November 7, 1997

Mr. Nicholas J. Liparulo, Manager
Nuclear Safety and Regulatory Analysis
Nuclear and Advanced Technology Division
Westinghouse Electric Corporation
P.O. Box 355
Pittsburgh, PA 15230

SUBJECT: OPEN ITEMS ASSOCIATED WITH CHAPTER 19 OF THE AP600 SAFETY EVALUATION REPORT (SER)

Dear Mr. Liparulo:

The Probabilistic Safety Assessment Branch has provided an SER for Chapter 19. The SER provided was for the level 1 portion of the probabilistic risk assessment. However, the input to these sections contained some open items. These open items have been extracted from the SER and can been found in Enclosure 1 to this letter.

You have requested that portions of the information submitted in the June 1992, application for design certification be exempt from mandatory public disclosure. While the staff has not completed its review of your request in accordance with the requirements of 10 CFR 2.790, that portion of the submitted information is being withheld from public disclosure pending the staff's final determination. The staff concludes that these follow on questions do not contain those portions of the information for which exemption is sought. However, the staff will withhold this letter from public disclosure for 30 calendar days from the date of this letter to allow Westinghouse the opportunity to verify the staff's conclusions. If, after that time, you do not request that all or portions of the information in the enclosures be withheld from public disclosure in accordance with 10 CFR 2.790, this letter will be placed in the Nuclear Regulatory Commission Public Document Room.

If you have any questions regarding this matter, you may contact me at (301) 415-1132.

Sincerely,

original signed by:

Joseph M. Sebrosky, Project Manager
Standardization Project Directorate
Division of Reactor Program Management
Office of Nuclear Reactor Regulation

Docket No. 52-003

Enclosure: As stated

cc w/encl: See next page

DISTRIBUTION: See next page

1/1 DF03

DOCUMENT NAME: A: SPSB_LV1.RAI
To receive a copy of this document, indicate in the box: "C" = Copy without attachment/enclosure "E" = Copy with attachment/enclosure "N" = No copy

OFFICE	PM:PDST:DRPM		SPSB:DSSA		SPSB:DSSA		SPSB:DSSA	E	D:PDST:DRPM	
NAME	JSebrosky:sg	/1/6	NSaltos	NTS	MPohida	MP	AEl-Bassioni	AEB	TQuay	TQ
DATE	11/6 /97		11/6 /97		11/6 /97		11/6 /97		11/7/97	

OFFICIAL RECORD COPY

Mr. Nicholas J. Liparulo
Westinghouse Electric Corporation

Docket No. 52-003
AP600

cc: Mr. B. A. McIntyre
Advanced Plant Safety & Licensing
Westinghouse Electric Corporation
Energy Systems Business Unit
P.O. Box 355
Pittsburgh, PA 15230

Ms. Cindy L. Haag
Advanced Plant Safety & Licensing
Westinghouse Electric Corporation
Energy Systems Business Unit
Box 355
Pittsburgh, PA 15230

Enclosure to be distributed to the following addressees after the result of the proprietary evaluation is received from Westinghouse:

Mr. Russ Bell
Senior Project Manager, Programs
Nuclear Energy Institute
1775 I Street, NW
Suite 300
Washington, DC 20006-3706

Dr. Craig D. Sawyer, Manager
Advanced Reactor Programs
GE Nuclear Energy
175 Curtner Avenue, MC-754
San Jose, CA 95125

Barton Z. Cowan, Esq.
Eckert Seamans Cherin & Mellott
600 Grant Street 42nd Floor
Pittsburgh, PA 15219

Mr. Frank A. Ross
U.S. Department of Energy, NE-42
Office of LWR Safety and Technology
19901 Germantown Road
Germantown, MD 20874

Mr. Ed Rodwell, Manager
PWR Design Certification
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303

Ms. Lynn Connor
DOC-Search Associates
Post Office Box 34
Cabin John, MD 20818

Mr. Robert H. Buchholz
GE Nuclear Energy
175 Curtner Avenue, MC-781
San Jose, CA 95125

Mr. Sterling Franks
U.S. Department of Energy
NE-50
19901 Germantown Road
Germantown, MD 20874

Mr. Charles Thompson, Nuclear Engineer
AP600 Certification
NE-50
19901 Germantown Road
Germantown, MD 20874

DISTRIBUTION: Letter to Mr. Nicholas J. Liparulo, Dated: November 7, 1997
*Docket File *Enclosure to be held for 30 days
*PUBLIC
PDST R/F
TQuay
JSebrosky
TKenyon
BHuffman
JNWilson
DScaletti
JMoore, O-15 B18
WDean, O-5 E23
ACRS (11)
NSaltos, O-10 E4
MPohida, O-10 E4
RPalla, O-8 H7
MSnodderly, O-8 H7

OPEN ITEM ASSOCIATED WITH CHAPTER 19
(Level 1 Portion of the Probabilistic Risk Assessment)

720.430F

The staff's review of the AP600 shutdown PRA is based on the results reported in draft Attachment 54B of the PRA and additional references from Attachment 54A and Chapter 54. Attachment 54B is a requantification of the baseline shutdown PRA results given that 1-out-of-4 4th stage ADS valves must open during reduced inventory conditions for successful gravity injection from the IRWST. Given this success criteria change, Westinghouse agreed to: (a) attach Attachment 54B to the shutdown PRA, (b) clearly document in Attachment 54B that these results represent a re-quantification of the shutdown PRA and should be used to derive insights, (c) update the shutdown PRA results in Chapter 59, and (d) correct the shutdown PRA results contained in the Shutdown Evaluation Report (WCAP-14837). These actions represent an open item.

720.431F

According to Chapter 54, recirculation is not required before 72 hours. Westinghouse has been requested to re-evaluate whether recirculation will be required before 72 hours. This re-evaluation represents an open item.

720.432F

Westinghouse has proposed availability controls on Normal Residual Heat Removal system (RNS) and its support systems (Service Water System (SWS), Component Cooling Water System (CCS), and AC power) when Reactor Coolant System (RCS) level is not visible in the pressurizer until the refueling cavity is half full and the upper internals are removed. The staff's review found that this additional regulatory oversight for RNS and its support systems (CCW, SSW and AC power) must be extended to Mode 5 operation when the RCS is open. Westinghouse needs to modify Section 16.3 of the SSAR to require additional regulatory oversight for RNS and its support systems (CCW, SSW and onsite AC power) for the whole period of Mode 5 when the RCS open. This is an open item.

720.433F

Westinghouse must include in Chapter 57 of the PRA the additional findings related to mid-loop operation during shutdown from their last revision of the fire risk analysis. The revision to the fire risk analysis was documented in Enclosure 2 of a September 29, 1997, letter (NSD-NRC-97-5347) from Westinghouse. This is an open item.

720.434F

As documented in a May 13, 1997, meeting summary of an April 15, 1997, meeting, Westinghouse proposed that the staff's set of insights resulting from their review of the PRA be shared with Westinghouse. Unless Westinghouse determined that there was technically incorrect information in the staff's list there would be no new meetings or information transfer, and the staff's insights would be added to the Westinghouse insights. To that end Enclosure 2 contains the staff's insights as a result of the review of the level 1 PRA. Enclosure 2 contains additional insights from those contained in Chapter 59 of Westinghouse's PRA. Incorporation of the additional insights that exist in Enclosure 2 to the Westinghouse insights is an open item.

Staff Insights as a Result of the Review of the AP600 Level 1 PRA

General & plant-wide requirements

1. WEC will maintain a list of risk important systems, structures and components (SSCs) in the D-RAP.

2. The COL Applicant should perform a seismic walkdown to ensure that the as-built plant conforms to the assumptions in the AP600 PRA-based seismic margins analysis and to assure that seismic spatial systems interactions do not exist. Details of the seismic walkdown will be developed by the COL applicant.

3. WEC will maintain a list of the SSC HCLPF values used in the AP600 Seismic Margins Assessment in the D-RAP. The COL Applicant should compare the as-built SSC HCLPFs to those assumed in the AP600 seismic margins analysis (SMA). Deviations from the HCLPF values or assumptions in the SMA should be evaluated by the COL Applicant to determine if any vulnerabilities have been introduced.

4. The COL Applicant will maintain an operation reliability assurance process based on the system reliability information derived from the PRA and other sources. The COL Applicant should incorporate the list of risk-important SSCs, as presented in the SSAR section on D-RAP, in its D-RAP and operation reliability assurance process.

5. The COL applicant should consider the information on risk-important operator actions from the PRA, as presented in Chapter 18 of the SSAR on human factors engineering, in developing and implementing procedures, training and other human reliability related programs.

6. During detailed design phase, the COL Applicant should update the PRA using the final design information and site-specific information. As deemed necessary, the COL Applicant should update the PRA, including the fire and flood analyses for both at-power and shutdown operation. Based on site-specific information, the COL Applicant should also re-evaluate the qualitative screening of external events. If any site specific susceptibilities are found, the applicable external event should be included in the updated PRA.

7. No safety-related equipment is located outside the Nuclear Island.

8. The AP600 low pressure systems which interface with the RCS are protected against interfacing systems LOCA (ISLOCA) by a combination of multiple isolation valves, valve interlocking, increase in the piping pressure limits and pressure relief capability.

9. Solid state switching devices and electro-mechanical relays resistant to relay chatter will be used in the AP600 I&C systems. Use of these devices and relays either eliminates or minimizes the mechanical discontinuities associated with similar devices at operating reactors.

10. There are no watertight doors used for flood protection in the AP600 design.

11. The AP600 design minimizes potential flooding sources in safety-related equipment areas, to the extent possible. The design also minimizes the number of penetrations through enclosure or barrier walls below the probable maximum flood level. All flood barriers (e.g., walls, floors and penetrations) are designed to withstand the maximum anticipated hydrodynamic loads as well as water pressures generated by floods in adjoining areas.

12. Drains are capable to remove flow from an assumed break in a line up to 4" in diameter and include features, such as check valves and siphon breaks, that prevent backflow.

13. There is no cable spreading room in the AP600 design.

14. The separation of equipment and cabling associated with different divisions of safety-related equipment as well as the separation of safety-related from nonsafety-related equipment, minimizes the likelihood that a fire or flood would affect more than one safety-related system or train.

15. The following minimize the probability for fire or flood propagation from one area to another and helps limit risk from internal fires and floods:

    - Fire barriers are sealed and flood barriers are watertight.

    - Each fire door is alarmed in the control room.

    - The COL Applicant will ensure the reliable performance of fire barriers through appropriate inspection and maintenance of doors, dampers, and penetration seals. Also, all water tight penetrations will be maintained with high reliability during power operation to prevent the propagation of water from one area to the next.

    - The COL Applicant will ensure the availability of proper fire fighting equipment in all plant areas, and especially in the most risk significant fire areas.

    - The COL Applicant will maintain an adequately staffed, well-trained, and well-prepared fire brigade.

    - When a fire door, fire barrier penetration, or flood barrier penetration must be open to allow specific maintenance (e.g., during plant shutdown), appropriate compensatory measures will be taken to minimize risk. Risk during shutdown is minimized by appropriate outage management, administrative controls, procedures, and operator knowledge of plant configuration. In particular, this will require configuration control of fire/flood barriers to ensure the integrity of fire and flood barriers between areas containing equipment performing redundant safe shutdown functions.

    - Drains include features, such as check valves and siphon breaks, that prevent backflow.

16. Fire detection and suppression capability as well as flooding control features and sump level indication are provided in the AP600 design. Appropriate compensatory measures will be taken by the COL Applicant to maintain adequate detection and suppression capability during maintenance activities.

17. In addition to the MCR which has its own dedicated ventilation system, separate ventilation systems are provided for each of the two pairs of safety-related equipment divisions supporting redundant functions (i.e., divisions A&C and B&D). Furthermore, the plant ventilation systems include features to prevent propagation of smoke from a non-safety related area to a safety-related area or between safety-related areas supported by two different divisions. The COL holder must ensure the reliable performance of such smoke propagation prevention features.

18. The COL applicant should implement the maintenance guidelines as described in the Shutdown Evaluation Report (WCAP14837)

19. The COL applicant should control transient combustibles during shutdown operations.

Main Control Room (MCR) and Remote Shutdown Workstation (RSW)

1. The automatic function of the AP600 actuation systems (i.e., PMS and DAS) is not affected by a fire in either the MCR or the RSW. This ensures an independent, automatic means, to reach safe shutdown even when a fire occurs in the MCR or the RSW (manual actuation is not needed unless the automatic actuation fails). Also, even though a fire in the MCR may defeat manual actuation of equipment from the MCR, it will not affect the manual operation from the RSW. This is because the I&C cabinets are located in fire areas outside the MCR and the RSW.

2. Redundancy in MCR operations, in terms of both monitoring and manual control of safe shutdown equipment, is provided within the MCR itself. This provides an alternative means for mitigating certain MCR fires before deciding to evacuate the MCR and use the RSW.

3. If MCR evacuation is necessary, the RSW provides complete redundancy in terms of control for all safe shutdown functions.

4. The MCR has its own dedicated ventilation system and is pressurized. This eliminates the possibility of smoke, hot gases, and fire suppressants, originated in areas outside the MCR, to migrate via the ventilation system to the control room.

5. The MCR and the RSW are in separate fire and flood areas. They have separate and independent ventilation systems.

6. AP600 MCR fire ignition frequency is limited as a result of the use of low-voltage, low-current equipment and fiber optic cables.

Containment/Shield Building

1. Containment isolation functions are protected from the impact of internal fires and floods by redundant containment isolation valves in each line

which are located in separate fire and flood areas and, if powered, are served by different power and control divisions. Always, one isolation component in a given line is located inside containment, while the other is located outside containment, and the containment wall is a fire/flood barrier.

2. Although the containment is a single fire area, redundant divisions are generally separated by continuous structural or fire barriers without penetrations and by labyrinth passageways. In a few situations, the divisions are separated by large open spaces without intervening combustibles.

3. There are only two compartments inside containment (PXS-A and PXS-B) containing safe shutdown equipment other than containment isolation valves that are floodable (i.e., below the maximum flood height). Each of these two compartments contains redundant and essentially identical equipment (one accumulator with associated isolation valves as well as isolation valves for one CMT, one IRWST injection line and one containment recirculation line). These two compartments are physically separated by 2 or 3-foot walls and floor slabs to ensure that a flood in one compartment does not propagate to the other. Drain lines from the PXS-A and PXS-B compartments to the reactor vessel cavity and steam generator compartment are protected from backflow by redundant backflow preventers.

4. Containment isolation valves located below the maximum flood height inside containment or in the Auxiliary Building are normally closed and are designed to fail closed when submerged.

5. The fragility of valve rooms, labeled 11206/11207, where the passive core cooling system valves are concentrated is an important factor in the AP600 capability to withstand earthquakes. The capacity of the as-built SSCs to meet the HCLPF values assumed in the AP600 PRA will be checked by a seismic walkdown.

6. The passive containment cooling system (PCS) cooling water not evaporated from the vessel wall flows down to the bottom of the inner containment annulus into floor drains. The redundant floor drains rout the excess water to storm drains. The drain lines are always open (without isolation valves) and each is sized to accept maximum PCS flow. The interface with the storm drain system is an open connection such that any blockage in the storm drains would result in the annulus drains overflowing the connection, draining the annulus independently of the storm drain system.

7. The annulus floor drains, which are essentially pipes embedded into the wall of the Shield Building, will have the same (or higher) HCLPF value as the Shield Building. This ensures that the drain system will not fail at lower acceleration levels causing water blocking of the PCS air baffle.

8. The COL applicant should develop and implement policies, procedures, and training to close containment penetrations during Modes 5 and 6 in accordance with TS 3.6.8.

Auxiliary Building

1. Separate ventilation systems are provided for each of the two pairs of safety-related equipment divisions supporting redundant functions (i.e., divisions A&C and B&D). This prevents smoke, hot gases, and fire suppressants originating in divisions A or C from propagating to divisions B and D.

2. The major rooms housing divisional cabling and equipment (the battery rooms, DC equipment rooms, I&C rooms, and penetration rooms) are separated by 3-hour rated fire walls without openings. There are no doors, dampers, or seals in these walls. The rooms are served by separate ventilation subsystems. In order for a fire to propagate from one divisional room to another, it must move past a 3-hour barrier (e.g., a door) into a common corridor and enter the other room through another 3-hour barrier (e.g., another door).

3. A two-foot concrete floor (barrier) protects important safety-related I&C equipment as well as the main control room and the remote shutdown panel, located in the north end of the Auxiliary Building, from potential debris produced by a postulated seismically-induced structural collapse of the adjacent Turbine Building and propagated through the access bay separating the two buildings.

4. There are no connections to sources of "unlimited" quantity of water in the Auxiliary Building.

5. To ensure that a flooding in a radiologically controlled area (RCA) in the Auxiliary Building does not propagate to non-RCAs (where all safety-related equipment except for some containment isolation valves is located), the non-RCAs are separated from the RCAs by 2 and 3-foot walls and floor slabs. In addition, electrical penetrations between RCAs and non-RCAs in the Auxiliary Building are located above the maximum flood level.

6. The two 72-hour rated Class 1E division B and C batteries are located above the maximum flood height in the Auxiliary Building considering all possible flooding sources (including propagation from sources located outside the Auxiliary Building).

7. Flood water propagated from the Turbine Building to the Auxiliary Building valve/piping penetration room at grade level (the only Auxiliary Building area that interfaces with the Turbine Building) is directed to drains and to outside through access doors. This, combined with the presence of water tight walls and floor of the valve/penetration room, limits the maximum flood height in the valve/piping penetration room (to about 36 inches) and ensures that the flooding does not propagate beyond this area.

8. The mechanical and electrical equipment in the Auxiliary Building are separated to prevent propagation of leaks from the piping and mechanical areas to the Class 1E electrical and Class 1E I&C equipment rooms.

Turbine Building

1. No safety-related equipment is located in the turbine building. There is a 3-hour fire barrier wall between the turbine building and the safety-related areas of the Nuclear Island.

4. Connections to sources of "large" quantity of water are located in the Turbine Building. They are the service water system (SWS) which interfaces with the component cooling water system (CCS) and the circulating water system (CWS) which interfaces with the turbine building closed cooling system (TCS) and the condenser. Features that minimize flood propagation to other buildings are:

   - Flow from any postulated ruptures above grade level (elevation 100'- 0") in the Turbine Building flows down to grade level via floor grating and stairwells. This grating in the floors also prevents any significant propagation of water to the Auxiliary or Annex Buildings via flow under the doors.

   - A relief panel in the Turbine Building west wall at grade level directs the water outside the building to the yard and limits the maximum flood level in the Turbine Building to less than 6 inches. Flooding propagation to areas of the adjacent Auxiliary and Annex Buildings, via flow under doors or backflow through the drains, is possible but is bounded by a postulated break in those areas.

Annex Building

1. There is no safety-related equipment located in the Annex Building.

2. Flood water in the Annex Building grade level is directed by the sloped floor to drains and to the yard area through the front door of the Annex Building.

3. Flow from any postulated ruptures above grade level in the Annex Building is directed by floor drains to the Annex Building sump which discharges to the Turbine Building drain tank. Alternate paths include flows to the Turbine Building via flow under access doors and down to grade level via stairwells and elevator shaft.

4. The floors of the Annex Building are sloped away from the access doors to the Auxiliary Building in the vicinity of the access doors to prevent migration of flood water to the non-radiologically controlled areas of the Nuclear Island where all safety-related equipment, except for some containment isolation valves, is located. [ITAAC].

5. There are no connections to sources of "unlimited" quantity of water in the Annex Building.

Reactor Coolant System

1. To prevent overdraining, the RCS hot and cold legs are vertically offset which permits draining of the steam generators for nozzle dam insertion with a hot leg level much higher than traditional designs. This level is nominally 80 percent level in the hot leg.

2. To lower the level in that hot leg the vortexing can occur, a step nozzle connection between the RCS hot leg and the RHR suction line is used. The step nozzle is a 20 inch schedule 140 pipe, approximately 2 feet long.

3. Should vortexing occur, the maximum air entrainment into the pump suction was shown experimentally to be no greater than 5 percent.

4. There are two safety-related RCS hot leg level channels, one located in each hot leg. These level instruments are independent and do not share instrument lines. These level indicators are provided primarily to monitor RCS level during midloop operations. One level tap is at the bottom of the hot leg, and the other tap is on the top of the hot leg as close to the steam generator as possible.

5. Wide range pressurizer level indication (cold calibrated) is provided that can measure RCS level to the bottom of the hot legs. The upper level tap is connected to an ADS valve inlet header above the top of the pressurizer. The lower level tap is connected to the bottom of the hot leg. This non-safety related pressurizer level indication can be used as an alternative way of monitoring level and can be used to identify inconsistencies in the safety related hot leg level instrumentation.

6. The RNS pump suction line is sloped continuously upward from the pump to the reactor coolant system hotleg with no local high points. This design eliminates potential problems in refilling the pump suction line if a RNS pump is stopped when cavitating due to excessive air entrainment. This self-venting suction line allows the RNS pumps to be immediately restarted once an adequate level in the hot leg is re-established.

7. The COL applicant should have procedures and policies to maximize the availability of the non-safety related wide range pressurizer level indication (cold calibrated) during RCS draining operations during cold shutdown. The operators shall be trained to use this indication to identify inconsistencies in the safety related hot leg level instrumentation to prevent RCS overdraining.

Passive Core Cooling Systems (PXS)

The passive core cooling system (PXS) is composed of (1) the accumulator subsystem, (2) the core makeup tanks (CMTs) subsystem, (3) the in-containment refueling water storage tank (IRWST) subsystem, and (4) the passive residual heat removal (PRHR) subsystem. In addition, the automatic depressurization system (ADS), which is part of the reactor coolant system (RCS), also supports passive core cooling functions.

Accumulators

The accumulators provide a safety-related means of safety injection of borated water to the RCS. The following are some important aspects of the accumulator subsystem as represented in the PRA:

- There are two accumulators, each with an injection line to the reactor vessel/direct vessel injection (DVI) nozzle. Each injection line has two check valves in series.

- The reliability of the accumulator subsystem is important. The COL will maintain the reliability of the accumulator subsystem.

- Diversity between the accumulator check valves and the CMT check valves minimizes the potential for common cause failures.

Core Makeup Tanks (CMTs)

The CMTs provide safety-related means of high-pressure safety injection of borated water to the RCS. The following are some important aspects of CMT subsystem as represented in the PRA:

- There are two CMTs, each with an injection line to the reactor vessel/DVI nozzle. Each CMT has a normally open pressure balance line from an RCS cold leg. Each injection line is isolated with a parallel set of air-operated valves (AOVs) which open on loss of Class 1E dc power, loss of air, or loss of the signal from the PMS. The injection line for each CMT also has two normally open check valves in series.

- The CMT AOVs are automatically and manually actuated from PMS and DAS and their positions are indicated and alarmed in the control room.

- CMT level instrumentation provides an actuation signal to initiate automatic ADS and provides the actuation signal for the IRWST squib valves to open.

- The CMTs are risk-important for power conditions because the level indicators in the CMTs provide an open signal to ADS and to the IRWST squib valves as the CMTs empty. The COL will maintain the reliability of the CMT subsystem. These AOVs are stroke-tested quarterly.

- CMT is required by the Technical Specifications to be available from power conditions down through cold shutdown with RCS pressure boundary intact.

In-Containment Refueling Water Storage Tank (IRWST)

The IRWST subsystem provides a safety-related means of performing (1) low-pressure safety injection following ADS actuation, (2) long-term core cooling via containment recirculation, and (3) reactor vessel cooling through the flooding of the reactor cavity by draining the IRWST into the containment. The following are some important aspects of the IRWST subsystem as represented in the PRA:

- IRWST subsystem has the following flowpaths:

  - Two (redundant) injection lines from IRWST to reactor vessel DVI nozzle. Each line is isolated with a parallel set of valves; each set with a check valve in series with a squib valve.

  - Two (redundant) recirculation lines from the containment to the IRWST injection line. Each recirculation line has two paths: one path contains a squib valve and a MOV, the other path contains a squib valve and a check valve.

- The two MOV/squib valve lines also provide the capability to flood the reactor cavity.

- There are screens for each IRWST injection line and recirculation line which ensure that they are not clogged by debris or other materials generated in the IRWST or containment sump. The COL Applicant will maintain the reliability of such screens.

- Explosive (squib) valves provide the pressure boundary and protect the check valves from any potential adverse impact of high differential pressures.

- The Squib valves and MOVs are powered by Class 1E dc power and their positions are indicated and alarmed in the control room.

- The squib valves and MOVs for injection and recirculation are automatically and manually actuated via PMS, and manually actuated via DAS.

- The squib valves and MOVs for reactor cavity flooding are manually actuated via PMS and DAS from the control room.

- Diversity of the squib valves in the injection lines and recirculation lines minimizes the potential for common cause failure between injection and recirculation/reactor cavity flooding.

- Automatic IRWST injection at shutdown conditions is provided using PMS low hot leg level logic.

- IRWST injection and recirculation check valves are exercised at each refueling. IRWST injection and recirculation squib valve actuators are tested every 2 years for 20 percent of the valves. IRWST recirculation MOVs are stroke-tested quarterly.

- The reliability of the IRWST subsystem is important. The COL will maintain the reliability of the IRWST subsystem.

- IRWST injection and recirculation are required by Technical Specifications to be available from power conditions to refueling without the cavity flooded.

The IRWST provides a safety-related long term source of water during shutdown conditions. The following are some additional important aspects of the IRWST subsystem as represented in the shutdown PRA.

- The COL applicant should provide administrative controls to control trash generated during shutdown operations from entering the RCS and the IRWST which could possibly plug the screens.

- On low hot leg level, the PMS actuates the squib valves to open allowing gravity injection from the IRWST.

Passive Residual Heat Removal (PRHR) System

The PRHR provides a safety-related means of performing the following functions: (1) removes core decay heat during accidents, (2) allows adequate

plant performance during transient (non-LOCA and non-ATWS) accidents without ADS, (3) allows automatic termination of RCS leak during a SGTR accident without ADS, and (4) provides core cooling and pressure control during the early phase of an ATWS accident.

The following important aspects of the PRHR design and operation features are incorporated in the PRA models:

- PRHR is actuated by opening redundant parallel air-operated valves (AOVs). These AOVs are designed to fail open on loss of Class 1E power, loss of air, or loss of signal from the protection and safety monitoring system (PMS).

- The PRHR AOVs are automatically actuated by two redundant and diverse I&C systems: (1) the safety-related protection and safety monitoring system (PMS) and (2) the nonsafety-related diverse actuation system (DAS). The PRHR can also be actuated manually from the control room using either PMS or DAS.

- Diversity of the PRHR AOVs from the AOVs in the core makeup tanks (CMTs) minimizes the probability for common cause failure of both PRHR and CMT AOVs.

- The positions of the inlet and outlet PRHR valves are indicated and alarmed in the MCR.

- The PRHR AOVs and isolation MOV are tested quarterly. The PRHR HX is flow tested at shutdown.

- Use of the PRHR heat exchanger (HX) for long-term cooling causes the IRWST water to heat up, resulting in inventory loss through evaporation. To ensure successful long-term cooling by the PRHR HX, the evaporated IRWST inventory must return to the IRWST after condensed on the containment liner and collected in the IRWST gutter system. The IRWST gutter system, which directs the water to the containment sump during normal plant operation, is automatically re-aligned to direct the water back to the IRWST during an accident. The following design features ensure proper re-alignment of the gutter system valves to direct water to the IRWST during accidents:

  - the IRWST gutter and its isolation valves are safety grade

  - the valves that re-direct the flow are designed to fail-safe on loss of compressed air, loss of Class 1E DC power, or loss of the PMS signal.

  - the isolation valves are actuated automatically by PMS and DAS.

- Use of the PRHR HX for long-term cooling will result in steaming to the containment. The steam will normally condense on the containment shell and return to the IRWST via the gutter system. If the condensate does not return to the IRWST, the IRWST volume is sufficient for at least 72 hours of PRHR operation. Connections to the IRWST are provided from the spent fuel system (SFS) and chemical and volume control system (CVS)

to extend PRHR operation. A safety-related makeup connection is also provided from outside the containment through the normal residual heat removal system (RNS) to the IRWST.

- Capability exists in the control room to identify a leak in the PRHR HX which could degrade to a tube rupture under the stress conditions, such as RCS pressure increase and temperature gradients inside the HX tube walls, likely to occur during a postulated accident requiring PRHR operation.

- Technical Specifications require the PRHR to be available, with RCS boundary intact, from power conditions down through cold shutdown. Guidance is provided for operator action when a leak is detected in the PRHR HX which could degrade to a tube rupture during normal power operation conditions or under stress conditions, such as RCS pressure increase and temperature gradients inside the HX tube walls, likely to occur during a postulated accident requiring PRHR operation.

- The PRHR systems provides a safety related means of removing decay heat following loss of shutdown cooling during safe/cold shutdown with the RCS intact.

Automatic Depressurization System (ADS)

ADS provides a safety-related means of depressurizing the RCS. The following are some important aspects of ADS as represented in the PRA:

- ADS has four stages. Each stage is arranged into two separate groups of valves and lines. Stages 1,2, and 3 discharge from the top of the pressurizer to the IRWST. Stage 4 discharges from the hot leg to the RCS loop compartment.

- Each stage 1, 2, and 3 line contains two MOVs in series. Each stage 4 line contains an MOV valve and a squib valve in series.

- The valve arrangement and positioning for each stage is designed to reduce spurious actuation of ADS.

  - Stage 1, 2, and 3 MOVs are normally closed and have separate controls.

  - Each stage 4 squib valve has redundant, series controllers.

  - Stage 4 is blocked from opening at high RCS pressures.

- The ADS valves are automatically and manually actuated via the protection and safety monitoring system (PMS), and manually actuated via the diverse actuation system (DAS).

- The ADS valves are powered from Class 1E dc power and their positions are indicated and alarmed in the control room.

- Stage 1, 2, and 3 valves are stroke-tested every 6 months. Note: Westinghouse has indicated that this requirement may change as a result of an NRC review. Stage 4 squib valve actuators are tested every 2 years for 20 percent of the valves.

- The reliability of the ADS is important. The COL will maintain the reliability of the ADS.

- ADS is required by the Technical Specifications to be available from power conditions down through refueling without the cavity flooded.

- Depressurization of the RCS through ADS minimizes the potential for high-pressure melt ejection events. Procedures will be provided for use of the ADS for depressurization of the RCS during a severe accident.

- Fire-induced hot shorts, especially in I&C copper cables from the protection logic cabinets to the squib valve operators, could cause detonation of a squib valve. This risk important concern should be addressed by appropriate power and control cable separation and routing and by the incorporation of features and requirements in the detailed design of ADS cabling.

- The first, second, and third-stage valves, connected to the top of the pressurizer, provide a vent path to preclude pressurization of the RCS during shutdown conditions if decay heat removal is lost. One fourth stage ADS valve is required to open if gravity injection is actuated during cold shutdown and refueling with the RCS is open to preclude surge line flooding. On low-low hotleg level (empty hot leg), the PMS signals the ADS 4th stage squibs to open to preclude surge line flooding.

Normal Residual Heat Removal System (RNS)

The normal residual heat removal system (RNS) provides the following nonsafety-related means of core cooling during accidents: (1) RCS recirculation at shutdown conditions, (2) low pressure pumped injection from the IRWST, and (3) long-term pumped recirculation from the containment sump. Such RNS functions provide defense-in-depth in mitigating accidents, in addition to that provided by the passive safety-related systems.

The following are some important aspects of RNS as represented in the PRA:

- The RNS has redundant pumps, powered by separate non-Class 1E buses with backup connections from the diesel generators, and redundant heat exchangers.

- The RNS provides safety-related means for (1) containment isolation at the penetration of the RNS lines, (2) RCS isolation at the RNS suction and discharge lines, and (3) IRWST and containment sump inventory makeup.

- The RNS is manually aligned from the control room to perform its core cooling functions [SSAR]. Emergency Response Guidelines (ERGs) are provided for aligning the RNS from the control room for RCS injection and recirculation.

- Recirculation from the containment sump is actuated automatically by a low IRWST level signal or manually from the control room, if automatic actuation fails.

- For long-term recirculation operation, the RNS pumps take suction from only one of the two sump recirculation lines. Unrestricted flow through both parallel paths (one containing an MOV and a squib valve in series, the other containing a check valve and a squib valve in series) is required for success of the sump recirculation function when both RNS pumps are running. If one of the two parallel paths fails to open, operator action (in the control room through PMS) is required to manually throttle the RNS discharge MOV (V011) to prevent pump cavitation. [ERGs].

- With the NRHR pumps aligned either to the IRWST or the containment sump, the pumps' net positive suction head (NPSH) is adequate to prevent pump cavitation and failure even when the IRWST or sump inventory is saturated.

- The RNS containment isolation and RCS pressure boundary valves are safety related. The MOVs are powered by Class 1E dc power.

- The containment isolation valves in the RNS piping close automatically via PMS with a high radiation signal. Westinghouse analyses indicate that under all accident conditions but large LOCAs, the containment radiation level is well below the point that would cause the RNS MOVs to automatically close.

- The following AP600 design features contribute to the low likelihood of interfacing system LOCAs through the NRHR system:

  - The portion of the RNS outside containment is capable of withstanding the operating pressure of the RCS.

  - A relief valve located in the common RNS discharge line outside containment provides protection against excess pressure.

  - Each RNS line is isolated by at least three valves.

  - The pressure in the RNS pump suction line is continuously indicated and alarmed in the main control room.

  - The pump suction isolation valves connecting the RNS pumps to the RCS hot leg are interlocked with RCS pressure so that they cannot be opened until the RCS pressure is less than 450 psig. This prevents overpressurization of the RCS when the RNS is aligned for shutdown cooling.

  - The two remotely operated MOVs connecting the suction and discharge headers, respectively, to the IRWST are interlocked with the isolation valves connecting the RNS pumps to the hot leg. This prevents inadvertent opening of any of these two MOVs when the RNS is aligned for shutdown cooling and potential diversion and draining of reactor coolant system.

- The power to the four isolation MOVs connecting the RNS pumps to the RCS hot leg is administratively blocked at their motor control centers during normal power operation. [COL].

- The operability of the RNS is tested, via connections to the IRWST, immediately before its alignment to the RCS hot leg, for shutdown cooling, to ensure that there are no any open manual valves in the drain lines. [SSAR, COL, Procedures].

- The IRWST suction isolation valve (V023) and the RCS pressure boundary isolation valves (V001A, V001B, V002A and V002B) are qualified for DBA conditions.

- The reliability of the IRWST suction isolation valve (V023) to open on demand (for RNS injection during power operation and for IRWST gravity injection via the RNS hot leg connection during shutdown operation) is important. The COL will ensure high reliability. [COL, D-RAP].

- An alternative gravity injection path is provided through RNS V-023 during cold shutdown and refueling conditions with the RCS open. The COL applicant should have policies that maximize the availability of this valve and procedures to open this valve during cold shutdown and refueling operations when the RCS is open.

- The COL applicant will maintain RNS and its support systems (CCS and SWS) during power operation.

- The COL applicant will have administrative controls to maximize the likelihood that RNS valve V-023 will be able to open if needed during Mode 5 when the RCS is open, and PRHR cannot be used for core cooling.

- Since inadvertent opening of RNS valve V024 results in a draindown of RCS inventory to the IRWST and requires gravity injection from the IRWST, the COL applicant will have administrative controls to ensure that inadvertent opening of this valve is unlikely. In addition, the COL applicant should evaluate this error in the human reliability analysis/human factors engineering integration implementation plan.

- The RNS is an important "defense-in-depth" system for accidents initiated while the plant is at power or at mid-loop during shutdown. The availability control of the RNS and its support systems (CCW, SWS and diesel generators) is covered in SSAR Section 16.3. [RTNSS].

Startup Feedwater System (SFW)

The SFW system provides a nonsafety-related means of delivering feedwater to the steam generators (SGs) when the main feedwater pumps are unavailable during an transient. This capability provides an alternate core cooling mechanism to the PRHR heat exchanger for non-LOCA and SGTR accidents which minimizes the PRHR challenge rate. The reliability of the SFW system will be maintained by the COL Applicant [D-RAP].

Instrumentation and Control (I&C)

The following three I&C systems are credited in the PRA for providing monitoring and control functions during accidents: (1) the safety-related Protection and Safety Monitoring System (PMS), (2) the nonsafety-related Diverse Actuation System (DAS), and (3) the nonsafety-related Plant Control System (PLS).

The PMS provides a safety-related means of performing the following functions:

- Automatic and manual reactor trip.
- Automatic and manual actuation of engineered safety features (ESF).
- Monitor the safety-related functions during and following an accident as required by Regulatory Guide 1.97.

The DAS provides a nonsafety-related means of performing the following functions:

- Automatic and manual reactor trip.
- Automatic and manual actuation of selected engineered safety features.
- Provides control room indication for monitoring of selected safety-related functions.

The PLS provides a nonsafety-related means of performing the following functions:

- Automatic and manual control of nonsafety-related systems, including "defense-in-depth" systems (e.g., RNS).
- Provides control room indication for monitoring overall plant and nonsafety-related system performance.

The following are some important aspects of PMS as represented in the PRA:

- The PMS has four (redundant) divisions of reactor trip and ESF actuation and automatically produces a reactor trip or ESF initiation upon an attempt to bypass more than two channels of a function that uses 2-out-of-4 logic.
- The PMS has redundant divisions of safety-related post-accident parameter display.
- Each PMS division is powered from its respective Class 1E dc division.
- The PMS provides fixed position controls in the control room.
- The reliability of the PMS is ensured by redundancy and functional diversity within each division:
  - The reactor trip functions are divided into two functionally diverse subsystems.

  - The ESF functions are processed by two microprocessor-based subsystems that are functionally identical in both hardware and software.

- Separate input channels are provided for the reactor trip and the ESF actuation functions, with the exception of sensors which may be shared.

- Sensor redundancy and diversity contribute to the reliability of PMS. Four sensors normally monitor variables used for an ESF actuation. Different type sensors, or same type sensors in different environment, minimize common cause failures.

- Continuous automatic PMS system monitoring and failure detection/alarm is provided.

- PMS equipment is designed to accommodate a loss of the normal heating, ventilation, and air conditioning (HVAC). PMS equipment is protected by the passive heat sinks upon failure or degradation of the active HVAC.

- The reliability of the PMS is important. The COL will maintain the reliability of the PMS.

- The PMS software is designed, tested, and maintained to be reliable under a controlled verification and validation program written in accordance with IEEE 7-4.3.2 (1993) that has been endorsed by Regulatory Guide 1.152. Elements that contribute to a reliable software design include:

  - A formalized development, modification, and acceptance process in accordance with an approved software QA plan (paraphrased from IEEE standard, Section 5.3, "Quality")

  - A verification and validation program prepared to confirm the design implemented will function as required (IEEE standard, Section 5.3.4, "Verification and Validation")

  - Equipment qualification testing performed to demonstrate that the system will function as required in the environment it is intended to be installed in (IEEE standard, Section 5.4, "Equipment Qualification")

  - Design for system integrity (performing its intended safety function) when subjected to all conditions, external or internal, that have significant potential for defeating the safety function (abnormal conditions and events) (IEEE standard, Section 5.5, "System Integrity")

  - Software configuration management process (IEEE standard, Section 5.3.5, "Software Configuration Management").

The following are some important aspects of DAS as represented in the PRA:

- Diversity is assumed in the PRA that eliminates the potential for common cause failures between PMS and DAS. The DAS automatic actuation signals are generated in a functionally diverse manner from the PMS signals.

Diversity between the DAS and PMS is achieved by the use of different architecture, different hardware implementations, and different software.

- DAS provides control room displays and fixed position controls to allow the operators to take manual actions.

- DAS actuates using 2-out-of-2 logic. Actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate signals. The normally de-energized output state, along with the dual 2-out-of-2 redundancy, reduces the probability of inadvertent actuation.

- The actuation devices of DAS and PMS are capable of independent operation that is not affected by the operation of the other. The DAS is designed to actuate components only in a manner that initiates the safety function.

- Capability is provided for on-line testing and calibration of the DAS channels, including sensors.

- The DAS manual initiation functions are implemented in a manner that bypasses the signal processing equipment of the DAS automatic logic. This eliminates the potential for common cause failures between automatic and manual DAS functions.

- The DAS reactor trip function is implemented through a trip of the control rods via the motor-generator (M-G) set which is separate and diverse from the reactor trip breakers. The COL will maintain the reliability of the M-G set breakers [D-RAP].

- DAS is an important "defense-in-depth" system. The availability of DAS, with respect to both its reactor trip and ESF actuation functions, will be controlled. [RTNSS]. The COL will maintain its reliability [D-RAP].

The following are some important aspects of PLS as represented in the PRA:

- PLS has redundancy to minimize plant transients.

- PLS provides capability for both automatic control and manual control.

- Redundant signal selectors provide PLS with the ability to obtain inputs from the integrated protection cabinets in the PMS. The signal selector function maintains the independence of the PLS and PMS. The signal selectors select those protection system signals that represent the actual status of the plant and reject erroneous signals.

- PLS control functions are distributed across multiple distributed controllers so that single failures within a controller do not degrade the performance of control functions performed by other controllers.

Onsite Power

The onsite power system consists of the main ac power system and the dc power system. The main ac power system is a non-Class 1E system. The dc power system consists of two independent systems: the Class 1E dc system and the non-Class 1E dc system.

The main ac power system is a non-Class 1E system comprised of a normal, preferred, and standby power system. It distributes power to the reactor, turbine, and balance of plant auxiliary electrical loads for startup, normal operation, and normal/emergency shutdown.

The Class 1E dc and uninterruptible power supply (UPS) system (IDS) provides reliable power for the safety-related equipment required for the plant instrumentation, control, monitoring, and other vital functions needed for shutdown of the plant.

The non-Class 1E dc and UPS system (EDS) consists of the electric power supply and distribution equipment that provide dc and uninterruptible ac power to nonsafety-related loads.

The following are some important aspects of the main AC power system as represented in the PRA:

- The arrangement of the buses permits feeding functionally redundant pumps or groups of loads from separate buses and enhances the plant operational reliability.

- During power generation mode, the turbine generator normally supplies electric power to the plant auxiliary loads through the unit auxiliary transformers. During plant startup, shutdown, and maintenance, the main ac power is provided by the preferred power supply from the high-voltage switchyard. The onsite standby power system powered by the two onsite standby diesel generators supplies power to selected loads in the event of loss of normal and preferred ac power supplies.

- Two onsite standby diesel generator units, each furnished with its own support subsystems, provide power to the selected plant nonsafety-related ac loads.

- On loss of power to a 4160 V diesel-backed bus, the associated diesel generator automatically starts and produces ac power. The normal source circuit breaker and bus load circuit breakers are opened, and the generator is connected to the bus. Each generator has an automatic load sequencer to enable controlled loading on the associated buses.

The following are some important aspects of the Class 1E dc and UPS system (IDS) as represented in the PRA:

- There are four independent, Class 1E 125 V dc divisions. Divisions A and D each consists of one battery bank, one switchboard, and one battery charger. Divisions B and C are each composed of two battery banks, two switchboards, and two battery chargers. The first battery bank in the four divisions is designated as the 24-hour battery bank. The second battery bank in Divisions B and C is designated as the 72-hour battery bank.

- The 24-hour battery banks provide power to the loads required for the first 24 hours following an event of loss of all ac power sources concurrent with a design basis accident. The 72-hour battery banks provide power to those loads requiring power for 72 hours following the same event.

- Battery chargers are connected to dc switchboard buses. The input ac power for the Class 1E dc battery chargers is supplied from non-Class 1E 480 V ac diesel-generator-backed motor control centers.

- The 24-hour and 72-hour battery banks are housed in ventilated rooms apart from chargers and distribution equipment.

- Each of the four divisions of dc systems are electrically isolated and physically separated to prevent an event from causing the loss of more than one division.

- Reliability of the Class 1E batteries is important. The COL will maintain the reliability of the equipment.

The following are some important aspects of the non-Class 1E dc and UPS system as represented in the PRA:

- The non-Class 1E dc and UPS system consists of two subsystems representing two separate power supply trains.

- EDS load groups 1, 2, and 3 provide 125 V dc power to the associated inverter units that supply the ac power to the non-Class 1E uninterruptible power supply ac system.

- The onsite standby diesel-generator-backed 480 V ac distribution system provides the normal ac power to the battery chargers.

- The batteries are sized to supply the system loads for a period of at least two hours after loss of all ac power sources.

Component Cooling Water System (CCS)

The component cooling water system (CCS) is a nonsafety-related system that removes heat from various components and transfers the heat to the service water system. The following are some important aspects of the CCS as represented in the PRA:

- The CCS is arranged into two trains. Each train includes one pump and one heat exchanger.

- During normal operation, one CCS pump is operating. The standby pump is aligned to automatically start in case of a failure of the operating CCS pump.

- The CCS pumps are automatically loaded on the standby diesel generator in the event of a loss of normal ac power. The CCS, therefore, continues to provide cooling of required components if normal ac power is lost.

Service Water System (SWS)

The service water system (SWS) is a nonsafety-related system that transfers heat from the component cooling water heat exchangers to the atmosphere. The following are some important aspects of the SWS as represented in the PRA:

- The SWS is arranged into two trains. Each train includes one pump, one strainer, and one cooling tower cell.

- During normal operation, one SWS train of equipment is operating. The standby train is aligned to automatically start in case of a failure of the operating SWS pump.

- The SWS pumps and cooling tower fans are automatically loaded onto their associated diesel bus in the event of a loss of normal ac power. Both pumps and cooling tower fans automatically start after power from the diesel generator is available.

Chemical and Volume Control System (CVS)

The chemical and volume control system (CVS) provides a safety-related means to terminate inadvertent RCS boron dilution. In addition, the CVS provides a nonsafety-related means to (1) provide makeup water to the RCS during normal plant operation, (2) provide boration following a failure of reactor trip, (3) provide coolant to the pressurizer auxiliary spray line, (4) safety related portions of the CVS provide inadvertent boron dilution protection, and (5) safety related portions of the CVS provide isolation of normal CVS letdown during shutdown operation on low hot leg level.

The following are some important aspects of CVS as represented in the PRA:

- The CVS has two makeup pumps and each pump is capable of providing normal makeup.

- One CVS pump is configured to operate on demand while the other CVS pump is in standby. The operation of these pumps will alternate periodically (monthly).

- On low hot leg level, the safety related PMS signals three safety related CVS AOVs to close automatically to isolate letdown during Mode 4 (when RNS is in operation), Mode 5, and Mode 6 (with the upper internals in place and the refueling cavity less than half full) as required by AP600 TS.

- The safety related PMS boron dilution signal automatically re-aligns CVS pump suction to the boric acid tank. This same signal also closes the two safety-related CVS demineralized water supply valves. This signal actuates on any reactor trip signal, source range flux multiplication signal, low input voltage to the Class 1E DC power system battery chargers, or a safety injection signal.

- The COL applicant will maintain procedures to respond to low hot leg level alarms.