Westinghouse Electric Corporation Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

NSD-NRC-96-4904
DCP/NRC0674
Docket No.: STN-52-003

December 9, 1996

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

ATTENTION: T. R. QUAY

SUBJECT: AP600 RESPONSE TO REQUESTS FOR ADDITIONAL INFORMATION, AND AP600 PRA PAGE MARKUPS

Dear Mr. Quay:

Enclosure 1 provides Westinghouse responses to NRC requests for additional information pertaining to the conditional containment failure probability distribution used in Chapter 42 of the AP600 Probabilistic Risk Assessment (PRA). Specifically, the responses to the following RAIs are included: 480.190 through 480.192, 220.95 through 220.99. These responses close, from a Westinghouse perspective, the addressed questions. The NRC technical staff should review these responses. The status of these RAIs will be changed to "Action N" in the OITS on January 2, 1997.

Enclosure 2 provides the draft responses to NRC requests for additional information pertaining to the AP600 at-power fire PRA. These responses are being provided to the NRC for discussion purposes at the December 18, 1996 NRC and Westinghouse AP600 fire PRA meeting. The staff is expected to review these draft responses and be prepared to discuss them at the meeting.

Enclosure 3 contains markup page changes to the AP600 PRA. These markups primarily fix typos found in the report since the issuance of Revision 8. These changes will be included in the next revision to the PRA. The staff reviewers should include these markup pages with their PRA report.

A listing of the NRC requests for additional information responded to in this letter is contained in Attachment A.

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

1/1
E004

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 enclosures)

Enclosure 1 to Westinghouse
Letter NSD-NRC-96-4904

December 9, 1996

Question: 220.95

In PRA Chapter 42, dated December 1, 1995, a coefficient of variance (COV) of 0.06 for random material uncertainty for SA537, Class 2 is used. This does not seem to be appropriate. The staff could not find where your Reference 42-2 recommends a COV between 0.06 and 0.08 for random material uncertainty. On page 77 in Reference 42-2, the material yield strength mean and standard deviation were taken as 1.1 and 0.11 times the specified σ_y for the uncertainty analysis of the five containments.

Based on "Development of a Probability Based Load Criterion for American National Standard A58," National Bureau of Standards Special Publication 577, US Government Printing Office, Washington, 1980, the use of 1.1 and 0.11 for the median and the COV, respectively, for material property is more appropriate. Figure 1 shows the probability of failure differences between the random material uncertainty COVs of 0.06 and 0.11.

Response:

As discussed in Revision 8 of Chapter 42, a coefficient of variation (COV) equal to 0.11 is used to represent the random uncertainty in material properties for all failure locations. This is based on the reference provided in RAI 220.95 ("Development of a Probability Based Load Criterion for American National Standard A58" and "Reliability of Containment Under Overpressure").

PRA Revision: None

Question: 220.96

In PRA Subsection 42.4.1, a COV of 0.1 for modeling error for containment cylindrical shell is used. This does not seem to be appropriate. The COV of 0.1 seems to come from the average of 0.12 (limit pressure calculations) and 0.08 (axisymmetric finite element analysis) in Reference 42-1. However, the COV of 0.08 is not directly applicable to AP600 since Reference 42-1 uses ANSYS with STIF 82 elements for six closed-end smooth cylinders which are different from that of the AP600. The COV of 0.12 is obtained after calibrating with respect to the finite element method in Reference 42-1. In this calibration, Reference 42-1 treats the von Mises yield criterion as a constant (15 percent increase). The use of COV of 0.12 for the constant von Mises yield criterion is acceptable. However, based on test data, the von Mises yield criterion should be treated as a random variable. For the complete modeling error COV determination, provide the median and its COV values with the legitimate distribution information for the von Mises yield criterion.

Response:

As discussed in Revision 8 of Chapter 42, a coefficient of variation (COV) equal to 0.12 is used to represent the subjective uncertainty associated with modelling of the ultimate containment failure pressure for all failure locations. This is based on the Greiman reference "Reliability of Steel Containment Strength."

PRA Revision: None

Question: 220.97

In letter NTD-NRC-96-4617, dated January 4, 1996, the response to RAI 2 (NRC letter dated September 14, 1995) stated that "Distribution is primarily influenced by imperfection. Measured imperfection must be less than the American Society of Mechanical Engineers (ASME) specified limit. Use of lognormal distribution is appropriate, similar to its use for material yield which must also exceed a minimum ASME specification." Is the lognormal distribution applicable here if it exceeds the ASME minimum specifications? The distribution should come from the existing test data and not be assumed. Clarify these statements.

Response:

The equipment hatch cover will be constructed within the ASME forming tolerance requirements for vessel shells as defined in Subsection NE (NE-4220). Buckling is significantly influenced by imperfection. The maximum imperfection defined by the ASME Code will determine code buckling capacity. The imperfections in the as-built conditions will be equal to or smaller than the ASME specified values, and therefore, the as-built buckling capacity will be higher.

No as-built measurements of the AP600 containment vessel are available. There is not that much existing test data (see RAI 230.32) in the public domain that can be used to make meaningful conclusions with respect to statistical distributions for the AP600 containment. This has been noted by L. Greimann and F. Fanous in Reference 220.97-1:

They state:

p. 839 "Again, as-built geometry of the containment would be very useful. Unfortunately, no as-built measurements of containment vessels exist. However, fabrication and erection tolerances were established and (presumably) met during the construction process."

p. 847 "Uncertainty in structural analysis ... is very difficult to quantify. A usual procedure is to describe statistically the ratio of experimental results to analytical results. Hence, if there are a number of experimental results, one can approximate the distribution of this ratio. Most typically, however, enough tests are not available to give sufficient statistical confidence. ... ."

The use of a lognormal distribution to represent uncertainty is, and has been, the accepted practice in structural analysis as well as risk analysis for a number of years. Many papers have been published on this subject, indicating the general acceptability of the lognormal distribution for the purposes used in the AP600 containment analyses. Two notable papers are References 220.97-1 and 220.97-2.

Both of these documents describe the use of the lognormal distribution for probabilistic and reliability analyses of steel containments. In NUREG/CR-3127 (Table 2.1) imperfection parameters are defined as lognormally distributed, and in the paper (Tables 6 and 7) and NUREG (Table 2.1) the analysis error is stated to be lognormally distributed.

Another consideration is the potential differences in the results if a different distribution was used. Although it is possible to show different results for any (less than infinite) data set through the use of a particular distribution,

assuming a reasonable choice of shaping parameters used with a distribution other than a lognormal one, the resulting failure probability is still expected to be very small.

It is important to note that the controlling failure mode is not buckling, but membrane yield of the cylindrical shell. In Chapter 42, results of the conditional containment failure probability distributions have been presented. In Tables 42-3 and 42-4, and Figures 42-1 and 42-2, it is seen that the cumulative containment failure probability is similar to that associated with cylinder yield. Therefore, cylinder yield is the dominant contributor to containment failure, and buckling does not control containment failure probability.

From the above discussion it can be concluded that a lognormal distribution is recommended in the literature for imperfections. Further, buckling does not control the cumulative failure probability, and the distribution used has little effect on containment failure probability.

References:

220.97-1 "Reliability of Containments Under Overpressure," L. Greimann and F. Fanous, Pressure Vessel and Piping Technology, A Decade of Progress, Paper 8.7, 1985, pp. 835-856.

220.97-2 NUREG/CR-3127, "Probabilistic Seismic Resistance of Steel Containments" prepared by L. Greimann, F. Fanous, et al, Ames Laboratory, January 1984.

PRA Revision: None

Question: 220.98

In PRA subsection 42.4.3, a COV of 0.14 is used for equipment hatch modeling error. However, this modeling error calculation in Reference 42-2 is based on internal pressure cases. Provide the justification that this COV can be used for the external pressure case.

Response:

The purpose of the PRA Chapter 42 analysis is to evaluate overpressure containment fragility for use in the AP600 PRA. A COV of 0.12 was used for internal limit pressure, which is consistent with analysis errors per Reference 220.98-1. External pressure does not apply for this evaluation.

Reference:

220.98-1 "Reliability of Containments Under Overpressure," L. Greimann and F. Fanous, Pressure Vessel and Piping Technology, A Decade of Progress, Paper 8.7, pp. 835-856.

PRA Revision: None

Question: 220.99

In PRA Section 42.1, it is stated that "Failures of the mechanical penetration bellows, and leakage of the equipment hatches due to ovalization, do not occur prior to general yielding of the cylinder." This implies that after the yield pressure is reached, the bellows will fail and the equipment hatches start to leak without restriction. Therefore, the probability of failure for bellows and leakage through equipment hatches due to ovalization beyond yield pressure should be given in PRA.

Response:

It is true as stated in the RAI that for the conditional containment failure probability analyses performed, it is assumed that once general yielding of the cylinder occurs, the bellows may fail and the equipment hatches may start to leak. However, it is not necessary to provide the probability of failure for bellows and leakage through equipment hatches due to ovalization since the sum of the probabilities of these specific mechanisms plus others that might occur, such as failure of other penetrations, is equal to or smaller than that given for the general yielding of the cylinder in the analyses performed.

PRA Revision: None

AP600

Question: 480.190 Containment Pressure Capacity

Describe how the impact of corrosion of the containment shell is accounted for in estimating the containment ultimate pressure capacity.

Response:

Corrosion protection of the containment vessel is described in SSAR subsection 3.8.2.6 and 6.1.2. Performance monitoring of the coating is described in subsection 6.1.2. This monitoring is intended to preclude significant corrosion of the containment vessel. Therefore, the impact of corrosion is not accounted for in estimating the ultimate capacity.

PRA Revision: None.

Question: 480.191 Containment Pressure Capacity

Provide an assessment of the pressure capability of the main steam line and main feedline bellows, and a corresponding failure probability distribution curve.

Response:

The pressure capability of the main steam line and main feedline bellows are discussed in SSAR subsection 3.8.2.4.5. The pressure capability exceeds the pressure at which the containment vessel cylinder yields. It is assumed that once general yielding of the cylinder occurs, the bellows may fail due to the large deflection of the cylinder. However, it is not necessary to provide the probability of failure for bellows separate from the probability of cylinder yield. The probability of failure of the bellows due to large deformation of the cylinder is a part of the probability given in PRA Chapter 42 for vessel failure due to the general yielding of the cylinder.

PRA Revision: None.

Question: 480.192 Containment Pressure Capacity

Provide further information regarding the ability of containment piping penetrations to accommodate the lateral motion of the containment shell anticipated in late over-pressure failures. For key penetrations, including the main steam and feedwater lines, provide an estimate of the extent to which the bellows would be compressed at containment pressures corresponding to (a) Service Level C and (b) the ultimate pressure capacity. This can be presented in terms of the percent of full compression, as described in NUREG/CR-6154.

Response:

The radial deflection of the containment vessel at 144 psig is 1.6 inches as given in SSAR subsection 3.8.2.4.2.1. This pressure is greater than the pressure corresponding to Service Level C and is well within the capability of the bellows. The bellows are expected to be fully compressed at the ultimate pressure capacity since the ultimate capacity is defined as the pressure at which there is gross yield of the cylinder.

PRA Revision: None.

Enclosure 2 to Westinghouse
Letter NSD-NRC-96-4904

December 9, 1996

Question: 720.334

The information documented in the submittal (Chapter 57, August 9, 1996, Internal Fire Analysis Draft Markup) does not state clearly the major assumptions made in modeling containment fires. The containment is a single fire area which is made up of several compartments, called fire "zones" (see Table 57-5). It appears that the several fire zones, included in the single containment fire area, are treated in the analysis similarly to the fire areas for fires outside the containment. However, it is not clear whether and how fire propagation between fire zones is modeled and what is the technical basis for distinguishing the different fire scenarios. Please provide this information, including relevant assumptions, in Chapter 57 of the PRA.

Response:

In the AP600 internal fire analysis, fire propagation across containment fire zone boundary has been judged not to be credible. Fire scenarios have been developed only based on the potential impact on safe shutdown function that could be caused by damaging components and cabling located in the fire exposing zone. The technical justification for this judgement is provided below.

In the AP600 internal fire analysis (consistent with the state-of-the-art methodology), fire propagation across a barrier has been judged not to be credible if the deterministic fire protection assessment had credited the barrier as being capable of preventing fire propagation, unless:

i. the barrier's integrity had been compromised by a barrier element failure (e.g. penetration seal failure)

AND

ii. if the fire suppression activities in the exposing location were to fail to contain the fire within the area.

For example, fire propagation across a fire area boundary which consists of a solid wall without any sealed openings (doors, vent louvers, cable penetrations, etc.) has been judged not to be credible, where as fire propagation across a barrier with any sealed openings has been considered to be credible and the barrier failure probability has been assessed based on the type of barrier elements.

As stated in the RAI, the containment fire area is a single fire area which is divided into several fire zones. Based on the AP600 SSAR's Appendix 9A, fire zones are physically separated from other fire zones such that fire propagation across a fire zone boundary can be dismissed. None of the containment inter-zone barriers are designed to contain sealed openings (e.g. doors or penetration seals). Therefore, fire propagation is not credible and no probabilistic treatment is needed.

It is worthwhile to repeat that in the current fire PRAs, including those performed using the EPRI FIVE methodology, generally the containment building is excluded from the analysis (i.e., it is screened out at the qualitative level). The basis for this exclusion includes the following justifications which are presented in the FIVE methodology:

- the unlikelihood of a hot gas layer forming in areas that would damage cabling;
- industry-wide improvements in RCP oil collection system design improvements, which has essentially eliminated this primary cause of past containment fires;
- a low frequency of containment fires in operating plant experience.

That is, it is generally accepted that containment fires do not pose a significant safety threat due to the lack of fire ignition sources in the area in combination with the limited amount of combustible materials in the containment and significant space available for spread of the energy which would be generated by a fire. These justifications are applicable to the AP600 design. Therefore, it is judged that there are no significant fire propagation mechanisms in the AP600 containment design (e.g., features that would allow formation of a hot gas layer) that would facilitate fire spread across a containment fire zone boundary.

Additionally, from the overall risk point of view, the AP600 design has an additional level of defense (i.e. nonsafety-related equipment) which are mainly located outside the containment and would be free of damage from fires in the containment.

Question: 720.335

One item of concern in the certification of advanced reactor designs is the impact of smoke, hot gases, and fire suppressants on safe shutdown equipment (especially due to sensitive electronics) and on operator actions. The issue is amplified when these elements migrate into other fire areas. Please address this issue in the internal fire PRA.

Response:

The impact of hot gases, fire suppression, and smoke has been addressed in the AP600 internal fire analysis either implicitly or explicitly as follows:

Impact on equipment

In all plant locations other than the control room, the components (of all types) and cabling located in an area where the fire originates or to which it propagates have been assumed lost independent of the hazard (i.e. independent of smoke, formation of hot gas layer, fire suppression activities, etc.). Note that, consistent with BTP CMEB 9.5-1 and NFPA recommendations, the AP600 ventilation systems are designed to confine smoke, hot gases, and fire suppressants within the fire area of fire origin.

In the control room, based on the available data and the fact the control room would be continuously occupied, it has been judged that the impact of fire-generated or fire-induced hazards (i.e. smoke/heat or water) would be limited if the fire did not, or was not allowed, to fully develop. For fully developed fires, all the equipment in the control room have been assumed lost (due to heat or smoke-induced damage) and no operator action from the control room has been credited. Additionally, in all fire areas, the impact of fire-induced spurious actuation (such as those that can be caused by smoke/soot or cable hot short) have been explicitly modeled.

Impact on Operators

In the AP600 internal fire analysis, other than in the control room, no local manual action has been credited. Therefore, the impact of fire-generated or fire-induced hazards on the local operator action did not need to be addressed. For the control room, the level of smoke which would impair the effectiveness of the operators and the time available to suppress the fire before the smoke concentration reaches the level of visual Impairment have been evaluated based on available experimental data, the AP600-design specific control room features and assessments made in other fire PRAs. Since only very localized/small fires have been assessed to have limited impact (i.e. large fires have been assumed to disable all the equipment) and the damage caused by such fires, based on available data, were assessed to be limited, it was judged that fire suppression activities related to such small fires would not significantly impede or adversely affect operators actions.

Question: 720.336

Burning liquids in the AP600 turbine building could fall on the floor at elevation 100 feet. It is not clear where they would go. Is it possible that the oil could enter the Auxiliary Building? Experience (the Vandellos turbine building fire) has shown that burning oil can spread away from the point of origin. Is it possible that an important scenario, which involves damage to other fire areas within the Auxiliary Building, was not analyzed because of the analysis groundrule preventing treatment of scenarios involving fire spread to multiple zones? Please explain and identify the specific design features that prevent this from happening.

Response:

In general terms, in the AP600 internal fire analysis, the ground rules followed in assessing the impact of fire propagation included the following:

a. Fires originating in a fire area (exposing fire area) could only propagate to an adjacent fire area (exposed fire area), and no further propagation beyond the exposed fire area was considered to be credible.

b. Simultaneous fire propagation from the exposing fire area to more than one adjacent fire area was not considered credible.

That is, fire propagation to more than one fire area was considered but sequential fire propagation (from a fire area to an unconnected fire area via an intermediatory fire area) or simultaneous fire propagation to more than one fire area were judged not to be credible.

Specifically, fire propagation from the AP600 turbine building to the auxiliary building has been considered credible where a mechanism to allow for fire propagation (e.g. a door) had been identified. More specifically, fire propagation from the AP600 turbine building (including oil-fueled fires) to fire area 1201 AF 04 located in the auxiliary building was considered to be credible and its consequences has been analyzed in the internal fire analysis.

Question: 720.337

Westinghouse claims that a conservative "bounding" assessment of the impact of fire-induced "hot shorts" was performed. The staff, however, cannot conclude that Westinghouse's analysis is bounding (based on the information provided in the submittal) because (a) the probability of a hot short (from NUREG/CR-2258) is based on judgment, (b) it is assumed that the probability of multiple hot short events is state-of-knowledge independent, and (c) the analysis does not refer to the specific AP600 PRA I&C models and logic diagrams to recognize any important features, and/or operational requirements, that are incorporated into the design to prevent fire-induced hot shorts from causing spurious actuations which in turn could have a significant impact on plant safety. Please explain the mechanism of fire-induced spurious actuations using the AP600 PRA I&C models, the location of the various I&C cabinets, the location of power source interfaces and assumptions made on cable characteristics and routing. Also, please list important design features, and/or operational requirements, that prevent fire-induced hot shorts from causing spurious actuations.

Response:

The AP600 internal fire analysis considers the effects of fire-related damage to safety equipment and associated instrumentation, control, and power cabling. Both open shorts and hot shorts in I&C and power circuits are considered. With respect to hot shorts, the internal fire analysis explicitly considers hot short-induced actuation of ADS valves, resulting in loss of coolant, for both at-power and shutdown conditions. Other potential hot short equipment actuations result in either less adverse events or in favorable conditions, such as have been documented elsewhere (Ref. 720.337-1). Potential fire-induced hot-short actuation of the automatic depressurization system (ADS) is the only fire-induced fault with potential to adversely affect the ability of the plant to achieve safe shutdown, and is treated in a limiting manner in the internal fire analysis, as described below.

The AP600 design is not susceptible to single hot short actuations of lines of ADS stages 1 through 3. Each such line has two normally-closed valves in series, and separate actuations are required for each valve in stages 1 through 3. The cabinets providing the actuation signal will have temperature monitoring and protection, in addition to software for detection of anomalous signals, to eliminate any significant probability of a single common fire-induced fault resulting in generation of a stage 1 ADS actuation signal.

Therefore, the fire analysis assumed that opening of ADS stages 1 through 3 requires multiple hot shorts for each ADS line. It has been assumed that these could occur in either the PMS or DAS actuation circuits. However, opening of the stages 1 through 3 valves was not explicitly considered in the fire analysis, because: ADS stage 4 actuations were modeled as resulting from single hot shorts (see below); opening of a single stage 4 valve produces a plant transient equivalent to a medium LOCA; and the focused PRA conditional core damage probability (CCDP) for medium LOCA is significantly higher than the CCDP for smaller LOCAs, such as would result from multiple hot-short-induced opening of both stage 1, 2, or 3 ADS valves in a given line. Multiple hot-short-induced ADS valve openings were modeled as large LOCAs.

Each of the four lines of ADS stage 4 has one normally open MOV and one squib valve, with each squib valve receiving actuation signals from two divisions, either of which can actuate the valve. Therefore, a single hot short somewhere between a final output cabinet and a squib valve could be postulated to result in valve actuation. Each output cabinet is protected as described above, such that a common single spurious signal to actuate both stage 4 valves powered by any particular division is unlikely. In addition, the actuation of each ADS stage 4 valve has two series control circuits in each division. This further reduces the chance that a fire in a cabinet could cause a spurious actuation.

It was assumed that there would be a "hot" power source of sufficient capacity to actuate the ADS valves. Squib valve actuation requires relatively high current, i.e., greater than expected to be available from most hot short sources, so that, depending on the power and control circuitry used, it might not be possible to achieve a hot short that would result in valve actuation. The possibility of hot shorts might also be negated by the type of cabling used. However, since these design details of the ADS actuation cabling are not final, it was assumed that hot short ADS stage 4 valve actuation could occur.

The fire analysis assumed that there could be a single hot short in either the PMS or the DAS actuation circuits that could result in opening of a single line of ADS stage 4 (i.e., a medium LOCA), and also that there could be multiple hot shorts that could result in opening of more than one line of ADS stage 4 (i.e., a large LOCA).

Reference:

720.337-1 WCAP-14477, "The AP600 Adverse System Interactions Evaluation Report."

Question: 720.338

Successful injection of core makeup tanks (CMTs) requires trip of all reactor coolant pumps (RCPs). Please address in your analysis the impact of an inadvertent RCP start (after initial trip) and whether this can occur in the same scenario with other fire-induced failures of safety equipment, such as spurious actuation of ADS valves, and/or with fire-induced control room indications.

Response:

The internal fire analysis models a fire in any fire area as resulting in failure of all equipment in that area. Thus, a fire in an area containing CMT valves or actuation circuitry was assumed to cause failure of the associated CMT train, so that potential RCP restart (or failure to trip) has no further adverse effect.

Restarting of the RCPs would require a hot-short actuation of the RCP start logic. The control wiring used to control the RCPs runs from the Protection Logic Cabinets located in the I&C Equipment Rooms to the Class 1E Feeder Breakers which power the Motor Control Centers for the RCPs. Each RCP has two 1E feeder breakers associated with it. One of the circuit breakers is controlled by PMS division B while the second breaker is controlled by PMS division C. Therefore, restart of an RCP would require a hot short on each of two PMS divisions for which, in general, the wiring is routed through separate fire zones.

The RCP trip signal, once generated, is "sealed in" such that subsequent loss of either the CMT actuation or the RCP trip signal source does not result in restarting of the RCPs. Restart of the RCP through the manual actuation circuits requires that the "seal-in" in each of the two divisions be cleared. Since the "seal-in" is done on a divisional basis, there is no single point in which the "seal-in" for each of the two divisions can be cleared. In addition, restart of the pumps requires that the soft control template be requested by the operators, that the control action be selected, and that the control action then be confirmed. There is no significant possibility that a fire can cause these specific actions to occur.

The PRA analyses assume that successful injection of core makeup tanks (CMTs) requires trip of all reactor coolant pumps (RCPs) except for events which cause a rapid depressurization of the RCS, such as medium and large LOCAs. For such breaks, tripping of the RCPs is not necessary for CMT injection. Since the fire analysis results are dominated by medium and large LOCA scenarios, spurious/inadvertent RCP restart, if this were possible, would not have a significant effect on the core damage frequency results.

Any potential impact of RCP restart (i.e., an assumed inability for CMT injection) would be for slower events, such as small LOCAs and transients with loss of decay heat removal. No fire-initiated small LOCA scenarios were identified in the internal fire analysis (spurious ADS valve actuations result in either medium or large LOCA as a result of the valve sizes), but it has been assumed that transients could result. In the focused PRA, for RCP trip to be of concern in transient scenarios, it is necessary that failure of passive residual heat removal (PRHR) first occur, resulting in a need for depressurization and CMT injection. (In the PRA, it would also first be necessary that main and startup feedwater also fail.) Logic train separation would preclude defeating PRHR actuation via a single fire for all but the final actuation cabling. Fire-induced failure of PRHR as a result of a fire affecting the final actuation cabling would require a hot short to prevent actuation, since this system actuates on loss of support or control. Subsequent inadvertent RCP restart would require additional fire-induced hot shorts to reclose the RCP breakers (see discussion above). In addition, for transients that progress relatively slowly, there would likely be sufficient time for operator response to recognize the inadvertent RCP restart and manually stop the pumps. This scenario is judged to be sufficiently unlikely that it need not be explicitly considered in the quantification. It would not contribute significantly to the fire core damage frequency results.

For these reasons, the contribution to core damage due to fire-induced RCP restart is judged to be sufficiently small that explicit modeling is not necessary.

Question: 720.339

Fire-induced failure of containment isolation valves was not treated in the analysis. It was assumed that such failure has no effect on core damage frequency (see item h, page 57-15) because "the PRA core damage success criteria are specified assuming failure of containment isolation." However, based on information presented in Appendix A of the AP600 PRA, it does not appear that containment isolation failure was assumed in determining success criteria for sump recirculation. Furthermore, the frequency of a core damage scenario with containment isolation failure should be investigated to determine its contribution to offsite consequences. Please explain.

Response:

The AP600 PRA success criteria for sump recirculation do not specify a requirement for containment isolation. There is a set of large LOCA break sizes identified for which containment isolation is required in order to avoid the need for ADS actuation in order to achieve IRWST injection. However, the large LOCA of concern for the internal fire analysis is fire-induced opening of the ADS valves. The success criteria for the internal fire analysis are the same as for the rest of the PRA regarding status of containment isolation.

More importantly, the AP600 is designed such that redundant safe shutdown components (i.e., redundant containment isolation valves in a given line) are located in separate fire areas or zones and served by different electrical divisions. Thus, the possibility of a fire that would cause failure of both isolation components in lines penetrating containment is judged to be sufficiently small that there would be no significant contribution to plant risk.

Question: 720.340

The barrier failure probabilities used in the analysis (see Table 57-3) assume certain inspection program for the barriers, which includes a sampling scheme and timing. Please include this information in Chapter 57 (internal fires) of the AP600 PRA.

Response:

The failure probabilities for fire barriers and fire barrier penetration seals, including electrical and mechanical seals, fire doors, and fire dampers are dependent on installation and maintenance practices followed for such equipment. The barrier failure probabilities used in the analysis are based on industry data that reflect current standard industry practices and requirements for such installation and maintenance. It has been assumed in the analysis that the AP600 will be subject to requirements and practices similar in effectiveness to those used in existing plants.

Question: 720.341

The first paragraph of Section 57.2 implies that probabilistic criteria allow screening of compartments with high fuel loading which do not contain PRA-credited equipment, regardless of propagation potential. However, the analysis does consider rooms where the only concern appears to be fire spread (e.g., the lube oil room in the turbine building). Is the statement in Section 57.2 correct? Please explain.

Response:

The statement presented in the first paragraph of section 57.2 does not accurately represent the methodology followed in the analysis. As stated on page 57-4 of the submittal, a fire area was not screened out from further analysis if a fire originating in the area created a demand for safe shutdown under normal plant operating conditions or was assessed to damage any PRA-credited equipment. The postulated consequences could occur either as a result of damage to the equipment located in the area or due to damage caused by propagation to another area. The report text will be revised to reflect this clarification.

Question: 720.342

The basis for defining the fire scenarios in Table 57-4 is not always clear, given the groundrules established in qualitative analysis Step 10. For example, what is the basis for distinguishing between scenarios 1 and 2 for Fire Area 1200 AF 01? Both do not seem to involve spurious signals. Does one involve propagation out of the area? Scenarios involving propagation out of the fire area should indicate explicitly which adjacent fire area is being treated (especially since the second bullet on page 57-4 states that simultaneous propagation to multiple areas is not treated). Please explain.

Response:

In general, in the AP600 internal fire analysis, four scenarios were considered for each fire area: two dealing with the consequences of fires which would be confined in the area, and two considering the consequences of fires propagating outside the area (if propagation had been found to be credible). In each set of propagating and non-propagating scenarios, in turn, the potential consequences of different cable failure modes (open and short) were evaluated. In summary, for each fire area the following scenarios were considered:

- Scenario 1 - Fire is confined in the area and disables all the equipment located in the area (i.e. only open circuit failure modes were considered).

- Scenario 2 - Fire is confined in the area, disables all the equipment in the area and causes safety significant hot short events.

- Scenario 3 - Fire propagates outside the area (if propagation was found to be credible) and disables all the equipment in the exposing and the exposed fire areas.

- Scenario 4 - Fire propagates outside the area, disables all the equipment in the exposing and the exposed fire areas, and causes safety significant hot short events.

Based on the equipment located in each area and the fire propagation potential, one or more of the above scenarios were dismissed from further considerations. For example, for fire area 1200 AF 01, only the first, third, and fourth above listed scenarios were considered to merit further analysis. That is, based on the equipment and cabling located in the area, a fire-induced hot short in the area was not considered to be safety significant. Additionally, fire propagation was considered to all fire areas with interconnecting pathway to the 1200 AF 01 fire area. However, only the consequences of fires propagating to an area with the potential to cause the most severe damage were found to merit further consideration. These consequences are represented by fire damage states 1AB2 and 1AB3.

Question: 720.343

Note 2 in Table 57-8 indicates that some components modeled in the focused PRA are failed for some initiators. Does this refer to the damage listed in the 4th column of the table, or are there additional component losses not explicitly identified? Please explain.

Response:

Note 2 in Table 57-8 was intended to be an explanation of the notation "(degraded)" that is used in column 3 of that table. The "degraded" notation was added as an indicator for the analysts that the focused PRA models listed (which already include no credit for nonsafety-related equipment) were to be further modified to remove credit for safety-related equipment listed in column 4 of the table. There may be several entries in column 3 for which the degraded label is missing, but the appropriate equipment losses appear in column 4 and were included in the modeling.

There are no additional component losses not listed in column 4 for scenarios involving safety-related equipment. However, for some of the scenarios resulting in transients, there is no entry in column 4, since these were all modeled using the focused PRA models, which take no nonsafety-related equipment credit.

Question: 720.344

Does the Remote Shutdown Workstation (RSW) panel have identical controls and displays of plant status information needed during accidents as the Main Control Room (MCR) panels? If the answer is no, please list the major differences and explain how they affect safety system redundancy and reliability, including operator actions.

Response:

As noted in AP600 SSAR Section 7.4.3, the remote shutdown workstation equipment is similar to the operator workstations in the main control room, and is designed to the same standards. The RSW contains controls and monitoring for the safety-related equipment required to establish and maintain safe shutdown conditions. There are no differences between the MCR and RSW controls and monitoring that would be expected to affect safety system redundancy and reliability. All important MCR operator actions credited in the PRA that might be required following a MCR fire (e.g., actuation of PRHR, CMTs, ADS, IRWST gravity injection, containment recirculation) can be accomplished from the RSW. However, as noted in the response to RAI 720.345, the MCR fire scenario quantifications include cases with no credit for any operator actions, in order to demonstrate that the results are not sensitive to possible changes in human error probabilities related to transfer of control and operation of equipment from the RSW.

Question: 720.345

Could a fire in the Main Control Room (MCR) affect the transferring of control to the Remote Shutdown Workstation (RSW) panel? Could control be inadvertently transferred back to the MCR? If the answer to these questions is no, please explain by referring to design features and characteristics (e.g., fiber optic switches and location of power sources to the light transmitters and receivers) and to emergency operating procedures and criteria for transferring control to the RSW. If the answer to any of the above two questions is yes, please model the failure to transfer control in the PRA.

Response:

A fire in the Main Control Room does not affect the transfer of control to the Remote Shutdown Workstation. The RSW transfer switch set (multiple transfer switches, one per safety-related division) is located in a fire area outside the MCR. The MCR/RSW transfer will utilize separate multiplexers for control inputs which originate in the MCR and RSW. The multiplexers will be enabled and disabled by the control transfer switches. There will be separate multiplexer sets associated with each of the four PMS divisions so that a single failure can not result in the transfer (or return) of more than one division.

Transfer is a manual operation initiated by the operators in the MCR, who would follow MCR evacuation procedures. Procedures will establish the decision-making authority and responsibility for MCR evacuation, specify the ex-control room responsibilities for the various on-shift operations personnel, and note the location(s) of equipment, controls, and instrumentation required for safe shutdown.

Inadvertent transfer of control from the RSW back to the MCR would not occur as a result of the fire in the MCR. It is possible to transfer control from the RSW back to the MCR by de-energizing the RSW multiplexer cabinets in the instrumentation and control rooms. This allows the operators to restore control to the MCR in the event that a fire damages the transfer set, resulting in inadvertent transfer of control to the RSW. However, the I&C rooms are in fire areas separate from both the MCR and RSW. Therefore, neither fire-induced nor random-failure-induced de-energization of the multiplexer cabinets would result in significant fire core damage frequency scenarios. Inadvertent manual repositioning of the RSW transfer switch set without rapid recognition and recovery is judged to be sufficiently unlikely that it need not be explicitly considered.

Note that the effects of potential failure to transfer control to the RSW (or loss of control from the RSW) can be seen in existing scenarios evaluated in the AP600 internal fire analysis. As an alternative to attempting to quantify a human error probability for an ex-control room action for which timing, stress, physical layouts, and other relevant factors are uncertain, MCR fire scenarios CR2A, CR3, and CR4A were all quantified assuming no credit for operator actions. This is equivalent to assuming a failure probability of unity for the action to transfer control from the MCR to the RSW. Similarly, RSW area 1232 AF 01 scenarios were also quantified assuming no credit for operator actions. This is equivalent to assuming unity failure probability for operator action to restore control to the MCR (further assuming that MCR control had been lost due to multiple fire-induced faults causing transfer of control away from the MCR). The results are presented in Table 57-15 of the Internal Fire Analysis.

Question: 720.346

The Main Control Room (MCR) evacuation scenario related to fire in the overhead mimic panel (scenario CR5) appears to be relevant for all control room panels, not just the overhead mimic panel. If all panels are included, the contribution from CR5-like scenarios should be around a factor of 30 higher. Please explain why fires in other control room panels are not postulated to lead to MCR evacuation and plant shutdown via the Remote Shutdown Workstation.

Response:

The contribution of the other cabinets to the main control room evacuation scenario is already included in other scenarios postulated for the control room. For example, scenario 3 postulates that a fire in the Dedicated Control panel grows beyond the incipient stage, causing the loss of all functions in this panel and evacuation of the control room due to effects of smoke or the operator interpretation of the evacuation procedures.

Question: 720.347

The frequency of fires in the AP600 Main Control Room (MCR) was assumed to be a factor of 10 smaller than the frequency of fires in a conventional control room. This was based on the observation that most of the cables in the AP600 MCR are low voltage as compared with conventional control room cables. Although it appears reasonable to postulate some reduction in fire frequency as compared with conventional control rooms, is there any data to support the reduction factor used? It is mentioned (page 57-26) that Westinghouse cable heatup calculations have shown that ignition is very improbable because low-voltage cables do not produce enough energy to heat up the cables. Do, the above mentioned Westinghouse calculations, account for insulation aging or the presence of dust? How many of the 12 MCR fires in the NSAC/178L database were initiated by electrical faults leading to ignition of the insulation? Please provide a breakdown of causes. Also, for each event, please provide: an event description, the basis for determining that the fire was not severe and the suppression time.

Response:

The reduction factor used in the analysis is purely a judgmental factor based on talking with experts in the fire protection field and electrical engineers.

Table 720.347-1 presents a break down of control room fires. Column 1 presents the fire event number as assigned in the NSAC/178L database. The database lists 12 control room fires. One fire occurring outside the control room (9/7/85) and one recurring fire were excluded from this table. It is noted that out of the eight electrical cabinet-induced fires with known cause, 7 were fires starting due to an electrical fault (relay or circuit board failures). It is not known whether these fires actually ignited cable insulation or not but it is judged that for a fire in an electrical cabinet inside a control room, cable insulation is the most likely source of the fuel.

It should be noted that none of the database events report the use of hose stations. Fire suppression method for two are unknown, two fires self extinguished, and six were suppressed with portable extinguishers.

TABLE 720.347-1
ELECTRICAL CABINET INDUCED FIRES IN THE CONTROL ROOM

Fire Event # (Date)	Initiating Component	Detection Means	Suppression Time < 10 Min.	Description implies a severe fire	Comments
163 (7/12/79)	Circuit Board	Personnel	Yes	No	Some damage to components outside the ignition source. However panel still in use after the fire. Thus, this is a potentially significant event.
329 (8/11/82)	Cable	Personnel	Yes	No	Due to a wire that shorted when pinched in the door. Quickly identified and distinguished.
369 (3/12/83) & 374 (3/30/83)	Relay	Personnel	No information	No	RPS relays remained operable after each fire.
425 (6/3/84)	Relay	No information	Yes	No	Only a few relays were affected.
464 (3/29/85)	Oven grease	No information	Yes	No	
480 (7/14/85)	Circuit card	Personnel	Yes (assumed)	No	No suppression time is given but it is stated that it was suppressed quickly.
481 (7/26/85)	No information	No information	No information	No	No description is available
537 (9/4/86)	Circuit card	Personnel/ smoke detector	Yes	No	
659 (12/30/87)	Relay	Personnel/ smoke detector	Yes	No	Only a few relays were damaged.
756 (10/14/88)	Relay	Personnel	Yes	Maybe	Four relays plus wiring damaged. Potentially significant.

Question: 720.348

The analysis of scenarios CR4 and CR4A (which treat the spurious actuation of both divisions of the ADS Stage 1 valves due to a fire in the Dedicated Control Panel) and Scenario CR4B (which treats the spurious opening of the Stage 4 valves) does not explain the mechanisms of spurious actuation using PRA I&C models and SAR I&C logic diagrams and does not state assumptions made. Furthermore, this analysis does not identify important features, and/or operational requirements, that are incorporated into the design to prevent fire-induced hot shorts from causing spurious actuations which in turn could have a significant impact on plant safety. Please provide this information. In your response please include answers to the following questions:

- Is Scenario CR4B properly labeled as a sensitivity case? Or should its results be added into the total CDF for the MCR?

- Can a fire that has grown past the incipient stage in the panel affect all ADS valves? If so, is there a technical basis for analyzing only a subset of fire effects?

- The effective spurious actuation probability for all three MCR scenarios (CR4, CR4A and CR4B) is 0.01. On the other hand, for scenarios outside the MCR, a value of 0.06 is used for a single spurious actuation of an ADS Stage 4 valve (leading to an medium LOCA) and a value of 0.0036 is used for the spurious actuation of both ADS Stage 4 valves (leading to a large LOCA). Is there a difference between the MCR and ex-MCR scenarios necessitating the different approaches to quantify the likelihood of spurious actuations?

Response:

In the final results, scenario CR4B is not treated as a sensitivity case. With reference to Table 57-15 of the submittal, the contribution of CR4B is added to the total core damage frequency for the main control room.

A discussion of spurious ADS actuation mechanisms and analysis assumptions is provided in the response to RAI 720.337.

It may be possible that a fire in a single MCR panel could affect all ADS valve stages in a given safety-related division. However, consistent with the modeling in the internal events PRA, the effects of plant response to various numbers of ADS valves opening correspond to different sizes of LOCA. A discussion of which LOCA models were used for different cases of ADS opening is provided in the response to RAI 720.337.

The difference in the likelihood of fire-induced spurious actuation of ADS valves between fires impacting the MCR and those impacting ex-MCR areas is as follows:

Difference in Cable Function. In the control room there are no ADS-related power cables whereas outside the control room there are. It was assumed in the analysis that only one hot short in power-related cabling (external or internal) would be required to cause spurious actuation of an ADS valve. However, two hot shorts in control-related cabling are needed to cause a hot short since an ADS valve requires the appropriate 2 out of 4 logic signals in the correct sequence to open. These conclusions were made based on a review of the Functional Diagrams for the automatic RCS Depressurization valve sequencing (SSAR Figure 7.2-1, sheet 15) and discussion with design engineers.

Difference in approach. In the control room analysis it was assumed that the fraction of fires that will result in hot shorts leading to the opening of a single ADS valve is 0.1 (i.e. conditional probability of hot short is assumed to be 0.1) as opposed to 0.06 which was assumed for ex-MCR fires. The 0.1 value is a conservative judgement whereas 0.06 value is based on the value provided in the referenced NUREG. Also, in the control room analysis it was assumed that the conditional probability of a second hot short (i.e. causing the two spurious signals) is 0.1 whereas in the ex-MCR areas this conditional probability is assumed to be 0.06.

Question: 720.349

The analysis assumes that MCR fires will not affect multiple cabinets, at least until control is transferred to the remote shutdown workstation. What design features are provided to ensure that fires do not propagate from one cabinet/panel to another?

Response:

In the AP-600 internal fire analysis, it was generally assumed that cabinet fires in the control room will not spread from the confines of the cabinet in which they originate if the cabinet has solid metal or fire resistant boundaries. This supposition is supported by the results of the Sandia cabinet fire tests, in which all test fires were self-extinguished, and by the reports of control room fires in the data base. The Sandia tests indicate that fire spread to an adjacent cabinet was prevented if the cabinets were separated by a double wall.

Question: 720.350

It is not clear which model was used to estimate the non-suppression probability. The analysis text refers to EPRI's HCR model, but the reference supplied is for ASEP (see p. 57-33, Ref. 57-6).

a) Please explain how the non-suppression probability of 0.0034 (used in the analysis) was obtained.

b) Aside from questions of its applicability to the analysis of fire suppression activities, the ASEP model deals with diagnosis (and non-response), as does EPRI's HCR model. Some time is required to actually extinguish the fire. Analysis of suppression time data indicates a mean suppression time of about 8 minutes. Does the AP600 analysis address the time required to extinguish the fire? Please explain.

c) Westinghouse's interpretation of the Sandia cabinet fire tests appears to differ from Sandia's interpretation. In questions to the utility regarding the South Texas fire risk assessment, the Sandia team stated that "Sandia sponsored large scale enclosure tests have shown that cabinet fires generate such intense smoke that within 6-8 minutes control of the plant from the control room would be virtually impossible. These tests were conducted with control room ventilation rates of up to ten room changes per hour." Please explain the basis for selecting a 15 minute time window (before control room evacuation is required).

d) Are there procedures dealing with control room evacuation? If so, what are the criteria used for determining when evacuation should/must take place?

Response:

a. The general philosophy for evaluation of AP600 control room fires follows the approach suggested in NSAC-181L. Per page 2-11 of NSAC-181L, 15 minutes is available before obscuration of the main control panel (leading to the control room evacuation). Also per page 2-11 of the NSAC-181L, the probability of non-suppression of a control room fire as a function of time was obtained from control room fire durations in the EPRI fire events database. Per page 3-23 of the NSAC report, the probability of non-suppression for a fifteen minute time window is estimated as 3.4E-3.

b & c The general philosophy for evaluation of AP600 control room fires follows the approach suggested in NSAC-181L. It is believed that the NSAC-181L approach (which includes the HEP calculation and interpretation of the Sandia fire tests) is reasonable and the most appropriate method available presently.

d. Procedures for dealing with main control room evacuation are expected to be prepared by the COL. Additional details regarding such procedures are discussed in the response to RAI 720.345. Such procedures for current plants rely on the Shift Supervisor (or similarly responsible position) to decide when conditions require transfer of control to the RSW. In general, it is undesirable and impractical to set prescriptive criteria specifying when a MCR evacuation must take place. The operators will be aware of the conditions in the MCR and of their option to transfer control to the RSW should conditions warrant this.

Question: 720.351

A fire in the MCR might cause spurious indications as well as spurious equipment operation. Such spurious indications could prompt incorrect operator actions ("errors of commission"). Please discuss the likelihood and potential consequences of such fire-induced errors. In your discussion please list important design features and operational requirements which help prevent such "errors of commission."

Response:

The results of the MCR fire scenarios from the internal fire analysis confirm that core damage frequency from such scenarios, assuming credit only for passive features and with no credit for operator actions, is very low for both at-power and shutdown initial conditions. Consistent with the state of the art approach for fire PRA, errors of commission were not explicitly addressed in this analysis. The probability that the operators would attempt to defeat automatic actuations because the fire was causing contrary indications is judged to be very small, because the operators would be expected and able to rely on confirmatory information available through the various displays. The displays used by the AP600 plant operators are video display units. Plant data is generated in either a digital or analog format. Data generated in an analog format is converted to a digital data format before being processed for the displays. Fires in the MCR may cause the loss of the display function; however there is no real possibility that the fire can cause the data to be altered such that incorrect data would be displayed. Fires outside the MCR could affect analog signals before processing and could result in the display of incorrect information in the MCR. However, signal redundancy and separation of cabling, along with the diversity of signals available to the operators, make it unlikely that fire damage would cause indications that would be sufficiently misleading to the operators that they would manually defeat automatic actuation of safety systems. These features help ensure that any risk associated with operator errors of commission are minimized.

If a fire were to cause spurious indications it is unlikely that the operators would be unaware that the fire was the source of such indications. If the spurious indications were such that they would be misinterpreted by the operators as a requirement for operation of a mitigating system, actuation of the mitigating system by the operators (e.g., SFW, PRHR, CMTs, ADS) would eventually lead to a safe condition. The fire analysis already models the effects of large and medium LOCAs caused by ADS valve opening, which have been assumed to occur directly as a result of a fire but could also be postulated to occur as a result of operator actions. The AP600 Adverse System Interactions Evaluation Report (WCAP-14477) provides discussions of the plant features that address various active and passive system interactions. If the spurious indications were such that they would be misinterpreted by the operators that no mitigating system actuation were required when such actuation was required, the automatic actuation features would initiate operation of the systems.

Question: 720.352

The Auxiliary Building contains the MCR as well as various I&C, battery and electrical equipment areas. Do any of the later areas share a common ventilation system and/or air intake system with the control room? If the answer is yes, please explain what barriers (including operator actions) prevent smoke, hot gases and fire suppressants from reaching the MCR and how such barriers can be defeated.

Response:

The Nuclear Island Nonradioactive Ventilation System (VBS), as described in AP600 SSAR Section 9.4.1, serves the Class 1E I&C, battery, and electrical equipment areas and the main control room. The VBS consists of several independent subsystems, including a main control room/technical support center HVAC subsystem and a Class 1E electrical room HVAC subsystem. The MCR is a separate fire area from the various electrical equipment room fire areas.

The MCR/TSC subsystem supplies outside air to the main control room and technical support center areas, and the supply and return air ducts that penetrate the MCR envelope include redundant safety-related seismic Category I isolation dampers located within the MCR envelope. The Class 1E electrical room HVAC subsystem serves the Class 1E electrical rooms, Class 1E instrumentation and control rooms, Class 1E electrical penetration rooms, Class 1E and spare Class 1E battery rooms, remote shutdown area, and reactor coolant pump trip switchgear rooms. The outside supply air intake enclosure for the portion of the Class 1E electrical room HVAC subsystem serving the division A and C electrical equipment areas is common to the MCR/TSC intake, but the intake serving the division B and D equipment is in a separate enclosure.

As noted in AP600 SSAR subsection 9.4.1.2.1.1, the MCR/TSC HVAC subsystem is designed so that smoke, hot gases, and fire suppressant will not migrate from one fire area to another to the extent that they could adversely affect safe shutdown capabilities, including operator actions. Fire or combination fire and smoke dampers are provided to isolate each fire area from adjacent fire areas during and following a fire in accordance with NFPA 90A requirements. These combination smoke/fire dampers close in response to smoke detector signals or in response to the heat from a fire.

As noted in SSAR subsection 9.4.1.2.1.2, the Class 1E electrical room HVAC subsystem is designed so that smoke, hot gases, and fire suppressant will not migrate from one fire area to another to the extent that they could adversely affect safe shutdown capabilities, including operator actions. Separate ventilation subsystems are provided to serve the electrical division A and C equipment rooms and the electrical division B and D rooms. The use of separate HVAC distribution subsystems for the redundant trains of electrical equipment prevents smoke and hot gases from migrating from one distribution division to the other through the ventilation system ducts. In addition, combination fire/smoke dampers are provided for Class 1E equipment rooms, including the remote shutdown workstation room, to isolate each fire area and block the migration of smoke and hot gases to or from adjacent fire areas in accordance with NFPA 90A requirements. These combination fire/smoke dampers close in response to smoke detector signals or in response to the heat from a fire.

The smoke/fire dampers on each Class 1E electrical room and on the MCR provide sufficient automatic protection against entry of smoke, hot gas, and fire suppressants into the MCR.

The degree of separation and redundancy in ventilation systems makes it unlikely that smoke, hot gases, or fire suppressants from fires outside the MCR would reach the MCR.

Enclosure 3 to Westinghouse
Letter NSD-NRC-96-4904

December 9, 1996

interlock would initiate a spurious actuation of the automatic depressurization system event. Both of these double failures are unlikely, given that the test conditions are normal (e.g., not emergency); performed in the control room; operators are aware of the implications of opening automatic depressurization system valves (e.g., causing a reactor trip and shutting the plant down); and supervision and other operators are present in the control room to observe the test (e.g., the operator would not likely skip the step of bringing up the in-service test soft controls). Additionally, the hardware failure of the interlock is small (passive system with a failure probability of 1E-3 or less).

Failure of each operator action is independent and is estimated to be on the order of 1E-03 (similar to omission or commission error with no stress factor, from THERP). Considering a recovery factor of 0.1 for the supervisor for the first error, the total expected error is estimated to be in the range of 1E-06 to 1E-07 (1E-03 * 1E-03 * 1E-01).

Based on the above discussion, the failure modes leading to the above scenarios are not further evaluated quantitatively.

Results of Spurious Actuation of Automatic Depressurization System

The yearly frequencies of the spurious actuation of the automatic depressurization system categories are calculated as shown in Table ~~3.3 in Appendix 32B~~ 3-3. The calculated initiating event frequencies are as follows:

- Spurious automatic depressurization system classified as intermediate loss-of-coolant accident 7.16E-07/yr
- Spurious automatic depressurization system classified as medium loss-of-coolant accident 1.45E-06/yr
- Spurious automatic depressurization system classified as large loss-of-coolant accident 5.4E-05/yr

3.6 References

3-1 *AP600 Probabilistic Risk Assessment Fault Trees*, WCAP-13275, Revision 2.

6.3.1.5 Containment Isolation

Analyses (documented in Appendix A) were conducted to show that sufficient water for long-term recirculation cooling of the core will be retained in containment even if containment integrity is unsuccessful. Therefore, sequences in which core damage has been avoided with successful in-containment refueling water storage tank (IRWST) injection and recirculation represent success (i.e., no core damage) regardless of the status of containment integrity or PCS water. Failure of PCS may result in exceeding the containment design pressure, but does not result in exceeding the containment ultimate pressure.

As a result, with one exception, neither containment integrity nor PCS are addressed on the core damage event trees. The status of containment integrity and PCS water are factored into the success criteria where they result in conditions affecting systems operation. Appendix A contains additional details of assumptions regarding PCS and containment isolation as used in the analyses.

The one exception to this is in the large LOCA modeling. For certain large LOCAs with break size close to that selected as the cutoff between medium and large LOCA, if containment isolation is not successful, the pressure in the RCS could prevent IRWST gravity injection. Therefore, the PRA large LOCA event tree requires the following, if containment isolation fails: CMT injection is required in order to generate both the automatic ADS actuation signal and the automatic IRWST squib valve actuation signals; and opening of ADS valves is required in order to reduce RCS pressure to the point at which gravity injection occurs.

Containment isolation is addressed in the containment event trees for core damage sequences in which IRWST injection fails, in order to determine long-term water availability in the reactor cavity. Success criteria for containment systems are provided in Chapter ~~{TBD}~~ 43.

6.3.2 Timing of Events and Key Operator Actions

Specific criteria for timing of important events within the various accident sequences are discussed in the following paragraphs.

6.3.2.1 Time to Respond to Loss of Decay Heat Removal

For events involving a loss of main and startup feedwater to the steam generators, the Passive RHR system would be expected to remove decay heat. If passive RHR failed to automatically actuate, the operators would be expected to manually actuate this function. If this were unsuccessful, the operators could initiate RCS depressurization using the ADS, in order to actuate core makeup tank or accumulator injection (i.e., feed and bleed).

The limiting loss of decay heat removal events are those that result in a loss of secondary side heat sink. A loss of offsite power (resulting in a loss of all main feedwater) without startup feedwater (resulting from either station blackout or failure of SFW) is analyzed, since this

which reduces to:

$$P(f:system) = (\lambda_1 * T) + (\lambda_2 * T)$$

Thus, for any intermediate single-point failure nodes of the tree, this modeling method implies that any failure of these parts at any time during the full mission time T will cause loss of the intermediate function being assessed. Therefore, application of this method correctly models single point failures that can lead to the undesired system event.

For AND gates in the tree, the same method is applied. For combinations of failures, resultant output effectively equals results that would have been obtained by using component input values based on $P(f) = \lambda T$ for initial part detectable failures and $P(f) = \lambda * 2R$ for subsequent redundant part detectable failures. For an example two-part redundant system, the AND relationship where both failures are detectable can be expressed as follows:

$$P(f:system) = P(f:Part\ 1) * P(f:Part\ 2)$$

Substituting the values per the method presented above:

$$P(f:system) = ((\lambda_1 * 2R) * (\lambda_2 * 2R)) * T/2R$$

the resulting equation is:

$$P(f:system) = (\lambda_1 * T) * (\lambda_2 * 2R)$$

This method implies that a loss of function requires two failures: failure of part 1 during full mission time T, and the subsequent failure of part 2 during twice the repair time of part 1. This result is consistent with the discussion of modeling repairable redundant systems presented above. For the spurious ADS model, T = 8760 hours, and R = 4 hours. Thus, all input failure rates used in the tree are multiplied by 8 hours (2R where R = 4 hours), and the final tree result is multiplied by 1095 hours (T/2R where T = 8760 hours, and 2R = 8 hours). This produces the probability of a spurious event over mission time T, which is then converted to a failure rate per mission time T, giving the number of spurious ADS events per year ~~equal to~~ 5.4E-5 events / year.

The number of spurious ADS events that could lead to an intermediate and medium LOCA are 1.8E-09 events/year and 1.1E-08 events/year, respectively.

which could cause a large LOCA as

26.5.4 Common Cause Failures

Several common cause failures within the PMS are considered credible and accounted for explicitly during construction of fault trees. Mainly two common cause failures are identified: hardware common cause failures due to the use of the same type of boards for many subsystems, and software common cause failures.

The hardware common cause failure evaluations are based on the multiple greek letter method, which uses beta, gamma, and delta factors to represent the conditional probabilities of second-,

the reactor coolant system and water covering the faulted steam generator tubes. These sequences are not considered to be bypass sequences.

For the steam generator tube rupture cases where the passive residual heat removal system is successful, followed by successful automatic depressurization system actuation and in-containment refueling water storage tank injection, and the failure of recirculation, core damage is assumed in the Level 1 analysis. With these circumstances, the loss of reactor coolant system fluid to the secondary side would be stopped due to the low primary-side pressure and the high water level in the faulted steam generator. This scenario assumes that the faulted steam generator would be kept filled, covering the tubes. Any release of fission products through the broken tube would be decontaminated by the ~~water covering the tubes.~~ precipitation of the fission products in the tube bundle. These sequences are not considered to be bypass sequences.

36.7 References

36-1 Theofanous, T. G., et. al., "In-Vessel Coolability And Retention of a Core Melt," DOE/ID-10460, July 1995.

36-2 "Creep Rupture Failure of Three Components of the Reactor Primary Coolant System During the TMLB Accident," EGG-EA-7431, EG&G Idaho, November 1986.

36-3 Theofanous, T. G. et. al., "Lower Head Integrity Under In-Vessel Steam Explosion Loads," DOE/ID-10541, issued for peer review, July 1996.

Table 52-5 (Sheet 1 of 2)

AT-POWER FOCUSED PRA SENSITIVITY STUDY CORE DAMAGE CONTRIBUTION BY INITIATING EVENT

	Baseline PRA CDF Contribution	Focused PRA CDF Contribution	Initiating Event	Percent Contribution	Initiating Event Frequency
1	9.0E-09	4.9E-06	ATWS percursors with MFW	64.06	1.17E+00
2	7.1E-10	2.0E-06	ATWS percursors without MFW	26.27	4.81E-01
3	3.2E-08	1.8E-07	Intermediate LOCA	2.38	7.70E-04
4	3.8E-10	8.6E-08	ATWS percursors with SI signal	1.12	2.05E-02
5	1.1E-09	8.1E-08	Transients with MFW	1.06	1.40E+00
6	5.6E-10	6.1E-08	PRHR tube rupture	0.79	2.50E-04
7	5.0E-08	5.8E-08	Large LOCA	0.75	1.05E-04
8	3.8E-08	5.7E-08	Safety injection line break	0.74	1.04E-04
9	6.2E-09	3.8E-08	Medium LOCA	0.50	1.62E-04
10	3.0E-10	3.0E-08	Loss of main feedwater	0.38	3.35E-01
11	4.1E-09	2.4E-08	Small LOCA	0.31	1.01E-04
12	3.5E-09	2.2E-08	CMT line break	0.28	8.94E-05
13	1.8E-10	1.7E-08	Loss of MFW to one steam generator	0.22	1.92E-01
14	6.1E-09	1.7E-08	Steam generator tube rupture	0.22	5.20E-03
15	2.3E-09	1.2E-08	RCS leak	0.15	5.02E-05
16	1.8E-09	1.1E-08	Core power excursion	0.14	4.50E-3
17	1.0E-09	1.1E-08	Loss of offsite power	0.14	1.20E-01

Attachment A to NSD-NRC-96-4904
Enclosed Responses to NRC Requests for Additional Information

Re: Conditional Containment Failure Probability

220.95	220.96
220.97	220.98
220.99	480.190
480.191	480.192

Re: Fire PRA (draft responses)

720.334	720.335	720.336
720.337	720.338	720.339
720.340	720.341	720.342
720.343	720.344	720.345
720.346	720.347	720.348
720.349	720.350	720.351
720.352		