Westinghouse Electric Corporation Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

NSD-NRC-97-5005
DCP/NRC0756
Docket No.: STN-52-003

February 28, 1997

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

ATTENTION: T. R. QUAY

SUBJECT: AP600 PRA-BASED INSIGHTS

Dear Mr. Quay:

Enclosed is a draft copy of AP600 Probabilistic Risk Assessment (PRA) Table 59-30, AP600 PRA-Based Insights. The purpose of the table is to summarize the important design features, operational assumptions, and risk insights of the AP600 PRA. This enclosure provides the insights of the AP600 Level 1 internal events PRA. The insights of the AP600 external events analyses (including the internal fire, internal flood, and seismic margins analyses) and the Level 2 and 3 PRA will be incorporated into this table in the next revision of the PRA. To facilitate the NRC review of the PRA, the external events and Level 2/3 PRA insights will be provided as they become available to the NRC.

Table 59-30 will be included in the next revision to the PRA (scheduled for early April, 1997). No changes to the existing information provided in this table are expected between the draft copy enclosed with this letter and the table that will be included in the next PRA revision. If there are any changes, they will be clearly identified to the staff.

The NRC should review this enclosure.

Please contact Cynthia L. Haag on (412) 374-4277 if you have any questions concerning this transmittal.

Brian A. McIntyre, Manager
Advanced Plant Safety and Licensing

jml
Enclosure

E004/1

cc: J. Sebrosky, NRC (enclosure)
J. Flack, NRC (enclosure)
R. Jones, NRC (w/o enclosure)
N. J. Liparulo, Westinghouse (w/o enclosure)

060032

Enclosure to Westinghouse
Letter NSD-NRC-97-5005

February 28, 1997

Table 59-30

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
1.	The passive core cooling system (PXS) is composed of the following: - Accumulator subsystem - Core makeup tank (CMT) subsystem - In-containment refueling water storage tank (IRWST) subsystem - Passive residual heat removal (PRHR) subsystem. The automatic depressurization system (ADS), which is part of the reactor coolant system (RCS), also supports passive core cooling functions.	
1a.	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:	SSAR 6.3.2
	- 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.	Certified Design Material
	- The reliability of the accumulator subsystem is important. The COL will maintain the reliability of the accumulator subsystem.	SSAR 16.2
	- Diversity between the accumulator check valves and the CMT check valves minimizes the potential for common cause failures.	SSAR 6.3.2

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
1b.	ADS provides a safety-related means of depressurizing the RCS.	Certified Design Material
	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.	Certified Design Material
	Each stage 1, 2, and 3 line contains two motor-operated valves (MOVs).	Certified Design Material
	Each stage 4 line contains an MOV valve and a squib valve.	Certified Design Material
	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.	SSAR 6.3.2
	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).	Certified Design Material
	The ADS valves are powered from Class 1E dc power.	Certified Design Material
	The ADS valve positions are indicated and alarmed in the control room.	SSAR 6.3.7
	Stage 1, 2, and 3 valves are stroke-tested every 6 months. Stage 4 squib valve actuators are tested every 2 years for 20% of the valves.	SSAR 3.9.6
	The reliability of the ADS is important. The COL will maintain the reliability of the ADS.	SSAR 16.2
	ADS is required by the Technical Specifications to be available from power conditions down through refueling without the cavity flooded.	SSAR 16.1
	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.	Emergency Response Guidelines

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
1c.	The CMTs provide safety-related means of high-pressure safety injection of borated water to the RCS.	SSAR 6.3.1
	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). - These AOVs 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.	SSAR 6.3.2
	The CMT AOVs are automatically and manually actuated from PMS and DAS.	Certified Design Material
	CMT level instrumentation provides an actuation signal to initiate automatic ADS and provides the actuation signal for the IRWST squib valves to open.	SSAR 6.3.1 & 7.3.1
	The CMT AOV positions are indicated and alarmed in the control room.	SSAR 6.3.7
	CMT AOVs are stroke-tested quarterly.	SSAR 3.9.6
	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.	SSAR 16.2
	CMT is required by the Technical Specifications to be available from power conditions down through cold shutdown with RCS pressure boundary intact.	SSAR 16.1

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
1d.	IRWST subsystem provides a safety-related means of performing the following functions: - Low-pressure safety injection following ADS actuation - Long-term core cooling via containment recirculation - Reactor vessel cooling through the flooding of the reactor cavity by draining the IRWST into the containment.	SSAR 6.3
	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.	Certified Design Material
	There are screens for each IRWST injection line and recirculation line.	Certified Design Material
	Squib valves provide the pressure boundary and prevent the check valves from normally seeing a high delta-P.	SSAR 6.3.3
	Squib valves and MOVs are powered by Class 1E dc power.	Certified Design Material
	The squib valves and MOVs for injection and recirculation are automatically and manually actuated via PMS, and manually actuated via DAS.	Certified Design Material
	The squib valves and MOVs for reactor cavity flooding are manually actuated via PMS and DAS from the control room.	Certified Design Material
	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.	SSAR 6.3.2
	Automatic IRWST injection at shutdown conditions is provided using PMS low hot leg level logic.	SSAR 7.3.1
	The positions of the squib valves and MOVs are indicated and alarmed in the control room.	SSAR 6.3.7

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

INSIGHT	DISPOSITION
1d. (cont.) 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% of the valves. IRWST recirculation MOVs are stroke-tested quarterly.	SSAR 3.9.6
The reliability of the IRWST subsystem is important. The COL will maintain the reliability of the IRWST subsystem.	SSAR 16.2
IRWST injection and recirculation are required by Technical Specifications to be available from power conditions to refueling without the cavity flooded.	SSAR 16.1

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
1e.	Passive residual heat removal (PRHR) provides a safety-related means of performing the following functions: - Removes core decay heat during accidents - Allows automatic termination of RCS leak during a steam generator tube rupture (SGTR) without ADS.	SSAR 6.3.1 & 6.3.3
	The following are some important aspects of the PRHR subsystem as represented in the PRA:	
	PRHR is actuated by opening redundant parallel air-operated valves. These air-operated valves open on loss of Class 1E power, loss of air, or loss of the signal from PMS.	SSAR 6.3.2
	The PRHR air-operated valves are automatically actuated and manually actuated from the control room by either PMS or DAS.	Certified Design Material
	Diversity of the PRHR air-operated valves from the CMT air-operated valves minimizes the probability for common cause failure of both PRHR and CMT air-operated valves.	SSAR 6.3.2
	Long-term cooling of PRHR will result in steaming to the containment. The steam will normally condense on the containment shell and return to the IRWST. If the steam condensation does not return to the IRWST, the IRWST volume is sufficient for at least 72 hours of PRHR operation. Connections are provided to IRWST 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.	SSAR 6.3.1 & system drawings
	Capability exists for the control room operator to identify a leak in the PRHR HX before it can degrade to a tube rupture during a subsequent design basis accident (DBA).	SSAR 6.3.3 & 16.1
	The positions of the inlet and outlet PRHR valves are indicated and alarmed in the control room.	SSAR 6.3.7
	PRHR air-operated valves are stroke-tested quarterly. The PRHR HX is flow tested to detect system performance degradation.	SSAR 3.9.6
	PRHR is required by the Technical Specifications to be available from power conditions down through cold shutdown with RCS pressure boundary intact.	SSAR 16.1

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
2.	The protection and safety monitoring system (PMS) provides a safety-related means of performing the following functions: - Initiates automatic and manual reactor trip - Automatic and manual actuation of engineered safety features (ESF).	Certified Design Material
	PMS monitors the safety-related functions during and following an accident as required by Regulatory Guide 1.97	SSAR 7.1.1
	PMS has four (redundant) divisions of reactor trip and ESF actuation. PMS automatically produces a safety-related reactor trip or ESF initiation upon an attempt to bypass more than two channels of a function that uses 2-out-of-4 logic.	Certified Design Material
	PMS has redundant divisions of safety-related post-accident parameter display.	SSAR 7.1.2.6 & Figure 7.1-8
	Each PMS division is powered from its respective Class 1E dc division.	Certified Design Material
	PMS provides fixed position controls in the control room.	Certified Design Material
	Reliability of the PMS is provided 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.	 SSAR 7.1.2.2.1 SSAR 7.1.2.2.6 & 7.1.2.3.1
	Four sensors normally monitor variables used for an ESF actuation. These sensors may monitor the same variable for a reactor trip function.	SSAR 7.3.1
	Continuous automatic PMS system monitoring and failure detection/alarm is provided.	SSAR 7.1.2
	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.	SSAR 7.1.4.1.6
	The reliability of the PMS is important. The COL will maintain the reliability of the PMS.	SSAR 16.2

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

INSIGHT	DISPOSITION
2. (cont.) 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").	SSAR App 1A (Compliance with Reg. Guide 1.152)

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
3.	The diverse actuation system (DAS) provides a nonsafety-related means of performing the following functions: - Initiates automatic and manual reactor trip - Automatic and manual actuation of selected engineered safety features.	Certified Design Material
	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 DAS and PMS is achieved by the use of different architecture, different hardware implementations, and different software.	Certified Design Material
	DAS provides control room displays and fixed position controls to allow the operators to take manual actions.	SSAR 7.7.1
	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.	SSAR 7.7.1.11
	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.	SSAR 7.7.1.11
	The DAS reactor trip function is to trip the control rods via the motor-generator set.	SSAR 7.7.1.11
	In the PRA it is assumed the following eliminates the potential for common cause failures between automatic and manual DAS functions. - DAS manual initiation functions are implemented in a manner that bypasses the signal processing equipment of the DAS automatic logic.	Certified Design Material
	The COL will maintain the reliability of the DAS.	SSAR 16.2

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
4.	The plant control system (PLS) provides a nonsafety-related means of controlling nonsafety-related equipment.	SSAR 7.1.3
	PLS has redundancy to minimize plant transients.	SSAR 7.7.1.12
	PLS provides capability for both automatic control and manual control.	SSAR 7.1.3
	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.	SSAR 7.1.3.2
	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.	SSAR 7.1.3.1
5.	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.	Certified Design Material

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
5a.	The onsite main ac power system is a non-Class 1E system comprised of a normal, preferred, and standby power system.	SSAR 8.3.1.1
	The main ac power system distributes power to the reactor, turbine, and balance of plant auxiliary electrical loads for startup, normal operation, and normal/emergency shutdown.	SSAR 8.3.1.1.3
	The arrangement of the buses permits feeding functionally redundant pumps or groups of loads from separate buses and enhances the plant operational reliability.	SSAR 8.3.1.1.1
	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.	SSAR 8.3.1.1.1
	Two onsite standby diesel generator units, each furnished with its own support subsystems, provide power to the selected plant nonsafety-related ac loads.	SSAR 8.3.1.1.2.1
	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.	Certified Design Material

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
5b.	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.	SSAR 8.3.2.1
	There are four independent, Class 1E 125 Vdc 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.	Certified Design Material
	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.	Certified Design Material
	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 Vac diesel-generator-backed motor control centers.	SSAR 8.3.2.1.1.1
	The 24-hour and the 72-hour battery banks are housed in ventilated rooms apart from chargers and distribution equipment.	SSAR 8.3.2.1.3
	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.	SSAR 8.3.2.1.3
	Reliability of the Class 1E batteries is important. The COL will maintain the reliability of the equipment.	SSAR 16.2
5c.	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.	Certified Design Material
	The non-Class 1E dc and UPS system consists of two subsystems representing two separate power supply trains.	SSAR 8.3.2.1.2
	EDS load groups 1, 2, and 3 provide 125 Vdc power to the associated inverter units that supply the ac power to the non-Class 1E uninterruptible power supply ac system.	Certified Design Material
	The onsite standby diesel-generator-backed 480 Vac distribution system provides the normal ac power to the battery chargers	Certified Design Material
	The batteries are sized to supply the system loads for a period of at least two hours after loss of all ac power sources	SSAR 8.3.2.1.2

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
6.	The normal residual heat removal system (RNS) provides a safety-related means of performing the following functions: - Containment isolation for the RNS lines that penetrate the containment - Isolation of the reactor coolant system at the RNS suction and discharge lines - Makeup of containment inventory.	Certified Design Material
	RNS provides a nonsafety-related means of core cooling through: - RCS recirculation at shutdown conditions - Low pressure pumped injection from the IRWST and long-term pumped recirculation from the containment.	SSAR 5.4.7
	The RNS has redundant pumps and heat exchangers. The pumps are powered by non-Class 1E power with backup connections from the diesel generators.	SSAR 5.4.7 & 8.3
	RNS is manually aligned from the control room to perform its core cooling functions. The performance of the RNS is indicated in the control room.	SSAR 5.4.7
	The RNS containment isolation and pressure boundary valves are safety-related. The motor-operated valves are powered by Class 1E dc power.	Certified Design Material
	The containment isolation valves in the RNS piping automatically close via PMS with a high radiation signal.	SSAR 7.3.1
	The RNS containment isolation MOVs are automatically and manually actuated via PMS.	SSAR 7.3.1
	Interfacing system loss-of-coolant accident (LOCA) between the RNS and the RCS is prevented by: - Each RNS line is isolated by at least three valves. - The RNS equipment outside containment is capable of withstanding the operating pressure of the RCS. - The RCS isolation valves are interlocked to prevent their opening at RCS pressures above its design pressure.	SSAR 5.4.7.2.2
	CCS provides cooling to the RNS heat exchanger.	Certified Design Material
	Planned maintenance of the RNS is performed at-power.	

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
7.	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.	Certified Design Material
	The CCS is arranged into two trains. Each train includes one pump and one heat exchanger.	Certified Design Material
	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.	SSAR 9.2.2.4.2
	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.	SSAR 9.2.2.4.5.4
8.	The service water system (SWS) is a nonsafety-related system that transfers heat from the component cooling water heat exchangers to the atmosphere.	Certified Design Material
	The SWS is arranged into two trains. Each train includes one pump, one strainer, and one cooling tower cell.	SSAR 9.2.1.2.1
	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.	SSAR 9.2.1.2.3.3
	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.	SSAR 9.2.1.2.3.6
9.	The chemical and volume control system (CVS) provides a safety-related means to terminate inadvertent RCS boron dilution.	Certified Design Material
	The CVS provides a nonsafety-related means to perform the following functions: - Makeup water to the RCS during normal plant operation - Boration following a failure of reactor trip - Coolant to the pressurizer auxiliary spray line.	Certified Design Material
	Two makeup pumps are provided. Each pump provides capability for normal makeup.	SSAR 9.3.6.3.1
10.	The operation of RNS and its support systems (CCS, SWS, main ac power and onsite power) is RTNSS-important for shutdown decay heat removal during reduced RCS inventory operations. - Reliability of these systems is covered by the Reliability Assurance Program (RAP)	SSAR 16.2

Table 59-30 (cont.)

AP600 PRA-BASED INSIGHTS

	INSIGHT	DISPOSITION
11.	Operator training is the responsibility of the COL. Westinghouse input is provided in WCAP-14655.	SSAR 18.10
12.	Sufficient instrumentation and control is provided at the remote shutdown workstation to bring the plant to safe shutdown conditions in case the control room must be evacuated.	SSAR 7.4.3