Docket File

52-003

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

August 1, 1996

APPLICANT: Westinghouse Electric Corporation

PROJECT: AP600

SUBJECT: SUMMARY OF MEETING WITH WESTINGHOUSE TO DISCUSS THE PROBABILISTIC RISK ASSESSMENT (PRA) FOR THE AP600

The Nuclear Regulatory Commission (NRC) staff and representatives of Westinghouse Electric Corporation held a meeting on June 24, 1996 through June 26, 1996 in Monroeville, Pennsylvania, to discuss issues associated with the PRA for the AP600. Attachment 1 is a list of meeting attendees. Attachment 2 is the agenda items for the meeting.

Highlights of the discussion are summarized as follows:

Changes in the PRA

The meeting began with a discussion of significant changes that had been made in the draft Revision 7 to the PRA. Westinghouse discussed the significant changes in the plant design that were incorporated into Revision 7 of the PRA and the significant changes that were made to the PRA Revision 7 models compared to the Revision 6 models. The significant changes in the plant design that were incorporated into the PRA included: The addition of squib valves to the in containment refueling water storage tank (IRWST) injection and recirculation lines, automatic actuation of the squib valves from the core makeup tank level instrumentation, and the change from 2 passive residual heat removal (PRHR) heat exchangers to 1 PRHR heat exchanger.

According to Westinghouse the significant changes in the PRA models included: more human reliability conditionals being added to the models, the automatic depressurization (ADS) success criteria being made more conservative, and the large break loss of coolant accident (LOCA) event tree models being revised to account for containment isolation. The ADS success criteria were made more conservative by the following changes: requiring 2 out of 4 stage 4 ADS valves to operate verses 1 out of 4, not taking credit for the function of stage 1 ADS but requiring stage 2 or stage 3 ADS to operate for small break LOCAs, and making human reliability response times shorter which made the human reliability numbers larger. For some smaller large-break LOCAs the event tree models were changed to reflect that containment isolation is needed to ensure that low pressure injection will work.

The changes to the draft Revision 7 PRA were then discussed on a chapter by chapter basis. In some cases Westinghouse agreed on making changes to the PRA based on the NRC staff's initial review of the revision. There was also a discussion on how Westinghouse obtained the values used for squib valve reliability and why these values differed from the Advanced Light Water Reactor Utility Requirements Document (ALWR URD) numbers that were used in the past.

Westinghouse explained that they did not rely solely on the ALWR URD number rather they received more data from the valve manufacturer knowing that the valves were used for other applications (e.g. defense and space applications). Not all the chapters that had changes made to them were discussed during this portion of the meeting and because of time restraints it was decided to have further discussions at a later date.

Discussion of the list of cutsets used for accident sequences

Westinghouse demonstrated their methodology for quantifying accident sequences. Prior to the meeting the staff had asked Westinghouse to provide the top cutsets for some sequences. The list of the sequences can be found in Attachment 3. Westinghouse responded to this request in a June 7, 1996, letter which supplied the requested information. Westinghouse explained that, because of the software used for the PRA, cutsets at intermediate stages of the process were difficult to extract. Westinghouse further explained that in their June 7, 1996 submittal some sequences did not have cutsets because they were below the quantification cutoff limit. The staff was interested in the intermediate results because insights could be gained into why some sequences which had been dominant contributors to core damage frequency (CDF) for past pressurized water reactor (PWR) designs are not dominant contributors to CDF for the AP600.

Focused PRA issues

Westinghouse provided an overview of the regulatory treatment of nonsafety systems (RTNSS) process (see Attachment 4). The questions that the staff had with the focused PRA were then discussed. Attachment 5 provides these questions. Westinghouse expressed concern that the staff was changing the intent of the agreement reached on RTNSS and the focused PRA found in the SECY Papers on the issue (SECY-94-084, and SECY-95-132). The staff was concerned that stopping the PRA at 24 hours did not model important phenomena that were known to occur around that time interval. For example the automatic initiation of the ADS after a station blackout occurs at about 24 hours. The staff and Westinghouse also discussed Westinghouse's March 8, 1996, response to draft safety evaluation report (DSER) Open Items 19.1.3.1-4 and 19.1.3.1-6 which addressed the issue.

The staff also expressed concern with how Westinghouse modeled the loss of the non-safety related systems in the focused PRA. Westinghouse contended that their process met the intent of the SECY papers and that it had been described in WCAP-13856 which had been published in 1993. It was agreed that Westinghouse would do a limited scope sensitivity analysis on the baseline PRA to address the staff's concerns. The limited scope sensitivity analysis would keep the following systems, unless the initiating event caused them to fail: main feedwater, condensate, AC power, plant control, Non-1E DC power, circulating water, main steam, chilled water, turbine building closed cooling water, component cooling water, service water, and instrument air. Westinghouse would not take credit for the following systems: chemical and volume control, startup feedwater, normal residual heat removal, diverse actuation,

and the diesel generators. It was also agreed that this sensitivity analysis would be done with the Revision 7 baseline at power analysis and that the results would represent a good approximation of the actual number. Westinghouse will submit the results of this analysis to the staff for review. The rest of the questions on Attachment 5 where then discussed in greater detail. Westinghouse in some cases provided clarifying information, and in other cases agreed to change the PRA to address the concern.

Breakout session on Thermal-Hydraulic Uncertainty

A breakout session was held to discuss requests for additional information (RAIs) related to AP600 thermal-hydraulic uncertainty and benchmarking of the MAAP4 code. Attachment 2 contains a list of the attendees. All RAIs provided to Westinghouse were reviewed, and staff expectations were clarified, where necessary. Written responses will be provided by Westinghouse in the near future. Westinghouse also presented preliminary results from selected MAAP4-NOTRUMP benchmarking cases over a range of break sizes. In general the staff thought, for the parameters presented, including safety injection flows and water levels, MAAP4 appeared to do a fairly good job compared to NOTRUMP, in terms of magnitudes and timing. However, larger discrepancies were noted between the two codes at smaller break sizes. While a considerable amount of work remains to be done on MAAP4 benchmarking, and the NOTRUMP thermal-hydraulic uncertainty analyses have not been started, due to delays in resolving design-basis analysis issues on NOTRUMP, the staff felt encouraged that progress was being made in performing initial analyses and in developing in greater detail the benchmarking and T/H uncertainty resolution process.

Instrumentation and Control PRA models

Attachment 6 contains the questions that served as the agenda for this portion of the meeting. The discussion began with Westinghouse presenting its April 4, 1996 response to a software common cause failure question which related to DSER Open Item 19.1.3.1-15. After this discussion the questions in Attachment 6 were addressed. In some cases, Westinghouse provided clarifying information concerning the questions and in other cases the questions were not resolved and further discussions were determined to be needed.

PRA input to the design certification process

The staff discussed an approach for systematically identifying Tier 1 and 2 design certification material (e.g. inspections tests analyses and acceptance criteria (ITAAC), Reliability assurance program (RAP) requirements, and combined operating license (COL) action items) based on PRA assumptions and insights. The staff explained that in this approach, PRA results and insights will be used to identify safety-significant assumptions made in the PRA. Once such assumptions are known, the next step will be to identify "requirements" (i.e. Tier 1 and 2 material) for ensuring that safety significant assumptions will come true when an AP600 plant is built. Westinghouse agreed to implement the above approach for a few systems and submit it to the staff for review. The staff agreed to review the material and provide feedback to Westinghouse.

Fire PRA

Westinghouse presented the methodology for the draft fire PRA that was provided to the staff in a June 14, 1996 letter. Attachment 7 includes the handouts provided by Westinghouse for this portion of the meeting. The staff did not have sufficient time to review the material and provide detailed comments to Westinghouse, however, based on the initial review the staff felt that Westinghouse's approach was acceptable. It was recognized that Westinghouse still needed to address the shutdown fire PRA. Westinghouse indicated that this analysis would be provided in Revision 8 to the PRA.

Breakout session with Idaho National Engineering Laboratory (INEL)

A breakout session was held with INEL to discuss the material that would be needed from Westinghouse to update INEL's codes. Westinghouse agreed to provide updated computer files on Revision 7 PRA models when the revision was finalized.

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

Attachments: As stated

cc w/attachments:
See next page

DISTRIBUTION w/attachments:

~~Docket File~~	PDST R/F	BKGrimes
PUBLIC	EAdensam	TRQuay
DTJackson	TJKenyon	Jsebrosky
WHuffman		

DISTRIBUTION w/o attachments:

WRussell/FMiraglia, O-12 G18	RZimmerman, O-12 G18	AThadani, O-12 G18
EJordan, T-4 D18	ACRS (11)	JMoore, O-15 B18
WDean, O-17 G21	NSaltos, O-10 E4	JFlack, T-10 F13
ALevin, O-8 E23	MGareri, O-8 H3	

DOCUMENT NAME: A:PRA 6 24.SUM (7G AP600 DISK) *See previous concurrence
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:ECGB:DRPM		D:PDST:DRPM		HICB:DRCH		D:PDST:DRPM	
NAME	JSebrosky:sg		JFlack		ALevin		MGareri*		TRQuay	
DATE	07/26/96		07/01/96		07/31/96		07/26/96		08/ 1 /96	

OFFICIAL RECORD COPY

Westinghouse Electric Corporation

Docket No. 52-003

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

Mr. John C. Butler
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
MEETING ATTENDEES
JUNE 24 THROUGH JUNE 26, 1996

NAME	ORGANIZATION
TIM BUETER	WESTINGHOUSE
BRUCE MONTY (PART TIME)	WESTINGHOUSE
CINDY HAAG (PART TIME)	WESTINGHOUSE
SELIM SANCAKTAR (PART TIME)	WESTINGHOUSE
TERRY SCHULZ (PART TIME)	WESTINGHOUSE
JIM FREELAND (PART TIME)	WESTINGHOUSE
BARRY SLOANE (PART TIME)	WESTINGHOUSE
AMIR AFZALI (PART TIME)	WESTINGHOUSE CONSULTAANT
NICK SALTOS	NRR/DSSA/SPSB
JOHN FLACK	NRR/DSSA/SPSB
ALAN LEVIN (PART TIME)	NRR/DSSA/SRXB
MARIO GARERI (PART TIME)	NRR/DRCH/HICB
JOE SEBROSKY	NRR/DRPM/PDST
LEON WOLFRAM (PART TIME)	INEL

THERMAL HYDRAULIC UNCERTAINTY MEETING
June 25, 1996

NAME	ORGANIZATION
CINDY HAAG	WESTINGHOUSE
LARRY HOCHREITER	WESTINGHOUSE
DEBRA OHKAWA	WESTINGHOUSE
ALAN LEVIN	NRR/DSSA/SRXB

CODE DISCUSSIONS
June 26, 1996

NAME	ORGANIZATION
JIM FREELAND	WESTINGHOUSE
LEON WOLFRAM	INEL

Attachment 1

WESTINGHOUSE/NRC MEETING ON AP600 PRA
JUNE 24 THROUGH 26, 1996
MONROEVILLE, PA

AGENDA

Monday, June 24, 1996

- Changes in draft markup Level 1 PRA (changes from Rev 6. to Rev 7.)
- Discuss list of cutsets for accident sequences which the staff will use for detailed confirmation review

Tuesday, June 25, 1996

- Focused PRA issues
  - Background of RTNSS & focused PRA
  - Discussion of items on focused PRA
- Breakout session to discuss thermal hydraulic uncertainty
- I&C PRA models
  - Discussion of items on I&C questions

Wednesday, June 26, 1996

- PRA input to the design certification process
- Fire PRA
- Breakout session with INEL to discuss computer codes

Attachment 2

SEQUENCES TO GET MINIMUM CUTSETS

Provide top 50 (or about) cutsets for each of the following sequences. Please use event designators and a brief event description with the associated probability (i.e., same format as the one used in Table 33-3 of the PRA).

SGTR

1. SGTR * /RTRIP * CVCS * /SGISO * CMT * /PRHR * /ADS-F * /ACC * NRHR * IRWST
2. SGTR * /RTRIP * CVCS * SGISO * /CMT * /PRHR * ADS-F * ADS-P
3. SGTR * /RTRIP * CVCS * SGISO * RCL * /PRHR * ADS-F * ADS-P
4. SGTR * /RTRIP * CVCS * /SGISO * RCL * /PRHR * /ADS-F * ACC
5. SGTR * /RTRIP * CVCS * SGISO * /CMT * /PRHR * /ADS-F * /ACC * NRHR * IRWST

CONSEQUENTIAL SGTR

1. SLB-V * /RTRIP * SGTR * /CMT * /PRHR * /ADS-F * /ACC * NRHR * IRWST
2. (LMFW or LOSP * R05 or LCAS or LCOND or LCCW * MFW or TRANS * MFW or LMFW1 * MFW) * /RTRIP * SLSOV * SGTR * PRHR * /CMT * ADS-F * ADS-P

STUCK-OPEN SECONDARY SIDE SAFETY VALVE

1. SLB-V * /RTRIP * NSGTR * /PRHR * (CMT or RCL) *CVCS * ADS-F * ADS-P
2. SLB-V * /RTRIP * NSGTR * /PRHR * (CMT or RCL) * CVCS * /ADS-F * /ACC * NRHR * IRWST
3. SLB-V * /RTRIP * NSGTR * /PRHR * (CMT or RCL) * CVCS * /ADS-F * ACC

LOOP

1. LOSP * /RTRIP * R05 * /DGEN * /SLSOV * SFW * PRHR * /PRSOV * /CMT * ADS-F * ADS-P
2. LOSP * /RTRIP * R05 * /DGEN * /SLSOV * SFW * PRHR * /PRSOV * /CMT * /ADS-F * NRHR * IRWST
3. LOSP * /RTRIP * R05 * /DGEN * /SLSOV * SFW * PRHR * /PRSOV * /CMT * /ADS-F * NRHR * /IRWST * RECIR

LOSS OF MAIN FEEDWATER (LMFW)

1. LMFW * /RTRIP * /SLSOV * SFW * PRHR * /PRSOV * (CMT or RCL) * ADS-F * ADS-P
2. LMFW * /RTRIP * /SLSOV * SFW * PRHR * /PRSOV * /CMT * ADS-F * ADS-P

OTHER

Sequenses, numbered 1 to 7 and 10 to 12 in Table 33-4 of the PRA (provide additional cutsets than what already provided for each of these sequences).

AP600 RTNSS PROCESS

T. L. SCHULZ
SYSTEMS ENGINEERING
June 25, 1996

AP600 RTNSS BACKGROUND

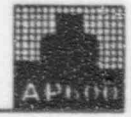
- **Industry and NRC Agreed on RTNSS Process**
  - Based on series of meetings
    - Significant discussion / debate
  - Agreement documented in SECYs 93-087(draft), 94-084, 95-132
    - Identified evaluation process and screening criteria
    - Uses both probabilistic and deterministic criteria
  - Westinghouse applied process to AP600
    - WCAP-13856 submitted to NRC 9/93
    - Documented our assumptions and approach
    - Identified several RTNSS important nonsafety features

RTNSS PROCESS / CRITERIA

- **RTNSS Process**
  - Identify nonsafety-related features with safety important functions
  - Develop specific RTNSS missions based on safety important functions
  - Propose additional oversight appropriate to their RTNSS missions

- **RTNSS Screening Criteria**
  - Criteria used to determine if a nonsafety feature is important
    - Sensitivity study on baseline PRA ("focused" PRA)
      - CMF / LRF without nonsafety mitigation
    - PRA initiating event frequency evaluation
    - ATWS rule (10 CFR 50.62)
    - Loss of all AC power rule (10 CFR 50.63)
    - Long term cooling (post 72 hour actions)
    - Containment performance
    - Adverse interactions with safety-related systems (WCAP-14477, 2/96)
    - Seismic considerations

FOCUSED PRA STUDY



- **Comprehensive Baseline PRA**
  - Level 3 PRA with adequate treatment of
    - Internal and external events (seismic margins)
    - At power and shutdown operation
    - Uncertainties, long-term operation, containment performance
    - Include adverse system interactions

- **Focused PRA**
  - Sensitivity study performed on baseline PRA
    - Initiating events remain unchanged
      - IE importance addressed in separate RTNSS evaluation
    - Mitigation of events by nonsafety features removed from PRA
      - SECY-94-084 says "event trees will not include DID functions and their support such as AC power"
  - Goal is for focused PRA to meet NRC safety goals
    - Core melt frequency 10^{-4}/yr, large release frequency 10^{-6}/yr

INITIATING EVENT EVALUATION

- **Importance of Nonsafety Features to IE**
  - SECY requires IE evaluation
    - SECYs do not provide specific criteria
  - Westinghouse developed evaluation criteria
    - Is nonsafety feature involved in determining IE frequency?
    - Is nonsafety feature important in determining IE frequency?
    - Is CMT / LRF associated with IE significant?
  - If answer to all of these questions is yes
    - The nonsafety feature involved is RTNSS important

QUESTIONS ON THE FOCUSED PRA FOR THE NRC/W MEETING

1. The staff recognizes that the focused PRA sensitivity study is being developed under several constraints stemming from assumptions, criteria and guidelines in the RTNSS process. In case some of these assumptions, criteria and guidelines are subject to multiple interpretations, Westinghouse should discuss this issue with the staff. The staff have pointed out to Westinghouse the following two areas where, in the staff's opinion, W's assumptions are contradictory and not consistent with standard PRA practices, the operation of the plant and the RTNSS process.

   - Long term cooling ***** the staff believes that W should address post-24-hour actions in the PRA (either by direct modeling or by explaining the reasons for not modeling these actions). According to W, it is "standard PRA practice" to terminate an accident sequence (by calling it a "success") if a system, whose continuous operation alone prevents core damage indefinitely, is available for 24 hours. The staff believes that this is "standard PRA practice" only if it can be shown that the specific system is likely to be available indefinitely, subject to a constant failure rate.

   - Nonsafety-related systems required for normal plant operation **** It is reasonable to assume that nonsafety-related systems which must be operating during normal plant operation, such as AC power, are available (subject to a certain constant failure rate) following an accident initiating event (unless the initiating event causes them to fail).

     ****** It should be noted that (based on the staff's understanding of the design) if AC power is assumed unavailable following an accident initiated event, then automatic ADS actuation at about 24 hours will occur and should be modeled in the focused PRA ******

The staff believe that the above two areas have to be addressed by Westinghouse (as a minimum by assessing their impact on the focused PRA results and insights). This is necessary to provide a better understanding and interpretation of the focused PRA results and insights in the RTNSS context.

2. Event PRSOV (Pressurizer relief valves open and stuck open) is not modeled in the focused PRA event trees.

3. Page 52-3, third full paragraph. The following statement is made: "....conservative assumptions in the base case event tree models are further developed..." Need to list and explain all these cases.

4. Page 52-3, fourth third full paragraph. Explain what do you mean by "consequential events that are not dependent upon success of nonsafety-related systems." Some examples could help understand this paragraph.

5. Page 52-7. Define/explain event tree CNLOCA (consequential intermediate LOCA event tree). Same for CSLB-V (consequential secondary-side safety valve stuck open event tree). Why are these two event trees not included with the other focused PRA event trees?

6. Page 52-8. What is a "baseline consequential small LOCA model?"

7. Page 52-11, second paragraph. This is an example of inconsistent assumptions made in the focused PRA.

AGENDA ITEMS RELATED TO THE AP600 I&C PRA MODELS

1. Discuss changes in Chapters 26-28 of PRA and their impact on other parts of the PRA (e.g., spurious actuation of ADS)

2. Discuss the development of risk-based safety insights for the I&C systems

3. Discuss guidelines for improving I&C PRA modeling documentation

4. Discuss modeling of software/hardware common cause failures

5. Discuss potential areas were sensitivity analyses could help resolve I&C related open issues and draw safety insights

****

SPECIFIC DRAFT I&C QUESTIONS

1. The first part of "Common Cause Failures" on page 6 (W response to RAI 720.307, Letter NSD-NRC-96-4688, April 4, 1996) states that immediate detectability of failure is provided by the on-line diagnostics.
   QUESTION: Does some type of automatic action take place after a failure is detected, such as setting off an alarm and/or starting something, or is it just an indication on back of a cabinet?

2. Explain the statement at the bottom of page 8 (W response to RAI 720.307, Letter NSD-NRC-96-4688, April 4, 1996) that safe failure modes are also relevant to CMF defense. How are the I&C components designed to ensure that a failure leads to a "safe-actuation state"? Is this a digital hardware or software function? Please discuss any mechanisms which could affect this behavior and the likelihood of these mechanisms. Wouldn't this increase the likelihood of spurious actuations? In addition, how is a well defined output produced for software failures? Specifically, what would the result of a register overflow be?

3. Clarify the statement at the middle of page 11 (W response to RAI 720.307, Letter NSD-NRC-96-4688, April 4, 1996) that "quantitative analysis of the I&C CMF contributions produces results that are below the acceptable goal level, but not further below the acceptable level is a result of the conservative approach taken in the quantitative modeling of CMF." How was this done? Show data sources and bases.

4. Clarify statement at the top of page 13 (W response to RAI 720.307, Letter NSD-NRC-96-4688, April 4, 1996) that diversity in the sensor types used in different protective functions minimizes the effects of sensor CMFs. How are these sensor types different?

5. At the bottom of page 14 (W response to RAI 720.307, Letter NSD-NRC-96-4688, April 4, 1996) it is stated that detectable failures result in preferred default states for the system. Is this true for common cause failures that could freeze the system where no action can be established other than reboot? How will it fail if this happens?

6. The middle of page 15 (W response to RAI 720.307, Letter NSD-NRC-96-4688, April 4, 1996) states that the output boards of the ESF, PLS, and DAS systems are all diverse from each other and have no CMF potential between them. Does this include different types of electrolytic capacitors in power supply for boards? Is power supply qualified for adverse conditions?

7. One of the assumptions for the DAS (Chapter 27) is that it has no common cause failure with the protection and safety monitoring system or the plant control system. However, the AP600 SAR states on page 7.7-18 (Revision 5) that "Actuation interfaces are shared between the diverse actuation system and the protection and safety monitoring system." Why is this statement in the SAR if this is a true diverse system?

8. The "Rolls Royce Method" was used by Westinghouse to obtain beta factors for CCF values of I&C components. What specific sub-factors were considered in the calculation to determine the causes of system failure? For example: What assumptions were made regarding physical separation of the various cabinets or subcomponents within the cabinets? Are all components susceptible to CCF separated by metal barriers? Are the I&C components used AP600 design specific or are they industry standard? What environmental effects were considered in the analysis?

9. Was the loss of the HVAC system on I&C considered? Environmental effects such as increased humidity have a significant effect the operability of I&C components. Chapter 2 of the PRA (reference to the section concerning normal ventilation initiating events) states:

   "... there is no attempt to model the environmental control systems and their support dependencies in detail, since it would substantially increase the complexity of the system fault trees with only a marginal gain in the modeling accuracy."

   Due to the significant effects that temperature and humidity have on the operability of I&C components, please clarify the assumptions and justification that were used to screen out the loss of HVAC. Specifically, please explain how the AP600 I&C design compensates for high humidity in the event of a loss of the HVAC system.

   WCAP-13382 Revision 0 states that for a comparable I&C system, the "abnormal operating environment" should not exceed the limits of +40 degrees F to +120 degrees F and a relative humidity of 5 percent to 95 percent. The maximum time of operation at the "abnormal operating environment" is 12 hours. Are there plant safeguards that monitor

humidity in specific I&C cabinets and plant locations and alert plant personnel of the approach of abnormal operating conditions? What is the required response if the limits are exceeded?

10. Was miscalibration of electrical components such as sensors, analog input/output modules considered in the PRA analysis? Was miscalibration considered in CCF basic events? The basic event list was checked and was not found any reference to miscalibration. If miscalibration was considered, where in the PRA was it done and what assumptions were made?

11. W's response (to RAI related to DSER OI 19.1.3.1.15) regarding the calculation of software CCF probabilities, only partially addresses the question. Please explain the "model" (parameters, values of parameters, assumptions and bases) used to calculate software CCF probabilities and explain how does this comply with IEEE 7-4.3.2, 5.15 (reliability).

12. What is the reason for the significantly higher failure rate used for Analog Input Boards as compared to Analog Output Boards.

13. Westinghouse states on page 22 (response to RAI 720.307, Letter NSD-NRC-96-4688, April 4, 1996) that the modular basic event PMAMOD11 models all other random failures in subsystem 1 of the division A PLC including the data highway transceiver and controller, the bus, the bus monitor, internal power supply and cabinet fan. A failure rate used in the PRA is 2.09E-3. However, information regarding the subcomponents of other modular basic events was not given. Additional explanation is needed to understand the basis for the failure rate assignment.

14. The estimated failures rates for "modular" basic events differ depending on what components are included in the module and the type of cabinet they are located in. For example, the basic event PMAMOD41 (used in the multiplexer cabinet) has a failure probability value of 6.35E-4 which is less than the 2.09E-3 used for PMAMOD11. What is the reason for this difference in failure rate probabilities between the two modular basic events? Because both are part of a digital cabinet subsystem, it can be assumed that each would have common components such as a power supply, controller and fan. These components alone usually put the failure rate in the range of 10-3. What design assumptions make the various modulars different from each other? Westinghouse should provide a basic breakdown of common electrical components used in the modular basic events.

    Also, it is stated that "... the contribution for failure of the cabinet fan has been included in the modeling of each cabinet subsystem." Is failure of the cabinet fan considered in all modules? For example do P##MOD1#, PL#MOD5#, etc. all include cabinet fan failure?

15. Page 3-7 (PRA), third paragraph. Clarify statement on ADS stage 4 spurious actuation. It is stated that there are two "redundant" controllers for each squib valve and <u>both</u> have to actuate to cause detonation. With respect to what function are they redundant? Explain the reason(s)

the frequency of spurious actuation (by PMS or DAS) of two stage #4 ADS paths (which contributes to a large LOCA) is much higher than the frequency of spurious actuation of only one ADS path, including one stage #4 path, which contributes to a medium or intermedium LOCA.

16. Pages 3-14 to 3-19, Table 3-3 (PRA). Reference is made to Chapter 26 (I&C PRA models) regarding frequencies of spurious ADS actuation and opening of paths that lead to various LOCA sizes. The staff were unable to find this information in Chapter 26 (note: this is the subject of a DSER open item and follow-up RAIs). **** A general approach (described in Chapter 26, pages 26-22 to 26-24) for spurious opening of ADS paths that lead to large LOCA, does not provide adequate information. This approach needs to be implemented to the specific cases of spurious opening of ADS paths that lead to the various LOCA sizes (all steps, including assumptions, must be clearly documented).

THE AP600 INTERNAL FIRE ANALYSIS

- Introduction
- Methodology Overview

INTRODUCTION

O Objectives Of Fire PSA

- To estimate the contribution of accident sequences induced by in plant fires to the overall plant core damage frequency

- To identify any potential fire vulnerabilities

- To provide recommendations for rectifying the identified fire vulnerabilities

O Basic Approach

- Performing a qualitative assessment of the internal fires impact on systems required for normal and safe shutdown of the plant

- Quantifying the risk posed by the postulated impact in terms of core damage frequency

- Analyzing the results for sensibility and gaining insights

QUALITATIVE ANALYSIS TASK

O Overall Approach

- Identification of plant fire areas

- Identification of the location of equipment which, if damaged by fire, would cause a plant shut down and degradation of shut down paths are identified.

- Systematically screening out risk insignificant fire areas based on the above information

QUALITATIVE ANALYSIS TASK (CONT.)

O Major Steps Of Qualitative Analysis Task

- Step 1: Plant was divided into independent fire areas corrosponding to those outlined in the AP600 SSAR.

- Step 2: A list of safety and non-safety-related systems required to bring the plant to safe shutdown was developed.

- Step 3: Safety-related and non-safety-related shutdown equipment which would be affected by a fire in each fire area/compartment was identified.

QUALITATIVE ANALYSIS TASK (CONT.)

- Step 4: Using the information obtained in Step 3, a summary of the shutdown systems disabled or degraded in each fire area was developed.

- Step 5: To the extent possible, all inter-fire area boundaries were identified. The objective of this task is to identify the risk from fire spread across fire area boundaries.

- Step 6: Analysis of fire area vs. plant trip/safe shutdown equipment damage was performed.

  * For fire areas with no credible fire propagation mechanism, the analysis was performed assuming that all equipment and cables in the exposign fire area were damaged.

  * For fire areas where fire propagation from them was determined to be possible, the analysis was performed assuming that all equipment and cables in both the exposing and the exposed fire areas were damaged.

QUALITATIVE ANALYSIS TASK (CONT.)

- Step 7: A fire area was screened out from further analysis based on the following criteria:

  * If the fire was not expected to create a demand for safe shutdown under normal plant operating conditions, and if none of the PRA-credited equipment were considered damaged.

  * If the fire was expected to cause a plant shutdown due to technical specification requirements but was not postulated to impact operability of any PRA-credited shutdown systems.

- Step 8: For those areas that did not screen out, a qualitative assessment of the consequences of the fire was performed. As a part of this qualitative evaluation, the consequences of different fire-induced cable failure modes (open or short) were considered.

QUANTITATIVE ANALYSIS TASK

O Overall Approach

- For each fire area surviving the qualitative screening, core damage frequency due to fire damage, coincident with fire unrelated unavailability of redundant/alternate safe shut down equipment was evaluated.

- CDF was evaluated based on the assumption that all fires damaged all potential targets in one step.

- Areas with a fire-induced core damage frequency of less than 1.0E-9 per year were screened out.

QUANTITATIVE ANALYSIS TASK (Cont.)

O Major Steps For Stage 1 Of Quantitative Analysis Task

- Step 1: The fire initiation frequency for each fire area was estimated based on the type and quantity of equipment located in a location, together with actual nuclear power plant fire incidents.

- Step 2: Based on the information collected during the qualitative analysis, the potential for fires to cause a particular type of initiating event, together with potential damage to the PSA-credited safe shutdown systems were identified.

- Step 3: Having determined the fire induced initiating event types and the safe shutdown equipment damage in each area, a set of unique fire damage categories were designated.

- Step 4: The conditional probability of core damage for each designated damage category was then evaluated by using the Focused PRA model.

- Step 5: The contribution of in plant fires to core damage frequency was calculated by suming up the contribution from each plant fire area.

QUANTITATIVE ANALYSIS TASK (CONT.)

o IMPORTANT SUBSTEPS

- Fire Propagation Probability- Probability of fire propagation was calculated based on the failure probability of the fire barrier and fire suppression system in the exposing fire area. Note that:

  * Fire suppression was not credited to limit fire damage within an area

  * Manual fire suppression, in either the exposing fire area or the exposed fire area were not credited to prevent fire propagation.

  * Automatic fire suppression system in the exposed fire area was not credited to prevent fire propagation to the area.

QUANTITATIVE ANALYSIS TASK (CONT.)

- Fire-Induced Suprious Actuation Probability- Probability of a specific fire-induced fault occurring was calculated based on the nature of the fault.

  * Based on NUREG/CR-2258 evaluation, the best estimate conditional probability of a hot short event was estimated as 0.06. Note that for large LOCA at least two hot shorts are required. Thus, the conditional probability of a fire-induced large LOCA was estimated to be 3.6E-3.