Westinghouse Electric Corporation
Energy Systems
Box 355
Pittsburgh Pennsylvania 15230-0355

NSD-NRC-97-4941
DCP/NRC0707
Docket No.: STN-52-003

January 14, 1997

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

ATTENTION: T. R. QUAY

SUBJECT: AP600 RESPONSE TO REQUESTS FOR ADDITIONAL INFORMATION

Dear Mr. Quay:

Enclosed are Westinghouse responses to NRC requests for additional information pertaining to the AP600 internal fire analysis, which is documented in Chapter 57 of the AP600 Probabilistic Risk Assessment report. Specifically, responses are provided for RAI 720.334, and 720.337 through 720.351.

The NRC comments provided during the Westinghouse/NRC December 19, 1996 AP600 internal fire analysis meeting have been addressed in the RAI responses. The responses close, from a Westinghouse perspective, the addressed questions. The NRC should review these responses and inform Westinghouse of the status to be designated in the "NRC Status" column of the OITS.

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

Brian A. McIntyre, Manager
Advanced Plant Safety and Licensing

/jml

Enclosure

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

E004

3049A

220055

Enclosure to Westinghouse
Letter NSD-NRC-97-4941

January 14, 1997

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 separated from other fire zones such that fire propagation across a fire zone boundary can be dismissed. Most fire zones in containment are separated by continuous structural or fire barriers without penetrations and by labyrinth passageways. The exceptions to this occur in two categories. In one case, a number of fire zones are open to the upper containment zone (1100 AF 11500). The upper containment zone is an open space with equipment very high on the containment shell. As a result, there is no mechanism, installed or transient, for fire to propagate into the zone. The other case is the single of fire zones 1100 AF 11300A and 1100 AF 11300B being two sides of the single maintenance floor. On this case, installed equipment in each are is separated from equipment in the other by a minimum of 30 feet. The fire sources are small and not fluid. Therefore, there is no installed mechanism for fire propagation. In addition, since material transfer access to this area is limited to shutdown and since the area should be kept free for maintenance access, there should be no transient sources of fire or fire propagation. It is expected that the COL holder will remove all transient combustibles

from this area prior to power operation. 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.

PRA Revision: None.

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. It is assumed in the fire analysis that fire-induced hot shorts are possible, independent of the type of cable (e.g., fiber-optics or copper) used to provide motive and control power for the ADS valves. 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."

PRA Revision:

Subsection 57.5.1, assumption m, will be revised as follows:

m. It was assumed that fire-induced hot shorts in safety- and DAS-related cables and equipment could result in a LOCA due to spurious opening of ADS valves. It was assumed that fire-induced hot shorts, resulting in a LOCA, are possible independent of the type of cable (e.g., fiber-optics or copper) used to provide motive and control power for the ADS valves.

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:

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.

PRA Revision: None.

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:

Fire-induced failure of containment isolation valves was not explicitly modeled in the analysis because the AP600 is designed such that containment isolation functions are not compromised by fire. Redundant containment isolation valves in a given line are located in separate fire areas or zones and served by different electrical divisions. Containment isolation for a typical penetration is provided by two series valves: one served by division A or C power and control (if powered) and located in a fire area or fire zone containing only division A or C equipment; and a second valve served by division B or D power and control (if powered), and located in a fire area or fire zone containing only division B or D equipment. Further, one isolation component in a given line is located inside containment, while the other is located outside containment, and the containment wall is a fire barrier. Thus, the possibility of a fire that would cause failure of containment isolation in lines penetrating containment is insignificant.

The conditional containment isolation failure probability given a fire resulting in core damage and also affecting one of the isolation components in a particular line required to be isolated would be higher than the conditional failure probability without the fire-induced failure. However, the design is such that at least one component random failure would still be required to prevent failure of containment isolation. Since there are only a small number of areas in which a fire affecting a containment isolation component could occur, the frequency of fire-induced core damage with fire-related containment isolation failure is sufficiently small that there would be no significant impact on plant risk.

PRA Revision:

Subsection 57.5.2, assumption h, will be revised as follows:

h. ~~Fire-induced failure of containment isolation valves is not modeled. The PRA core damage success criteria are specified assuming failure of containment isolation, so there is no effect on core damage frequency as a result of such fire-related failures.~~

Fire-induced failure of containment isolation valves was not explicitly modeled in the analysis because the AP600 is designed such that containment isolation functions are not compromised by fire. Redundant containment isolation valves in a given line are located in separate fire areas or zones and served by different electrical divisions. Containment isolation for a typical penetration is provided by two series valves: one served by division A or C power and control (if powered) and located in a fire area or fire zone containing only division A or C equipment; and a second valve served by division B or D power and

control (if powered), and located in a fire area or fire zone containing only division B or D equipment. Further, one isolation component in a given line is located inside containment, while the other is located outside containment, and the containment wall is a fire barrier. Thus, the possibility of a fire that would cause failure of containment isolation in lines penetrating containment is insignificant.

The conditional containment isolation failure probability given a fire resulting in core damage and also affecting one of the isolation components in a particular line required to be isolated would be higher than the conditional failure probability without the fire-induced failure. However, the design is such that at least one component random failure would still be required to prevent failure of containment isolation. Since there are only a small number of areas in which a fire affecting a containment isolation component could occur, the frequency of fire-induced core damage with fire-related containment isolation failure is sufficiently small that there would be no significant impact on 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 that are at least as effective as those used in existing plants. Such requirements and practices are specified, at a high level, in Appendix R and applicable NFPA requirements, and will be implemented in COL programs subject to NRC review.

PRA Revision: None.

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.

PRA Revision:

Section 57.2 will be revised as follows:

> The purpose of the qualitative analysis is to identify the boundaries of the plant fire areas and, if necessary, their respective compartments, together with the location of fire-susceptible equipment and cables within the areas which, if damaged by fire, could cause a plant shutdown and degradation of shutdown paths identified in the AP600 PRA. That information is used as a basis for systematically screening out fire areas from further consideration if a fire originating in these areas is not postulated to damage any PRA-credited accident mitigating equipment. The postulated consequences could occur either due to damage to the equipment located in the area or as a result of damage caused by propagating to another area. ~~using the non-probabilistic criteria developed in the FIVE methodology document and additional probabilistic arguments. This additional probabilistic criterion states that fire areas that do not contain compartments or cabling, which if damaged would degrade any PRA-credited equipment, can be screening out based on their low contribution to core damage frequency.~~ Further use was made of the information gathered during this stage in the quantitative analysis.

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.

Note that the scenario numbers listed in Table 57-4 for a given fire area are sequential as identified, and so do not necessarily correspond to the order shown above if some of the scenario types do not apply. For example, although Table 57-4 lists scenarios 1, 2, and 3 for area 1200 AF 01, scenario number 2 is fire propagation without hot shorts, since a hot short scenario was not identified within the area. The information provided in Table 57-4 generally indicates the type of scenario considered for a given scenario number.

PRA Revision:

The above discussion will be inserted in Section 57.6, page 57-17, before the last paragraph in the section.

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.

PRA Revision: None.

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.

PRA Revision: None.

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.

PRA Revision: None.

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.

PRA Revision:

Section 57.8.4.1, step 2, will be revised as follows:

Step 2 Determine the likelihood a fire will occur in a critical cabinet.

The frequency of fire in any individual cabinet can be derived from generic data on cabinet-induced control room fires. As mentioned in subsection 57.8.3.3, data from the industry show that the ignition frequency from cabinets in the control room is 9.5E-03 per year. This is based on "conventional" control rooms, which typically contain between 30 to 40 electrical cabinets. Assuming an average of 35 cabinets per typical control room, and assuming that an AP600 control cabinet does not pose a greater fire hazard than a typically control room cabinet (in terms of fire frequency), the ignition frequency per cabinet is approximately 3E-04 per year.

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.

PRA Revision: None.

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.

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
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.

PRA Revision: None.

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 AP600 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.

In the fire analysis, it has been assumed that the cabinets of concern in the AP600 control room are the following panels and associated displays used by the operators: two (redundant) reactor operator panels, one dedicated control panel, one senior reactor operator panel, and one overview mimic panel. Each of these panels has its own metal housing and is physically separated from each other panel. This configuration will preclude fire spread, consistent with the Sandia cabinet fire test results.

For fires with no growth beyond the incipient stage, the operators would be able to maintain control from the main control room using the remaining panels (i.e., panels except the one affected by the fire). For these scenarios, with no fire growth beyond the incipient stage, the potential for smoke damage sufficient to affect the operability of the remaining panels is insignificant, because: for these fires the level of smoke generated is not sufficient to require evacuation by the operators; and the panels are not susceptible to erroneous indications due to smoke damage because of the digital display technology used in AP600. Long term exposure to smoke may cause the displays to fail due a breakdown of electrical insulation; however, such failure would be by a complete failure of the display, not a failure resulting in the display of incorrect information. The main control room scenarios with no growth beyond the incipient stage therefore credit operator backup actuations of automatic safety-related systems.

PRA Revision: None.

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.

The amount of time taken by the operators to initiate transfer of control to the RSW is not expected to have an impact on the ability to transfer control. This is because the transfer occurs outside the MCR using the transfer switches in the RSW area, and no equipment required to assume control via the RSW is located in the MCR.

The amount of time assumed before evacuation is required is not expected to have a significant impact on fire core damage frequency or insights, since MCR scenarios are relatively small contributors to total fire core damage frequency (CDF), even with no credit taken for operator actions for scenarios requiring relocation to the RSW.

Note that, although the results for the MCR cases for Safe Shutdown as presented in Chapter 57 do not appear to support the above statement, an erroneous entry in Table 57-25, page 57-135, has been identified. When this error is corrected, the MCR contribution to CDF for the Safe Shutdown case is actually much smaller than the contribution indicated in the report. In Table 57-25, page 57-135, there are two similar scenarios, F(CR3-SD(I)) and F(CR4-SD(I)). These have the same impact except that the latter scenario also results in a hot-short-induced LOCA. In the report, the CDF for F(CR4-SD(I)) dominates the MCR core damage results. This is because the scenario frequency for F(CR4-SD(I)) was entered and used in subsequent calculations incorrectly. The value for Scenario Freq. for F(CR4-SD(I)) was incorrectly reported in Table 57-25 as 1.92E-05; the correct value is 1.93E-09. With this correction, the CDF for F(CR4-SD(I)) becomes 9.94E-13, and the total MCR core damage frequency at safe shutdown becomes 1.29E-12, which is a small contribution to the total fire CDF at safe shutdown.

PRA Revision:

The following paragraph will be added to Subsection 57.8.4.2, at the end of consideration #3 (page 57-27) in response to this question:

The amount of time taken by the operators to initiate transfer of control to the RSW is not expected to have an impact on the ability to transfer control. This is because the transfer occurs outside the MCR using the transfer switches in the RSW area, and no equipment required to assume control via the RSW is located in the MCR.

The following changes will be made to the indicated sections, to address the correction to the Safe Shutdown analysis noted in the response:

In Table 57-25:

- Entry for Scenario Freq. for F(CR4-SD(I)) changes from 1.92E-05 to 1.93E-09
- Entry for CDF for F(CR4-SD(I)) changes from 9.89E-09 to 9.94E-13.

The second paragraph in Subsection 57.10.2 is revised as follows:

> The total calculated contribution to core damage frequency caused by fires that occur during safe shutdown is estimated as ~~3.5E-8~~ 2.5E-8 per year, and the contribution to core damage frequency from fires that occur during mid-loop operation is estimated as 3.1E-7 per year. Of these totals, the contribution from control room fires is very small, specifically ~~9.9E-9~~ 1.3E-12 per year for safe shutdown and 7.8E-10 for mid-loop operation.

In the discussion of Dominant Contributors During Safe Shutdown in Section 57.10.2 (page 57-43), the following changes are made:

- The first entry (1242 AF 01 Main control room 9.9E-9 /yr) in the list of dominant contributors is deleted.
- In the first sentence of the last paragraph on page 57-43, the word *approximately* is inserted between *contribute* and *94 percent*.
- The first paragraph on page 57-44 is deleted.

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.

There is a significant difference in the manner in which information is provided to the operators in AP600 as compared to current plants. Conventional plants use discrete indicators to provide information to the operators. The displays used by the AP600 plant operators are video display units. Plant data is generated in either a digital or analog format, with data generated in an analog format 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 because digital processing and video display units are used, there is no real possibility that the fire can cause the data to be altered such that incorrect data would be displayed to the operators. In addition to design features such as signal redundancy, separation of cabling, and the diversity of signals available to the operators, transmission of the digital data is assured by parity checks and check sums. These tests provide assurance that the data which is received is exactly the same as the data which was transmitted. Further, data which is not updated is assigned a poor or bad quality attribute. This quality attribute is used by all algorithms which process the data so that any calculational outputs that are based on the suspect data are also assigned a degraded quality attribute. The quality attribute is included in the data which is displayed to the operators so that such data is highlighted. These features 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, and help ensure that any risk associated with operator errors of commission are minimized.

If a fire were to cause spurious and inconsistent 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 (Ref. 720.351-1) provides discussions of the plant features that address various active and passive system interactions. In the unlikely event that the possibility of occurrence of spurious indications leading to misinterpretation by the operators that no mitigating system actuation is required when such actuation actually is required is remote, because of the design features discussed in the previous paragraph. However, if this did occur, the automatic actuation features would initiate operation of the systems.

Reference:

720.351-1 WCAP-14477, "The AP600 Adverse System Interactions Evaluation Report."

PRA Revision: None.