip setpoints considering the following factors:

- Repeatability
- Tolerance

SSAR Revision: NONE

Question 435.73

Address the grounding system and lightning protection features for the AP600.

Response:

The AP600 grounding system will comply with the guidelines provided in IEEE Standard 665-1987, "Guide for Generating Station Grounding." The grounding system consists of the following four subsystems:

- Station grounding grid
- System grounding
- Equipment grounding
- Instrument/computer grounding

The station grounding grid subsystem consists of buried, interconnected bare copper conductors and ground rods (Copperweld) forming a plant ground grid matrix. The subsystem will maintain a uniform ground potential and limit the step-and-touch potentials to safe values under all fault conditions.

The system grounding subsystem provides grounding of the neutral points of the main generator, main stepup transformers, auxiliary transformers, load center transformers, and onsite standby diesel generators. The main and diesel generator neutrals will be grounded through grounding transformers providing high-impedance grounding. The main stepup and load center transformer neutrals will be grounded solidly. The auxiliary (unit and reserve) transformer secondary winding neutrals will be resistance grounded.

The equipment grounding subsystem will provide grounding of the equipment enclosures, metal structures, metallic tanks, ground bus of switchgear assemblies, load centers, MCCs, and control cabinets with two ground connections to the station ground grid.

The instrument/computer grounding subsystem will provide plant instrument/computer grounding through separate radial grounding systems consisting of isolated instrumentation ground buses and insulated cables. The radial grounding systems will be connected to the station grounding grid at one point only and will be insulated from all other grounding circuits.

For the lightning protection system description, see the response to Q435.64.

The design of the grounding grid system and the lightning protection system depends on the soil resistivity and lightning activity in the area. Therefore, the design of both systems is site-specific and is the responsibility of the combined license applicant.

SSAR Revision: NONE

Question 460.12

Provide justification for concluding that the exhausts to the environment from the personnel areas in the Annex I building, electrical and mechanical equipment rooms in the Annex I and auxiliary buildings, and the diesel generator rooms will not be radioactive and, therefore, need not be monitored. (Sections 9.4 and 11.5)

Response:

Justification for not monitoring exhausts for radiation from the personnel areas in the annex I building, electrical and mechanical equipment rooms in the annex I and auxiliary buildings, and diesel generator rooms follows.

Diesel Generator Rooms

The diesel generator rooms are in a stand-alone diesel generator building, which is separate from any other plant building. Outside air is utilized for building ventilation. The building houses only the diesel generators and mechanical and electrical components directly related to diesel generator operation. The building does not store, utilize, or contain any radioactive materials.

The building does not contain any radioactive materials and has no potential for the transfer of radioactive materials from other buildings via piping, ductwork, or building connections. Since any exhaust from the building to the environment has no potential for radioactivity, monitoring is not required.

Annex I Building Personnel Areas and Equipment Rooms and Auxiliary Building Electrical Rooms

The annex I building personnel areas occupy the first and second floors of the building. The electrical and mechanical rooms are on the second and third floors of the annex I building. A partial third floor of the annex I building contains an HVAC equipment room. Portions of the annex I building are adjacent to the annex II building; however, the majority of the building walls and the entire roof are not adjacent to any other building or plant area.

Interfaces with the adjacent buildings are limited to doorways, airlocks, and ductwork. Doorways from the annex I building open to clean areas of the annex II building. Ductwork connecting the annex I building and adjacent areas consists entirely of supply air ductwork handling outside air for the fuel handling area, health physics area, containment purge supply, and main control room. The main control room supplemental air filtration unit is in the HVAC equipment room; however, this unit has no radioactive material during normal plant operation.

The annex I building general area HVAC system normally maintains the personnel areas at a slightly positive pressure with respect to adjacent areas.

The auxiliary building contains two electrical penetration rooms and two reactor trip switchgear rooms that are served by the annex/auxilliary nonradioactive ventilation system. These rooms are on elevations 100' and 117'-6" of the auxiliary building adjacent to a controlled access corridor for the main control room, main control room areas, and other electrical equipment areas.

The areas do not contain any radioactive materials. The potential for the transfer of radioactive contamination from adjacent areas is prevented through interfaces with only clean areas and through general pressurization of the annex 1 building. No potentially contaminated ductwork is contained in the areas. Therefore, any exhaust from the areas to the environment has no potential for radioactivity. Monitoring is not required.

SSAR Revision: NONE

Question 630.1

Section 16.2.1.1 of the SSAR states that both phases of the RAP include the safety-related plant SSCs which are identified as risk-significant in the AP600 PRA, and also include several non-safety-related systems that provide defense-in-depth or that are used in the PRA evaluation to provide credit for event mitigation. This section further states that the AP600 RAP begins during the design stage (D-RAP) and continues throughout plant operation (O-RAP).

a. The staff's position is that RAP provides a commitment to include all risk-significant SSCs throughout plant life, using PRA and other industry sources to identify and prioritize those SSCs that are important to risk. Limiting the RAP to those SSCs that are identified in the AP600 PRA is too narrow a scope for the RAP; other industry sources should also be used and considered, as discussed in Section 16.2.3.2 of the SSAR. Therefore, revise Section 16.2.1.1 of the SSAR to be consistent with Section 16.2.3.2 regarding the use of other sources in identifying risk-significant SSCs.

b. It appears that the terms "risk-significant SSCs" and "safety-related and important non-safety-related systems that provide defense-in-depth or that are used in the PRA evaluation to provide credit for event mitigation" are used interchangeably. Consistent use of the term "risk significant SSCs" is preferred by the staff. Therefore, revise Section 16.2.1.1 of the SSAR so that consistent terminology is used.

c. The scope of the RAP should be consistent with 10 CFR 50.65 (the maintenance rule). A RAP should encompass those SSCs identified as those that (1) are relied upon to remain functional during and following a design-bases accident to ensure that the integrity of the reactor coolant pressure boundary is maintained; (2) retain the capability to shutdown the reactor (required to take the plant from hot shutdown to cold shutdown) or mitigate consequences of accidents; (3) prevent a safety system from performing its intended safety function; (4) could directly cause a reactor scram or actuation of a safety system; and (5) are used in plant Emergency Operating Procedures (EOP). Revise Section 16.2.1.1 of the SSAR to state that the scope of the RAP should be consistent with that of 10 CFR 50.65 (the maintenance rule).

Response:

a. The industry effort underway to resolve the issue involving the regulatory treatment of non-safety systems will include a process to identify risk-significant structures, systems, and components. When the process is finalized, Section 16.2 will be revised to include the SSCs identified as risk-significant.

b. See the response to item a.

c. The maintenance rule as required by 10 CFR 50.65 is the responsibility of the combined license applicant. While it is believed that the RAP program described in Section 16.2 is consistent with the maintenance rule, it is not the purpose of this program to establish compliance with 10 CFR 50.65. NUMARC is working to develop an industry position and guidelines for compliance with the maintenance rule. All or portions of the

RAP may be appropriate for establishing compliance with the maintenance rul. in accordance with the industry guidelines.

SSAR Revision: NONE

Question 630.2

Section 16.2.2 of the SSAR states that the objective of the two-phase Reliability Assurance Program is to design reliability into the plant and to maintain the AP600 reliability consistent with the PRA evaluations.

The staff position is that the objective of the RAP is to (1) identify the plant SSCs that are significant contributors to plant safety, as quantified by the PRA and other sources, (2) ensure that the plant design provides SSCs that are at least as reliable as those assumed in the PRA, and (3) ensure that the risk-significant SSCs are built and operated throughout plant life at least as reliably as assumed in the PRA. Once the risk-significant SSCs have been identified, the D-RAP should describe the process for achieving this overall objective and should also identify key assumptions regarding any operation, maintenance and monitoring activities that a referencing COL applicant should consider in developing its O-RAP.

State in greater detail what the objective of the RAP is in Section 16.2.2 of the SSAR, including the objective of the D-RAP and O-RAP.

Response:

SSAR Subsection 16.2.2 will be revised as follows:

SSAR Revision:

16.2.2 Objective

The objective of the two-phase Reliability Assurance Program is to design reliability into the plant and to maintain the AP600 reliability consistent with the ~~PRA evaluation~~ NRC safety goals.

The following goals have been established for the D-RAP:

- Provide a mechanism for establishing baseline reliabilities for SSCs consistent with the NRC Safety Goals
- Provide a mechanism for establishing baseline reliabilities for SSCs consistent with the defense-in-depth functions to minimize challenges to the safety-related systems
- Provide information to be used by a combined license applicant for ongoing plant reliability assurance activities

The O-RAP is the responsibility of the combined license applicant. The purpose of the O-RAP is to ensure that reliability is maintained consistent with overall safety goals and that the capability to perform safety functions is maintained. Individual component reliabilities are expected to change throughout the course of plant life because of aging and of changes in suppliers and technology. Changes in individual component reliabilities are acceptable

as long as overall plant safety performance is maintained within the NRC safety goals and the deterministic licensing design bases.

The following goals for the O-RAP are provided:

- Provide reasonable assurance that the SSCs included in the O-RAP are maintained in such a way that the intended safety, accident mitigation, and defense-in-depth functions can be performed and that maintenance is managed to achieve acceptable availability

- Focus resources and priorities on systems commensurate with their importance to safety

Question 630.3

Section 16.2.3.1 of the SSAR states that the AP600 design organization described in Section 1.4 of the SSAR formulates and implements the AP600 D-RAP.

The staff concludes that the description of the design organization should include the organizational and administrative aspects applicable to the D-RAP, including a discussion on organizational accountability for implementing the design portion of a RAP, and means for disposition of vendor and plant design organization equipment recommendations. The D-RAP should describe the programmatic interfaces (i.e., how various parts of the design organization interface). The description of the design organization should include how the performance of risk-significant SSCs, when compared to that specified in PRA, will be fed back to the designer to resolve reliability discrepancies.

The staff position is that the D-RAP applies to the certified design applicant and the design entity that completes the site-specific portions of a plant (e.g., an architect/engineer (A/E) under contract or a COL applicant acting as its own A/E). Provide a discussion regarding the D-RAP and its applicability to an architect/engineer in Section 16.2.3.1 of the SSAR.

Response:

SSAR Subsection 16.2.3.1 will be revised to provide additional information related to organizational and administrative aspects applicable to the D-RAP.

The AP600 design process involved integration of design activities and PRA risk evaluation of the design. The PRA report and the response to Q720.2 provide an overview of the integrated design and risk evaluation process used for the AP600.

Westinghouse agrees with the NRC staff position that the D-RAP is applicable to the responsible design organization until such time as the O-RAP is in place during plant implementation. This includes the Combined License applicant and the design entity that completes the site-specific portions of the plant.

SSAR Subsection 16.2.3.1 will be revised as follows:

SSAR Revision:

16.2.3.1 The AP600 Design Organization

The AP600 design organization described in Section 1.4 formulates and implements the AP600 D-RAP.

The AP600 Program Director and his management staff are responsible for the AP600 design and licensing.

The AP600 staff coordinates the program activities including those performed within Westinghouse, as well as work completed by the supporting organizations, including architect-engineers, listed in SSAR Section 1.4. The NSSS engineering is the direct responsibility of the AP600 staff, with support from diverse engineering functional groups within Westinghouse. The balance-of-plant engineering is completed by external organizations under the guidance and direction of the AP600 staff.

The AP600 staff is responsible for development of the D-RAP and the various design, analyses, and risk and reliability engineering required to support development of the D-RAP. The AP600 safety analyses are completed by the nuclear safety analyses section of Westinghouse. Reliability analyses for the AP600 systems are performed by the reliability engineering section of Westinghouse. The PRA evaluation is the responsibility of the risk analysis section of Westinghouse. The risk and reliability analyses are performed using common data bases provided from within Westinghouse and from industry sources such as INPO and EPRI. The AP600 staff coordinates the system and component design, safety analyses, reliability analyses, and risk analyses to ensure integration.

Question 630.4

Section 16.2.3.3 of the SSAR states that extensive efforts are involved in optimizing the AP600 design for operational availability as well as safety. This section also discusses that the use of consistent reliability information provides confidence that the calculated system availabilities are based on the same data and assumptions as the PRA evaluation. Whenever an alternative design is proposed to improve performance in either area, the revised design is first reviewed to provide confidence that the current assumptions in the other areas are not violated. Additionally, Section 16.2.3.3 of the SSAR states that the identification and prioritization of the various possible failure modes for each component leads to suggestions for failure prevention or mitigation, and that this information is provided as input to the O-RAP because it defines the means by which component reliability can be maintained. The final designs approved for construction reflect the reliability requirements assumed in the design and PRA as part of their procurement specifications.

Although extensive efforts are involved in optimizing the AP600 design for operational availability as well as safety, these objectives may, at times, be conflicting (e.g., operational availability goals may be in conflict with the plant safety goals). The staff's position is that it should be clearly stated that safety goals take priority over other goals whenever a potential conflict exists. Revise Section 16.2.3.3 of the SSAR to explicitly state that plant safety goals take priority over other goals.

Response:

Westinghouse is committed to meeting the NRC safety goals.

SSAR Subsection 16.2.3.3 will be revised as follows:

SSAR Revision:

16.2.3.3 Design Considerations

Extensive efforts are involved in optimizing the AP600 design for operational availability as well as safety. The use of consistent reliability information provides confidence that the calculated system availabilities are based on the same data and assumptions as the PRA evaluation. Whenever an alternative design is proposed to improve performance in either area, the revised design is first reviewed to provide confidence that the current assumptions in the other areas are not violated. Whenever a potential conflict exists between safety goals and other goals, these conflicts are ~~always~~ resolved with priority placed on the ~~to provide~~ protection of ~~for~~ the health and safety of the public.

As part of the design process, risk-significant components are evaluated to determine their dominant...

Question 630.5

In order for the staff to ensure a workable reliability assurance program has been proposed at the design stage, provide one example of how the AP600 RAP would be implemented (e.g., from the design phase through the end of the operating phase) using a specific SSC identified as risk-significant in the PRA. In the example, identify where the interface occurs between the D-RAP (including the A/E) and the O-RAP. In addition, does the Westinghouse AP600 RAP description differ from the EPRI ALWR Requirements Document (Volume III) description of a RAP? If so, describe the differences.

Response:

Revisions to the ALWR requirements document description of the RAP are currently undergoing industry review. Westinghouse is working with the industry to develop an appropriate set of requirements applicable to the RAP. The AP600 RAP will be modified based on the finalized requirements.

Following is an example of D-RAP implementation for the accumulator tank portion of the passive core cooling system. This example is based on the current ALWR requirements document.

Example of D-RAP Implementation

The accumulator tank portion of the passive core cooling system is presented as an example of D-RAP implementation. The accumulator tanks provide rapid injection of borated water following a large loss of coolant accident. They are modeled in the AP600 PRA analysis for this event, and play an important role in the plant response.

System Description

The accumulator subsystem consists of two large, spherical tanks containing borated water and pressurized by nitrogen cover gas. The tanks are inside the containment building, and the discharge from each tank is connected to one of the direct vessel injection lines. Additional details of the system design can be found in SSAR Section 6.3, Passive Core Cooling System.

System Operation

During normal operation, each accumulator is isolated from the reactor coolant system by the two series check valves in the direct vessel injection line. The motor-operated isolation valve is normally open, with control power removed.

During a large loss of coolant accident, when reactor coolant system pressure falls below the accumulator pressure, the check valves open and borated water is forced into the reactor coolant system by the gas pressure.

Additional details pertaining to system operation can be found in SSAR Section 6.3, Passive Core Cooling System.

System Fault Tree Results

The accumulator subsystem of the passive core cooling system is important in reducing plant risk as determined in the PRA evaluation. The following list contains typical component failure mechanisms that are considered in the PRA evaluation:

- Check valve A fails to open
- Check valve B fails to open
- Gas relief valve fails open/leaks
- Check valve external leak
- Fill valve external leak
- Motor-operated isolation valve spuriously closes
- Vessel rupture

The PRA results rank these potential mechanisms in order of their importance.

Design Implementation

The SSCs identified by the PRA evaluation for the accumulator subsystem are submitted to D-RAP implementation. If the results of the PRA are not acceptable or if the system availability is not acceptable, or both, then the system is a candidate for redesign.

For most of the failures included in the PRA, the failure mode is also provided. Failure Modes and Effects Analysis (FMEA) for the components provides information about failure modes and causes. With this information, the designer investigates alternatives if required to meet the PRA reliability assumptions and plant availability goals.

If any design change is made to improve component or system reliability, then that change is factored into the reliability analysis. The reanalysis verifies that the change provides the desired reliability or indicates that additional design changes are required.

Based on the dominant failure modes and likely causes identified, the designer provides recommendations for surveillance and maintenance aimed at preserving the component reliability assumed in the final design.

When the design meets both the PRA reliability assumptions and plant availability goals, then the limiting reliability assumptions are preserved for inclusion with the procurement specifications for a component and for inclusion in the O-RAP.

SSAR Revision: NONE