Westinghouse Electric Corporation
Energy Systems
Box 355
Pittsburgh Pennsylvania 15230-0355

NTD-NRC-94-4264
DCP/NRC0187
Docket No.: STN-52-003

August 12, 1994

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 April 15, 1994, May 5, 1994, May 16, 1994, and June 8, 1994. In addition, revisions of responses previously submitted are provided.

A listing of the NRC requests for additional information responded to in this letter is contained in Attachment A.

These responses are also provided as electronic files in WordPerfect 5.1 format with Mr. Kenyon's copy.

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 And Licensing Activities

/nja

Enclosure

cc: B. A. McIntyre - Westinghouse
T. Kenyon - NRR

180088

2019A

E004
1/1

NTD-NRC-94-4264
ATTACHMENT A
AP600 RAI RESPONSES
SUBMITTED AUGUST 12, 1994

RAI No.	Issue
260.012R01	Quality assurance on D-RAP systems
410.120	CCS criteria
440.056	Instrumentation available during shutdown/midloop
440.162	RVLIS
440.219	RCS makeup in steamline break event tree
440.225	Sequences of LOOP event tree with PRHRS success
440.228	Effect of pzr safety valve flow on CMT operation
440.231	Deboration during startup; LOOP during deboration
440.239	Wide range level instrumentation
440.240	Time available to restore offsite power
440.241	RCS conditions 2 hours after loss of RNS
460.001R01	Liguid waste management
460.002R01	Steam generator blowdown rates
460.014R01	SG blowdown & CCW radiation monitors
620.036R01	Verification and validation
620.048R01	SPDS

Response Revision 1

Question 260.12

Table 16.2-1 of the SSAR describes those D-RAP non-safety-related systems that provide defense-in-depth or that are used in the PRA evaluation to provide credit for event mitigation. Table 3.2.3 shows, by AP600 class, those systems for which Appendix B of 10 CFR Part 50 applies including most of the D-RAP systems. Describe the quality assurance requirements for those D-RAP systems of the AP600 that are not covered by Table 3.2-3.

Response:

SSAR Revision 1, dated January 1994, includes ~~revisions to Table 16.2-1 to reflect the implementation of the regulatory treatment of nonsafety-related systems process~~ a reference to WCAP-13856 (SSAR Reference 2, see Subsection 16.2.6). The RTNSS process implementation is documented in WCAP 13856. The nonsafety-related systems identified by the RTNSS process as important are ~~included in Table 16.2-1~~identified in WCAP-13856 and are included in the D-RAP. These nonsafety-related systems are classified as AP600 Class D. This classification corresponds to Quality Group D of Regulatory Guide 1.26. The quality standards identified by the regulatory guide as applicable to Quality Group D SSC are applied to those AP600 SSCs classified as AP600 Class D except AP600 applies API 610 or Hydraulic Institute Standards to pumps instead of "manufacturers standards" as recommended by Regulatory Guide 1.26. In addition, AP600 applies NEMS MG1 1972 (National Electric Manufacturers Association) to ac motors and generators, and ANSI/IEEE C37, 1989 to circuit breakers, switchgear, relays, substations, and fuses. These items are not addressed in Regulatory Guide 1.26.

Quality assurance requirements for the diverse actuation system are discussed in the response to RAI 260.14.

SSAR Revision: NONE

AP600

Question 410.120

In WCAP-13856, the AP600 RTNSS evaluation identified that the component cooling water system (CCS) provides defense-in-depth functions during shutdown, reduced inventory operations. Demonstrate that the following criteria are met by the system, or justify the deviation, if any.

a. Does the CCS have an electric supply from both normal station ac and on-site non-safety-related ac power supplies that is separated, to the extent practicable?

b. Is the CCS designed and arranged for conditions or an environment anticipated during and after events to ensure functional operability, maintenance accessibility, and plant recovery?

c. Is the CCS protected against internal flooding and other in-plant hazards, such as the effects of pipe ruptures, jet impingement, fires, and missiles?

d. Can the CCS withstand the effects of natural phenomena that have a reasonable likelihood? Important systems and components should be designed to remain functional after a natural phenomena, such as a seismic event, that is of reasonable likelihood or may persist longer than 72 hours.

e. Is there a quality assurance program applied to the CCS that follows guidelines comparable to those of Generic Letter 85-06 for ATWS, and Appendices A and B of Regulatory Guide 1.155, "Station Blackout," for station blackout non-safety-related equipment?

f. Is the CCS included in the reliability assurance and maintenance programs for proper maintenance, surveillance, and inservice inspection and testing to ensure the system's reliability is consistent with the determined goals for this system?

g. Does the CCS have availability control mechanisms, including allowable outage time and surveillance requirements?

h. Does the CCS have proper administrative controls for shutdown configurations?

i. Does the CCS have sufficient redundancy to ensure defense-in-depth functions, assuming a single active failure of equipment or unavailability due to maintenance.

AP600

Response:

The component cooling water system (CCS) performs no safety-related function except for containment isolation and need not meet the listed criteria which are applicable to safety-related systems. However, the following provides component cooling water design information in response to the listed requests.

a. Each of the two CCS pumps and associated active components are supplied from independent, permanent, nonsafety-related electrical buses. Each bus is capable of being supplied from one of two onsite standby diesel generators. The onsite standby diesel generators and permanent onsite 4160 volt buses are physically separated. No separation is required or provided for the 480 volt load centers or the supply cables for the system electrical loads.

b. The CCS containment penetrations and isolation valves have been designed and arranged for conditions anticipated during or after events to ensure functional operability, maintenance accessibility and plant recovery. The design of the nonsafety-related portions of the CCS does not ensure functional operability, maintenance access or support plant recovery following design basis events. Maintenance accessibility is provided consistent with the pump nonsafety-related functions and plant availability goals.

c. Except for the safety-related containment isolation functions, protection from internal hazards is neither required or provided for the CCS.

d. Except for its containment isolation function, the CCS is not protected from natural phenomenon and is not required to remain functional after a natural phenomenon. There is no requirement for CCS functionality after 72 hours following an event.

e. As a defense-in-depth system, the CCS is classified as an AP600 Class D system. As discussed in SSAR Subsection 3.2.2.6, this classification invokes industrial quality assurance and industry design standards. The portions of the CCS that perform the containment isolation function are classified as AP600 Class B. As discussed in SSAR Subsection 3.2.2.4, this classification invokes 10 CFR 50, Appendix B.

f. The extent of CCS inclusion in reliability assurance and maintenance programs is discussed in SSAR Subsection 3.2.2.6 for Class D structures, systems and components. The Reliability Assurance Program is further described in SSAR Section 16.2 and includes a discussion of the applicability to the nonsafety-related defense-in-depth systems, which includes the CCS.

g. Except for the containment isolation valves, the CCS does not have technical specification availability control mechanisms (i.e., limiting conditions for operation) nor allowable outage times or surveillance requirements. This system is not safety-related and not required for plant shutdown, and therefore not required to have technical specifications. The CCS function of supplying cooling flow to the normal residual heat removal system during reduced reactor coolant system inventory, midloop operations, is identified as an RTNSS-significant function in Reference 410.120-1. This reference also provides short-term availability recommendations for the equipment used to support this function.

h. Reference 410.120-1 provides recommended availability controls for those portions of the CCS that perform RTNSS-significant functions during reduced reactor coolant inventory operations.

i. Appropriate redundancy is provided such that the CCS can support normal operation and defense-in-depth functions assuming a single active component failure.

Reference:

410.120-1 WCAP-13856, AP600 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process. September 1993.

SSAR Revision: NONE

Question 440.56

a. Provide a description of plant instrumentation designed to operate properly during shutdown and mid-loop operations. The instrument accuracy, availability, appropriateness of key parameters (RCS level, RCS temperature, and RHR system performance), and the intended monitoring ranges should be addressed for shutdown operations.

b. Identify any deviations, and provide the technical bases and justification for these deviations, from the guidance of NUREG-1449 (Page xiii, Sections 6.6.1.1 and 7.3.3 of the report) that requests each plant to provide an independent and diverse means of accurately monitoring RCS water level, the capability to continuously monitor decay heat removal system (DHR) when a DHR system is being used for cooling the RCS, and visible and audible indications of abnormal conditions in temperature, level, and DHR system performance (see also Q440.53, Q440.55, Q440.58, Q440.71, and Q440.72).

c. Identify safety- and non-safety-related instruments used during shutdown operations. For the safety-related instruments, confirm that the instruments will be within the scope of environmental qualifications and quality assurance criteria. For non-safety-related instruments, provide a description of the quality assurance program that will be used to provide instruments with accurate information in the expected ranges of shutdown measurement that will enhance operator confidence in the instruments, and the training program for operators to understand and interpret data provided by the instruments.

Response:

a. The following table includes the RCS and related instrumentation that operate during shutdown. Instrument channel accuracy will be dependent on final intrument selection.

Instrumentation Description	Safety Class	Number of Channels	Approximate Range	Comments
RCS Hot Leg Wide Range Temperature	C	1 per hot leg	0 - 700°F	Available during shutdown operations including mid-loop
RCS Cold Leg Wide Range Temperature	C	1 per cold leg	0 - 700°F	Available during shutdown operations except for mid-loop
Core Exit Thermocouples	C	2	200 - 2200°F	Available during shutdown operations including mid-loop
RCS Wide Range Pressure	C	4	0 to 3300 psig	Available during shutdown operations including mid-loop

Instrumentation Description	Safety Class	Number of Channels	Approximate Range	Comments
RCS Hot Leg Level	C	1 per hot leg	Bottom of hot leg to top of hot leg bend into SG	Available during shutdown operations including mid-loop
Pressurizer Wide Range Level	E	1	Top of pressurizer to bottom of hot leg	Available during shutdown operations including mid-loop
RCS Flow	C	4 per cold leg	0 - 120%	Available during RCP operation (RCS temperature > 160°F)
Reactor Coolant Pump Speed	C	1 per pump	0 - 120%	Available during RCP operation (RCS temperature > 160°F)
Reactor Coolant Pump Bearing Temperature	C	4 per pump	70°F - 450°F	Available during RCP operation (RCS temperature > 160°F)
Reactor Coolant Pump Vibration	E	2 per pump		Available during RCP operation (RCS temperature > 160°F)
Reactor Coolant Pump Stator Temperature	E	1 per pump		Available during RCP operation (RCS temperature > 160°F)
RHR Pump Suction and Dicharge Pressure	D	4	0 - 900 psig	Available during shutdown after the RNS is aligned
RHR Heat Exchanger Inlet and Outlet Temperature	D	4	0 - 450 °F	Available during shutdown after the RNS is aligned
RHR Pump Discharge Flow	D	2	0 - 3000 gpm	Available during shutdown after the RNS is aligned

b. The AP600 conforms to the guidance of NUREG-1449 as follows:

NUREG Guidance:

" ...provide an independent and diverse means of accurately monitoring RCS water level...."

AP600 Conformance:

Independent hot leg level channels are available to measure the level in each hot leg. In addition, independent and diverse instrumentation are available to provide an indication of core cooling during mid-loop operations. As shown in the above table, the AP600 provides diverse indication of core cooling via the core exit thermocouples, the hot leg wide range temperature, hot leg level, and RNS flow and temperature.

The AP600 provides diverse means of core cooling during mid-loop. The normal RHR system provides decay heat removal during shutdown including mid-loop operation. If the normal RHR system fails the passive core cooling system provides safety-related core cooling. The passive core cooling system is operable during mid-loop operations. Since the AP600 provides diverse means of core cooling, and provides diverse indication of core cooling during shutdown (including mid-loop), diverse hot leg level indication is not required for the AP600.

As discussed in SSAR section 5.4.7.2.1, the AP600 normal RHR system has numerous design features that significantly improve mid-loop operations. The probability of losing the normal RHR system due to errors ocurring during mid-loop operations is reduced for the AP600.

NUREG Guidance:

"provide...the capability to continuously monitor decay heat removal system (DHR) when a DHR system is being used for cooling the RCS"

AP600 Conformance:

As shown in the table above, instrumentation is provided to continuously monitor the normal RHR system as well as the RCS to monitor decay heat removal.

NUREG Guidance:

"provide...visible and audible indications of abnormal conditions in temperature, level, and DHR system performance."

AP600 Conformance:

RCS temperature and level, and normal RHR temperatures and flow indication and alarms are provided in the main control room.

c. Please see the response to (a.) regarding the safety classification of the instrumentation available during shutdown. The environmental qualification of the safety-related instrumentation accounts for the most severe

environmental conditions applicable as provided in SSAR Appendix 3D. The nonsafety-related equipment class D instrumentation is designed in accordance with the requirements of ASME NQA-1-1989 Edition through NQA-1b-1991 Addenda.

SSAR Revision: NONE

Question 440.162

The staff reviewed EPRI's ALWR Utility Requirements Document for passive plants and concluded that ALWR designs should have a reactor vessel level indication system (RVLIS) to provide an unambiguous indication of inadequate core cooling, as required in TMI Action Item II.F.2, and that each ALWR PWR designer should identify system design and performance criteria, including the system's potential accident management role and the resulting severe environment it may be subjected to. The AP600 design does not have a RVLIS. Address conformance of the AP600 design to this position.

Response:

The AP600 provides the RVLIS function with reactor vessel water level indication for a range spanning from the bottom of the hot leg to approximately the elevation of the reactor vessel mating surface. This reactor vessel water level indication complies with the requirements of TMI Action Item II.F.2 as a result of the AP600 design features, actuation logic, and operator responses as described below.

BACKGROUND

TMI Action Item II.F.2 describes the requirements for plants to incorporate new instrumentation to monitor inadequate core cooling. The requirements of TMI Action Item II.F.2 are provided in Table 440.162-1. These requirements resulted in current Westinghouse PWRs incorporating a reactor vessel level indication system (RVLIS) that provides indication of reactor coolant system void fraction when the reactor coolant pumps are operating, and reactor vessel water level when the reactor coolant pumps are tripped. This instrumentation was designed specifically for PWRs that rely on operator action to trip the reactor coolant pumps following a LOCA.

Prior to TMI, the accepted philosophy for PWRs was that during a LOCA, operation of the reactor coolant pumps, if available, was always desirable in that they provided improved core cooling. However, during the TMI scenario, the reactor coolant pumps continued to operate during a loss of coolant accident caused by a stuck open pressurizer PORV. Although pressurizer level remained high (which was interpreted as an indication of adequate coolant inventory), the continuous loss of reactor coolant and subsequent inadequate core cooling caused the reactor coolant to become highly voided. As long as the reactor coolant pumps continued to operate, core cooling was maintained.

However, eventually the reactor coolant pumps were tripped, and due to the high void content in the coolant, the water level dropped to below the top of the core causing core damage. Therefore, the RVLIS systems were designed to provide the operators with an unambiguous indication of void content in the reactor coolant when the reactor coolant pumps are operating. Void content indication is used to manually trip the reactor coolant pumps following a LOCA, to avoid the possibility of core uncovery later during the event, if the RCPs were tripped when the coolant was highly voided.

In current Westinghouse PWR's, RVLIS is also used to provide the measurement of reactor vessel level during a LOCA event after the RCPs are tripped. For these plants, water level in the vessel is an indication of inadequate core cooling and coolant inventory. This measurement is used to prioritize operator recovery actions, and is used to instruct the operator to:

- establish / re-establish safety injection flow,
- manually depressurize the RCS.

AP600 REACTOR VESSEL LEVEL INDICATION

The AP600 design complies with the requirements of TMI Action Item II.F.2. The requirements for reactor vessel level indication are provided by redundant, safety-related reactor vessel level instrumentation. As shown in SSAR Figure 5.1-5, these instrument channels (LT-160 and LT-170) have one level tap that connects to the bottom of a hot leg, and one level tap that connects to the top of the hot leg bend that connects to the steam generator. This instrumentation is used to provide reactor vessel water level during an accident, and also is used to provide hot leg level during shutdown operations including mid-loop. This instrumentation provides indication of reactor vessel water level for a range spanning from the bottom of the hot leg to approximately the elevation of the reactor vessel mating surface. This instrumentation is temperature compensated and provides accurate level measurement during all modes of operation. This instrumentation complies with the requirements of TMI Action Item II.F.2 as a result of the AP600 design features, actuation logic, and operator responses described below.

AP600 Design Features:

Automatic Depressurization

The AP600 passive safety-related systems operate in conjunction with automatic depressurization system (ADS) valves that automatically reduce the pressure in the RCS in response to a loss of coolant accident. Following a small break LOCA, the AP600 core makeup tanks (CMTs) inject water into the RCS. After the CMTs have injected approximately one-third of their inventory, the ADS valves receive a signal to open. The ADS valves are comprised of four stages of valves, three stages connected to the pressurizer and the fourth stage connected to the hot legs. The first stage opens on the low CMT level signal, and the second and third stages open sequentially on a time delay. The fourth stage ADS valves open when the CMTs are approaching empty. See SSAR Subsection 5.4.6 for a description of the ADS valves.

Opening of the ADS valves will cause a significant disturbance of the water level in the RCS. Initially water and steam will be discharged via the first three stages of ADS valves connected to the pressurizer. Water level in the RCS will vary greatly during the transient, and water level will not be a reliable indication of inadequate core cooling during ADS. Eventually the CMTs will reach a low level and the fourth stage ADS valves connected to the hot legs will open. This will reduce the pressure in the RCS sufficiently to enable gravity injection from the IRWST. Once the fourth stage ADS valves are opened and IRWST injection is established, the water level in the RCS will remain at a relatively constant level, and its measurement will provide a reliable indication.

Passive RHR Heat Exchangers

The AP600 passive RHR heat exchangers provide safety-related core cooling during accident events including loss of heat sink accidents such as loss of normal feedwater and feedline break accidents. As described in the response to RAI 440.126, the passive RHR heat exchangers provide sufficient core cooling during these events, even if RCS subcooling is not maintained. Unlike current plants that rely on the steam generators (in conjunction with safety-

related auxiliary feedwater pumps) that require RCS subcooling be maintained in the hot legs to ensure core cooling during these events, the AP600 relies on the passive RHR heat exchanger that provides sufficient core cooling without requiring RCS subcooling. This eliminates the need to use vessel head steam space indication as a means of detecting a loss of RCS subcooling. Since passive core cooling does not require maintaining subcooling, reactor vessel level indication above the mating surface is not an indication of inadequate core cooling.

AP600 Protection and Safety Monitoring System Actuation Logic:

Automatic Reactor Coolant Pump Trip

The AP600 does not require the operators to manually trip the RCPs following a LOCA because of the automatic trip of the RCPs on a safeguards actuation signal (i.e. CMT actuation). This eliminates the need for a RVLIS to provide a safety-related measurement of coolant void fraction to be used to manually trip the RCPs following a safeguards actuation signal. RCS subcooling is continuously monitored and is determined by the safety-related measurements of RCS pressure (wide range or pressurizer pressure) and RCS temperature (hot leg wide range, narrow range, and core exit thermocouples). The AP600 instrumentation described provides an unambiguous indication of inadequate core cooling and provides an advanced warning of an approach to inadequate core cooling.

AP600 Operator Responses:

In current PWRs, RVLIS is used to provide the measurement of reactor vessel level during a LOCA event after the RCPs are tripped. For these plants, water level in the vessel is an indication of inadequate core cooling and coolant inventory. This measurement is used to prioritize operator recovery actions, and is used to instruct the operator to perform the following actions:

- Establish / re-establish safety injection flow,
- Manually depressurize the RCS.

The AP600 operator responses do not rely on reactor vessel level indication. Operator actions are not required to establish safety injection flow or to depressurize the RCS. Following a safeguards actuation, the operators will monitor plant parameters that provide indication of successful operation of the passive safety-related systems. These parameters are:

- PXS valve position indication (CMT, accumulator and IRWST discharge valves)
- CMT water level and temperature
- IRWST level
- RCS pressure, temperature
- Reactor vessel water level
- RCS core exit thermocouples
- ADS valve position indication

Upon actuation of the CMTs, the water temperature in the CMT will increase, and water level will eventually begin to decrease. Eventually CMT level will be reduced and the operators will be alerted when ADS actuation is to occur.

Valve position indication of the safety injection discharge isolation valves will indicate that these valves have opened. The operator will monitor these parameters to determine if the CMTs have been initiated. If these parameters indicate failure of the CMTs to actuate, the operator will manually actuate the CMTs. Failing this, the operators would manually depressurize the RCS using the ADS valves.

If the CMTs actuate but ADS fails to actuate when required, the operator will manually actuate the ADS valves. The operator will have unambiguous indication that ADS is to occur, and unambiguous indication of its failure to occur. The use of RVLIS for the AP600 is not required to alert the operator to depressurize the RCS to mitigate accidents.

Following a safeguards actuation signal, the operators are not required to perform manual operations on the passive safety-related systems. Operators will monitor the key parameters described above. In addition, the operators will control operation of the nonsafety-related CVS makeup pumps and RNS pumps to provide high pressure and low pressure RCS makeup based on the instrumentation listed above, and the additional instrumentation provided with each system (RNS flow rate, CVS flow rate). The CVS makeup pumps will operate automatically based on pressurizer water level. The RNS pumps will be manually started upon a safeguards signal. In the event of a small LOCA where the RCS pressure is not reduced immediately to below the RNS pump shut-off pressure, the RNS pumps will operate on miniflow. As the pressure in the RCS is reduced (due to operation of the ADS) to below the RNS pump shut-off pressure, the RNS pumps will provide makeup flow via the direct vessel injection lines. For these events, the operator will not rely on any RCS parameter (such as reactor vessel level, pressurizer level, RCS pressure) to start the RNS pumps and heat exchangers, but will use the safeguards actuation signal.

Following ADS, the water level in the vessel will be maintained within the range of the reactor vessel water level instrumentation. A high level reading will be used to confirm adequate safety injection and core cooling. A low water level (below the range of the reactor vessel water level instrumentation), when combined with core exit thermocouple readings, will provide an indication of inadequate core cooling.

SUMMARY

The AP600 has been designed to provide the operators with an unambiguous indication of inadequate core cooling before, during, or after a loss of coolant accident. Indication of inadequate core cooling is provided by the various RCS instrumentation such as hot leg and core exit temperature. Indication of RCS inventory and reactor vessel level are provided by the reactor vessel instrumentation. Indication of RCS subcooling is provided by the RCS wide range pressure and core exit temperature. Indication of safety injection operation and ADS operation are provided by the various parameters discussed above. Therefore the AP600 design complies with the requirements of TMI Action Item II.F.2. Table 440.162-1 summarizes the compliance of the AP600 design with the ten requirements contained in TMI Action Item II.F.2

Table 440.162-1 Summary of AP600 Compliance to TMI Action Item II.F.2

TMI Action Item II.F.2	AP600 Compliance
(1) Design of new instrumentation should provide an unambiguous indication of inadequate core cooling. This may require new measurements or a synthesis of existing measurements which meet design criteria (item 7)	Indication of inadequate core cooling is provided by the following parameters: - Core exit and hot leg temperature - Reactor vessel water level - RCS wide range pressure - Pressurizer level In addition, the following instrumentation provides indication of operation of the safety-related and nonsafety-related systems that perform core cooling: - Safety-related valve position indication - CMT water level and temperature - IRWST water level - PRHR flow rate, temperature - RNS flow rate temperature - CVS flow rate
(2) This evaluation is to include reactor-water-level indication.	The AP600 provides reactor vessel water level indication from the bottom of the hot leg to approximately the mating surface of the reactor vessel flange.
(3) Licensees and applicants are required to provide the necessary design analysis to support the proposed final instrumentation system for inadequate core cooling and to evaluate the merits of various instruments to monitor water level and to monitor other parameters indicative of core-cooling conditions.	The instrumentation that monitors the plant parameters described above are designed and qualified in accordance with their safety classification as described in SSAR section 7.5.
(4) The indication of inadequate core cooling must be unambiguous in that it should have the following properties: *a) It must indicate the existence of inadequate core cooling caused by various phenomena (i.e. high-void fraction-pumped flow as well as stagnant boil-off); and,* *b) It must not erroneously indicate inadequate core cooling because of the presence of an unrelated phenomenon.*	a) High void fraction pumped flow is not an issue because the AP600 RCPs are tripped on a safeguards actuation signal. RCS subcooling is determined by the core exit thermocouples in conjunction with RCS pressure. Stagnant boil-off is monitored with the reactor vessel water level instrumentation. b) Unrelated phenomenon does not compromise the indication of inadequate core cooling.

TMI Action Item II.F.2	AP600 Compliance
(5) The indication must give advanced warning of the approach of inadequate core cooling.	An advanced warning of inadequate core cooling is provided by the instrumentation that monitors the parameters described in (1).
(6) The indication must cover the full range from normal operation to complete core uncovery. For example, water-level instrumentation may be chosen to provide advanced warning of two-phase level drop to the top of the core and could be supplemented by other indicators such as incore and core-exit thermocouples provided that the indicated temperatures can be correlated to provide indication of the existence of inadequate core cooling and to infer the extent of core uncovery. Alternatively, full-range level instrumentation to the bottom of the core may be employed in conjunction with other diverse indicators such as core-exit temperatures to preclude misinterpretation due to any inherent deficiencies or inaccuracies in the measurement system selected.	Reactor vessel water level provides an advanced warning of two-phase level drop to the top of the core. Core exit thermocouples are provided and can be used to indicate core uncovery.
(7) All instrumentation in the final inadequate core cooling system must be evaluated for conformance to Appendix A, "Design and Qualification Criteria for Accident Monitoring Instrumentation" as clarified or modified by the provisions of items 8 and 9 that follow. This is a new requirement.	The instrumentation that monitors the parameters described in (1) are included in SSAR Table 7.5-1. The instrumentation provided is designed in accordance with their safety-related functions as described in SSAR Section 7.5.

TMI Action Item II.F.2	AP600 Compliance
8) *If a computer is provided to process liquid-level signals for display, seismic qualification is not required for the computer and associated hardware beyond the isolator or input buffer at a location accessible for maintenance following an accident. The single-failure criteria of item 2, Appendix A, need not apply to the channel beyond the isolation device if it is designed to provide 99% availability with respect to functional capability for liquid-level display. The display and associated hardware beyond the isolation device need not be Class 1E but should be energized from a high-reliability power source which is battery backed. The quality assurance provisions cited in Appendix A, item 5, need not apply to this portion of the instrumentation. This is a new requirement*	The instrumentation provided is designed in accordance with their safety-related functions as described in SSAR Section 7.5.
9) *Incore thermocouples located at the core exit or at discrete axial levels of the inadequate core cooling monitoring system and which are part of the monitoring system should be evaluated for conformity with Attachment, "Design and Qualification Criteria for PWR Incore Thermocouples," which is a new requirement.*	The incore instrumentation is described in SSAR Subsection 4.4.6.1. Core exit thermocouples are safety-related as described.
10) *The types and locations of displays and alarms should be determined by performing a human-factors analysis taking into consideration:* *a) the use of this information by an operator during both normal and abnormal plant conditions,* *b) integration into emergency procedures* *c) integration into operator training, and* *d) other alarms during emergency and need for prioritization of alarms.*	The instrumentation provided to monitor inadequate core cooling are displayed in the main control room. SSAR Chapter 18 discusses the AP600 Human Factors Engineering.

AP600

SSAR Revision: SSAR subsection 1.9.3 will be modified as follows:

(2)(xviii) Inadequate Core Cooling Instrumentation (NUREG 0737 Item II.F.2)

"Provide instruments that provide in the control room an unambiguous indication of inadequate core cooling, such as primary coolant saturation meters in PWRs, and a suitable combination of signals from indicators of coolant level in the reactor vessel and in-core thermocouples in PWRs and BWRs."

AP600 Response:

The AP600 reactor system includes instrumentation for detecting voids in the reactor vessel head and other reactor vessel inventory deficits that could lead to inadequate core cooling.

The available instrumentation includes core subcooling margin monitors, core exit thermocouples, pressurizer level indicators, reactor coolant system reactor vessel level, ~~reactor coolant system hot leg level,~~ and reactor coolant pump status (motor current). Reactor vessel level indication is provided from a range in the vessel from the bottom of the hot leg to approximately the reactor vessel mating flange via level instrumentation connected to the hot legs.

~~The AP600 design does not employ a reactor pressure vessel level instrumentation system. The plant has a number of design features that make the occurrence of sustained voiding in the reactor pressure vessel during anticipated transients unlikely.~~

The AP600 features that provide margin to or indication of inadequate core cooling include the following:

- A larger pressurizer than most current PWRs, with a pressurizer that is located above the reactor pressure vessel head
- No automatic power-operated relief valves
- An improved reactor vessel head venting capability
- A passive core cooling system
- A passive containment cooling system
- No dependence on ac power to maintain adequate core and containment cooling
- Reactor coolant system hot leg level instrumentation
- Improved reactor system instrumentation

- A core subcooling monitor.

See Sections 6.3 and 7.5 for additional information.

SSAR Table 7.5-1 will be modified as follows:

Table 7.5-1 (Sheet 3 of 12)

Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required (Note 1)	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Startup feedwater flow	0-1000 gpm	D2, F2	Harsh	Yes	1/pump	1E	Yes	
Startup feedwater control valve status	Open/ Closed	D2	None	None	1/valve	Non-1E	No	
Containment pressure	-5 to 10 psig	B1, C2, D2, F2	Harsh/Mild	Yes	3 (Note 4)	1E	Yes	Located outside containment
Containment pressure (extended range)	0 to 180 psig	C1	Harsh	Yes	3 (Note 4)	1E	Yes	
Containment area radiation (high range)	10^{0}-10^{7} R	B1, C2, E2, F2	Harsh	Yes	2 1/division	1E	Yes	Diverse measurement: sampling
Reactor vessel - hot leg water level~~Hot leg water level~~	0-100%	B2, B3	Harsh~~None~~	Yes~~None~~	2/unit~~1/unit~~	1E~~Non-1E~~	Yes~~No~~	

SSAR Table 7.5-5 will be modified as follows:

Table 7.5-5

Summary of Type B Variables

Function Monitored	Variable	Type/ Category
Reactivity control	Neutron flux	B1
	Control rod position	B3
	Boric acid concentration	B3
Reactor coolant system integrity	RCS pressure	B1
	WR T_{hot}	B1
	WR T_{cold}	B1
Reactor coolant inventory control	Pressurizer level	B1
	Pressurizer reference leg temperature	B1
	Reactor vessel-h~~h~~ot leg water level	B3
Reactor core cooling	Core exit temperature	B1
	RCS subcooling	B1
	WR T_{hot}	B2
	WR T_{cold}	B2
	RCS pressure	B2
	Reactor vessel-hot leg water level	B2
Heat sink maintenance	IRWST water level	B1
	PRHR flow	B1
	PRHR outlet temperature	B1
	PCS storage tank water level	B1
	Passive containment cooling flow	B1
Containment environment	Containment pressure	B1
	Containment area high range radiation	B1
	Containment water level	B1
	Hydrogen concentration	B1

AP600

Question 440.219

Based on the PRA, in the event trees for steam line break or stuck open secondary relief valve, the PRHRS alone is not sufficient, and RCS makeup is needed. Is there any analysis that demonstrates that the inventory is or is not sufficient to support PRHRS operation?

Response:

The event trees require core makeup tanks or chemical volume and control system operation to provide reactor coolant system boration and not for reactor coolant system makeup. SSAR Subsection 15.1.5 provides the analysis that indicates that the core makeup tank injection is sufficient for boration during a steam line break with conservative assumptions.

SSAR Revision: NONE

PRA Revision: NONE

AP600

Question 440.225

In the LOOP event tree of the PRA, with PRHRS operation successful, the sequences are terminated successfully. PRHR operation will cause a low pressurizer pressure signal that will actuate the CMT. How does the CMT operation affect PRHR? Will the ADS be actuated due to low CMT level? Is it possible to reach the ADS actuation setpoint without losing RCS inventory? What does the operator need to do regarding the operation of the CMT and the ADS?

Response:

The core makeup tanks, in the short term (approximately one hour), act in conjunction with the passive residual heat removal heat exchanger to remove the sensible heat and the decay heat from the reactor coolant system. The core makeup tank injection stops once the core makeup tanks becomes heated.

During a loss of offsite power event, automatic depressurization system actuation does not result as a consequence of passive residual heat removal system operation. During such events, the core makeup tanks remain essentially full of water and therefore the low core makeup tank water level setpoint for actuating the automatic depressurization system is not reached. Refer to the response to RAI 440.203 and to the steam line break analysis provided in section 4.1 of Reference 440.225-1.

No operator action is required to actuate the core makeup tanks or to prevent automatic depressurization system actuation during this event.

References:

440.225-1 AP600 Design Change Description Report, February 15, 1994

SSAR Revision: NONE

PRA Revision: NONE

Question 440.228

There are many sequences in the event trees of the PRA that transfer to the medium-break LOCA event trees with a stuck open pressurizer safety valve. How does the CMT work with stuck open pressurizer safety valves (PSV)? Does the phenomenology of inadvertent opening of a PSV differ from a cold leg medium-break LOCA analyzed in the PRA success criteria analyses?

Response:

A stuck open pressurizer safety valve results in a low pressurizer pressure. In the design as it existed at the time of PRA Rev. 0, this would cause the CMT/Pressurizer line to close. The pressurizer pressure balance line has been deleted from the design , as documented in Reference 440.228-1. The core makeup tanks operate with the cold leg balance line. If the cold leg is filled, then the water recirculates. If voiding occurs in the cold leg, then the core makeup tanks drain, with steam displacement. There is no interaction between the pressurizer and the core makeup tanks.

The phenomenology of inadvertent pressurizer safety valve opening differs from that of the cold leg medium-break LOCA, but is less limiting. For the inadvertent pressurizer safety valve opening, depressurization would occur with less reactor coolant mass loss. As a result, there would be more peak clad temperature margin than shown in the cold leg medium-break LOCA analyzed in the PRA success criteria analysis.

Reference:

440.228-1 The AP600 Design Change Description Report dated June 30, 1994

SSAR Revision: NONE

PRA Revision: NONE

Question 440.231

Describe how de-boration during plant startup is done, in terms of the lineup of equipment in supplying unborated water and discharging borated water. What is the flow rate and boron concentration in the flow paths? How is this process controlled? How long does it take? What is the effect of a LOOP on this mode of operation? For the boron dilution scenario due to restart of RC pumps following a LOOP discussed in Section F.4.7.3 of the PRA, determine the amount of unborated water that can be injected, and the reactivity effect it has on the reactor, taking into consideration the possibility of mixing of the unborated water with reactor coolant.

Response:

The chemical and volume control system (CVS) makeup pumps are operated to supply demineralized water to the RCS so the boron concentration can be reduced to the level required for criticality during plant startup. The makeup pump suction is aligned to the demineralized water system and the makeup pumps provide unborated water (at approximately 100 gpm) to the RCS. The makeup pumps continue to provide demineralized water until the RCS boron concentration is reduced to the calculated level. Effluent being removed from the RCS is routed from the CVS purification loop to the WLS as the unborated makeup is provided by the makeup pumps.

Deboration during plant startup is performed as described in PRA Subsection F.4.7.3.. The operator switches control of the makeup from the automatic makeup mode to the dilute mode and starts the CVS makeup pumps. The operator selects a calculated amount of makeup and sets the makeup pump flowrate. The makeup pumps run automatically to supply demineralized water to the RCS. Dilution from RCS refueling shutdown concentration to the beginning of life, hot full power, no xenon operating concentration lasts about 2 to 4 hours.

The AP600 chemical and volume control system is designed to address a potential rapid boron dilution scenario in the event of a loss of power to the two CVS remotely-operated demineralized water system isolation valves and the CVS makeup pumps. This is discussed in the response to RAI 440.54. When power is interrupted, the unborated water source is isolated and the CVS makeup pump suction is automatically aligned to the boric acid tank. If the CVS makeup pumps are restarted following a power interruption, borated (greater than 4000 ppm) water will be injected to the RCS.

Refer to the responses to RAIs 440.120, 440.122 and 440.54 for related discussions.

SSAR Revision: NONE

Question 440.239

During a drained maintenance, what kind of wide range level instrumentation is available? Does it need a standpipe system that is used for current PWRs? Without it, how is the RCS level determined during drain down?

Response:

The AP600 hot leg level and pressurizer wide range level are available during drained maintenance. No standpipe system is required. This is discussed in SSAR Subsection 5.4.7.2.1. See the response to RAI 440.240 for a related discussion.

SSAR Revision: NONE

Question 440.240

In the shutdown PRA, the time available to restore offsite power is taken to be 1.5 or 2 hours based on the time to core uncovery. This implies that the RNS pumps can operate with saturated RCS coolant. Is this correct?

Response:

The AP600 normal residual heat removal pumps are designed to minimize cavitation. The plant piping layout configuration (such as piping elevations and routing) and the available and required pump net positive suction head characteristics allow the normal residual heat removal pumps to be started and operated at their full design flow rates, with saturation conditions in the reactor coolant system (associated with boiling in the reactor vessel).

SSAR Revision:

SSAR Subsection 5.4.7 will be revised as follows:

5.4.7.2.1 Design Features Addressing Mid-loop Operations

The following is a summary of the specific AP600 design features that address Generic Letter (GL) 88-17 regarding mid-loop operations.

Loop Piping Offset - As described in Subsection 5.3.4.1, the reactor coolant system hot legs and cold legs are offset. This results in the level to which the hot leg must be drained in order to facilitate venting of the steam generators for nozzle dam insertion is much higher than traditional designs. The reactor coolant system must be drained to a level which is sufficient to provide a vent path from the pressurizer to the steam generators. This is nominally 80 percent level in the hot leg, which provides the vent path required. Furthermore, this loop piping offset allows a reactor coolant pump to be replaced without removing a full core.

Step-nozzle Connection - The normal residual heat removal system employs a step-nozzle connection to the reactor coolant system hot leg. The step-nozzle connection has two effects on mid-loop operation. One effect is to substantially lower the RCS hot leg level at which a vortex occurs in the residual heat removal pump suction line due to the lower fluid velocity in the hot leg nozzle. This increases the margin from the nominal mid-loop level to the level where air entrainment into the pump suction begins.

Another effect of the step-nozzle is that, if a vortex should occur, the maximum air entrainment into the pump suction has been shown experimentally to be no greater than 5 percent. This level of air ingestion will make air binding much less likely.

No RHR Throttling During Mid-loop - The normal residual heat removal pumps are designed to minimize cavitation. The plant piping layout configuration (such as piping elevations and routing) and the available and required pump net positive suction head characteristics allow the normal residual heat removal pumps to be started and operated at their full design flow rates, with saturation conditions in the reactor coolant system

(associated with boiling in the reactor vessel). The normal residual heat removal system is designed to operate without the need for throttling the residual heat removal control valve when the level in the reactor coolant system is reduced to a mid-loop level. The normal residual heat removal system is readily restored after a temporary loss of decay heat removal during mid-loop operations.

~~*No RHR Throttling During Mid-loop* - The normal residual heat removal system is designed to operate without the need for throttling the residual heat removal control valve when the level in the reactor coolant system is reduced to a mid-loop level.~~

Self-venting Suction Line - The residual heat removal pump suction line is sloped continuously upward from the pump to the reactor coolant system hot leg with no local high points. This eliminates potential problems with refilling the pump suction line following a residual heat removal pump trip caused by excessive air entrainment. With the self-venting suction line, the line will refill and the pumps can be immediately restarted once an adequate level in the hot leg is re-established.

Hot Leg Level Instrumentation - The AP600 reactor coolant system contains level instrumentation in each hot leg with a readout in the main control room. In addition, the wide-range pressurizer level instrumentation used during cold plant operations is expanded to the bottom of the hot legs. This provides a continuous level indication in the main control room, from the normal level in the pressurizer to the range of the two narrow-range hot leg level instrumentation. This reactor coolant system level instrumentation provides an accurate readout of reactor coolant system level in the control room. Alarms are also provided to alert the operator when the reactor coolant system hot leg level is approaching a low level. ~~This instrumentation provides an accurate readout of reactor coolant system level in the control room. Alarms are also provided to alert the operator when the reactor coolant system level is approaching a low level.~~ Furthermore, the isolation valves in the line used to drain the reactor coolant system are interlocked to close on a low reactor coolant system level during shutdown operations. Those operations required during mid-loop are performed by the operator in the main control room. The level monitoring and control features significantly improve the reliability of the AP600 during mid-loop operations

Reactor Vessel Outlet Temperature - Reactor coolant system hot leg wide range temperature instruments are provided in each hot leg. The orientation of the wide range thermowell-mounted resistance temperature detectors enable measurement of the reactor coolant fluid in the hot leg drained maintenance operations. In addition, at least two incore thermocouple channels are available to directly measure the core exit temperature during midloop residual heat removal operation. These two thermocouple channels are associated with separate electrical divisions.

ADS Valves - The automatic depressurization system first-, second-, and third-stage valves, connected to the top of the pressurizer, are open whenever the core makeup tanks are blocked during shutdown conditions while the reactor vessel upper internals are in place. This provides a vent flow path to preclude pressurization of the reactor coolant system during shutdown conditions when decay heat removal is lost. This also allows the in-containment refueling water storage tank to automatically provide injection flow if it is actuated on a sustained loss of decay heat removal.

Administrative controls require containment integrity during midloop operation. In addition, the capability to restore containment integrity during shutdown conditions is provided. The containment equipment hatches are equipped with guide rails that allow reinstallation of the hatches in about six hours, with a loss of nonsafety-related ac power sources, to re-establish containment integrity. The containment design also includes penetrations for temporary cables and hoses needed for shutdown operations. These penetrations are isolated in an emergency.

In addition to these design features, appropriate procedures are defined to guide and direct the operator in the proper conduct of midloop operation and to aid in identifying and correcting abnormal conditions that might occur during shutdown operations.

Question 440.241

For hot and cold shutdown conditions, what is the condition of the reactor at 2 hours after a loss of the RNS? What is the system pressure during this 2 hours? It appears that the only relief valve available is the one in the RNS. A bubble will form in the vessel while coolant is spilled out of the RNS relief valve. Can the RNS withstand the expected pressure? What is the flow path and flow rate to the RNS relief valve? How does this flow affect the operation of PRHRS? When is the operator expected to actuate the PRHRS? Will the PRHR HXs be drained at some time? What about the SG tubes? In this scenario, will the bubble in the vessel prevent CMT injection and ADS actuation? If some of the systems have to be manually actuated, what is the information that tells the operator to do so? How much time does the operator have to perform the actions?

Response:

The loss of RNS from hot shutdown or cold shutdown conditions is addressed in Section 3.2 of Reference 440.241-1. As described in reference 440.241-1, the conditions in the RCS two hours after a loss of the RNS are scenario dependent. For this event, the RCS pressure would increase to the set pressure of the RNS relief valve. The resulting loss of inventory would result in automatic actuation of the CMTs and PRHR heat exchanger on low pressurizer level. If the RNS relief valve failed to open the pressurizer safety valves are available to provide overpressure protection for the RCS.

As described in SSAR Subsection 5.4.7.2.2, the RNS is designed to an ultimate rupture strength of full RCS pressure. Following this loss of RNS cooling, the PRHR heat exchangers, and the RNS relief valve would limit the pressure in the RCS. In addition, operator action could be taken to isolate the RNS, which would stop the loss of reactor coolant out the RNS relief valve.

As described in SSAR Subsection 5.4.7, the RNS relief valve is attached to the RNS suction line connected to an RCS hot leg. As specified in SSAR Table 5.4-17, the RNS relief valve flow rate is 555 gpm at a set pressure of 563 psig.

The response to RAI 440.218 discusses the operation of the PRHR heat exchanger during transients where the RCS inventory is reduced. During this event, the PRHR is automatically actuated on low pressurizer level.

The PRHR HX and the steam generator tubes will remain full due to the operation of the CMTs. A bubble in the reactor vessel head will not prevent operation of the PRHR or the CMTs. The passive safety-related systems are automatically actuated for this scenario.

References:

440.241-1 WCAP-13793, "AP600 System / Event Matrix," June 1994.

SSAR Revision: NONE

Response Revision 1

Question 460.1

In accordance with Sections 11.2 "Liquid Waste Management Systems" (Section III.2.C) and 11.3 "Gaseous Waste Management Systems" (Section III.2.b) of the SRP, the staff uses reactor coolant fission product source terms corresponding to 1 percent failed fuel as the basis for determining the design adequacy of the liquid and gaseous radwaste systems for processing the liquid and gaseous radwastes at design basis fission product levels. In view of the above practice, either justify the 0.25 percent failed fuel design basis used in Section 11.1.1.1 and Tables 11.1-1, 11.1-2 and 11.3-4 of the SSAR or revise the subject SSAR section and tables to be consistent with 1 percent failed fuel (Sections 11.1 and 11.3).

NRC Comment (from letter of May 12, 1994) on the original response:

The staff believes that the shielding criterion is not a valid basis. Evaluation findings in SRP 11.3 does refer to 1% FF. The EPRI Requirements Document for Passive Reactors also uses 1% FF for radwaste systems design and demonstration of subject compliance. Tables 11.2-7 and 11.3-4 of the SSAR should be revised to demonstrate subject compliance for effluent concentrations in unrestricted areas. Effluent concentrations can be based on annual average.

Response:

The use of 1 percent failed fuel as the basis for the evaluation of design adequacy for the AP600 radwaste systems is inappropriate since the AP600 design basis is 0.25 percent fuel defects. The 0.25 percent fuel defect level is the basis for radiation shielding design (see SSAR Subsection 12.2.1.1) and is also the basis for the Technical Specification limits for primary coolant activity (see Technical Specification basis discussion B 3.4.10). Selection of 0.25 percent fuel defects is consistent with the guidance provided in Section 12.2 of the SRP; additionally, operating plant experience indicates that extremely low fuel defect levels would be expected, far below the 0.25 percent value selected as the AP600 design basis.

The SRP guidance that is referred to in this question is that of the Review Procedures, where it is stated that review of the waste treatment systems is to include determination of "the system capability to process wastes at design basis fission product leakage levels, i.e., from 1 percent of the fuel-producing power in a PWR." The direction to use 1 percent fuel defects for the design basis fission product leakage level is a presumption that the design basis is 1 percent fuel defects. While this may be true historically, it is not correct for the AP600. Operation of the AP600 with fuel defect levels in excess of 0.25 percent is outside the AP600 design basis.

The use of 0.25 percent fuel defects remains a valid design basis for the AP600 since operation of the plant is to be restricted to fuel defect levels no greater than this. However Tables 11.2-8 and 11.3-4 will be revised to include consideration of operation with a fuel defect level of 1.0 percent, consistent with the historical guidance provided in Regulatory Guide 1.70, Revision 3 and Sections 11.2 and 11.3 of the Standard Review Plan.

Revision of SSAR Tables 11.2-8 and 11.3-4 to reflect consideration of 1.0 percent fuel defects will be provided in Revision 2 of the SSAR. The tables will reflect both the design basis fuel defect limit of 0.25 percent and the beyond-design-basis assumption of 1.0 percent fuel defects.

SSAR Revision: Revision of Tables 11.2-8 and 11.3-4 will be included in Revision 2 of the SSAR.

Response Revision 1

AP600

Question 460.2

Correct or clarify the following information obtained from the identified tables in the SSAR relating to secondary coolant concentration (Sections 11.1 and 11.2):

Tables 11.1-4 and 11.1-7:	Total steam generator (SG) blowdown flowrate - 4.2×10^4 lb/hr
Table 11.2-6:	Total SG blowdown flowrate - 8.4×10^4 lb/hr

Response:

~~The total steam generator blowdown flow rate shown in SSAR Tables 11.1-4 and 11.1-7 (4.2×10^4 lb/hr) is used to calculate the secondary coolant concentrations for use in in-plant evaluations. The lower blowdown rate (compared to Section 11.2) tends to retain more radioactivity in the secondary coolant, resulting in conservative shielding, ALARA, and accident source terms. Because the intended use of the parameters in SSAR Section 11.2 is to estimate offsite releases and determine if the radwaste systems are adequate to maintain effluent releases to uncontrolled areas within the limits specified in 10 CFR 50, Appendix I, the maximum continuous capacity of the system as shown in SSAR Table 11.2-6 (8.4×10^4 lb/hr) is used.~~

The range of blowdown flow for the AP600 is from a minimum of 8.4×10^3 lb/hr to a maximum of 8.4×10^4 lb/hr. The use of the midpoint value of 4.2×10^4 lb/hr is appropriate to both analyses.

The GALE code analysis will be rerun using a total SG blowdown flowrate of 4.2×10^4 lb/hr. The results of this reanalysis will be provided in Revision 2 of the SSAR. At that time, Table 11.2-6 will also be revised to reflect the change in assumed blowdown flowrate.

SSAR Revision: Revision of Table 11.2-6 will be included in Revision 2 of the SSAR.

Question 460.14

Clarify whether the steam generator blowdown system and component cooling water (CCW) radiation monitors provide any automatic control features. If not, indicate for what essential purpose these monitors are provided (e.g., manual actions to isolate the affected CCW loop or terminate SG blowdown on detection of high radiation by the subject monitor) (Section 11.5).

Response: (Revision 1)

Radiation monitors are provided on the component cooling system (CCS) for detection of radiological leakages into the CCS. This feature is described in SSAR Subsection 9.2.2.7. With this detection, the CCS may be manually isolated and leaks repaired.

The steam generator blowdown system (BDS) contains a radiation monitor for detection of radioactivity. When ~~preset levels of the~~ radioactivity is ~~are~~ detected in BDS, an operator remotely actuates a ~~manual diversion~~ valve to directs BDS fluid to the liquid radwaste system (WLS) for processing as contaminated water. The BDS radiation monitor is located downstream of the BDS demineralizers. The diversion of BDS water to the WLS is an abnormal event as the result of exhaustion of the BDS ion exchange resin, inadvertant bypass of the demineralizers or significant primary to secondary leak. Automatic isolation, if high levels of radiation are detected, is provided through the system's blowdown control valve and an automatic isolation valve located upstream of the system's heat exchangers. Refer to SSAR Subsection 10.4.8 on BDS.

SSAR Revision: NONE

Question 620.36

Who performed, or is performing, the verification and validation activities (for Phases 1 and 2) discussed in Section 18.8 of the SSAR? What are their roles (i.e, how did they perform these activities)? What is the process used to accomplish them (p. P18.8-21, Figure 18.8.2-5)?

Response: (Revision 1)

Evaluations 16 and 17 described in SSAR Section 18.8 provide a high level description of the human factors verification and validation activities that will be performed for the AP600 M-MIS. These two evaluations correspond to Element 10 - Human Factors Verification and Validation, of the draft Human Factors Engineering Program Review Model for Advanced Nuclear Power Plants, dated January 25, 1994.

A detailed implementation plan for human factors verification and validation will be provided to support completion of the AP600 man-machine interface system ITAAC. Refer to revision 2 of the response to RAI 620.51.

The human factors verification and validation will be performed by a multi-disciplinary team that will include human factors specialists, M-MIS designers, and staff from the systems engineering, procedures development, training, and probabilistic risk assessment.

~~The verification and validation activities described in the SSAR are being conducted by a multi-disciplinary team that includes: 1) man-machine interface design specialists from the Man-Machine Design group at NATD with extensive experience in designing computerized systems and displays for Nuclear Power Plant control room application; and 2) specialists in human factors, applied psychology, and cognitive engineering from the Human Sciences group at the Westinghouse Science and Technology Center. These two groups are primarily responsible for the design and implementation of the M-MIS verification and validation plan. In performing their work they have access to and support from multiple sources of expertise including personnel with expertise in: AP600 system and I&C engineering; AP600 procedures development; AP600 training development; and AP600 human reliability analysis and probabilistic risk assessment.~~

~~The verification and validation plan described in the SSAR was primarily developed by staff from the Human Sciences group at the Westinghouse Science and Technology Center, who have extensive experience in analysis and modeling of Nuclear Power Plant (NPP) operator performance in emergencies, human reliability analysis, and the development of training programs and decision aids to support operator cognitive performance.~~

~~The process that they used to develop the verification and validation plan is summarized schematically in SSAR Figure 18.8.2-5 and the accompanying text in SSAR Subsection 18.8.2.3. Briefly a set of major human performance issues that need to be evaluated as part of the AP600 verification and validation was identified (Phase 1). For each issue a set of verification and validation tests was then defined to establish that the AP600 M-MIS supports the human performance requirements (Phase 2). In developing the Verification and Validation plan the Human Sciences group drew heavily on 1) the Rasmussen model of operator decision-making as extended by Westinghouse; 2) their own empirical research and modeling of NPP operator performance in emergencies, the sources of cognitive demands~~

and potential for human error; 3) the general Human Factors literature, including recent results from related industries on the pitfalls associated with new automation and display technologies (e.g., experience in the aircraft industry).

The verification and validation plan generated by the Human Sciences group was then subjected to several review and revision cycles that included critical input from the Man-Machine design group; the AP600 I&C design group; and the AP600 management team. The studies specified in the verification and validation plan will be implemented by a multi-disciplinary team that will include staff from the Westinghouse STC Human Sciences group who will provide technical expertise in design and analysis of the evaluation tests; staff from the NATD Man-Machine group who will be responsible for the design of the M-MIS computerized displays, alarms and procedures to be used in the V&V tests; and staff from the procedures development, training, and probabilistic risk assessment groups, who will provide technical guidance in designing test scenarios, procedures, and training materials to be used in the V&V tests.

SSAR Revision: NONE

Response Revision 1

AP600

Question 620.48

Exactly how does the alarm system meet the requirements of the SPDS? Where is the SPDS function located in the control room? Does it meet all the requirements for SPDS as specified in NUREG-0737, Supplement 1 and amplified in NUREG-1342 ("A Status Report Regarding Industry Implementation of Safety Parameter Display Systems," 1989) (Section 18.9.2.2.6, p. P18.9-6)?

Response: (Revision 1)

Our position with regard to the SPDS in the AP600 control room is the same as that reviewed by the NRC for the SP-90 or Advanced Pressurized Water Reactor (APWR) in the late 1980's. This position, in turn, is a derivative of the SPDS design activity that Westinghouse submitted for NRC review in the early 1980's and which received an SER on the generic or non-plant specific design as cited in the SSAR. Our position is that the need for an SPDS is really an indictment against the performance of the alarm system at Three Mile Island Unit 2 during the March, 1979 incident. That indictment, as stipulated in NUREG-0696, suggested that better performance of the alarm system could have been had during the TMI-2 incident if the alarms had been better organized (around the concept of Critical Safety Functions), had cause-effect relationships been more clearly presented, had fewer alarms been presented (aggregate and abstract detailed alarms to more clearly show the current overall state of the plant's processes), and show, in an analog fashion, the plant's processes deviating from their expected normal states prior to reactor trip.

The Westinghouse AWARE System, which is the basis for the AP600 alarm system does all of these, with one notable exception. The User Behavior/Decision Making model is the basis for the organization of the alarm messages. This model provides the mapping to the Critical Safety Functions. The number of alarm messages presented to the operators is vastly reduced by using a queuing scheme based upon the User Behavior/Decision Making model (i.e., messages are formed to answer the questions ala Figure 18.6-13, p. P18.6-20, and queued as per the User Behavior/Decision Making model) and the most urgent are provided the most salient presentation space based upon an on-line prioritization scheme that is again primarily based upon the "goal-means" (User Behavior/Decision Making) model.

The notable exception, as was noted in the NRC review of the SP-90, is the fact that an alarm system is not an analog presentation system. It is binary. A message is presented when a setpoint is reached, off or on. During the review of the SP-90, the NRC noted that the control board CRT displays, also based upon the User Behavior/Decision Making model, did provide the analog presentation of the plant process state and is highly coordinated with the alarm presentation so that in combination, the alarm system and the display system together achieved the intent of the SPDS requirements. This is the objective of Westinghouse with these new plant designs. We feel that the requirements of the currently stand-alone back-fit devices need to be examined as part of the total requirements for the design of the M-MIS and integrated in a complete sense into the appropriate portions of the M-MIS, not left as stand-alone devices. Included in this overall integration effort for the AP600 are the SPDS (NUREG-0696) requirements, the By-Passed and Inoperable Status Indication System (Reg. Guide 1.47), and Post-Accident Monitoring System (Reg. Guide 1.47).

Safety Parameter Display System

The following information provides information to address the integration of the Safety Parameter Display System function in the AP600 main control room.

SSAR Subsection 18.9.2 states that there will not be a stand-alone Safety Parameter Display System (SPDS), and that the regulatory requirements will be met by "integrating" the requirements into the design requirements for the alarm and display systems. The following explains the approach to meeting the regulatory requirements for a Safety Parameter Display System (SPDS) by addressing the requirements individually and showing how they are met in the main control room design.

Three documents comprise the regulatory requirements for a Safety Parameter Display System. These are:

1.) NUREG-0696, Functional Criteria for Emergency Response Facilities, Feb. 1981,

2.) NUREG-0737-SUP-N1, Clarification of TMI Action Plan Requirements, Supplement Number 1 Requirements for Emergency Response Capability, Jan. 1983, and

3.) Generic Letter No. 89-06, TASK ACTION PLAN ITEM I.D.2 - SAFETY PARAMETER DISPLAY SYSTEM - 10 CFR 50.54(f), April 12, 1989.

Supplement 1 to NUREG-0737 establishes the regulatory requirements for SPDS, therefore NUREG 1342 is not addressed.

The checklist enclosed in Generic Letter 89-06 supersedes, for the regulatory acceptability of an SPDS, the acceptance criteria established in NUREG-0835, Specific Acceptance Criteria Keyed to NUREG-0696.

The functional criteria for SPDS are discussed in Section 5 of NUREG-0696 and the discussion in NUREG-0737, Supplement 1 does not supersede these criteria, but references them.

One of the criteria found in Section 5 is the need for human-factors engineering in the design of the SPDS. Westinghouse intends to reduce the number of individual computerized operator support systems required for the AP600 control room operators. This will be accomplished by incorporating the requirements for the SPDS into the design requirements for the AP600 M-MIS, specifically in those portions of the system that produce and display the process abnormality messages (i.e.,alarm messages) and the process graphical Visual Display Unit (VDU) displays.

As noted in Section 4.1.a of NUREG-0737 Supplement 1, "...the principle purpose and function of the SPDS is to aid the control room personnel during abnormal and emergency conditions in determining the safety status of the plant and in assessing whether abnormal conditions warrant corrective action by operators to avoid a degraded core. This can be particularly important during anticipated transients and the initial phase of an accident." Since the main intended use is during process abnormalities, particularly severe abnormalities, i.e., relatively rare occurrences, human-factors engineering suggests that the operators will find that the use of data acquisition habits acquired and built during the normal operation of the plant will be the most successful. This suggests that a system in the control room that only varies its output during abnormalities may require a shift in mental focus and in data acquisition

habits and subsequent analysis. A more effective means for conveying the safety state of the plant is to provide an environment for normal operation that employs the SPDS required principles for data synthesis, concentration and display. This environment is operational over the range of plant conditions specified by the SPDS requirements, as well as during normal operations. This is the AP600 approach to SPDS.

Also, the first paragraph of Section 5.1 of NUREG-0696 states: "The primary function of the SPDS is to aid the operator in the rapid detection of abnormal operation conditions." This means that the SPDS must be able to aid the operator in detecting subsequent equipment failures and subsequent process degradation in and during the context of terminating and mitigating the consequences of an initial abnormality. This need for addressing subsequent failures leads to an SPDS design that includes the instrumentation required for the main control room. The operator-interface to the plant is improved by integrating SPDS requirements into the overall M-MIS design to avoid the need for another system that is useful only infrequently.

The following is an item-by-item response to the checklist found in NRC Generic Letter No. 89-06. The checklist assumes that the SPDS has been designed, built and in operation at the plant for some period of time. There are some items in the checklist that are not applicable. In such instances, the AP600 response is "Not Applicable".

1.0 *GENERAL DESCRIPTION*

1.1 *Plant Name:* AP600

1.2 *Who/What organization developed the original version of the SPDS software implemented at your site?*

Westinghouse

1.3 *If the SPDS software has undergone significant modification (i.e., more than 25 percent of software replaced or modified) since original implementation, list the organization performing the modification:*

Not Applicable

1.4 *What is the hardware host on which the current SPDS software is implemented?*

Westinghouse will evaluate the available hardware at the time of plant purchase. See Chapter 7 of the AP600 SSAR.

1.5 *How many total CPUs are accessible by the SPDS software on the computer system described in the previous question?*

See Chapter 7 of the AP600 SSAR. The relevant CPUs are those that drive or provide data for the alarm system (the Wall Panel Information System) and the process graphical displays shown on the workstation VDUs.

1.6 *What is the approximate MIPS rating of all the CPUs counted above?*

The AP600 M-MIS equipment architecture as shown in Chapter 7 of the AP600 SSAR is a distributed network architecture employing an array of layered data highways designed to support through-put of process data and command instructions. Due to this distributed nature, MIPS is not a meaningful term. Sufficient distributed resources will be made available to meet system performance requirements. The data processing requirements are highly distributed, permitting the AP600 M-MIS to take advantage of "parallel processing". This means that several data processing tasks are done simultaneously rather than in series, as is the case with a centralized computer architecture.

If SPDS does not run on a single computer system, provide the following information for the minority parameter set provided by a second computer system. For example, a frequent occurrence of this case is where a separate but adjacent computer terminal provides radiological parameters.

The AP600 M-MIS equipment architecture as shown in Chapter 7 of the AP600 SSAR is a distributed network architecture which does not have a primary or secondary computer. It is task oriented. Different CPUs do different tasks, providing results to others or to VDUs through the network.

1.7 *Manufacturer:*

See Chapter 7 of the AP600 SSAR.

1.8 *Model Number:*

See Chapter 7 of the AP600 SSAR.

1.9 *List parameters provided:*
(on the second system)

The distributed equipment architecture of the AP600 M-MIS supports a distributed computing approach to the allocation of computational tasks. The process parameter data base is distributed throughout the System with no one or even two CPUs containing or holding the entire data base at one time.

1.10 *Are significant changes in hardware or software planned in the next two years?*

See item 1.4, above.

2.0 *PARAMETER SELECTION*

This section is divided into two parts: the safety functions, and the parameters used to depict each safety function.

2.1 *List the title of the Plant-specific safety function(s) displayed on your SPDS that is (are) equivalent to the safety function in Supplement 1 to NUREG-0737.*

The presentation of process data through the abnormality (alarm) messages on the Wall Panel Information System and through the VDU graphical displays is organized around the five safety functions noted in the checklist as items 2.1.1 through 2.1.5. The only exception is item 2.1.2, Core Cooling and Heat Removal. Because the controls and automatic control systems are designed around directly measurable parameters such as RCS temperature, RCS water mass inventory, RCS pressure, RCS circulation, steam generator water level, RHR flow, and RHR heat exchanger delta-temperature, the safety functions will be defined at this level. Aggregating or synthesizing these into a single function of core cooling and heat removal increases operator mental work load. For example, if an abnormality which degrades this function occurs, then the operator must mentally determine which of the sensed variables, or control loops, must be adjusted in order to correct the problem (an issue of control/display integration - see the opening paragraph of Section 5.0 of the Generic Letter checklist).

The AP600 M-MIS will support the operator activity of situation assessment or process state identification, at the same level of abstraction as the control devices with which the operators can take corrective action. There is no core cooling and heat removal switch available on the AP600 workstations, only temperature, pressure, level, and flow. Westinghouse is lowering the level of abstraction for the presentation of the process data relative to this safety function. The level of abstraction that Westinghouse is using for describing the AP600 process functions is the fourth level shown in Fig. 18.6-18.

The other safety functions have a much closer connection to their sensed/controlled variables and require fewer of them than does the Core Cooling and Heat Removal function. The mental workload in translating, interpreting or transforming degradations in the safety function into procedural or corrective actions is reduced.

2.2 *Parameters Selected to Display Each Safety Function*

The purpose of this section is to specify a list of parameters used to depict each of the five safety functions identified in Supplement 1 to NUREG-0737. Lists of parameters that have been found acceptable to NRC through previous SPDS post-implementation reviews have been provided. One list of parameters applies to pressurized water reactors in general, and the other list applies to boiling water reactors.

The AP600 M-MIS includes the display of the variables that depict each of the five safety functions as listed in SSAR Table 7.5-5.

2.3 *Detailed Parameter Questions*

2.3.1 *Are containment isolation demand signals input to SPDS (e.g., PWR - Phase A/B Isolation Demand Signal...)?*

Yes. Engineered safety features actuation signals (reactor trip, safety injection initiation, containment isolation) are signals that are available for display within the AP600 M-MIS.

2.3.2 *Does the SPDS use actual containment isolation valve position as an input to monitor successful isolation?*

Yes, for all remotely-operated containment isolation valves.

3.0 *DISPLAY OF SAFETY FUNCTIONS*

3.1 *Does the SPDS provide the status of all five safety functions on one display page?*

Yes.

3.2 *Are the individual parameters that support the safety functions grouped by safety function?*

Yes.

3.3 *Is the status of all five safety functions always displayed on the SPDS?*

Yes, using the alarm management system.

4.0 *RELIABLE DISPLAY*

4.1 *Is the SPDS hosted on the same computer system as the plant process computer?*

Yes.

If NO, does the SPDS computer receive some of the computer point inputs from the process computer?

Not applicable.

4.2 *List location of accessible(e.g., keyboards) devices capable of changing SPDS data.*

The design includes the capability to build password or key-lock accessibility on nearly every part of the M-MIS database (see Chapter 7 of the AP600 M-MIS). In addition, the system carries and displays data quality on each piece of data in the system. The data quality scheme is capable of including a data quality that is appropriate for "MANUALLY ENTERED" data, if needed.

4.3 *Are SPDS hardware availability data documented?*

No, such data is not available.

4.4 *Are the SPDS computer points included in the routine instrument loop surveillance?*

Yes. The instruments that are necessary to support the SPDS functions are included in the M-MIS maintenance surveillance.

4.5 *What percentage of software verification and validation has been completed?*

See WCAP-14080, "AP600 Instrumentation and Control Software Description."

4.6 *Have changes to the SPDS host computer and software been maintained under a formal Software/Hardware Change Request (or equivalent) system?*

See WCAP-14080, "AP600 Instrumentation and Control Software Description."

4.7 *How frequently does the SPDS display invalid or erroneous information?*

Not Applicable.

4.8 *How frequently have any of the critical safety functions been in a false alarm condition?*

Not Applicable.

4.9 *Does the SPDS display valid parameter information during adverse containment conditions?*

Yes, for data derived from qualified sensors.

5.0 *HUMAN FACTORS*

Human factors in the context of SPDS design includes the usefulness of the technical information displayed on the screen to users and their performance during emergency operations. Human factors also includes display design techniques, such as labeling, display layout, and control/display integration.

This section provides a sample of the kinds of questions to be asked to help determine the degree to which the SPDS incorporates accepted human factors principles.

5.1 *Who is the prime user of the SPDS?*

SPDS data and data display organization are available to the entire control room staff.

Since the AP600 M-MIS design philosophy is an extension of that dictated by the SPDS requirements, particularly in the application of human factors, the plant process data organization and techniques of presentation to each of the users complies with the SPDS requirements. There are anticipated to be some differences in the abstraction level and plant scope of the data presentations to the Shift Supervisor, Shift Technical Advisor or Operators.

5.2 *Are All SPDS controls located at the SPDS workstation?*

Yes.

5.3 *Is all SPDS-related information physically displayed such that the information can clearly be read from the SPDS user's typical position?*

Yes.

5.4 *How are SPDS displays accessed?*

On the workstation CRTs using a cursor.

5.5 *Does the SPDS consistently respond to user commands in less than 10 seconds?*

Yes.

5.6 *Does the SPDS sampling rate for parameters match the display update rate for those parameter?*

Yes.

5.7 *Are all parameter units of measure displayed on SPDS consistent with the units of measure included in the Emergency Operating Procedures?*

Yes.

5.8 *Are all parameter labels and abbreviations consistent with the labels and abbreviations included in the emergency operating procedures?*

Yes.

5.9 *Is any of the displayed information in a form that requires transformation or calculation?*

No.

5.10 *Are the high-and low-level setpoints consistent with hard-wired parameter instrumentation and reactor protection system setpoints?*

Yes, the high- and low-level setpoints are consistent with the reactor protection system setpoints and any hardwired parameter instrumentation setpoints. The intent is not to have hardwired instrumentation.

5.11 *Does SPDS display high-and low-level setpoints?*

Yes.

5.12 *Are the SPDS calculated values such as subcooling margin, consistent with calculated values on the plant process computer?*

Yes.

5.13 *Are all parameter units of measure displayed on SPDS consistent with the hard-wired instrumentation?*

Yes, see item 5.10.

5.14 *Are all parameter labels and abbreviation consistent with hard-wired instrument labels and abbreviations?*

Yes, see item 5.10.

5.15 *Were the technical basis for software specifications verified with plant-specific data (for example, heat-up and cool-down limits, variable steam generator setpoints and high and low level alarm setpoints)?*

Yes.

5.16 *List LERs written as a result of SPDS software problems.*

Not applicable.

6.0 *TRAINING*

6.1 *Does the simulator training include training in the use of the SPDS?*

Yes.

6.2 *How long is formal classroom training for SPDS users?*

Since the SPDS requirements are fully integrated into the AP600 control room resources, training along the lines described in Section 18.9.9 of the AP600 SSAR is training that is applicable to the SPDS functions.

6.3 *Is there periodic requalification training for SPDS?*

Yes, see SSAR Subsection 18.9.9.

6.4 *When are SPDS users given training regarding the relationship of the parameters to the plant safety functions?*

See item 6.2 above.

7.0 *ELECTRICAL ISOLATION*

7.1 *What isolation devices are currently used?*

See SSAR Chapter 7.

7.2 *Are these devices the same ones that were originally installed and approved by NRC?*

Not applicable.

Bypassed and Inoperable Status Indication

The following discussion addresses each of the criteria contained in the four paragraphs of Section C of U. S. Atomic Energy Commission Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, May 1973.

Position C.1 *Administrative procedures should be supplemented by a system that automatically indicates at the system level the bypass or deliberately induced inoperability of the protection system and the systems actuated or controlled by the protection system.*

AP600 design: The bypassed or deliberately-induced inoperability of equipment is displayed in both the abnormality messages of the AP600 M-MIS alarm system and in the graphic representations of equipment state and system functions in the process displays.

There are two aspects of the AP600 M-MIS design that work together to provide this capability. First, the distributed M-MIS hardware and software architecture is designed so that data is shared by all users. The intent of this sharing is to improve the coordination and communication of plant personnel and to maximize the cost effective use of computational resources within the M-MIS. This means, for example, that within the AP600 M-MIS architecture, the switching and tagging (S&T) center makes available for use in other workstations the data related to equipment outage due to testing and maintenance. This is a general rule, not confined to equipment that is safety-related. This data is then incorporated in the AP600 M-MIS control room displays and alarm messages.

Second, the general organization of data presentation (i.e., process displays and abnormality messages) is based on the concept of plant process functions. This concept is realized in the AP600 M-MIS design process in the form of the Function Based Task Analysis. By organizing the presentation of plant data around plant process functions, the impact of disabled or degraded equipment is reflected on and linked directly to the purposes of that equipment. A plant system definition does not necessarily reflect the equipment's purpose or it may only represent one of its many purposes.

The AP600 M-MIS shares data so that change of state in equipment that is the result of the switching and tagging operation is available for use in the displays and the alarm messages. The presentation of process data is organized around the concept of plant process functions so that the operator can better understand the operational consequences of equipment degradation, failure and reconfiguration. This is true for the equipment monitored by the M-MIS, not just the safety-related equipment.

Position C.2 *The indicating system of C.1. above should also be activated automatically by the bypassing or deliberately induced inoperability of any auxiliary or supporting system that effectively bypasses or renders inoperable the protection system and the systems actuated or controlled by the protection system.*

AP600 design: As noted in the response to C.1., above, this kind of operation is inherent in the operation and performance of the AP600 M-MIS. Changes in the availability of equipment, systems, and system purpose are displayed through the alarm system abnormality messages and the graphical process displays.

Position C.3 *Automatic indication in accordance with C.1. and C.2. above should be provided in the control room for each bypass or deliberately induced inoperable status that meets all of the following conditions:*

a. Renders inoperable any redundant portion of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety-related functions;

b. Is expected to occur more frequently than once per year; and

c. Is expected to occur when the affected system is normally required to be operable.

AP600 design: AP600 M-MIS design includes instrumentation of the safety-related equipment to a level that meets these requirements. This is also required in order to meet the Reg. Guide 1.97 (Post-Accident Monitoring) requirements. For auxiliary, supporting systems and other nonsafety-realted equipment, manual entry of equipment state data into the AP600 M-MIS will be done at the switching and tagging center.

Position C.4 *Manual capability should exist in the control room to activate each system-level indicator provided in accordance with C.1. above.*

AP600 design: Since the requirements of C.1., above, are an integral part of the design, operation and performance of the AP600 M-MIS, there is no separate display or analysis capability to be manually activated. The data gathering and display processing necessary to meet this requirement is always operational.

SSAR Revision: NONE