UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

March 3, 1997

APPLICANT: Westinghouse Electric Corporation

FACILITY: AP600

SUBJECT: SUMMARY OF JANUARY 21, AND 22, 1997, MEETING WITH WESTINGHOUSE TO DISCUSS THE AP600 PROBABILISTIC RISK ASSESSMENT (PRA) INSIGHTS

The Nuclear Regulatory Commission (NRC) staff and representatives of Westinghouse Electric Corporation held a meeting on January 21, and 22, 1997, at Westinghouse's office in Monroeville, Pennsylvania, to discuss issues associated with the insights from the AP600 PRA. Attachment 1 is a list of meeting attendees. Attachment 2 was the agenda for the meeting.

The main purpose of the meeting was to discuss important PRA insights and assumptions that should be included in the PRA portion of the design control document (DCD). A secondary purpose of the meeting was to discuss Westinghouse's modeling of steam generator tube rupture (SGTR) events.

Insights and assumptions

The process for developing the insights and assumptions was based on the process used during the review of the evolutionary plants. Prior to the meeting Westinghouse submitted what they considered to be important insights, assumptions, and design features in a November 25, 1996, letter.

The staff reviewed this document and provided its own PRA insights and assumptions for the passive residual heat removal (PRHR) system, the normal residual heat removal system (NRHR), the protection and safety monitoring system (PMS), the diverse actuation system (DAS), and the plant control system (PLS). These insights and assumptions were faxed to Westinghouse prior to the meeting and are provided as Attachment 3. It should be noted that this attachment was a draft document and it included comments and questions to be discussed with Westinghouse and with other NRC reviewers at the meeting.

During the first day and a half of the meetings the staff and Westinghouse discussed the differences between the two documents for the PRHR, PMS, DAS, and the PLS. In some cases Westinghouse agreed to modify their document which will eventually be incorporated into the PRA and then into the DCD. In other cases Westinghouse provided clarifying information and the staff agreed that some of the insights they developed were not appropriate. In other cases the staff and Westinghouse could not come to agreement on what the final insights for the system should entail. (There were some insights that the staff felt were important, however, Westinghouse did not consider these insights to be important enough to be captured in the DCD). However, based on the meeting Westinghouse felt that they had enough information on what the staff considered to be important to develop insights for the rest of the AP600 systems. Westinghouse indicated that insights for the rest of the systems would be

submitted to the staff around the end of February. Westinghouse agreed to consider for this submittal the staff's insights related to the NRHR system which were not discussed at the meeting due to limited time.

For its part the staff agreed to continue reviewing the rest of the systems that Westinghouse had provided in its November 25, 1996, letter (i.e. the core makeup tank, the in-containment refueling water storage tank, the automatic depresurization system, and the accumulators).

Modeling of SGTR events

The modeling of SGTR events in the PRA was also discussed. Attachment 4 lists the concerns (in bullet form) that the probabilistic safety assessment branch had with the SGTR modeling. Westinghouse presented Attachment 5 during the meeting to address some of the staff's concerns. The discussion clarified previously requested information from Westinghouse (Request for additional information number 720.325). The staff asked Westinghouse to perform thermal-hydraulic analyses as necessary to support the success criteria assumed in the SGTR event tree. The following specific staff concerns were mentioned:

1) Lack of thermal-hydraulic analyses supporting the assumption that the AP600 design can rely on non-safety related systems only as a first line of defense to mitigate SGTR accidents (sequence 1 SGR-OK1 in event tree, see page 4-128 of PRA).

2) Conflicting statements in the PRA regarding the assumed size of the break (e.g. complete severance of a single tube vs an 1/8 inch break). Westinghouse indicated that they modeled a complete severance of a single tube and the reference to a 1/8 inch break was a typographical error.

3) Lack of thermal-hydraulic analyses supporting the success criteria and modeling of sequences involving failure to trip of one or more RCPs.

The staff requests that Westinghouse enter the three concerns listed above as meeting open items in the open item tracking system.

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

DISTRIBUTION:
See next page

Attachments: As stated

cc w/attachments:
See next page

DOCUMENT NAME: A:INSITES.SUM
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		BC:SPSB:DSSA		D:PDST:DRPM					
NAME	JMSebrosky		JFlack		TRQuay					
DATE	2/26/97		2/26/97		3/3/97					

OFFICIAL RECORD COPY

cc: 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

Mr. B. A. McIntyre
Advanced Plant Safety & Licensing
Westinghouse Electric Corporation
Energy Systems Business Unit
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

Mr. M. D. Beaumont
Nuclear and Advanced Technology Division
Westinghouse Electric Corporation
One Montrose Metro
11921 Rockville Pike
Suite 350
Rockville, MD 20852

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

Mr. S. M. Modro
Nuclear Systems Analysis Technologies
Lockheed Idaho Technologies Company
Post Office Box 1625
Idaho Falls, ID 83415

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

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

Mr. Ronald Simard, Director
Advanced Reactor Program
Nuclear Energy Institute
1776 Eye Street, N.W.
Suite 300
Washington, DC 20006-3706

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

Mr. James E. Quinn, Projects Manager
LMR and SBWR Programs
GE Nuclear Energy
175 Curtner Avenue, M/C 165
San Jose, CA 95125

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

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

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

WESTINGHOUSE AP600 PRA INSIGHTS
MEETING ATTENDEES
January 21, and 22, 1997

NAME	ORGANIZATION
CINDY HAAG	WESTINGHOUSE
TERRY SHULZ (PART TIME)	WESTINGHOUSE
KEN DEUTSCH (PART TIME)	WESTINGHOUSE
JIM FREELAND (PART TIME)	WESTINGHOUSE
SELIM SANCAKTAR (PART TIME)	WESTINGHOUSE
TIM BUETER (PART TIME)	WESTINGHOUSE
STEVE FOWLER (PART TIME)	WESTINGHOUSE
JIM SCOBEL (PART TIME)	WESTINGHOUSE
CHARLES THOMPSON (PART TIME)	DEPARTMENT OF ENERGY
HULBERT LI (PART TIME)	NRR/DRCH/HICB
JOHN GALLAGHER (PART TIME)	NRR/DRCH/HICB
NICK SALTOS	NRR/DSSA/SPSB
JOHN FLACK	NRR/DSSA/SPSB
JOE SEBROSKY	NRR/DRPM/PDST

Attachment 1

WESTINGHOUSE/NRC AP600 PRA MEETING

AGENDA

January 21, 1996

I. Discussion of assumptions, features, and insights associated with the following systems:

- Normal Residual Heat Removal System
- Passive Residual Heat Removal System (Other systems associated with the Passive Core Cooling System may also be discussed)

January 22, 1996

I. Discussion of assumptions, features, and insights associated with the following systems:

- Protection and Safety Monitoring System
- Diverse Actuation System
- Plant Control System

II. Discussion of the PRA modeling of steam generator tube rupture events.

III. Summary and Conclusion

Attachment 2

IMPORTANT PRA ASSUMPTIONS AND SAFETY INSIGHTS

****

DISCLAIMER: This is draft working material on important PRA assumptions and safety insights as currently understood by NRC reviewers of the AP600 PRA. It includes comments and questions to be discussed with Westinghouse and with other NRC reviewers.

****

Passive Residual Heat Removal (PRHR) System

The PRHR is a single-train dedicated safety system capable of providing emergency core decay heat removal by natural circulation during non-LOCA accidents involving loss of heat removal via the SGs. It is a key system in ensuring adequate plant performance in non-LOCA events to avoid ADS actuation. It also helps cool down and depressurize the RCS during a small LOCA or SGTR event.

The following are important PRHR design and operation features assumed in the PRA:

- The PRHR is actuated automatically 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.

- The PRHR is actuated by the opening of at least one of two redundant air-operated valves (AOVs) in parallel paths. These AOVs are designed to fail open upon loss of 125V DC control power or loss of compressed air or loss of the signal from the PMS *** why not also from DAS? Note that these AOVs can be automatically actuated by either PMS or DAS ****.

- The air-operated valves in the PRHR are diverse ***how are the diverse?*** from the air operated valves in the core makeup tanks (CMTs). This minimizes the probability of common cause failure among PRHR and CMT AOVs.

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

- The PRHR heat exchanger and lines are flow tested at shutdown. The inlet isolation MOV and the two AOVs are tested quarterly at power.

Leak detection in the PRHR ...***Need to be more specific. For example, what is a significant leak? Would the plant be allowed to operate once a leak of a certain magnitude is detected? What are the criteria for deciding when a leak is large enough to require a plant shutdown? How is it assured that a leak that exists during normal operation and which is not judged to be large enough to shut the plant down will not become a rupture during an accident requiring PRHR operation.*****

The PRHR system operates by transferring heat from the RCS to the IRWST. After some initial time of PRHR operation, the IRWST water starts boiling releasing steam directly into the containment. If all steam is condensed in the containment and all condensate returns to the IRWST via the gutter system, the PRHR can keep operating without replenishing the IRWST inventory. Westinghouse calculations have shown that if all steam escapes through an open containment, or if the gutter system is unavailable to return any amount of condensate to the IRWST, the PRHR can keep operating for at least 72 hours without replenishing the IRWST inventory. This analysis shows that there is plenty of time for operator action to replenish the IRWST.

Safety-grade (?) connections are provided in the AP600 design to allow replenishment of the IRWST water if necessary ***** Need more details. How? From where? W mentions connections to IRWST from SFS and CVCS which are not safety related. How about connections for post-72 hour IRWST inventory replenishment in case of a seismic event? *****

Normal Residual Heat Removal (NRHR) System

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

The NRHR is a nonsafety-related system with defense-in-depth functions. For accidents initiated at power and requiring depressurization, successful operation of the NRHR system (in the "low pressure injection/sump recirculation" mode) prevents opening the stage 4 ADS valves which release directly into the containment. It also prevents challenging the passive safety-related IRWST injection and sump recirculation systems.
For accidents initiated during shutdown, successful NRHR operation (in the "shutdown cooling" mode) prevents challenging the .....***explain***

The NRHR includes redundant pumps and heat exchangers but with common suction and discharge headers, two redundant (parallel) paths connecting the NRHR pump suction header to the RCS hot leg (for shutdown cooling) and two redundant DVI lines. During normal plant operation, the NRHR system is in a standby mode isolated from both the RCS and the IRWST.

In the "low pressure injection/sump recirculation" mode of operation, at least one NRHR pump is required to operate taking suction either from the IRWST (for low pressure injection) or from the containment sump (for sump recirculation). Recirculation from the sump is necessary for long-term core cooling after the IRWST inventory is depleted.

- Operator action, from the control room, is required to align the NRHR for low pressure injection (open several MOVs at both the pump suction and discharge lines) and start the NRHR pumps following receipt of an automatic depressurization signal

- The NRHR system starts injecting when the RCS pressure falls below the shutoff head of the NRHR pumps (approximately 150 psig) and is capable of bringing the RCS to cold shutdown conditions using only one pump (initially for injection and later for sump recirculation)

- Containment sump recirculation can be actuated manually, from the control room, if automatic actuation fails. Based on the NRHR design, only one of the two sump recirculation lines (line B) can be used for this operation. Unrestricted flow through both parallel paths of line B (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 NRHR pumps are running. If only one of the two parallel paths in line B opens, operator action (in the control room through PMS) is required to manually throttle the NRHR discharge valve (V011) to prevent pump cavitation. ****Note: If NRHR injection is successful but NRHR recirculation fails (e.g., one of the parallel paths in line B fails to open) is the RCS depressurized enough to allow recirculation flow by gravity? **********

- The valves that must open to align the NRHR for injection are designed to close automatically on a high containment 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 NRHR MOVs to automatically close.

In the "shutdown cooling" mode of operation the NRHR pumps take suction from a RCS hot leg and inject through the DVI lines. To align the NRHR for shutdown cooling operation, manual action (from the control room) is required to open several MOVs at both the pump suction and discharge lines.

- Inadvertent opening of any of the two remotely operated MOVs (connecting the suction and discharge headers, respectively, to the IRWST) when the NRHR is aligned for shutdown cooling, could divert reactor coolant and drain the RCS. To preclude this, these two valves are interlocked with the four normally closed MOVs in the two parallel paths connecting the NRHR pumps to the hot leg.

- To prevent overpressurization of the NRHR system, the pump suction isolation valves (i.e., the four normally closed MOVs in the two parallel paths connecting the NRHR 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.

- The operability of the NRHR is tested, via connections to the IRWST, immediately before its alignment to the RCS hot leg to ensure that there are no any open manual valves in the drain lines. *** Note: Are there any potentially open manual valves in the NRHR being modeled in the PRA for NRHR injection? **********

The NRHR MOVs which have containment isolation function (V011 and V022), RCS pressure boundary isolation function (V001A, V001B, V002A and V002B) and IRWST suction isolation function (V023) are safety related and are powered from 125 V dc class 1E busses.

The air cooled NRHR pump motors can operate for at least 24 hours without room cooling ***how will this be verified***

Loss of NRHR pump seal cooling would not impact pump operation for at least 24 hours **how will this be verified?**. The NRHR pump design includes features **specify** which protect the pump motors from water spray caused by seal failure.

The NRHR system is capable to perform its "low pressure injection/sump recirculation" function even when the component cooling water (CCW) is unavailable to remove the RCS decay heat loads

The NRHR pumps receive power from separate 480 V AC buses. These buses, on loss of offsite power (LOOP), transfer automatically to the onsite nonsafety-related diesel generators. An automatic restart of the NRHR pumps is provided when, after LOOP, transfer onto DG power has been completed.

Operation of the NRHR during an accident requiring depressurization prevents opening the stage 4 ADS valves that release directly into the containment.

Installed instrumentation provides the capability to monitor NRHR performance, including performance of its major components, from the MCR and the RSW

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 pressure which is established at the suction side of the NRHR pumps at the time the system is switched from the injection to the recirculation mode of operation, allows the sump recirculation check valve to open without any operator action. This prevents NRHR cavitation.

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

- The portion of the NRHR system outside containment has an ultimate rupture strength in excess of the full normal operation RCS pressure

- There is a relief valve in the common NRHR discharge line which provides protection against excess pressure in the portion of the NRHR system outside containment

- The pump suction isolation valves connecting the NRHR 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....***(explain)***

- The two remotely operated MOVs connecting the suction and discharge headers, respectively, to the IRWST are interlocked with the isolation valves connecting the NRHR pumps to the hot leg. This prevents....***explain***

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

- At least three normally closed isolation MOVs in series have to fail open to expose the NRHR portion located outside containment to full RCS pressure

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

A portion of the NRHR system can be aligned for gravity injection from the IRWST via the NRHR hot leg connection during shutdown operation. This requires operator action (risk important). *****To be included in the list of important human actions/errors*****

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

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

PRA results indicate that NRHR availability (including support systems) is important for reduced inventory operation during shutdown ***Tech Spec?*** *** Explain why is important ***

The loss of NRHR during shutdown conditions is a risk important initiating event *** what requirements would assure NRHR reliability during shutdown?****

Safety-related MOVs and supporting systems provide the containment isolation function at each NRHR piping containment penetration ***this could be a generic plant requirement for all containment penetrations****

Instrumentation and Control (I&C)

From a PRA perspective the I&C system is made up of three major systems: (1) Protection and Safety Monitoring System (PMS), (2) Diverse Actuation System (DAS), and (3) Plant Control System (PLS).

The Protection and Safety Monitoring System (PMS) is a safety-related I&C system which provides both automatic and manual control of safety-related equipment and components during an accident. Specifically, it performs the following functions: (1) initiates reactor trip, (2) actuates and controls safety-related equipment and components (engineered safety feature actuation function), and (3) provides control room indication for monitoring of safety-related functions.

The Diverse Actuation System (DAS) is a nonsafety-related system which backs up the PMS. Being diverse from the PMS, the DAS provides an alternate means of initiating reactor trip, actuating and controlling selected engineered safety features and providing control room indication for monitoring of safety-related functions.

The Plant Control System (PLS) is a nonsafety-related system which provides both automatic and manual control of nonsafety-related equipment and components during normal plant operation (at power or at shutdown) as well as during an accident. In addition, the PLS provides control room indication for monitoring overall plant and nonsafety-related system performance.

Protection and Safety Monitoring System (PMS)

The PMS is made up of three main subsystems: (1) the Reactor Trip Subsystem (RTS); (2) the Engineered Safety Features Actuation Subsystem (ESFAS); and (3) the Qualified Data Processing Subsystem (QDPS). The RTS has four redundant divisions, each with capability for both automatic and manual reactor trips. The ESFAS has four redundant divisions to perform its control and indication functions. Each ESFAS division has capability for both automatic and manual control of safety related components. The QDPS has two redundant divisions that provides inputs to main (and alternate) control room displays.

Each PMS division is powered from a separate division of class 1E power.

In addition to the QDPS indication displays, key indications of critical function status for post-accident monitoring is provided in the control room by the four redundant divisions of the ESFAS.

To minimize common cause failure within ESFAS, sufficient diversity and defense-in-depth is provided by the addition of manual hardwired controls as well as hardwired displays of key indications of critical function status for post-accident monitoring.

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

High sensor reliability is assured by redundancy and diversity. **** Redundancy is achieved by using multiple sensors to measure same parameter. Diversity is achieved by using a voting logic with inputs from diverse types of sensors. ******

Each of the four ESFAS divisions is composed of two redundant microprocessor-based "trains" which are physically and electrically separated and are interfacing with safety-related components.

Built in test and diagnostic features, such as on-line system monitoring and failure alarming, minimize the time required to test the system operability and identify failed components. These features, combined with the ease of replacement of failed components, minimize component down times.

It is assumed in the PRA that the operator will be trained to recognize, in a very short time, the need to manually trip the reactor when automatic trip fails following a LOCA or transient event that requires reactor trip.

*** Separate hardware and application software modules are dedicated to the reactor trip and ESF functions of the PMS. Note: a limited set of software

modules which control fundamental computer operations are common to the reactor trip and ESF functions (see response to RAI 720.307). Was this modeled in the PRA? ******

The following CCF events were identified by the PRA as very risk significant (high "risk achievement worth") but were assumed to have a very low probability to occur during an accident ****** Need to identify the important design features and assumptions made in the PRA (or assumptions that should have been made to justify models and data used) when calculating the probability of these events. Defense mechanisms against hardware CCF include separation, operational testing, maintenance, and immediate detectability of failure provided by the on-line diagnostics.**********

- CCF of the reactor trip breakers to open on demand (event RCX-RB-FA ** mechanical failure given signal ok?) *** High redundancy: there are eight reactor trip breakers****
- CCF of the reactor coolant pump trip breakers (event RCX-CB-GO, mechanical failure given signal ok?) *** High redundancy: there are eight (?) RCP trip breakers****
- CCF of the reactor trip subsystem hardware or software (event CCX-PMS-HARDWARE, electrical failure, i.e., no signal to breakers?)
- CCF of pressure-type sensors that interface with high pressure environments, such as pressurizer pressure and SG narrow-range and wide-range level sensors (event CCX-XMTR) *** same type in PMS, DAS and PLS****
- CCF of pressurizer level sensors, both narrow and wide(?) range (event CCX-XMTR195) *** same type in PMS, DAS and PLS****
- CCF of pressure-type sensors in a lower pressure environment, such as steam line and containment pressure sensors (event CCX-TRNSM) ***** same type in PMS, DAS and PLS****
- CCF of the IRWST tank level transmitters (event IWX-XMTR) ***** same type in PMS, DAS and PLS****
- CCF of all PMS and PLS software (event CCX-SFTW)
- CCF of ESFAS input channel software (event CCX-IN-LOGIC-SW)
- CCF of ESFAS output logic software (event CCX-PMXMOD1-SW)
- CCF of ESFAS actuation logic software (event CCX-PMXMOD2-SW)
- CCF of ESFAS manual input multiplexer software (event CCX-PMXMOD4-SW)
- CCF of ESFAS input channel hardware (event CCX-INPUT-LOGIC)
- CCF of ESFAS output driver card (event CCX-EP-SAM)

****

Comments on the nature of software failures

Digital I&C systems are designed as complex combinations of hardware and software (i.e., computer programs) components. Although computer software do not wear out, as hardware do, they fail due to the excitation of residual design errors when a particular combination of inputs occurs. If one could eliminate all the design errors before a software product is put in operation, it would work perfectly for ever. However, it is impossible to be certain that a software product is error free. On the contrary, experience shows that there are always residual faults which do not show up, and thus they do not cause a software failure, unless the program is exposed to an environment for which it was not designed or tested. Exposure to such an environment is possible because, due to the large number of possible states and inputs in most software programs, it is extremely difficult to comprehend perfectly program requirements and implementation and virtually impossible to test more than a small subset of all possible input combinations during development. Thus, software reliability is essentially a measure of the confidence one has in the design of the software and its ability to function properly in its expected environment.

Quantification of software reliability may be too difficult, especially for software which must meet high reliability requirements such as those used in the AP600 design. This is due to the random nature of a large number of possible inputs, the unknown mechanisms of human failure which create errors during the development process and the randomness of the testing process used to detect errors. However, regardless of whether the reliability of software can be accurately quantified, the design goal must be to minimize the number of residual errors, their frequency of occurrence, and their effect on system performance. This can be achieved by following formal and disciplined methods during the development process combined with an expected use-based testing program. For these reasons, each software product is unique and extrapolation of statistical data for other products is meaningless.

From the basic properties of software it follows that commonly used hardware redundancy techniques do not improve software reliability. The several defense mechanisms against hardware CCFs that are incorporated in the design (such as redundancy, separation, operational testing, maintenance, and immediate detectability of failure provided by the on-line diagnostics) cannot be relied upon to prevent software CCFs. If the same programs are executed in two or more channels (or divisions) in parallel, a software fault would lead to a common mode software failure in all channels (or divisions) at the same time, i.e., it would be a common cause failure (CCF) of redundant channels or divisions. Thus, a highly reliable software product is needed whenever the same program is executed in two or more channels (or divisions) in parallel. Since the reliability of a software product is basically determined during development and testing, the importance of the software development process in achieving high reliability cannot be overestimated.

****

Although it is not easy to quantify software reliability, it is generally accepted that high reliability can be achieved by following formal and disciplined methods during the development process combined with an expected

use-based testing program. The AP600 design PRA assumes high reliability for all software used in the digital I&C systems. Westinghouse expects to develop highly reliable software for the AP600 I&C systems by setting reliability goals and design requirements and by incorporating features in the software design which act as "defenses" against CMF. Such requirements and design features include: (1) requirements for formalized design phases, for following design standards and for performing formal design reviews; (2) requirement for an expected use-based software testing/verification program; (3) incorporation of "fail safe" capability in the design, i.e., incorporation of mechanisms (independent of the source of error) for detecting errors at the module or intermediate level and producing a well defined output which results in an application specific safe action; and (4) incorporation of "functional diversity" which allows initiation of automatic protection functions even when errors associated with some plant parameters are present (different plant parameters initiate same automatic protection function independently).
*** Others? E.g., construction of full scale prototypes******

Diverse Actuation System (DAS)

The DAS has the capability to perform its reactor trip and control functions both automatically and manually.

The automatic DAS function is accomplished by two redundant microprocessor-based subsystems (or channels) which are physically and electrically separated and are interfacing with selected engineered safety features.

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

Common cause failure between PMS and DAS, with the exception of sensors, is assumed to be negligible due to the diversity and complete physical separation of the two systems. The hardware and software of DAS are diverse from both the PMS and the PLS, with the exception of sensors which are redundant (not shared) but of the same type. Hardware diversity is achieved by the use of different architecture and microprocessor platform. Software diversity is achieved by the use of different operating systems and by programming in different computer languages.

The selection of setpoints and time responses are such that an automatic DAS signal is not generated unless the automatic PMS signal has failed.

Interface with actuated devices (engineered safety features) is assumed to be arranged to prevent failures in either DAS or PMS from blocking the actuation signal from the other system.

In addition to the diverse indication displays of DAS, diverse key indications of critical function status for post-accident monitoring is provided by DAS in the control room by dedicated hardwired displays.

Common cause failure between manual and automatic DAS controls is assumed to be negligible. The controls used to perform the manual DAS function (reactor trip and control of selected engineered safety features) are completely separate from the automatic DAS controls as well as from the PMS (automatic and manual) controls.

Diversity and defense-in-depth within DAS is provided by manual dedicated hardwired controls, which completely bypass the DAS automatic actuation logic but not necessarily the final switching actuation device which may be shared between the manual and automatic functions, as well as by hardwired displays of key indications of critical function status for post-accident monitoring. ****Are the actuation devices (switches) shared between PMS and DAS also? If yes, was this modeled in the PRA?***

The DAS reactor trip function is implemented through a trip of the control rods via the motor-generator set which is diverse from the PMS reactor trip breakers.

The DAS is powered by the non-class 1E uninterruptible power system.

The DAS actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate contacts. The normally de-energized output state, along with the two-out-of-two voting logic for all DAS actuation functions but reactor and turbine trip, minimize the likelihood for spurious actuation.

It is assumed in the PRA that the operator will be trained to recognize the need for and manually actuate a reactor trip, in a very short time, via both PMS or DAS when automatic trip (via PMS and DAS) fails following a LOCA or transient event that requires reactor trip.

To prevent spurious actuations, the DAS employs a two-out-of-two voting logic for all engineered safety feature control functions (a two-out-of-four voting logic is employed for its reactor and turbine trip functions).

Plant Control System (PLS)

The functions of the PLS are performed by physically and electrically separate assemblies. These assemblies include distributed controllers that perform both logic and modulating control functions for the non-class 1E systems of the plant ***many of whom are credited in the PRA and have defense-in-depth functions*** with capability for both automatic and manual control (at both the system and the component level). The control architecture employs a redundancy scheme (signal selector) which enhances its reliability and provides assurance against the occurrence of transients due to control system failures.

To increase the reliability of PLS and provide assurance against the occurrence of transients due to sensor failures, redundant inputs to a signal selector for automatic control are received from local sensors as well as from the PMS (auctioneered inputs from the Integrated Protection Cabinets via the PMS communications subsystems). Signal selectors are incorporated in the PLS design to reject erroneous input signals from the PMS and ensure that the control system does not cause an unsafe control action to occur even if two of four redundant protection channels are degraded by random failure or by being bypassed for test or maintenance.

It is assumed in the PRA that, in case of an ATWS event with manual reactor trip failure, the operator will be trained to act very fast (within about one minute from ATWS event occurrence) to manually step-in the control rods via

the rod control system *** PRA event ATW-MAN01***. This action is necessary to provide sufficient negative reactivity to allow the pressurizer safety valves to maintain the RCS peak pressure below the ASME stress level C limit (conservatively assumed to be 3200 psig) even when an unfavorable (positive) moderator temperature coefficient (MTC) is present at the time of the ATWS event.

Built in test and diagnostic features, such as on-line system monitoring and failure alarming, minimize the time required to test the system operability and identify failed components. These features, combined with the ease of replacement of failed components, minimize component down times.

The CCF of redundant but identical PLS Logic Output Cards ***PRA event CCX-EP-SA*** would fail all PLS logic control functions (RAW about 10 times). **** What design features ensure that the probability of this CCF is low?****

To provide adequate defense-in-depth during a station blackout event, one of the two subsystems of PLS is powered by the non-class 1E 120V AC uninterruptible power supply. Loss of control power causes failure of the control function without changing the state of any component.

AP600 SGTR PRA MODELING

1. SIZE OF BREAK ASSUMED

2. T-H ANALYSES SUPPORTING ASSUMPTIONS AND SUCCESS CRITERIA

3. USE OF CVCS FOR INVENTORY CONTROL

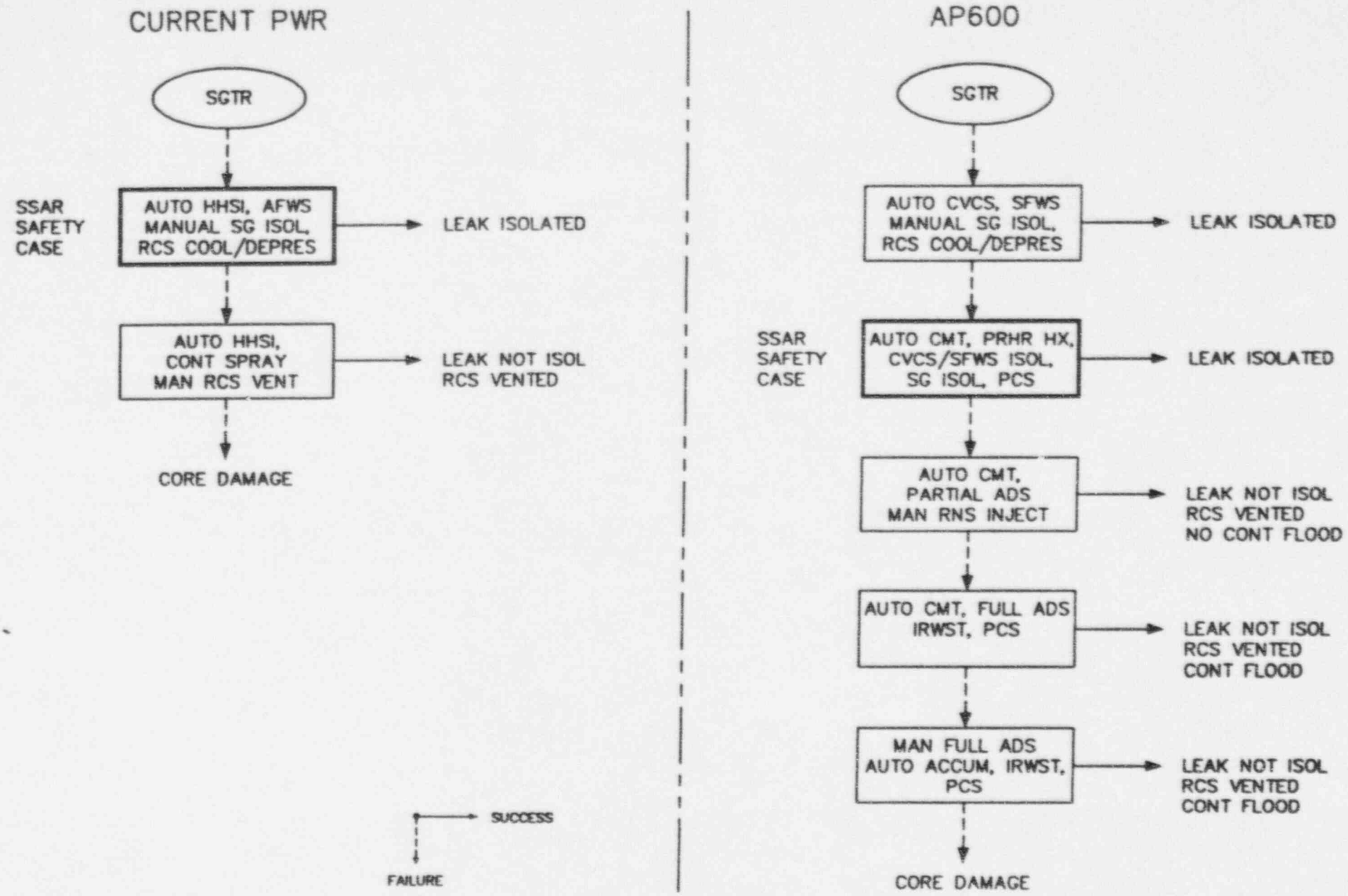
4. MODELING OF SCENARIOS WITH RCP FAILURE TO TRIP

5. MODELING OF UNISOLABLE PATHS TO THE ATMOSPHERE

6. ASSUMPTIONS AND FAULT TREE MODELING OF THE TBVs

Attachment 4

STEAM GENERATOR TUBE RUPTURE



Attachment 5

SGTR Injection Supply Comparsion

RCS Pres (psig)	AP600 2 CMT* (gpm)	AP600 1 CVS Pmp (gpm)	Operating 2 Loop Plant 1 HHSI (gpm)	1 CVCS Pmp (gpm)
2200	158	120	0	60
2000	158	150	0	60
1800	158	170	266	60
1600	158	170	302	60
1400	158	170	396	60
1200	158	170	403	60

* CMT operates in recirculation mode, providing this net injection.

DISTRIBUTION w/attachments:
Docket File
PUBLIC
PDST R/F
TQuay
TKenyon
BHuffman
DTJackson
JSebrosky

DISTRIBUTION w/o attachments:
SCollins/FMiraglia, 0-12 G18
AThadani, 0-12 G18
RZimmerman, 0-12 G18
TMartin
DMatthews
DRoss
WDean, 0-17 G21
JMoore, 0-15 B18
ACRS (11)

DF03 1/1

050097