Westinghouse Electric Corporation Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

November 25, 1996

NSD-NRC-96-4891
DCP/NRC0664
Docket No.:STN-52-003

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

ATTENTION: T. R. QUAY

SUBJECT: SAMPLE OF AP600 PRA INSIGHTS, FRAMEWORK FOR AP600 SEVERE ACCIDENT MANAGEMENT GUIDANCE (WCAP-13914, Rev. 1), AND RESPONSE TO REQUEST FOR ADDITION INFORMATION

Dear Mr. Quay:

Enclosure 1 provides the important AP600 PRA design features, operational assumptions, and risk insights for the passive core cooling system (which includes automatic depressurization system, core makeup tanks, in-containment refueling water storage tank, passive residual heat removal, and accumulators), normal residual heat removal system, and the instrumentation and control systems (protection and safety monitoring system, diverse actuation system, and plant control system). This information is being provided, as requested by the NRC Probabilistic Safety Analysis Branch, for developing the final listing of PRA insights that will be included in Chapter 59 of the AP600 Probabilistic Risk Assessment. The staff is expected to review this information and be prepared to support a meeting by January 10, 1997 with Westinghouse to discuss the enclosure with the intent of finalizing the information. Cindy Haag will contact Mr. Joe Sebrosky of the NRC to arrange the meeting.

Enclosure 2 is a copy of revision 1 of WCAP-13914, "Framework for AP600 Severe Accident Management Guidance." This WCAP was revised to incorporate commitments Westinghouse made in response to RAI 480.439.

Enclosure 3 provides the revised response to accident management RAI 720.56.

E004

030013

November 25, 1996

NSD-NRC-96-4891
DCP/NRC0664

WCAP-13914, revision 1, and the response to the RAI closes, from a Westinghouse perspective, the accident management DSER open item 19.2.5-1. The status of this item in OITS will be changed to Action N. The NRC technical staff should review this WCAP.

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

Enclosures

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

Enclosure 2 to Westinghouse
Letter NSD-NRC-96-4891

November 25, 1996

Enclosure 1 to Westinghouse
Letter NSD-NRC-96-4891

November 25, 1996

AUTOMATIC DEPRESSURIZATION SYSTEM ASSUMPTIONS, FEATURES, INSIGHTS

A. DESIGN FEATURES

1. ADS provides a safety-related means of depressurizing the RCS.
2. 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 above the post-accident flood up level.
3. Each stage 1, 2, and 3 line contains two motor-operated valves
4. Each stage 4 line contains a motor-operated valve and a squib valve. The motor-operated valve is normally open.
5. The MOVs in Stages 1, 2, and 3 are diverse from the squib valves in Stage 4.
6. 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
   - In stages 1, 2, and 3, interlocks prevent opening of two MOVs in series during testing
   - Each stage 4 squib valve has redundant, series controllers
   - Stage 4 is blocked from opening at high RCS pressures
7. The ADS valves are automatically and manually actuated via PMS, and manually actuated via DAS.
8. The ADS valves are powered from Class 1E dc power.
9. The ADS valve positions are indicated and alarmed in the control room.

B. OPERATION ASSUMPTIONS

1. Stage 1, 2, and 3 valves are stroke-tested every 6 months.
2. Stage 4 squib valve actuators are tested every 2 years for 20% of the valves.
3. The COL will maintain the reliability of the ADS.
4. ADS is required by the Technical Specifications to be available from power conditions down through refueling without the cavity flooded.

C. RISK INSIGHTS

1. ADS is a risk-important system for at-power conditions. Common cause failure of the squib vales is a risk-important event.
2. Spurious actuation of ADS is an important contributor to the large LOCA initiating event frequency.
3. Depressurization of the RCS through ADS reduces the probability of HPME events.

CORE MAKEUP TANK
ASSUMPTIONS, FEATURES, INSIGHTS

A. DESIGN FEATURES

1. The CMTs provide safety-related means of high pressure safety injection of borated water to the RCS.
2. 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 AOVs.
   - These AOVs open on loss of Class 1E dc power, loss of compressed air, or loss of the signal from PMS.
   - The injection line for each CMT also has two normally open check valves in series.
3. The CMT AOVs are automatically and manually actuated from PMS and DAS.
4. CMT level instrumentation provides an actuation signal to initiate automatic ADS and provides the actuation signal for the IRWST squib valves to open.
5. The CMT AOV positions are indicated and alarmed in the control room.

B. OPERATION ASSUMPTIONS

1. CMT AOVs are stroke-tested quarterly.
2. CMT check valves are exercised at each refueling.
3. The COL will maintain the reliability of the CMT subsystem.
4. CMT is required by the Technical Specifications to be available from power conditions down through cold shutdown with RCS pressure boundary intact.

C. RISK INSIGHTS

1. 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.
2. The CMT RCS makeup function is not risk-important since the accumulators with manual ADS provide a diverse means for RCS makeup.
3. Diversity of the CMT AOVs and PRHR AOVs minimizes the potential for common cause failures.
4. Diversity of the CMT check valves and accumulator check valves minimizes the potential for common cause failures.
5. Risk important events in the CMT subsystem are:
   a. Common cause failures of the AOVs
   b. Level sensors are important.

IRWST ASSUMPTIONS, FEATURES, INSIGHTS

A. DESIGN FEATURES

1. 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 following a severe accident.
2. 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 recirc. 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.
3. There are screens for each IRWST injection line and recirculation line.
4. Squib valves provide the pressure boundary and protect the check valves from adverse delta-P.
5. Squib valves and MOVs are powered by Class 1E vdc power.
6. The squib valves and MOVs for injection and recirculation are automatically and manually actuated via PMS, and manually actuated via DAS.
7. The squib valves and MOVs for reactor cavity flooding are manually actuated via PMS and DAS from the control room.
8. Automatic IRWST injection at shutdown conditions is provided using PMS 2-out-of-2 low hot leg level logic.
9. The positions of the squib valves and MOVs are indicated and alarmed in the control room.

B. OPERATION ASSUMPTIONS

1. IRWST injection and recirc check valves are exercised at each refueling.
2. IRWST injection and recirc squib valve actuators are tested every 2 years for 20% of the valves
3. IRWST recirc. MOVs are stroke-tested quarterly.
4. The COL will maintain the reliability of the IRWST subsystem.
5. IRWST injection and recirculation are required by Technical Specifications to be available from power conditions to refueling without the cavity flooded.

C. RISK INSIGHTS

1. The IRWST subsystem is risk-important.
2. Reactor cavity flooding is an important operator action.
3. Diversity of the squib valves in the injection lines and recirc lines minimizes the potential for common cause failure between injection and recirculation/reactor cavity flooding.
4. The dominant contributors to IRWST unavailability are:
   a. CCF of squib valves in recirculation lines
   b. CCF of IRWST injection check valves
   c. CCF of IRWST injection squib valves
   d. CCF of screens in IRWST tank plugging
   e. CCF of recirculation screen plugging.

PASSIVE RESIDUAL HEAT REMOVAL ASSUMPTIONS, FEATURES, INSIGHTS

A. DESIGN FEATURES

1. PRHR provides a safety-related means of performing the following functions:
   - core decay heat removal during design basis events
   - automatically terminating RCS leak during a SGTR.
2. There is one PRHR HX which is submerged in the IRWST.
3. The PRHR HX flowpath is isolated by parallel air-operated valves. These air-operated valves open on loss of Class 1E 125 vdc control power, loss of compressed air, or loss of the signal from PMS.
4. The PRHR air-operated valves are automatically actuated and manually actuated from the control room by PMS and DAS.
5. 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 SFS and CVS to extend PRHR operation.
6. Capability exists for control room operator to identify a leak in the PRHR HX before it can degrade to a tube rupture.
7. The positions of the inlet and outlet PRHR valves are indicated and alarmed in the control room.

B. OPERATION ASSUMPTIONS

1. PRHR air-operated valves are stroke-tested quarterly.
2. PRHR is required by the Technical Specifications to be available from power conditions down through cold shutdown with RCS pressure boundary intact.

C. RISK INSIGHTS

1. PRHR is not one of the most risk-important systems. It is of "medium" importance with respect to the systems modeled in the PRA.
2. The contribution to CDF associated with PRHR HX tube rupture event is small.
3. 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.

ACCUMULATOR ASSUMPTIONS, FEATURES, INSIGHTS

A. DESIGN FEATURES

1. The accumulators provide a safety-related means of safety injection of borated water to the RCS.
2. There are two accumulators, each with an injection line to the reactor vessel / DVI nozzle. Each injection line has two check valves in series.
3. The accumulators are pressurized with nitrogen gas.

B. OPERATION ASSUMPTIONS

1. Accumulator check valves are exercised at each refueling.
2. The COL will maintain the reliability of the accumulator subsystem.

C. RISK INSIGHTS

1. The accumulators are risk-important.
2. Diversity between the accumulator check valves and the CMT check valves minimizes the potential for common cause failure.
3. The dominant contributor to the accumulator subsystem failure is common cause failure of the check valves.

NORMAL RESIDUAL HEAT REMOVAL SYSTEM
ASSUMPTIONS, FEATURES, INSIGHTS

A. DESIGN FEATURES

1. RNS provides a safety-related means of performing the following functions:
   - containment isolation for the RNS piping that penetrates the containment
   - isolation of the reactor coolant system at the RNS suction and discharge lines
   - makeup of containment inventory following a severe accident.
2. RNS provides a nonsafety-related means of core cooling through:
   - hot leg recirculation at shutdown conditions
   - low pressure pumped injection from the IRWST and long term recirculation from the containment.
3. The RNS has redundant pumps and heat exchangers. The pumps are powered by non-Class 1E power with backup connections from the diesel generators.
4. The RNS containment isolation and pressure boundary valves are safety-related. The motor-operated valves are powered by Class 1E dc power.
5. 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.
6. The containment isolation valves in the RNS piping automatically close via PMS with a high radiation signal.
7. The RNS containment isolation MOVs are automatically and manually actuated via PMS. The RNS pumps are manually actuated via PLS.
8. Interfacing system LOCA between the RNS and the RCS is prevented by:
   - each RNS line is isolated by at least 3 valves
   - the RNS equipment outside containment is capable of withstanding normal RCS pressure.
9. CCS provides cooling to the RNS heat exchanger.

B. OPERATION ASSUMPTIONS

1. The RCS pressure boundary isolation MOVs and CVs are exercised during each cold shutdown.
2. The containment isolation MOVs and CVs are exercised quarterly.
3. Planned maintenance of the RNS is performed at-power.
4. Operating procedures require RNS and its supporting systems (CCS, SWS, ac power) be available during reduced inventory operations.

C. RISK INSIGHTS

1. RNS is not a risk important mitigating system for at-power and shutdown conditions.
2. A loss of RNS is an important initiating event for shutdown conditions.

PROTECTION AND SAFETY MONITORING SYSTEM
ASSUMPTIONS, FEATURES, INSIGHTS

A. DESIGN FEATURES

1. 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).
2. PMS has four redundant divisions of reactor trip and ESF actuation. PMS automatically produces a safety-related reactor trip and ESF actuation using 2-out-of-4 logic.
3. PMS has two redundant divisions of post-accident parameter display.
4. Each division is powered from its respective Class 1E power division.
5. PMS provides fixed position controls in the control room
6. PMS software development and verification will be performed in a way to minimize the potential for common cause failure of software.

B. OPERATION ASSUMPTIONS

1. Continuous automatic PMS system monitoring and failure detection/alarm is provided.
2. The COL will maintain the reliability of the PMS.
3. PMS is required by the Technical Specifications to be available from power conditions down to refueling.

C. RISK INSIGHTS

1. PMS is risk-important.
2. The dominant contributors to PMS unavailability are:
   a. Common cause failure of PMS software (includes ESF output logic, ESF actuation logic, and ESF input channel software)
   b. Common cause failure of ESF hardware (includes ESF output driver card and input channel hardware)
   c. Common cause failure of reactor trip breakers.

DIVERSE ACTUATION SYSTEM
ASSUMPTIONS, FEATURES, INSIGHTS

A. DESIGN FEATURES

1. 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 (ESF).
2. The DAS automatic actuation signals are generated in a functionally diverse manner from the PMS signals. Diversity between DAS and PMS includes different architecture, different hardware implementations and different software. This diversity eliminates the potential for CCF between PMS and DAS
3. DAS provides control room displays and fixed position controls to allow the operators to take manual actions.
4. DAS has two channels and actuates using 2-out-of-2 logic.

B. OPERATION ASSUMPTIONS

1. Operating procedures require DAS reactor trip capability be available during power operations.
2. The COL will maintain the reliability of the DAS.

C. RISK INSIGHTS

1. DAS is not one of the most risk-important systems. It is of "medium" importance with respect to the systems modeled in the PRA

PLANT CONTROL SYSTEM
ASSUMPTIONS, FEATURES, INSIGHTS

A. DESIGN FEATURES

1. PLS provides a nonsafety-related means of controlling nonsafety-related equipment.
2. PLS receives some of its sensor inputs from isolated PMS sensor inputs.
3. PLS has redundancy to minimize plant transients.
4. PLS provides capability for both automatic control and manual control.

B. OPERATION ASSUMPTIONS

None

C. RISK INSIGHTS

1. PLS is not risk-important.