

Appendix 1 Thermal Hydraulics

1. Spent Fuel Heatup Analyses

Spent fuel heatup analyses model the decay power and configuration of the fuel to characterize the thermal hydraulic phenomena that will occur in the SFP and the building following a postulated loss of water accident. This appendix reviews the existing studies on spent fuel heatup and zirconium oxidation, the temperature criteria used in the analyses, and how it applies to decommissioned plants.

1.1 Accident Phenomena and Spent Fuel Failure Criteria

Since mechanistic accident progression calculations have not been performed, engineering analyses performed to address spent fuel pool performance during various accidents have used a temperature criterion to evaluate the potential for significant fuel damage. This temperature was intended as an acceptance criterion beyond which one would expect the onset of significant, global, fuel damage and substantial release of fission products (e.g., 50-100% of inventory of volatiles) associated with such damage. Further, the temperature criterion cited (generally about 900°C) has been selected on the basis that it represented a threshold for self sustained oxidation (RES Ref. 1) of cladding in air and on that basis it has been argued that if cooling of the spent fuel could limit fuel temperatures in equilibrium below this threshold then large releases of fission products need not be considered. Self sustaining reaction in this sense means the reaction rate and thus heat generation rate is sufficient, to roughly balance heat losses for given cooling mechanisms, resulting in an isothermal condition. Once the fuel temperature exceeds this threshold temperature (alternatively identified as an ignition or autoignition temperature) it was presumed that subsequent heat up and further increases in reaction rates would be escalating and rapid and that serious fuel damage would ensue. The temperature escalation associated with oxidation in this regime would not be balanced by any reasonable cooling afforded by natural circulation of air. While it was not expected that fission product releases associated with core melt accidents would immediately emerge at this temperature (based on reactor research in various steam and hydrogen environments) it was recognized that the time window for subsequent fuel heating would be relatively small once oxidation escalated. This also did not preclude gap type releases associated with fuel failures below the threshold temperature but these generally were not considered to be significant compared to the releases associated with higher fuel temperatures and significant fuel damage.

In the report, "Draft Final Technical Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Power Plants", February 2000, the temperature criterion selected, 800°C, was used in two ways. First, it was used to determine the decay heat level and corresponding time at which heat generation and losses for complete and instantaneous draining of the pool would lead to heating of the fuel (to 800°C) after 10 hours. This time period would allow for the implementation of effective emergency response without the full compliment of regulatory requirements associated with operating reactors. Secondly, the temperature criterion was also used to evaluate the decay heat level and time ("critical decay time") at which heat generation and losses for a fully drained fuel pool would result in an equilibrium temperature of 800°C (typically this critical decay time has been on the order of 5 years) On that basis it was reasoned that since serious overheating of the fuel had not occurred, the fission product release associated with core melt need not be considered.

The NRC has received a number of comments related to the use of this temperature criterion

and has reassessed the appropriateness of such a value for both its intended purposes. At the outset RES acknowledges that an ignition temperature, or more precisely in this case a temperature for incipient temperature escalation is dependent on heat generation and losses which in turn is dependent on system geometry and configuration. In fact much of the data on oxidation is produced in isothermal tests up to near the melting temperature of zirconium. In examining an appropriate criterion, it is useful to consider the range of available data including core degradation testing in steam environments since it is likely that many spent fuel pool accidents may involve some initial period during which steam kinetics controls the initial oxidation, heatup, and release of fission products. In various experimental programs around the world (e.g., PBF-SFD, ACRR, CORA, NSRR, PHEBUS and QUENCH) repeatable phenomena have been observed for the early phase of core degradation (in steam) which proceeds initially at rates associated with decay heat (at levels characteristic of reactor accidents) until cladding oxidation becomes dominant and temperature escalation occurs. The point at which the escalation occurs, which does vary between tests, has been attributed to heat losses (RES Reference 2) characteristic of the facility and to the monoclinic to tetragonal phase change of ZrO_2 over a temperature range. The threshold at which temperature escalation occurred has been reported to vary from approximately 1100°C to 1600°C. In a CORA test performed with a lower initial heat up rate (to simulate reduced decay heat during shutdown conditions) it was reported that uncontrolled temperature escalation did not occur, raising the prospect that heating rate may be a factor. In more recent QUENCH tests (Quench 04 and 05) the effect of preoxidation was evaluated for its effect on hydrogen generation and temperature escalation. In Quench 04 temperature escalation was reported to occur at 1300°C; in Quench 05 with approximately 200µm preoxidation temperature escalation was reported to be delayed until the fuel rod temperature reached 1620°C.

Because of interest in air ingress phenomena for reactor accidents, recent severe accident research has also examined oxidation in air environments. Publication of results from the DRESSMAN and CODEX test programs (RES Reference 3) has provided much of the transient data on fuel rod and rod bundle behavior for air kinetics as well as data on fuel oxidation and volatility. Early studies of zirconium oxidation in air (RES References 4 and 5) were performed to compare isothermal oxidation and scaling of fresh samples to determine the influence of different atmospheres and materials as well as to examine potential for fire hazards. The general observation is that, at least at higher temperatures (>1000°C), the oxidation rate is higher in air than in steam. Another observation of the early studies was, under the same conditions, oxidation in an air environment produced an oxide layer or scale less protective than that for steam owing to the possible instability of a nitride layer beneath the outer oxide layer leading to scale cracking and a breakaway in the oxidation rate. The onset of this breakaway in the oxidation rate occurred at about 800°C after a time period of 10 hours in the studies performed by Evans et al (RES Ref. 4). As breakaway oxidation occurs the oxidation behavior observed no longer reflects a parabolic rate dependence but takes on a linear rate dependence. Also, at lower temperatures the kinetics of reaction indicate near cubic rate dependence thus the representation of the oxidation behavior at both high and low temperatures with a parabolic rate dependence may introduce unnecessary simplification and an understatement of the low temperature behavior. Breakaway scaling in an isothermal test may not translate to similar behavior under transient heatup conditions where initial oxidation occurs at lower temperatures and may involve steam oxidation. The presence of hydrides in the cladding may also increase the potential for exfoliation and a breakaway in the oxidation; the effect of this has, however, been seen more clearly in testing conducted with steam and high hydrogen concentrations.

Autoignition is known to occur in zirconium alloys and zirconium hydride, especially when clean metal at high temperature (800°C) is suddenly exposed to air (RES Reference 8). The temperature of ignition is also highly dependent on the surface area to volume ratio. Generally, the mechanism of abrupt exposure of hot zircalloy metal to an air environment is not applicable to spent fuel pool accidents where fuel rods are covered with a relatively thick oxide layer. However, if there is clad failure by ballooning and burst (over a temperature range of 700-850°C) there is potential for hot oxide-free metal to be abruptly exposed to air. In this instance though, the surface area to volume ratio will be small and it is considered that the likelihood for any localized ignition to propagate is small.

In the CODEX tests annular clad fuel (in a 9 rod bundle) were heated with an inner tungsten heater rod to examine fuel degradation, with preoxidized cladding, in an air environment. Oxidation kinetics were evaluated as well as the oxidation of the fuel. In the CODEX AIT -1 test the early phase of the test involved creating a preoxidation using an argon-oxygen mixture. The intent was to achieve a controlled preoxidation at a temperature of 900-950°C, but it was reported (RES Ref. 3) that preoxidation was started at a slightly higher temperature than planned. What subsequently occurred was an uncontrollable temperature escalation up to approximately 2200°C before it was cooled with cold argon flow. After restabilization of the rods at 900°C air injection was started, electrical heatup commenced, and a second temperature escalation occurred. In the CODEX AIT-2 test, designed to proceed to a more damaged state, the preoxidation phase was conducted in an argon/steam mixture at 820°C and 950°C. (a malfunction occurred during the preoxidation phase resulting in the admission of a small air flow as well). No temperature escalation was seen during the preoxidation phase. Following the restabilization of the fuel rods, a linear power increase was started and a temperature excursion subsequently occurred.

In addition to examining relevant test data RES also looked at determining a temperature based threshold for temperature escalation in an air environment by determining equivalent heat generation from steam transient tests. In this exercise we posited that at equivalent heat generation rates, i.e., accommodating different reaction rates and different heats of reaction for air and steam we should be able to predict the corresponding temperature for escalation in air based on temperature escalations seen in severe fuel damage tests conducted in steam. Using this approach, the heat generation rate was estimated, assuming parabolic kinetics, and the following equation for a rate constant in air:

$$k_p = 52.67 \exp(-17597/T) \quad (1)$$

It was predicted that based on an escalation temperature of 1200°C in steam (observed in many of the steam tests) the equivalent heat generation rate in air would produce a temperature escalation at approximately 925°C. The above equation for air kinetics was identified in RES Reference 3 as the best fit for the CODEX AIT test data, i.e., it provided the best agreement to the temperature transient in the peak position. For steam kinetics, the rate equation used in MELCOR was selected for calculating the heat generation rate. The prediction of an escalation temperature in air using this approach seems to conform quite well with the observed behavior in the transient CODEX tests and lends further credence to the relative effect of oxidation in air with respect temperature escalation. The assumption of parabolic kinetics is routine in oxidation calculations and has been shown to provide a good match with a wide spectrum of experimental data even though, over select temperature ranges,

deviations from that formulation have been observed. At temperatures above 900°C, the reaction rate in air is high, regardless of whether parabolic or linear kinetics is assumed at that point and distinguishing between the rates of escalation is unimportant for our purposes.

In assessing a temperature criterion for escalation of the oxidation process and subsequent temperature escalation it is necessary to reconsider the intended uses of the criterion: 1) to evaluate the decay time after which the fuel heatup, in the case of complete fuel uncover, leads to reaching that temperature at 10 hours and 2) to evaluate the decay time after which the fuel heatup, in the case of complete uncover will never exceed the temperature criterion.

On balance it appears that a reasonable criteria for the threshold of temperature escalation in an air environment is a value of approximately 900°C. This value is supported by both limited experimental data as well as by inference from the more abundant steam testing data. While certain weight gain data indicate the onset of a break away in the oxidation rate at lower temperatures after a period of 10 hours this additional time period then exceeds the time interval for which the first use of the criterion is intended. With regard to the second use of the criterion, determination of the point at which severe fuel heatup is precluded, the onset of breakaway indicated in certain tests indicates that the temperature criterion should be lowered to 800°C. It is important to stress that, in both instances, the temperature criteria should be used together with a thermal-hydraulic analysis that considers heat generation (i.e., decay heat and zircalloy reactions) and heat losses. For the second use of the criterion, i.e., establishing a threshold for precluding escalation, the analysis must demonstrate that heat losses, through convection, conduction and radiation, are sufficient to stabilize the temperature at the value selected.

In the case of slow, complete draining of the pool or partial draining of the pool it is appropriate to consider use of a higher temperature criterion for escalation, perhaps as high as 1100 to 1200°C. This would be appropriate if the primary oxidation reaction was with steam. Such a temperature criterion is relevant for the first intended use of the criterion, determining the point at which the temperature is not exceeded for 10 hours, however it is not appropriate for use as a long term equilibrium temperature since over long intervals at such high temperature one might reasonably expect significant fission product releases.

In addition to comments on the selection of an ignition temperature the staff received comments related to the effect of intermetallic reactions and eutectic reactions. With respect to intermetallic reactions, the melting temperature of aluminum, which is a constituent in BORAL poison plates in some types of spent fuel storage racks, is approximately 640°C. Molten aluminum can dissolve stainless steel and zirconium in an exothermic reaction forming intermetallic compounds. In the spent fuel pool configuration, zircalloy cladding will be covered with an oxide layer and unless, significant fresh metal surface is exposed through exfoliation there will be no opportunity to interact metallic zircalloy with aluminum (which similarly will be oxidized). Aluminum and steel will form an intermetallic compound at a temperature of 1150°C, (RES Ref. 5) which is above the temperature criterion selected for fuel damage.

Besides intermetallic compounds, eutectic reactions may take place between pairs of various reactor materials, e.g., Zr-Inconel (937°C), Zr-steel (937°C), Zr-Ag-In-Cd (1200°C), Zr-B₄C (1627°C), steel-B₄C (1150°C), etc. (RES Ref. 6). Consideration of eutectics and intermetallics is important from the standpoint of heat addition as well as assuring the structural integrity of the storage racks and maintaining a coolable configuration. Noting the eutectic and

intermetallic reaction temperatures, however it does not appear that formation of these compounds imposes any additional temperature limit on the degradation of cladding in an air environment.

Since the temperature criterion is also a surrogate of sorts for the subsequent release of fission products it is useful to consider the temperature threshold versus temperatures at which cladding may fail and fission products be released. Cladding is likely to fail by ballooning and burst in the temperature range of 700-850°C, resulting in the release of fission products and fuel fines. At burst, clean Zircaloy metal will also be exposed, leading to an increase in oxidation although the total amount of metal involved will be limited. Creep failure of the cladding at or above 600°C is also a possibility. This temperature limit is roughly associated with the 10 hour creep rupture time (565°C) which has been used as a regulatory limit. While failure of the cladding at these lower temperatures will lead to fission product release, such release is considerably smaller than that assumed for the cases where the temperature criterion is exceeded and significant fuel heatup and damage occurs. Low temperature cladding failures might be expected to produce releases similar to those associated with dry cask accident conditions as represented in Interim Staff Guidance (ISG)-5. This NRC guidance document prescribes release fractions for failed fuel (2×10^{-4} for cesium, ruthenium and 3×10^{-5} for fuel fines). Use of these release fractions would reduce the offsite consequences dramatically from the fuel melt cases, early fatalities would be eliminated and latent cancer fatalities would be reduced by a factor of 100. As the temperature limit increases from 600°C to 900°C there is some reason to believe that ruthenium releases would be increased based on ORNL test data from unclad pellets. Canadian data indicate though, that in the case of clad fuel the ruthenium release did not commence until virtually all of the cladding had oxidized, by this point it might be surmised that the fuel configuration would be more closely resembling a debris bed than intact fuel rods. Selection of a temperature criterion for fuel pool damage also depends on the intended use, i.e., whether it is intended as the criterion for the 10 hour delay before the onset of fission product release or whether it is being used as a threshold for long term fission product release. If the criteria is being used to judge when 10 hours are available for evacuation then it may be argued that a higher temperature could be adopted, one associated with the significant release of fission products, 1200°C, since the release of fission products at lower temperatures will likely be small. However, in air it may be that the oxidation rate above 900°C is sufficient to reduce the additional time gained to reach 1200°C to a relatively small amount. Selection of a temperature criterion for long term fuel pool integrity needs to consider that ruthenium release rates, in air, become significant at approximately 800°C, based on the data of Parker et al. (RES Ref. 7).

Selection of an acceptance criterion for precluding significant offsite release, after roughly 5 years, should also consider that ruthenium with a 1 year half life will be substantially decayed and that at 5 years cesium (and perhaps fuel fines such as plutonium) will dominate the dose calculation. For these reasons NRC RES believes that the long term viability of the pool, in a completely drained condition (air environment), if it concerns time periods of approximately 5 years pool degradation should be assessed for a temperature of approximately 800°C. Again, an analysis needs to be performed to demonstrate that at that temperature an equilibrium condition can be established. While this would result in an offsite release there would be substantial time available to take corrective action after a 5 year decay time for the most recently loaded fuel. If shorter decay time periods are proposed for achieving the long term equilibrium temperature criterion then the impact of ruthenium releases would dictate

reconsideration of this value.

In summary, we conclude that for assessing the onset of fission product release under transient conditions (to establish the critical decay time for determining availability of 10 hours to evacuate) it is acceptable to use a temperature of 900°C if fuel and cladding oxidation occurs in air. If steam kinetics dominate the transient heatup case, as it would in many boildown and drain down scenarios, then a suitable temperature criterion would be around 1200°C. For establishing long term equilibrium conditions for fuel pool integrity during spent fuel pool accidents which preclude significant fission product release it is necessary to limit temperatures to values of 600°C to 800°C. If the critical decay time is sufficiently long (>5 yrs) that ruthenium inventories have substantially decayed then it would be appropriate to consider the use of a higher temperature, 800°C, otherwise fission product releases should be assumed to commence at 600°C. These cases are marked by substantial time for corrective action to restore cooling and prevent smaller gap type releases associated with early cladding failures.

The degradation of fuel during spent fuel pool accidents is an area of uncertainty since most research on severe fuel degradation has focused on reactor accidents in steam environments. Because of this uncertainty we have tended to rely on the selection of conservative criterion for predicting the global behavior of the spent fuel pool. It is our recommendation that the modeling of spent fuel pool accidents be performed with codes capable of calculating the heat generation and losses associated with the range of accidents including phenomena associated with both water boiloff and air circulation. Further, the calculation of critical decay times for establishing both the validity of ad hoc evacuation and precluding fission product release must also include consideration of the exothermic energy of reactions (i.e., reactions with air and steam) with cladding or alternatively demonstrate that such energy contribution is negligible in comparison to decay heat at that point. Severe accident codes, such as MELCOR, developed for modeling the degradation of reactor cores, would seem to be a reasonable approach for analysis of integral behavior and would possess the general capabilities for modeling liquid levels and vapor generation, air circulation, cladding oxidation and fission product release. Use of a severe accident code also facilitates the use of self consistent modeling and assumptions for the analysis. The proper calculation of fission product releases depends in large part on the prediction of thermal hydraulic conditions. More detailed CFD modeling would improve the calculation of boundary conditions for air circulation and could be used in conjunction with integral codes to better evaluate convective cooling. The kinetics of cladding reactions should be confirmed with experiments designed to simulate the range of conditions of interest under steady state and transient heating. The experimental database on ruthenium releases under conditions applicable to spent fuel pool accidents is inadequate and we are currently extrapolating data from conditions which tend to maximize such releases.

While there is uncertainty in the analysis of spent fuel degradation, especially for the conditions of air ingress, it is also true that elements of the analysis contain conservatism. The assumption of 75-100% release of ruthenium initiated at lower temperatures is based in large part on tests with bare fuel pellets, testing of clad fuel indicates that the cladding acts as a getter of oxygen limiting release of ruthenium until virtually all of the cladding has oxidized. Further, before significant ruthenium release occurs (in its more volatile oxide form) the surrounding fuel matrix must be oxidized. During transient heatup of a spent fuel pool with temperature escalation one would expect the ruthenium release to follow the oxidation of the cladding at which point the fuel would more likely resemble a debris bed (the seismic event may also contribute in that regard) limiting the release fraction. The competition between formation

of hyperstoichiometric UO_2 and U_3O_8 may also limit the release fraction below that seen in the data. The use of a temperature criterion of 600°C to preclude significant fission product releases is conservative in that it is based on large part on data that discounts the effect of cladding to limit releases. The cladding failures at low temperatures will still allow substantial retention of fuel fines and the presence of unoxidized zircalloy will prevent formation of volatile forms of ruthenium. More prototypic experimental data on releases under these kinds of conditions may reveal that the onset of significant releases, especially ruthenium, would not occur under spent fuel pool accident conditions until fuel rod temperatures reached much higher temperatures associated with complete oxidation of the cladding.

Use of the hottest fuel assemblies to predict global release of fission products from the entire spent fuel inventory is a significant conservatism as well. Transient fuel damage testing indicates that at temperature escalation not all of the rod bundle undergoes rapid heating, cooler regions can avoid the oxidation transient. Prediction of the propagation of the temperature escalation to the cooler regions of the pool needs to be carefully examined to see if significant benefit can be gained, at a minimum it will lengthen the period of fission product release reducing the concentration of activity in the plume of fission products for offsite consequence analysis.

1.2 Evaluation of Previous Spent Fuel Heatup Analyses

In the 1980's, severe accidents in operating reactor SFPs were evaluated to assess the significance of the results of some laboratory studies on the possibility of self-sustaining zirconium oxidation and fire propagation between assemblies in an air-cooled environment, and also to assess the impact of the increase in the use of high density spent fuel storage racks on severe accidents in spent fuel pools. This issue was identified as Generic Safety Issue (GSI) 82. Sandia National Laboratory (SNL) and Brookhaven National Laboratory (BNL) used the SFUEL and SFUEL1W computer codes to calculate spent fuel heatup in these studies. While decommissioned plants were not addressed in the study, many of the insights gained from these studies are applicable to decommissioned plants.

More recently, BNL developed a new computer code, SHARP, that was intended to provide a simplified analysis method to model plant-specific spent fuel configurations for spent fuel heatup calculations at decommissioned plants. Some of this work was built on the assumption used by SNL and BNL in their studies in support of GSI 82.

1.2.1 SFUEL Series Based Analyses

Extensive work on the phenomena of zirconium oxidation in air for a SFP configuration was performed by SNL and BNL in support of GSI 82. SNL investigated the heatup of spent fuel, the potential for self-sustaining zirconium oxidation, and the propagation to adjacent assemblies [Ref. 1, 10]. SNL used SFUEL and SFUEL1W computer codes to analyze the thermal-hydraulic phenomena, assuming complete drainage of the SFP water. In NUREG/CR-4982 [Ref. 5], BNL extended the SNL studies on the phenomenology of zirconium-air oxidation and its propagation in spent fuel assemblies. The SFUEL series of codes includes all modes of heat transfer, including radiation. However, radiation heat transfer may have been underestimated due to the assumed fuel bundle arrangement.

In NUREG/CR-0649, SNL concluded that decay heat and configuration are important parameters. SNL found that key configuration variables are the baseplate hole size,

downcomer width, and the availability of open spaces for airflow. They also found that building ventilation is an important configuration variable.

The draft SNL report investigated the potential for oxidation propagation to adjacent assemblies. If decay heat is sufficient to raise the clad temperature in a fuel assembly to within approximately one hundred degrees of the point of runaway oxidation, then the radiative heat from an adjacent assembly that reached the onset of rapid oxidation could raise the temperature of the first assembly to the runaway oxidation temperature. The report also discusses small-scale experiments involving clad temperatures greater than 1000 °C. SNL hypothesized that molten zirconium material would slump or relocate towards the bottom of the racks and consequently would not be involved in the oxidation reaction. NUREG/CR-4982 did not allow oxidation to occur at temperatures higher than 2100 °C to account for the zirconium melting and relocation. Otherwise, temperatures reached as high as 3500 °C. It was felt that not cutting off the oxidation overstated the propagation of a zirconium fire because of the fourth power temperature dependence of the radiation heat flux. The SFUEL series of codes did not mechanistically model melting and relocation of materials.

In NUREG/CR-4982, BNL reviewed the SFUEL code and compared it to the SNL small-scale experiments and concluded that SFUEL was a valuable tool for assessing the likelihood of self-sustaining clad oxidation for a variety of spent fuel configurations in a drained pool. SNL reported the following critical decay times in NUREG/CR-0649 based on having no runaway oxidation. Critical decay time is defined as the length of time after shutdown when the most recently discharged fuel temperature will not exceed the chosen fuel failure criteria when cooled by air only.

700 days	PWR, 6 kW/MTU decay power per assembly, high density rack, 10.25" pitch, 5" orifice, 1-inch from storage wall
280 days	PWR, same as above except for 1 foot from storage wall
180 days	BWR, 14 kW/MTU decay power per assembly, cylindrical baskets, 8.5" pitch, 1.5" orifice
unknown	BWR, high-density rack, SFUEL1W code was limited to computation of BWR low-density racks.

High-density racks with a 5-inch orifice are the most representative of current storage practices. A critical decay time for high-density BWR racks was not provided due to code limitations. Low-density and cylindrical storage rack configurations are no longer representative of spent fuel storage. All currently operating and recently shutdown plants have some high-density racks in the pool. For an assembly in a high-density PWR rack with a 5-inch orifice, a decay power below 6 kW/MTU did not result in runaway zirconium oxidation. All of these estimates were based on perfect ventilation (i.e., unlimited, ambient-temperature air) and burnup rates of 33 GWD/MTU. Currently, some PWRs are permitted to burn up to 62 GWD/MTU and some BWRs to 60 GWD/MTU. For fuel burnup of 60 GWD/MTU, the staff estimates the decay time for a bundle to reach 6 kW/MTU will increase from 2 years to approximately 3 years. Therefore, the staff expects the difference between critical decay times for PWRs and BWRs to decrease and that the BWR critical decay time for current burnups and rack designs would now be longer than the SNL estimate for high-density PWR racks. The SNL calculations also do not appear to have included grid spacer loss coefficients, which can have a significant effect since

the resistance of the grid spacers is greater than the resistance of a 5-inch orifice. There is no mixing between the rising air leaving the fuel racks, and the relatively cooler air moving down into the pool. Including the grid spacer resistance, accounting for mixing and limiting the building ventilation flow to rated conditions, will result in the critical decay power to be less than 6 kW/MTU. The SNL calculations may have understated the effective radiation heat transfer heat sink due to the assumed fuel geometry in the calculations. A more realistic fuel configuration pattern in the SFP would give a better estimate of the radiation heat sink and raise the critical decay power needed for significant oxidation.

While the studies in support of GSI 82 provided useful insights to air-cooled spent fuel assemblies, it is the opinion of the staff that they do not provide an adequate basis for exemptions. The studies were not meant to establish exemption criteria and lack sufficient information for all the parameters that could affect the decay time. Additionally, the reports are based on burnup values at that time. Since burnup values have increased, the results may not be directly applicable to today's spent fuel. The SFUEL code has undergone very little assessment.

The general conclusions and the phenomena described in the studies assist in assessing issues for decommissioned plants. However, the calculated decay time values do not represent current plant operational and storage practices.

1.2.2 SHARP Based Analyses

In NUREG/CR-6451 [Ref.11], BNL investigated spent fuel heatup that could lead to a zirconium fire at permanently shutdown plants. BNL developed a new computer code, SHARP (Spent Fuel Heatup Analytical Response Program), to calculate critical decay times to preclude zirconium oxidation for spent fuel. The code was intended to study thermal hydraulic characteristics and to calculate spent fuel heatup up to temperatures of approximately 600 °C. SHARP is limited to low temperatures since it lacks models for radiation heat transfer, zirconium oxidation, and materials melting and relocating. SHARP also lacks modeling for grid spacer losses and neglects mixing between the rising hot air and the falling cooler air in the SFP. BNL reported the following generic critical decay times using the SHARP code.

17 months for a PWR, high density rack, 60 GWD/MTU burnup; 10.4" pitch; 5" orifice
7 months for a BWR, high density rack, 40 GWD/MTU burnup; 6.25" pitch; 4" orifice

The above decay times are based on a maximum cladding temperature of 565 °C. The parameters listed with the critical decay times are generally representative of operating practices. Current fuel burnups in some plants, however, have increased to values higher than those used by BNL and perfect ventilation was assumed, which could lead to an underestimation of the critical decay times.

The SHARP code was not significantly benchmarked, validated or verified. The critical decay times above are shorter than those calculated in NUREG/CR-0649 and NUREG/CR-4982, particularly when the lower cladding temperature used for fuel failure and the higher decay heats used in the earlier analyses are taken into account. This appears to be driven in part, by the fact that the decay heat at a given burnup in the SHARP calculations is significantly lower than what is used in the SFUEL calculations. The staff has identified several areas that require code modifications, which will increase the calculated critical decay times. It is not adequate for use as technical bases by licensees without further code modifications and verification.

NUREG/CR-6541 was intended as an assessment to steer rulemaking activities. The report was neither intended nor structured to provide a basis for exemptions. The staff does not rely on this study for heatup analysis information due to the code that the decay time conclusions were based upon.

1.2.3 FLUENT Calculations

RES performed FLUENT calculations of a loss of water spent fuel pool accident that are documented in NUREG-1726. FLUENT is a three dimensional CFD (computational fluid dynamics) computer code. FLUENT is used to model the entire spent fuel build^{up} and pool, including the fuel and the fuel racks. A porous media approach is used to model the fuel and the racks. A detailed description of the FLUENT spent fuel pool modeling and the results of the FLUENT calculations are in NUREG-1726.

1.2.4 TEMPEST-COBRA Calculations

PNNL has performed calculations of a loss of water spent fuel pool accident with a methodology that uses the TEMPEST CFD code and the COBRA-SFS spent fuel cask analysis code. TEMPEST is a PNNL developed three dimensional CFD code that uses a cartesian grid. COBRA-SFS is a single phase computer code that was developed to model spent fuel casks. It has the capability to model fuel racks and fuel bundles down to the single fuel pin and subchannel level of detail including thermal radiation transport. The TEMPEST code is used to model the build and spent fuel pool down to the top of the fuel racks. The code calculates the average temperature immediately above the top of the spent fuel racks using a uniform average power as a heat source at the top of the fuel racks. TEMPEST does not model the flow through the fuel rack and bundles. The average temperature from the TEMPEST calculations is input as a boundary condition for the downcomer inlet conditions for the COBRA-SFS calculations. The COBRA-SFS calculations calculate the thermal response of the fuel and racks based on the power and the TEMPEST generated boundary condition.

1.3 Heatup Calculation Uncertainties and Sensitivities

The phenomenology needed to model spent fuel heatup is dependent on the chosen cladding temperature success criterion and the assumed accident scenario. Many assumptions and modeling deficiencies exist in the current calculations. The staff reviewed the models to assess the impact of those modeling assumptions. Some of these uncertainties for the SFUEL series codes are further discussed in NUREG/CR-4982. For cases of flow mixing, decay heat, bundle flow resistance and other severe accident phenomena, additional information is provided here.

Calculations performed to date assume that the building, fuel, and rack geometry remain intact. This would not be a valid assumption if a seismic event or a cask drop damaged some of the fuel racks or the building. Rack integrity may not be a good assumption after the onset of significant zirconium oxidation due to fuel failure criteria issues discussed in Section 1.1. The building may also be hot enough to ignite other materials. Assuming that the racks remain intact is the most optimistic assumption that can be made about the rack geometry. Any damage to the racks or the building could significantly reduce the coolability of the fuel.

Previous SFUEL, SFUEL1W, and SHARP calculations, used in the resolution of GI 82 and decommissioning studies, used a perfect ventilation assumption. With the perfect ventilation assumption an unlimited amount of fresh, ambient-temperature air is available. This

assumption would be valid if the building failed early in the event or if large portions of the walls and ceilings were open. If the building does not fail, the spent fuel building ventilation flow rate would dictate the airflow available. Mixing between the rising hot air and the descending cooler air in the spent fuel pool is ^{also} not modeled in the codes.

The spent fuel building ventilation flow rate is important in determining the overall building energy balance. Airflow through the building is an important heat removal mechanism. Most of the air would recirculate in the building and the air drawn under the racks would be higher than ambient temperature and, therefore, less heat removal would occur. Airflow also provides a source of oxygen for zirconium oxidation. Sensitivity studies have shown that heatup rates increase with decreasing ventilation flow, but that very low ventilation rates limit the rate of oxidation. Other oxidation reactions (fires) that occur in the building will also deplete available oxygen in the building. Zirconium-Nitrogen reaction modeling is not included in the SFUEL code and may have an impact on zero and low ventilation cases. GSI 82 studies concluded that the perfect ventilation assumption was more conservative than no ventilation because the oxidation reaction became oxygen starved with no ventilation. Since these studies did not consider the failure modes of the building under high temperature scenarios or the reaction of nitrogen with zirconium at high temperatures they should not be considered as reliable information. Intermediate ventilation rate results were not studied and give longer critical decay times than the perfect ventilation case.

The dominant heat removal mechanism is buoyancy-driven natural circulation. The calculated airflow and peak temperatures are very sensitive to the flow resistance in the storage racks, fuel bundles and downcomer. The downcomer flow resistance is determined by the spacing between the fuel racks and the wall of the SFP. The storage rack resistance is primarily determined by the orifice size at the bottom entrance to the fuel bundle. Smaller inlet orifices have higher flow resistance. As shown by SFUEL and SHARP calculations, changes in the rack-wall spacing and the orifice size over the range of designs can shift critical decay times by more than a year. The fuel bundle flow resistance is determined by the rod spacing, the grid spacers, intermediate flow mixers and the upper and lower tie plates. SFUEL and SHARP calculations have neglected the losses from the grid spacers, intermediate flow mixers and the tie plates. These flow resistances will be higher than those from the rack inlet orifice in some cases. Therefore, inclusion of this additional flow resistance may extend the critical decay time for some cases. NUREG/CR-4982 concluded that the largest source of uncertainty was due to the natural circulation flow rates.

The downcomer and bundle inlet air temperatures and mass flow rates are important in determining the peak cladding temperature. The extent of flow mixing will determine the air temperatures at the downcomer and bundle inlet. The SFUEL and SHARP calculations assume a well-mixed building air space. The downcomer inlet temperature is set equal to the bulk building temperature. This assumption neglects the mixing that occurs between the hot air rising from the bundles and the cooler air descending down the SFP wall. FLUENT calculations [Ref 12] performed by RES indicate that fully 3-dimensional calculations are needed to accurately predict the mixing and flow fields because unrealistic flow topologies in 2-dimensional approximations may overstate the mixing. The calculations also indicate that the quasi-steady state assumptions for conditions above the fuel rack may not be appropriate. Time varying temperature fluctuations on the order of ± 20 °C have been observed in 3D FLUENT calculations.

The FLUENT calculations are the only calculations that have simulated the global flow pattern.

The calculations have shown several interesting results that can be used to assess the approximations and simplifying assumptions made in the other calculations. The FLUENT calculations indicate that the fluid temperature under the fuel racks is close to the building exit temperature which is the average building temperature in the SFUEL and SHARP calculations. The downcomer inlet temperature used in the TEMPEST-COBRA calculations is higher than this value. Almost half of the downcomer is in upflow in the FLUENT calculations. All other calculations assume that the downcomer is entirely in downflow.

Radiation heat transfer is important in spent fuel pool heatup calculations. Radiation heat transfer can affect both the onset of a zirconium fire and the propagation of a fire. Both the SFP loading pattern and the geometry of the fuel racks can affect the radiation heat transfer between adjacent bundles. Simple gray body calculations show that at clad temperatures of 800 °C, a temperature difference of 100 °C between adjacent bundles would cause the radiation heat flux to exceed the critical decay power of 6 kW/MTU. Therefore, the temperature difference that could be maintained between adjacent bundles is highly constrained by the low decay heat levels. SFUEL calculations performed by SNL and BNL included radiation heat transfer, but the radiation heat transfer was underpredicted since the spent fuel placement is two-dimensional and the hottest elements are in the middle of the pool with cooler elements placed progressively toward the pool walls. Heat transfer between hotter and cooler assemblies has the potential to be significantly higher if the fuel bundles were intermixed in a realistic loading pattern. PNNL COBRA calculations have shown that not including radiation heat transfer will increase cladding temperature approximately 50 °C at a base temperature of approximately 500 °C under one actual plant fuel loading.

At temperatures below 800 °C, the SFP heat source is dominated by the spent fuel decay heat if breakaway oxidation does not occur. SNL and BNL found that, for high-density PWR racks, that 6 kW/MTU was the critical decay heat level for a zirconium fire to occur in configurations resembling current fuel storage practices. At the fuel burnups used in the calculations, this critical decay heat level was reached after two years. Decay heat calculations in NUREG/CR-5625 [Ref. 13] were performed to be the basis for calculating fuel assembly decay heat inputs for dry cask storage analyses. These decay heat calculations are consistent with the decay heat used in SFUEL calculations. Extrapolation of the decay heat calculations from NUREG/CR-5625 to current burnups indicate that approximately 3 years will be needed to reach a decay heat of 6 kW/MTU. The extrapolation has been confirmed to provide a reasonable decay heat approximation by performing ORIGEN calculations that extend to higher burnup. The critical decay heat may actually be less than 3 kW/MTU when in-bundle peaking effects, higher density rack configurations and actual building ventilation flows are taken into account.

Several licensees have proposed using the current Standard Review Plan (NUREG-0800) Branch Technical Position ASB 9-2 decay heat model for SFP heatup calculations. Using ASB 9-2 decay heat with a "k factor" of 0.1 produces non-conservative decay heat values in the range of 1 to 4 years after shutdown. ASB 9-2 explicitly states that it is good for times less than 10,000,000 seconds (~ 116 days). The basis of ASB 9-2 is the 1971 ANS draft decay heat standard. The standard gives "k factors" to use beyond 10,000,000 seconds. The staff has found that a "k factor of 0.2" will produce conservative decay heat values compared to ORIGEN calculations for the range of 1 to 4 years after shutdown.

It should be noted that none of the analysis codes have all of the required models or enough

experimental assessment to be considered as properly qualified to analyze the spent fuel pool heatup problem. Proper qualification would require a substantial research effort involving experiments, code development and analysis.

1.5 Estimated Heatup Time of Uncovered Spent Fuel

The staff recognized that the decay time necessary to ensure that air cooling was adequate to remain below the temperature of self-sustaining zirconium oxidation was a conservative criteria for the reduction in emergency preparedness criteria. Using the fact that the decay heat of the fuel is reducing with time, credit could be given, if quantified, for the increasing length of time for the accident to progress after all water is lost from the SFP. The staff sought to quantify the decay time since final shutdown such that the heatup time of the fuel after uncovering was adequate for effective protective measures using local emergency response. The heatup time was defined as the amount of time to heat the fuel from 30 C to 800 C.

The heatup time of the fuel depends on the amount of decay heat in the fuel, and the amount of heat removal available for the fuel. The amount of decay heat is dependent on the burnup. The amount of heat removal is dependent on several variables, as discussed above, that are difficult to represent generically without making a number of assumptions that may be difficult to confirm on a plant and event specific basis.

For the calculations, the staff used a decay heat per assembly and divided it equally among the pins. It assumed a 9X9 assembly for the BWRs and a 17x17 assembly for the PWRs. Decay heats were computed using an extrapolation of the decay power tables in NUREG/CR-5625 [Ref. 8]. The decay heat in NUREG/CR-5625 is based on ORIGEN calculations. The tables for the decay heat extend to burnups of 50 GWD/MTU for PWRs and 45 GWD/MTU for BWRs. The staff recognizes that the decay heat is only valid for values up to the maximum values in the tables, but staff ORIGEN calculations of the decay power, with respect to burnup for values in the table, indicate that extrapolation provides a reasonable and slightly conservative estimate of the decay heat for burnup values beyond the limits of the tables. Current peak bundle average burnups are approximately 50 GWD/MTU for BWRs and 55 GWD/MTU for PWRs. The BWR decay heat was calculated using a specific power of 26.2 MW/MTU. The PWR decay heat was calculated using a specific power of 37.5 MW/MTU. Both the PWR and BWR decay heats were calculated for a burnup of 60 GWD/MTU and include an uncertainty factor of 6 percent.

The staff used a specially modified version of TRAC-M to estimate the heatup time. Modifications were made to the wall drag model, the wall heat transfer, and the oxidation models so that they would be applicable to the spent fuel pool heatup problem. The transfer of heat between high powered bundles and low powered bundles was not modeled and only the fuel and fuel rack heat structures were modeled so the heatup time estimates should be conservative if the rack geometry is intact after the pool draining.

The staff examined the effect of zirconium oxidation models on spent fuel pool heatup. Several parabolic rate equations were used in heatup calculations. The oxidation rate equations that were used do not model the effect of breakaway oxidation. The heatup times are sensitive to the oxidation model used in the heatup calculations.

The staff has also considered a scenario with a rapid partial draindown to a level at or below the top of active fuel with a slow boiloff of water after the draindown. This could occur if a large breach occurred in the liner at or below the top of active fuel. Section 5.1 of NUREG/CR-0649

analyzes the partial draindown problem. For the worst case draindown and a lower bound approximation for heat transfer to the water and the building the heatup time is less than the heatup time for the corresponding air cooled case.

Calculations, assuming an instant draindown of the pool and air-cooling, show a heatup time to fission product release of 4 hours at 1 year after shutdown for a PWR with 60 Gwd/MTU fuel burnup. The worst case partial draindown could also release fission products in 4 hours at 1 year after shutdown. At 5 years after shutdown the release of fission products may occur approximately 24 hours after the accident. The results are calculated the oxidation the parabolic rate equation defined in equation 1. This oxidation model ~~is~~ leads to the fastest heatup times of the oxidation models that were examined. The results are shown in figure 1.

Heatup Time to Release (Air Cooling)

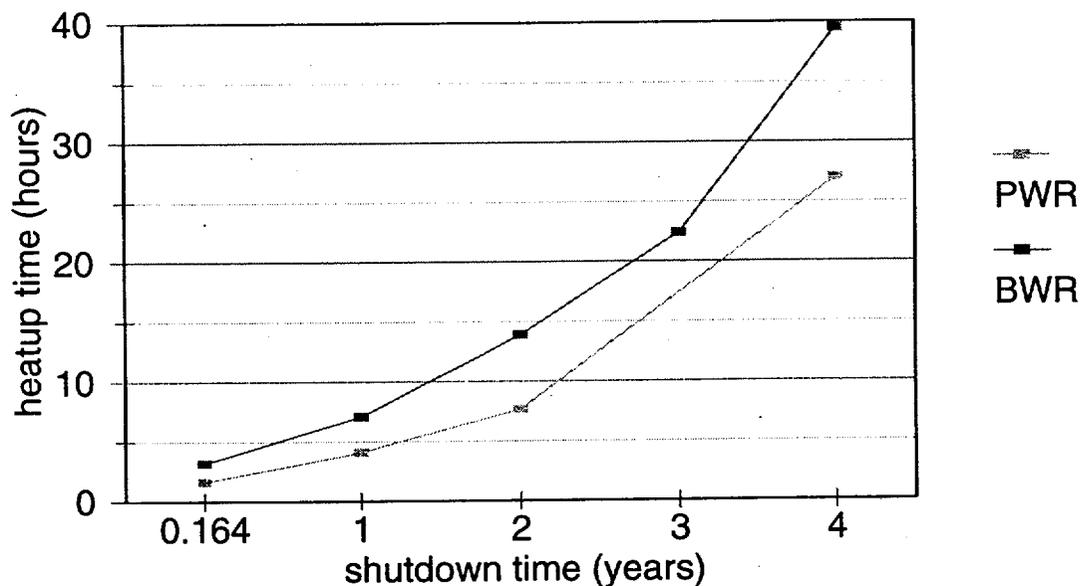


Figure 1. Heatup time from 30 C to 800 C

1.6 Critical Decay Times to Reach Sufficient Air Cooling

Calculations using the SFUEL code in support of GI-82 have determined a critical specific decay heat of 6 kW/MTU is needed for the onset of runaway zirconium oxidation. The 6 kW/MTU estimate calculated using SFUEL in a high-density storage rack configuration is reasonable and is based on the best calculations to date. However, this estimate is based on perfect ventilation conditions in the building and lower density rack configurations than exist today.

For high burnup PWR and BWR fuel, the staff estimates it will take approximately 3 years to reach the critical decay heat level cited in NUREG/CR-4982. Better modeling of flow mixing and accounting for the grid spacer and tie plate flow resistance could reduce the critical decay power level and increase the critical decay time beyond 3 years, but this may be counterbalanced by increased radiation heat transfer from realistic fuel bundle loading. Other assumptions, such as imperfect ventilation, could extend the critical decay time for the onset of

a zirconium fire by 1 to 2 years. FLUENT calculations show that the critical decay heat is less than 3 kW/MTU for the pool and building configuration that was studied at a building ventilation rate of 2 building volumes per hour. The staff estimates it will take approximately 5 years to reach a decay heat less than 3 kW/MTU for current BWR plant fuel and approximately 7 years for current PWR fuel burnups. Plant-specific calculations using fuel decay heat based on the actual plant operating history and spent fuel configurations could yield significantly shorter critical decay times. Calculations performed using checkerboard fuel loadings indicate that the critical decay time can be reduced by one year or more if the highest power fuel is interspersed with low powered fuel or empty rack spaces. Lower building ventilation rates or more restrictive rack flow configurations will extend this time.

The critical decay time will depend on the specific pool configuration and accident scenario being analyzed. The critical decay time will be a function of building configuration, building ventilation flow rate, fuel pool loading, rack geometry and the oxidation modelling. A generically applicable critical decay time can not be readily defined for the following reasons.

The building ventilation flow is unknown since the dominating initial event is a well beyond design basis earthquake. The consequences of such an event on available ventilation for air cooling is highly variable. Power will not be available to run forced ventilation systems, the fuel pool may contain debris, an unspecified amount of water may remain in the pool, and the fuel racks may not be in a well defined geometry. Since the availability of air cooling is assumption driven a probability distribution on parameters such as available air flow rate would be required to properly integrate the T/H analysis with the risk analysis. Reducing the building ventilation flow will increase fuel temperatures at a given decay time. Since the building ventilation rate may be close to zero after the postulated accident, the critical decay time could essentially extend indefinitely. Calculations of the partial draindown indicate that consideration of this event will extend the critical decay time to well in excess of 5 years.

Spent fuel pool reracks have continuously increased the fuel power density and decreased the downflow area available for cooling flow. Since the design basis for spent fuel pools involves water cooling only, no restrictions have been put on parameters that increase severe accident risk. Recent reracks have left as little as 2 inches of downcomer width available for air downflow. The downcomer width assumption was approximately 6 inches in the FLUENT calculations. Smaller downcomer widths will extend the critical decay time at a given building flow rate beyond the times listed in the NUREG-1726 study.

1.7 Fire Propagation

The staff has not performed a sufficient amount of research to fully understand and predict the propagation of zirconium fires in a spent fuel pool. Based on the limited amount of work performed to date, the propagation is probably limited to less than 2 full cores at a time of 1 year after shutdown. This estimate is based on lowering the GSI 82 estimate of the 6 KW/MTU fire threshold to 3KW/MTU to account for building ventilation effects. This does not consider potentially important effects such as rubble formation after loss of fuel integrity. The actual propagation will probably be dependent on the actual fuel loading configuration in the spent fuel pool. A long term experimental and analytical research program would be required to reliably predict the propagation of a zirconium fire in a spent fuel pool.

1.8 Conclusions and Recommendations

The staff has concluded that it is not possible to perform a generically applicable analysis to determine heatup times or critical decay times without further research including experimentation. Therefore the times cited in this report should only be considered as rough estimates of what the staff believes are realistic conditions for what is possible based on currently available information. The staff also has a poor understanding of the accident progression and source term from a spent fuel pool fire. There are many specific weaknesses in the present and past studies that have been identified. Some of the primary weaknesses were also identified as weaknesses in the studies for resolution of GSI 82. To support a more accurate assessment of what may occur following the postulated seismic initiating event, the following areas need additional development and study:

- 1.) A realistic accident scenario for the dominant risk sequence or a number of scenarios with associated probabilities should be defined.
- 2.) Potential restrictions or limitations on fuel loading patterns, allowable rack configurations, and maximum fuel burnups should be considered.
- 3.) Additional oxidation data and oxidation model development should be pursued for all zirconium alloys used in fuel cladding under a wide range of clad burnup and temperature conditions.
- 4.) Properly scaled experimental data should be obtained for code assessment.
- 5.) A validated computer code to accurately predict the accident progression and the source term from the accident should be developed.

Additional Recommendations

- 1.) The above issues need to be addressed in order to provide more accurate and realistic information for a risk analysis. A CSAU [Ref 18] like study should be performed after the experimental and code development work has been completed to quantify the uncertainty in the validated analysis code for a fixed pool configuration.
- 2.) RES should consider whether GSI 82 should be reopened to examine the impact of recent spent fuel pool configuration changes and new information on source terms in the presence of air. The higher rack densities, higher fuel burnups, larger source term, and uncertainties in physical phenomena have the potential to significantly change the conclusions reached in GSI 82.

References:

1. Benjamin, et. al., "Spent Fuel Heatup Following Loss of Water During Storage", NUREG/CR-0649, March 1979.
2. D.A. Powers, L.N. Kmetyk, and R.C. Schmidt, "A Review of the Technical Issues of Air Ingression During Severe Reactor Accidents," NUREG/CR-6218, SAND94-0731, Sandia National Laboratories, 1994
3. Nourbakhsh, et. al., "Analysis of Spent Fuel Heatup Following Loss of Water in a Spent

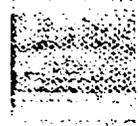
- Fuel Pool", NUREG/CR-6441.
4. Smith, C. W., "Calculated Fuel Perforation Temperatures, Commercial Power Reactor Fuels", NEDO-10093, September 1969.
 5. Sailor, et. al., "Severe Accidents in Spent Fuel Pools in Support of Generic Issue 82", NUREG/CR-4982.
 6. E. B. Evans et. al., "Critical Role of Nitrogen Dure High Temperature Scaling of Zirconium," Proc. Conf. Met. Soc. AIME, Boston, USA, 1972, pp. 248-281
 7. S. Leistikow and H. v. Berg, " Investigation under Nuclear Safety Aspects of Zircaloy-4 Oxidation Kinetics at High Temperatures in Air," Second Workshop of German and Polish Research on High Temperature Corrosion of Metals, Juelich, Germany, 2-4 December, 1987
 8. H. M. Chung and S. Basu, "Spent Fuel Cladding Behavior Following Loss-of-Water Accident During Pool Storage," July 2000
 9. MELCOR 1.8.1 Computer Code Manual, Volume 2: Reference Manuals and Programmers' Guides, June 1991.
 10. Pisano, et. al., "The Potential for Propagation of a Self-Sustaining Zirconium Oxidation Following Loss of Water in a Spent Fuel Pool", NRC draft report, January 1984.
 11. "A Safety and Regulatory Assessment of Generic BWR and PWR Permanently Shutdown Nuclear Power Plants," NUREG/CR-6451, dated August 1997.
 12. "Predictions of Spent Fuel Heatup After a Complete Loss of Spent Fuel Pool Coolant", NUREG-1726, June 2000
 13. Hermann, et.al., "Technical Support for a Proposed Decay Heat Guide Using SAS2H/ORIGEN-S Data", NUREG/CR-5625, September 1994.
 14. "Compendium of ECCS Research for Realistic LOCA Analysis", NUREG-1230, December 1988.
 15. I. Sheppard et al., "Oxidation Phenomena in Severe Accidents - Final Report," INV-OPSA(99)-P0008, European Commission Joint Research Center, 2000.
 16. Cooper, T. D., "Review of Zirconium-Zircaloy Pyrophoricity, RHO-RE-ST-31P, Rockwell International, November 1984.
 17. Kullen, et. al., " An Assessment of Zirconium Pyrophoricity and Recommendations for Handling Wast Hulls", ANL-77-63, Argonne National Laboratory, November 1977.
 18. Technical Program Group, "Quantifying Reactor Safety Margins, Application of Code Scaling, Applicability, and Uncertainty Evaluation Methodology to a Large Break Loss-of-Coolant Accident," NUREG/CR-5249, December 1989.

RES referencesReferences

- [1] Benjamin, A., et al., "Spent Fuel Heatup Following Loss of Water During Storage", NUREG/CR-0649, SAND77-1371, Sandia National Laboratories, 1979.
- [2] Haste, T., et al., "In-Vessel Core Degradation In LWR Severe Accidents", EUR 16695 EN, 1996.
- [3] Shepherd, I., et al., "Oxidation Phenomena in Severe Accidents- Final Report", INV-OPSA(99)-P0008, EUR 19528 EN, 2000.
- [4] Evans, E., et al., "Critical Role of Nitrogen During High Temperature Scaling of Zirconium", Proc. Symp. Metallurgical Society of AIME, May 1972.
- [5] Fischer, S. and M. Gruebelich, "Theoretical Energy Release of Thermites, Intermetallics, and Combustible Metals", 24th International Pyrotechnics Seminar, July 1998.
- [6] Gauntt, R., et al., "MELCOR Computer Code Manuals Version 1.8.4", NUREG/CR- 6119, SAND97-2398, July 1997.
- [7] Powers, D. et al., " A Review of the Technical Issues of Air Ingression During Severe Accidents", NUREG/CR-6218, SAND-0731, September 1994.
- [8] Letter from H. M. Chung to J. Flack, dated August 24, 2000.

Appendix 2. B

912
8



that the public and the nuclear industry could track the NRC's evaluation and provide comments. In addition, the preliminary risk assessment was subjected to a technical review and requantification by the Idaho National Engineering and Environmental Laboratory (INEEL). The NRC continued to refine its estimates, putting particular emphasis on improving the human reliability assessment (HRA), which is central to the analysis given the long periods required for lowering the water in the spent fuel pool for most initiators. We identified those characteristics that a decommissioning plant and its utility should have to assure that the risks driven by fuel handler error and institutional mistakes are maintained at an acceptable level. In conjunction with our HRA effort and our ongoing reassessment of risk, the nuclear industry through NEI developed a list of commitments (See NEI letter dated November 12, 1999, Appendix 6) that provide boundaries within which the risk assessment's assumptions have been refined. The draft final risk assessment reflects the commitments made by industry, the additional requirements we have developed to ensure the assumptions in the assessment remain valid, the technical review by INEEL, and our ongoing efforts to improve the assessment. The report provides a technical basis for determining the acceptability of exemption requests and future rulemaking on decommissioning plant risk.

In performing the preliminary risk assessment, we chose to look at the broad aspects of the issue. We investigated a wide range of initiators (internal and external events including loss of inventory events, fires, seismic, aircraft, and tornadoes). We modeled a decommissioning plant's spent fuel pool cooling system based on the sled-mounted systems that are used at many current decommissioning plants. We chose one representative spent fuel pool configuration (See Appendix 2a, Figure 2.1) for the evaluation except for seismic events, where the PWR and BWR spent fuel pool designs (i.e., the difference in location of the pools in PWRs and BWRs) were specifically considered. Information about existing decommissioning plants was gathered from decommissioning project managers and during visits to four sites covering all four major nuclear steam supply system vendors (General Electric, Westinghouse, Babcock & Wilcox, and Combustion Engineering). Plant visits gathered information on the as-operated, as-modified spent fuel pools, their cooling systems, and other support systems.

From the perspective of offsite consequences, we only concerned ourselves with the zirconium fire end state, because there has to be an energetic source (e.g., a large high temperature fire) to transport the fission products offsite in order to have potentially significant offsite consequences. We chose the timing of when the spent fuel pool inventory is drained to the top of the spent fuel as a surrogate for onset of the zirconium fire because once the fuel is uncovered, the dose rates at the edge of the pool would be in the tens of thousands of rem per hour, because it is unclear whether hydrides could cause ignition at lower cladding temperatures than previously predicted, and because there was uncertainty in the heat transfer rate as the fuel was uncovered. In addition, from the point of view of estimation of human error rates, since for initiating events (other than seismic and heavy load drop) it would take five or more days to uncover the top of the fuel pool, it was considered of small numerical benefit (and significant analytical effort) if the potential additional two days until the zirconium fire began were added to the timing.

After the preliminary draft risk assessment was released in June 1999, we sent the assessment to INEEL for review and held public meetings and a workshop to assure that our models appropriately accounted for the way decommissioning plants operate today and to help

Formatted Version, Rev. 5 1/22/00 1600 hours

determine if some of the assumptions we made in the preliminary draft risk assessment needed improvement. Following our workshop, NEI provided a list of general commitments (See Appendix 6) that proved very instrumental in refining the assumptions and models in the draft final risk assessment. Working with several PRA experts, we subsequently developed improved HRA estimates for events that lasted for extended periods.

This appendix describes how the risk assessment was performed for beyond design bases internal event accident sequences (i.e., sequences of equipment failures or operator errors that could lead to a zirconium cladding fire and release of radionuclides offsite). We developed event trees and fault trees that model the initiating events and system or component failures that lead to fuel uncovering (these trees are provided in the back of Appendix 2a).

Appendix 2.0 Assessment of Spent Fuel Pool Risk at Decommissioning Plants

Introduction

As the number of decommissioning plants increases, the ability to address regulatory issues generically has become more important. After a nuclear power plant is permanently shut down and the reactor is defueled, most of the accident sequences that normally dominate operating reactor risk are no longer applicable. The predominant source of risk remaining at permanently shut down plants involves accidents associated with spent fuel stored in the spent fuel pool. Previously, requests for relief from regulatory requirements that are less safety significant for decommissioning plants than operating reactors were decided on a plant-specific basis. This is not the best use of resources and led to differing requirements among decommissioning plants. The NRC Commission urged its staff to develop a risk-informed basis for making decisions on exemption requests and to develop a technical basis for rulemaking for decommissioning reactors in the areas of Emergency Preparedness, indemnification, and security. This draft final report is one part of that basis.

Our assessment found that the frequency of spent fuel uncover leading to a zirconium fire at decommissioning spent fuel pools is on the order of 4×10^{-6} per year when a utility follows certain industry commitments and certain of our recommendations. We also determined that if these commitments and recommendations are ignored, the estimated frequency of a zirconium fire could be significantly higher. Appendix ~~ZZZ~~ discusses the steps necessary to assure that a decommissioning plant operates within the bounds assumed in the risk assessment.

Previous NRC-sponsored studies have evaluated some severe accident scenarios for spent fuel pools at operating reactors that involved draining the spent fuel pool of its coolant and shielding water. Because of the significant configuration and staffing differences between operating and decommissioning plants, we performed this assessment to examine the risk associated with decommissioning reactor spent fuel pools.

First, we examined whether or not it was possible from a deterministic view point for a zirconium cladding fire to occur. We chose zirconium fires as the key factor because radionuclides require an energetic source to transport them offsite if they are to have a significant health effect on local (first few miles outside the exclusion area) and more distant populations. Deterministic evaluations (see Appendix 1) indicate that zirconium cladding fires cannot be ruled out for loss of spent fuel pool cooling for fuel that has been shut down and removed from an operating reactor within approximately five years⁷. Our consequence analysis (Appendix 3) indicates that zirconium cladding fires could give offsite doses that the NRC would consider unacceptable. To assess the risk (essentially, "frequency" times "consequences") in the window from final shut down of a reactor to one year following shutdown, we initially performed a broad preliminary risk assessment, which modeled many internal and external initiating events. This assessment was the most comprehensive performed on spent fuel pool risk. The preliminary risk assessment was made publicly available early in the process (June 1999) so

⁷ This estimate can be significantly shorter or perhaps somewhat longer depending on fuel enrichment, fuel burnup, and configuration of the fuel in the spent fuel pool.

Tr. H. Ed. 13 1/2 7/00
S/18

Formatted Version, Rev. 5 1/27/00 1600 hours

Appendix 2.0 Assessment of Spent Fuel Pool Risk at Decommissioning Plants

Introduction

As the number of decommissioning plants increases, the ability to address generically regulatory issues has become more important. After a nuclear power plant is permanently shut down and the reactor is defueled, most of the accident sequences that normally dominate operating reactor risk are no longer applicable. The predominant source of risk remaining at permanently shut down plants involves accidents associated with spent fuel stored in the spent fuel pool. Previously, requests for relief from regulatory requirements that are less safety significant for decommissioning plants than operating reactors were decided on a plant-specific basis. This is not the best use of resources and led to differing requirements among decommissioning plants. The NRC Commission urged its staff to develop a risk-informed basis for making decisions on exemption requests and to develop a technical basis for rulemaking for decommissioning reactors in the areas of emergency preparedness, indemnification, and security. This draft final report is one part of that basis.

The staff's assessment found that the frequency of spent fuel uncover leading to a zirconium fire at decommissioning spent fuel pools is on the order of 3×10^{-6} per year when a utility follows certain industry commitments and certain of our recommendations. This frequency is made up of contributors from a detailed risk assessment of initiators (4.3×10^{-7} per year), both internal and external, and a quasi-probabilistic contribution from seismic events ($< 3 \times 10^{-6}$ per year) that have ground motions many times larger than individual site design basis earthquake ground motions (and higher uncertainty). It was also determined that if these commitments and recommendations are ignored, the estimated frequency of a zirconium fire could be significantly higher. Section 4 of this report discusses the steps necessary to assure that a decommissioning plant operates within the bounds assumed in the risk assessment.

Previous NRC-sponsored studies have evaluated some severe accident scenarios for spent fuel pools at operating reactors that involved draining the spent fuel pool of its coolant and shielding water. Because of the significant configuration and staffing differences between operating and decommissioning plants, the staff performed this assessment to examine the risk associated with decommissioning reactor spent fuel pools.

First, the staff examined whether or not it was possible from a deterministic view point for a zirconium cladding fire to occur. Zirconium fires were chosen as the key factor because radionuclides require an energetic source to transport them off-site if they are to have a significant health effect on local (first few miles outside the exclusion area) and more distant populations. Deterministic evaluations (see Appendix 1) indicate that zirconium cladding fires cannot be ruled out for loss of spent fuel pool cooling for fuel that has been shut down and removed from an operating reactor within approximately five years⁷. The consequence analysis (Appendix 4) indicates that zirconium cladding fires could give off-site doses that the NRC would consider unacceptable. To assess the risk (essentially, "frequency" times

⁷ This estimate can be significantly shorter or perhaps somewhat longer depending on fuel enrichment, fuel burnup, and configuration of the fuel in the spent fuel pool.

“consequences”) during the period of vulnerability to zirconium cladding fires, the staff initially performed a broad preliminary risk assessment, which modeled many internal and external initiating events. This assessment was the most comprehensive performed on spent fuel pool risk. The preliminary risk assessment was made publicly available early in the process (June, 1999) so that the public and the nuclear industry could track the NRCs evaluation and provide comments. In addition, the preliminary risk assessment was subjected to a technical review and requantification by the Idaho National Engineering and Environmental Laboratory (INEEL). The NRC continued to refine its estimates, putting particular emphasis on improving the human reliability assessment (HRA), which is central to the analysis given the long periods required for lowering the water in the spent fuel pool for most initiators. The staff identified those characteristics that a decommissioning plant and its utility should have to assure that the risks driven by fuel handler error and institutional mistakes are maintained at an acceptable level. In conjunction with the staff’s HRA effort and ongoing reassessment of risk, the nuclear industry through NEI developed a list of commitments (See NEI letter dated November 12, 1999, Appendix 6) that provide boundaries within which the risk assessment’s assumptions have been refined. The draft final risk assessment reflects the commitments made by industry, the additional requirements we have developed to ensure the assumptions in the assessment remain valid, the technical review by INEEL, and the staff’s ongoing efforts to improve the assessment. The report provides a technical basis for determining the acceptability of exemption requests and future rulemaking on decommissioning plant risk.

In performing the preliminary risk assessment, the staff chose to look at the broad aspects of the issue. A wide range of initiators (internal and external events including loss of inventory events, fires, seismic, aircraft, and tornadoes). The staff modeled a decommissioning plant’s spent fuel pool cooling system based on the sled-mounted systems that are used at many current decommissioning plants. One representative spent fuel pool configuration (See Appendix 2a, Figure 2.1) was chosen for the evaluation except for seismic events, where the PWR and BWR spent fuel pool designs (i.e., the difference in location of the pools in PWRs and BWRs) were specifically considered. Information about existing decommissioning plants was gathered from decommissioning project managers and during visits to four sites covering all four major nuclear steam supply system vendors (General Electric, Westinghouse, Babcock & Wilcox, and Combustion Engineering). Plant visits gathered information on the as-operated, as-modified spent fuel pools, their cooling systems, and other support systems.

From the perspective of off-site consequences, the staff only concerned itself with the zirconium fire end state, because there has to be an energetic source (e.g., a large high temperature fire) to transport the fission products off-site in order to have potentially significant off-site consequences. The staff chose the timing of when the spent fuel pool inventory is drained to the top of the spent fuel as a surrogate for onset of the zirconium fire because once the fuel is uncovered, the dose rates at the edge of the pool would be in the tens of thousands of rem per hour, because it is unclear whether hydrides could cause ignition at lower cladding temperatures than previously predicted, and because there was uncertainty in the heat transfer rate as the fuel was uncovered. In addition, from the point of view of estimation of human error rates, since for initiating events (other than seismic and heavy load drop) it would take five or more days to uncover the top of the fuel pool, it was considered of small numerical benefit (and significant analytical effort) if the potential additional two days until the zirconium fire began were added to the timing.

After the preliminary draft risk assessment was released in June, 1999, the staff sent the assessment to INEEL for review and held public meetings and a workshop to assure that models appropriately accounted for the way decommissioning plants operate today and to help determine if some of the assumptions we made in the preliminary draft risk assessment needed improvement. Following a workshop, NEI provided a list of general commitments (See Appendix 6) that proved very instrumental in refining the assumptions and models in the draft final risk assessment. Working with several PRA experts, the staff subsequently developed improved HRA estimates for events that lasted for extended periods.

This appendix describes how the risk assessment was performed for beyond design bases internal event accident sequences (i.e., sequences of equipment failures or operator errors that could lead to a zirconium cladding fire and release of radionuclides off-site). Event trees and fault trees were developed that model the initiating events and system or component failures that lead to fuel uncover (these trees are provided in the back of Appendix 2a).

that the public and the nuclear industry could track the NRC's evaluation and provide comments. In addition, the preliminary risk assessment was subjected to a technical review and requantification by the Idaho National Engineering and Environmental Laboratory (INEEL). The NRC continued to refine its estimates, putting particular emphasis on improving the human reliability assessment (HRA), which is central to the analysis given the long periods required for lowering the water in the spent fuel pool for most initiators. We identified those characteristics that a decommissioning plant and its utility should have to assure that the risks driven by fuel handler error and institutional mistakes are maintained at an acceptable level. In conjunction with our HRA effort and our ongoing reassessment of risk, the nuclear industry through NEI developed a list of commitments (See NEI letter dated November 12, 1999) that provide boundaries within which the risk assessment's assumptions have been refined. The draft final risk assessment reflects the commitments made by industry, the technical review by INEEL, and our ongoing efforts to improve the assessment. The report provides a technical basis for determining the acceptability of exemption requests and future rule making on decommissioning plant risk.

In performing the preliminary risk assessment, we chose to look at the broad aspects of the issue. We investigated a wide range of initiators (internal and external events including loss of inventory events, fires, seismic, aircraft, and tornadoes). We modeled a decommissioning plant's spent fuel pool cooling system based on the sled-mounted systems that are used at many current decommissioning plants. We chose one representative spent fuel pool configuration (See Figure 2.0-1) for the evaluation except for seismic events, where the PWR and BWR spent fuel pool designs (i.e., the difference in location of the pools in PWRs and BWRs) were specifically considered. Information about existing decommissioning plants was gathered by decommissioning project managers and during visits to four sites covering all four major nuclear steam supply system vendors (General Electric, Westinghouse, Babcock & Wilcox, and Combustion Engineering). Plant visits gathered information on the as-operated, as-modified spent fuel pools, their cooling systems, and other support systems.

From the perspective of offsite consequences, we only concerned ourselves with the zirconium fire end state, because there has to be an energetic source (e.g., a large high temperature fire) to transport the fission products offsite in order to have potentially significant offsite consequences. We chose the timing of when the spent fuel pool inventory is drained to the top of the spent fuel as a surrogate for onset of the zirconium fire because once the fuel is uncovered, the dose rates at the edge of the pool would be in the tens of thousands of rem per hour, because it is unclear whether hydrides could cause ignition at lower cladding temperatures than previously predicted, and because there was uncertainty in the heat transfer rate as the fuel was uncovered. In addition, from the point of view of estimation of human error rates, since for initiating events (other than seismic and heavy load drop) it would take five or more days to uncover the top of the fuel pool, it was considered of small numerical benefit (and significant analytical effort) if the potential additional two days until the zirconium fire began were added to the timing.

After the preliminary draft risk assessment was released in June 1999, we sent the assessment to INEEL for review and held public meetings and a workshop to assure that our models appropriately accounted for the way decommissioning plants operate today and to help determine if some of the assumptions we made in the preliminary draft risk assessment needed

improvement. Following our workshop, NEI provided a list of general commitments (See November 12, 1999 letter) that proved very instrumental in refining the assumptions and models in the draft final risk assessment. Working with several PRA experts, we subsequently developed improved HRA estimates for events that lasted for extended periods. We developed a basis (see Section YYY) for helping to assure that the HRA values we used in our improved HRA analysis come true at decommissioning plants in the future.

SectionXX describes how the risk assessment was performed for beyond design bases internal event accident sequences (i.e., sequences of equipment failures or operator errors that could lead to a zirconium cladding fire and release of radionuclides offsite). We developed event trees and fault trees that model the initiating events and system or component failures that lead to fuel uncover (these trees are provided in Appendix XXX). Table 2A.1-1 lists the internal and external initiating events⁸ found to be potentially important by qualitative screening processes in the above references. The table identifies the source of each frequency estimate (they are generic and not plant-specific). Our estimates of conditional failure probabilities of mitigating systems and components (both active and passive) are given in Table 2A.1-2. Table 2A.1-3 summarizes the calculations of frequency of fuel uncover for all initiators analyzed. Section 3.2 discusses beyond design bases external event accident sequences. Section 3.3 provides the working group's insights from this final risk evaluation.

The risk from sabotage is not normally evaluated in a PRA, in part because such acts cannot be easily analyzed analytically. We have identified to the NRC safeguards staff the structures, systems, components, industry commitments, and staff requirements that are most important in helping assure that the spent fuel pools do not represent an undue risk to the public. The safeguards staff will use this information to assist them in making decisions on the degree, location, and type of safeguards necessary to protect the public safety at decommissioning plant spent fuel pools.

2a. Detailed Assessment of Risk from Decommissioning Plant Spent Fuel Pools

⁸ Internal initiating events are events that begin within the confines of the nuclear power plant and cause plant disruption. Two examples are inadvertent closure of the spent fuel pool cooling system suction valves and a pipe break in the spent fuel pool cooling system. External events are those events that begin outside the confines of the nuclear power plant. Two examples are seismic events and hurricanes. There are a few events that begin inside plants, such as internal floods and fires, that have been characterized in some PRAs as external events.

264 # 918

Appendix 2a

2/1/00
11:00 a.
AK

Formatted Version, Rev. 5 2/1/00 1100 hours

Appendix 2a Detailed Assessment of Risk from Decommissioning Plant Spent Fuel Pools

1.0 Introduction

In reference 1, the NRC performed a preliminary study of spent fuel pool risk at decommissioning plants to: examine the full scope of potentially risk-significant issues; identify credible accident scenarios; document the assessment for public review; and to elicit feedback from all stakeholders regarding analysis assumptions and design and operational features expected at decommissioning plants. In this current analysis, Ref. 1 was updated based on:

- stakeholder feedback on the original analysis
- NEI commitments as documented in Ref. 2
- a revised human reliability analysis (HRA) approach
- peer review of the technical analysis by the Idaho National Engineering and Environmental Laboratory (INEEL).

This updated PRA, performed by a combination of INEEL and NRC staff, addresses the following initiating events:

- loss of spent fuel pool cooling
- fire leading to loss of spent fuel pool cooling
- loss of off-site power due to plant centered and grid related causes
- loss of off-site power due to severe weather
- non-catastrophic loss of spent fuel pool inventory

Those low frequency events such as earthquakes, aircraft crashes, heavy load drops, and tornado strikes that could lead to catastrophic pool failure are dealt with elsewhere. The analysis is based on the following input. The assumed system configuration is typical of the sled-mounted systems that are used at many current decommissioned plants. Information about existing decommissioned plants was gathered by decommissioning project managers (NRC Staff) during visits to four sites covering all four major nuclear steam supply system vendors (General Electric, Westinghouse, Babcock & Wilcox, and Combustion Engineering). The assumptions made about the operation of the facility are based in part on a set of commitments made by NEI (Ref. 2), supplemented by an interpretation of how some of those commitments might be applied.

2.0 System Description

Figure 2.1 is a simplified drawing of the system assumed for the development of the model. The spent fuel pool cooling (SFPC) system is located in the SFP area and consists of

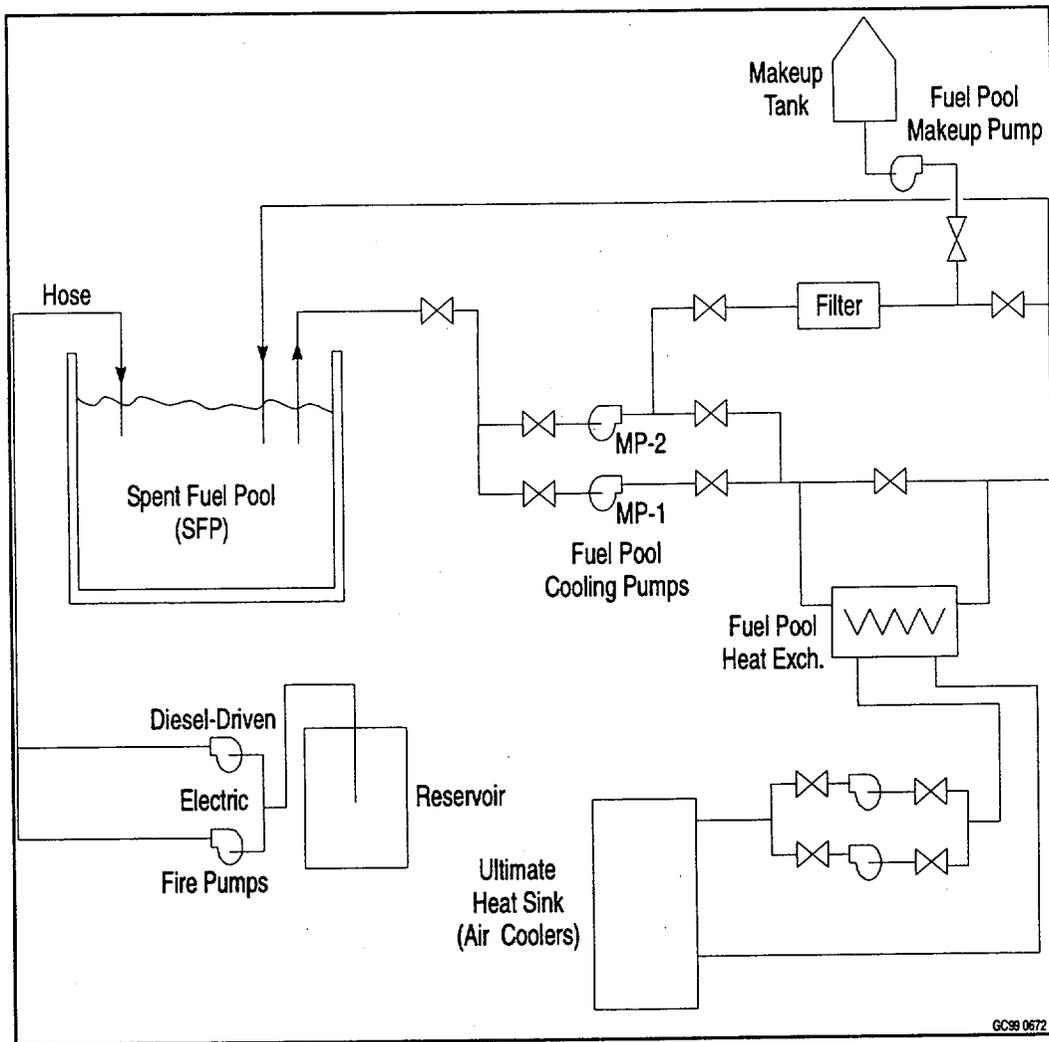


Figure 2.1 Simplified Diagram of Spent Fuel Pool Cooling and Inventory Makeup Systems

motor-driven pumps, a heat exchanger, an ultimate heat sink, a makeup tank, filtration system and isolation valves. Suction is taken via one of the two pumps on the primary side from the spent fuel pool and is passed through the heat exchanger and returned back to the pool. One of the two pumps on the secondary side rejects the heat to the ultimate heat sink. A small amount of water from the suction line is diverted to the filtration process and is returned to the discharge line. A regular makeup system supplements the small losses due to evaporation. In the case of prolonged loss of SFPC system or loss of inventory events, the inventory in the pool can be made up using the firewater system. There are two firewater pumps, a motor-driven (electric) and a diesel-driven, which provide firewater throughout the plant. A firewater hose station is provided in the SFP area. The firewater pumps are located in a separate structure.

3.0 Methodology

3.1 Logic Model

This section summarizes the spent fuel pool PRA model developed in this study. The description of the modeling approach and key assumptions is intended to provide a basis for interpreting the results in Sections 4 and 5. The detailed model documentation is provided in Attachments A and B. The event trees and fault trees presented in this report are meant to be generic enough to apply to many different configurations.

The endstate for this analysis is defined as loss of coolant inventory to the point of fuel uncover from either leakage or boil-off. Dose calculations (Ref. 3) show that less than 3 feet of water above the top of the fuel results in an environment that is rapidly lethal to anyone at the edge of the pool. For accident scenarios in which coolant inventory level has dropped to less than 3 feet above the top of fuel, recovery may require operators to approach the pool. Therefore, 3 feet has been adopted as an effective limit for recovery purposes. In other words, the endstate for this analysis is effectively defined as loss of coolant inventory to a point 3 feet above the top of the fuel. One of the NEI commitments is that there should be a provision for remote alignment of the makeup source to the pool, which would make this assumption conservative. However, the impact of this conservatism on the conclusions of this analysis is minor.

The event tree and fault tree models were developed and quantified using Version 6 of the SAPHIRE software package (Ref. 4), using a fault tree linking approach. Event trees were developed for each of the initiators identified in Section 1.

3.2 HRA Methodology

3.2.1 Introduction

One of the key issues in performing a probabilistic risk assessment (PRA) for the spent fuel pool during the decommissioning phase of a nuclear power plant's lifecycle is how much credit can be given to the operating staff to respond to an incident that impacts the spent fuel pool that would, if not attended to, lead to a loss of cooling of the spent fuel and eventually to a zirconium fire.

The objective of the HRA analysis in this PRA is to assess whether the design features and operational practices assumed can be argued to suggest that the non-response probabilities should

be low. The design features include the physical plant characteristics (e.g., nature and number of alarms, available mitigation equipment) and the operational practices include operational and management practices (including crew structure and individual responsibilities), procedures, contingency plans, and training. Since the details will vary from plant to plant, the focus is on general features and operational practices that can support low non-response probabilities.

Section 3.2.2 discusses the differences between the full power and decommissioning modes of operation as they impact human reliability analysis, and the issues that need to be addressed in the analysis of the decommissioning mode are identified. Section 3.2.3 discusses the factors that recent studies have shown to be significant in establishing adequacy of human performance.

3.2.2 Analysis Approach

The human reliability analysis (HRA) approaches that have been developed over the past few years have primarily been for use in PRAs of nuclear power plants at full power. Methods have been developed for assessing the likelihood of errors associated with routine processes such as restoration of systems to operation following maintenance, and those errors in responding to plant transients or accidents from full power. For spent fuel pool operation during the decommissioning phase, there are unique conditions not typical of those found during full-power operation. Thus the human reliability methods developed for full power operation PRAs, and their associated error probabilities, are not directly applicable. However, some of the methods can be adapted to provide insights into the likelihood of failures in operator performance for the spent fuel pool analysis by accommodating the differences in conditions that might impact operating crew performance in the full power and decommissioning phases. There are both positive and negative aspects of the difference in conditions with respect to the reliability of human performance.

Examples of the positive aspects are:

- For most scenarios, the time-scale for changes to plant condition to become significant are protracted. This is in contrast to full power transients or accidents in which response is required in a relatively short time, ranging from a few minutes to a few hours. In the staff's analysis, times ranging from 50 to greater than 120 hours were estimated for heat up and boil off following loss of spent fuel pool cooling. Thus, there are many opportunities for different plant personnel to recognize off-normal conditions, and a long time to take corrective action, such as making repairs, hooking up alternate cooling or inventory make-up systems, or even bringing in help from off site.
- There is only one function to be maintained, namely decay heat removal, and the systems available to perform this function are relatively simple. By contrast, in the full power case there are several functions that have to be maintained, including criticality, pressure control, heat removal, containment integrity.
- With respect to the last point, it is also expected that the number of controls and indications that are required in the control room are considerably fewer than for an operating plant, and therefore, there is less cause for confusion or distraction.

Examples of the negative aspects are:

- The plant operation is not as constrained by regulatory tools (technical specifications are not as comprehensive and restrictive as they are for operating plants), and there is no requirement for emergency procedures.
- Because the back-up systems are not automatically initiated, operator action is essential to successful response to failures of the cooling function.
- There is expected to be little or no redundancy in the on-site mitigating capability as compared with the operating plant mode of operation. (In the staff's initial evaluation, because little redundant on-site equipment was assumed to be available, the failure to bring on off-site equipment was one of the most important contributors.) This implies that repair of failed functions is relatively more significant in the risk analysis for the spent fuel pool case.

In choosing an approach for developing the estimates documented in this report, the following issues were considered to be important:

- Due to the long time scales, it is essential to address the potential for recovery of failures on the part of one crew or individual by other plant staff, including subsequent shifts.
- Potential sources of dependency that could lead to a failure of the organization as a whole to respond adequately should be taken into account.
- The approach should be consistent with current understanding of human performance issues (see for example, Refs. 5, 6, and 7).
- Those factors that the industry has suggested that will help ensure adequate response (instrumentation, monitoring strategies, procedures, contingency plans) should be addressed (Ref. 2).
- Where possible, any evaluations of human error probabilities (HEPs) should be calibrated against currently acceptable ranges for HEPs.
- The reasoning behind the assumptions made should be transparent.

3.2.3 Human Performance Issues

In order to be successful in coping with an incident at the facility, there are three basic functions that are required of the operating staff, and these are either explicit (awareness) or implicit (situation assessment and response planning and response implementation) in the definitions of the human failure events in the PRA model.

- Plant personnel must be able to detect and recognize when the spent fuel cooling function is deteriorating or pool inventory is being lost (Awareness).
- Plant personnel must be able to interpret the indications (identify the source of the

- problem) and formulate a plan that would mitigate the situation (Situation Assessment and Response Planning).
- Plant personnel must be able to perform the actions required to maintain cooling of and/or add water to the spent fuel pool (Response Implementation).

In the following sections, factors that are relevant to determining effective operator responses are discussed. While not minimizing the importance of such factors as the establishment of a safety culture and effective intra-crew communication, the focus is on factors which can be determined to be present on a relatively objective basis. A review of LERs associated with human performance problems involved in response to loss of fuel pool cooling revealed a variety of contributing factors, including crew inexperience, poor communication, and inadequate administrative controls. In addition, there were some instances of design peculiarities that made operator response more complex than necessary.

The factors discussed below were used to identify additional assumptions made in the analysis that the staff considered would provide for an effective implementation of the NEI commitments.

3.2.3.1 Awareness/Detection of Deviant Conditions

There are two types of monitoring that can be expected to be used in alerting the plant staff to deviant conditions: a) passive monitoring in which alarms and annunciators are used to alert operators; b) active monitoring in which operators, on a routine basis, make observations to detect off-normal behavior. In practice both would probably be used to some extent. The amount of credit that can be assumed depends on the detailed design and application of the monitoring scheme.

In assessing the effectiveness of alarms there are several factors that could be taken into account, for example:

- alarms (including control room indications) are maintained and checked/calibrated on a regular basis
- the instruments that activate instruments and alarms measure, as directly as possible, the parameters they purport to measure
- alarm set-point is not too sensitive, so that there are few false alarms
- alarms cannot be permanently canceled without taking action to clear the signal
- alarms have multiple set-points corresponding to increasing degradation
- the importance of responding to the alarms is stressed in plant operating procedures and training
- the existence of independent alarms that measure different primary parameters (e.g., level, temperature, airborne radiation), or provide indirect evidence (sump pump alarms, secondary side cooling system trouble alarms)

Formatted Version, Rev. 5 2/1/00 1100 hours

The first and last of these factors may be reflected in the reliability assumed for the alarm and in the structure of the logic model (fault tree) for the event tree function control room alarms (CRA), respectively. The other factors may be taken into account in assessing the reliability of the operator response.

For active monitoring, examples of the factors used in assessing the effectiveness of the monitoring include:

- scheduled walk-downs required within areas of concern, with specific items to check (particularly to look for indications not annunciated in, or monitored from, the control room, for example, indications of leakage, operation of sump pumps if not monitored, steaming over the pool, humidity level)
- plant operating procedures that require the active measurement of parameters (e.g., temperature, level) rather than simply observing the condition of the pool
- requirement to log, check, and trend results of monitoring
- alert levels specified and noted on measurement devices

These factors can all be regarded as performance shaping factors (PSFs) that affect the reliability of the operators.

An important factor that should mitigate against not noticing a deteriorating condition is the time scale of development, which allows the opportunity for several shifts to notice the problem. The requirement for a formal shift turnover meeting should be considered.

3.2.3.2 Situation Assessment and Response Planning

The principal operator aids for situation assessment and response planning are procedures and training in their use.

The types of procedures that might be available are:

- annunciator/alarm response procedure that is explicit in pointing towards potential problems
- detailed procedures for use of alternate systems indicating primary and back up sources, recovery of power, etc..

The response procedures may have features that enhance the likelihood of success, for example:

- guidance for early action to establish contingency plans (e.g., alerting off-site agencies such as fire brigades) in parallel with a primary response such as carrying out repairs or lining up an on-site alternate system.
- clearly and unambiguously written, with an understanding of a variety of different scenarios and their timing.

In addition:

- training for plant staff to provide an awareness of the time scales of heat up to boiling and fuel uncovering as a function of the age of the fuel would enhance the likelihood of successful response.

3.2.3.3 Response Implementation

Successful implementation of planned responses may be influenced by several factors, for example:

- accessibility/availability of equipment
- staffing levels that are adequate for conducting each task and any parallel contingency plans, or plans to bring in additional staff
- training
- timely feedback on corrective action

3.2.4 Quantification Method

Three quantification methods were applied, and each is briefly described below.

- The Technique for Human Error Prediction (THERP, Ref. 8). This method was used to quantify the initial recognition of the problem. Specifically, the annunciator response model (Table 20-23) was used for response to alarms. The THERP approach was also used to assess the likelihood of failure to detect a deviant condition during a walk-down, and also the failure to respond to a fire.
- The Exponential Repair Model (while not strictly a human reliability model) was applied to calculate the probability of failure associated with the repair of systems and components in this analysis. This method is described in the main body of the report. In cases where dependency exists with prior repair tasks, the dependency model used in THERP was used to assess the impact of that dependency.
- The Simplified Plant Analysis Risk Human Error Analysis Method (SPAR HRA, Ref. 9) was employed for all other HEPs. This method separately evaluates the diagnosis or response planning errors and the execution errors.

3.3 Other Inputs to the Risk Model

A variety of other inputs were required for this PRA, including generic configuration data used in the fault tree models, radiological calculations, and timing calculations. Initiating event frequencies and generic reliability data, were derived from other studies sponsored by the NRC. The times available for operator actions are based on calculations of the time it would take for bulk boiling to begin in the pool, or on the time it takes for the level in the pool to fall to the level of the fuel pool

cooling system suction, or to a height of approximately 3 ft above the fuel, as appropriate to the definition of the corresponding human failure event.

It takes a relatively long time to uncover the fuel if inventory is lost in this manner due to the large amount of water in a spent fuel pool, the large specific heat of water, and the large latent heat of vaporization for water. Simple calculations for a typical-sized spent fuel pool yield the results in Table 3.1. These results are based on the following assumptions:

- no heat losses
- atmospheric pressure
- Heat of vaporization $h_{fg} \approx 2258$ kJ/kg
- base pool heat load for a full pool of 2 MW
- core thermal power of 3293 MW
- typical pool size (based on Tables 2.1 and 2.2 of NUREG/CR-4982, Ref. 10)
 - typical BWR pool is 40' deep by 26' by 39'
 - typical PWR pool is 43' deep by 22' by 40'

Table 3.1 Time to Bulk Boiling, and Boil-off Rates

Time after discharge (days)	Decay power from last core (MW)	Total heat load (MW)	Time to bulk boiling (hr)	Boil-off rate (gpm)	Level decrease (ft/hr) ¹
2	16.4	18.4	5.6	130	1.0
10	8.6	10.6	9.8	74	0.6
30	5.5	7.5	14	52	0.42
60	3.8	5.8	18	41	0.33
90	3.0	5.0	21	35	0.28
180	1.9	3.9	27	27	0.22
365	1.1	3.1	33	22	0.18 ~ 0.2

Notes: (1) using typical pool sizes, it is estimated that for BWRs, we have 1040 ft³/ft depth, and for PWRs, we have 957 ft³/ft depth. Assume ≈ 1000 ft³/ft depth for level decreases resulting from boil-off.

In a SFP, the depth of water above the fuel is typically 23 to 25 feet. Subtracting 3 feet to account for shielding requirements, it is estimated that approximately 20 feet of water will have to boil-off before the start of fuel uncovering. Therefore, using the above table, the available time for operator actions for the loss of cooling type accidents is estimated as follows:

For one-year-old fuel, the total time available equals the time to bulk boiling plus the time to boil-down to 3 ft above the top of the fuel. Therefore, the total time available for operator action is as follows:

$$\begin{aligned} \text{Total Time} &= 33 \text{ hr} + (20 \text{ ft}) / (0.2 \text{ ft/hr}) \\ &= 133 \text{ hours} \end{aligned}$$

It is assumed that the operator will not use alternate systems (e.g., firewater) until after bulk boiling begins and the level drops to below the suction of the cooling system. It is assumed that the

suction of the cooling system is 2 ft below the nominal pool level. Therefore, if bulk boiling begins at 33 hours, and the boil-off rate is 0.2 ft/hr, then the total time available to provide makeup using the firewater system to prevent fuel uncovering is as follows:

$$133 \text{ hrs} - (\text{Time to Bulk Boiling} + \text{Time for Boil-off}) = 133 - \left(33 \text{ hrs} + \frac{2 \text{ ft}}{0.2 \text{ ft/hr}}\right) = 133 - 43 \text{ hrs} = 90 \text{ hrs}$$

3.4 General Assumptions

This analysis is based on the assumption that the commitments for procedures and equipment proposed by NEI in their November 12, 1999 letter to Richard J. Barrett (Ref. 2) are adopted. These are reproduced below:

1. Cask drop analyses will be performed or single failure proof cranes will be in use for handling of heavy loads, (i.e., phase II of NUREG 0612 (Ref. 11) will be implemented).
2. Procedures and training of personnel will be in place to ensure that on site and off site resources can be brought to bear during an event.
3. Procedures will be in place to establish communication between on site and off site organizations during severe weather and seismic events.
4. An off site resource plan will be developed which will include access to portable pumps and emergency power to supplement on site resources. The plan would principally identify organizations or suppliers where off site resources could be obtained in a timely manner.
5. Spent fuel pool instrumentation will include readouts and alarms in the control room (or where personnel are stationed) for spent fuel pool temperature, water level, and area radiation levels.
6. Spent fuel pool boundary seals that could cause leakage leading to fuel uncovering in the event of seal failure shall be self limiting to leakage or otherwise engineered so that drainage cannot occur.
7. Procedures or administrative controls to reduce the likelihood of rapid drain down events will include (1) prohibitions on the use of pumps that lack adequate siphon protection; or (2) controls for pump suction and discharge points. The functionality of anti-siphon devices will be periodically verified.
8. An on site restoration plan will be in place to provide for repair of the spent fuel pool cooling systems or to provide access for makeup water to the spent fuel pool. The plan will provide for remote alignment of the makeup source to the spent fuel pool without requiring entry to the refuel floor.

9. Procedures will be in place to control spent fuel pool operations that have the potential to rapidly decrease spent fuel pool inventory. These administrative controls may require additional operations or administrative limitations such as restrictions on heavy load movements.
10. Routine testing of the alternative fuel pool makeup system components will be performed and administrative controls for equipment out of service will be implemented to provide added assurance that the components would be available if needed.

Since the commitments are stated at a relatively high level, additional assumptions have been made as detailed below.

- It is assumed that the operators (through procedures and training) are aware of the available backup sources that can be used to replenish the SFP inventory (i.e., the fire protection pumps, or off-site sources such as from fire engines). Arrangements have been made in advance with fire stations including what is required from the fire department including equipment and tasks.
- The site has two operable firewater pumps, one diesel-driven and one electrically driven from off-site power.
- The makeup capability (with respect to volumetric flow) is assumed as follows:

Make-up pump:	20 - 30 gpm
Firewater pump:	100 - 200 gpm
Fire engine:	100 - 250 gpm [depending on hose size: 1-½" (100 gpm) or 2-½" (250 gpm)]
- It is therefore assumed that, for the larger loss of coolant inventory accidents, makeup through the makeup pumps is not feasible unless the source of inventory loss can be isolated.
- The operators perform walk-downs of the SFP area once per shift (8- to 12-hour shifts). A different crew member is assumed for the next shift. It is also assumed that the SFP water is clear and pool level is observable via a measuring stick in the pool that can alert operators to level changes.
- Requirements for fire detection and suppression may be reduced (when compared to those for an operating plant) and it is assumed that automatic detection and suppression capability may not be present.
- All equipment, including external sources (fire department), are available and in good working order.
- The emergency diesel generators and support systems such as residual heat removal and service water (that could provide SFP cooling or makeup prior to the plant being decommissioned) have been removed from service.

Formatted Version, Rev. 5 2/1/00 1100 hours

- The SFP cooling system, its support systems, and the electric driven fire protection pump are fed off the same electrical bus.
- Procedures exist to mitigate small leaks from the SFP or for loss of the SFP cooling system.
- The only significant technical specification applicable to SFPs is the requirement for radiation monitors to be operable when fuel is being moved. There are no technical specifications requirements for the cooling pumps, makeup pumps, firewater pumps, or any of the support systems.
- Generic industry data was used for initiating event frequencies for the loss of off-site power, the loss of pool cooling, and the loss of coolant inventory.
- For the purposes of timing, the transfer of the last fuel from the reactor to the SFP is assumed to have occurred one year previously.

4.0 Model Development

This section describes the risk models that were developed to assess the likelihood of core uncover from spent fuel pool loss of cooling events, fire events, loss of off-site power, loss of inventory events.

4.1 Loss of Cooling Event Tree

This event tree (Figure 4.1) models generic loss of cooling events (i.e., those not related to other causes such as fire or loss of power, which are modeled in later sections). The top events and the supporting functional fault trees are discussed in the following sections.

4.1.1 Initiating Event LOC – Loss of Cooling

4.1.1.1 Event Description

This initiating event includes conditions arising from loss of coolant system flow due to the failure of the operating pumps or valves, from piping failures, from an ineffective heat sink (e.g., loss of heat exchangers), or from a local loss of power (e.g., failure of electrical connections).

4.1.1.2 Quantification

This initiating event is modeled by a single basic event, IE-LOC. An initiation frequency of $3.0E-3/\text{yr}$ is taken from NUREG-1275 Volume 12 (Ref. 12). This represents the frequency of loss of cooling events in which temperatures rise more than 20°F.

4.1.2 Top Event CRA – Control Room Alarms

4.1.2.1 Event Description and Timing

This event represents a failure to respond to conditions in the pool that are sufficient to trigger an alarm. Failure could be due to operator error (failure to respond), or loss of indication due to equipment faults. Success for this event is defined as the operator recognizing the alarm and understanding the need to investigate its cause. This event is quantified by fault tree LOC-CRA and includes hardware and human failures basic events that represent failure of control room instrumentation to alarm given that SFP cooling has been lost, and the operators fail to respond to the alarm, respectively.

4.1.2.2 Relevant Assumptions

- Within 8 to 12 hours of the loss of cooling, one or more alarms or indications will reflect an out-of-tolerance condition to the operators in the control room (there may be level indication available locally or remotely, but any change in level is not likely to be significant until later in the sequence of events).
- The SFP has at least one water temperature measuring device, with an alarm and a readout in the control room (NEI commitment no. 5). There could also be indications or alarms associated with pump flow and pressure, but no credit is taken here.
- The instrumentation is tested on a routine basis and maintained operable.
- Procedures are available to guide the operators in their response to off-normal conditions, and the operators are trained on the use of these procedures (NEI commitment no. 2).

4.1.2.3 Quantification

Human Error Probabilities

The basic event HEP-DIAG-ALARM models operator failure to respond to an indication in the control room and diagnose a loss of cooling event. Such an alarm would likely be the first indication of trouble, so the operator would not be under any heightened state of alertness. On the other hand, it is not likely that any other signals or alarms for any other conditions would be present to distract the operator. The error rate is taken from THERP (Table 20-23).

Hardware Failure Probabilities

The value used for local faults leading to alarm channel failure (event SPC-LVL-LOF, 2.0E-3) was estimated based on information in reference 11. This event includes failure of instrumentation and local electrical faults.

4.1.2.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-DIAG-ALARM	3.0E-4
SPC-LVL-LOF	2.0E-3

4.1.3 Top Event IND – Other Indications of Loss of Cooling

4.1.3.1 Event Description and Timing

This top event models subsequent operator failures to recognize the loss of cooling during walkdowns over multiple shifts. Indications available to the operators include: temperature readouts in the control room (NEI commitment no. 5), local temperature measurements, and eventually, increasing area temperature and humidity, low water level from boil-off, and local alarms. Success for this event is defined as the operator recognizing the abnormal condition and understanding the need to investigate its cause, leaving sufficient time to attempt to correct the problem before the pool level drops below the spent fuel pool cooling system suction. The event is modeled by fault tree LOC-IND.

4.1.3.2 Relevant Assumptions

- The loss of cooling may not be noticeable during the first two shifts but conditions are assumed to be sufficient to trigger high temperature alarms locally and in the control room.
- Operators perform walk-downs and control room readouts once per shift (every 8 to 12 hours) and document observations in a log.
- Regular test and maintenance is performed on instrumentation (NEI commitment no. 10).
- During walk-downs, level changes in the SFP can be observed on a large, graduated level indicator in the pool.
- Procedures are available to guide the operators on response to off-normal conditions, and the operators are trained on the use of these procedures (NEI commitment no. 2)

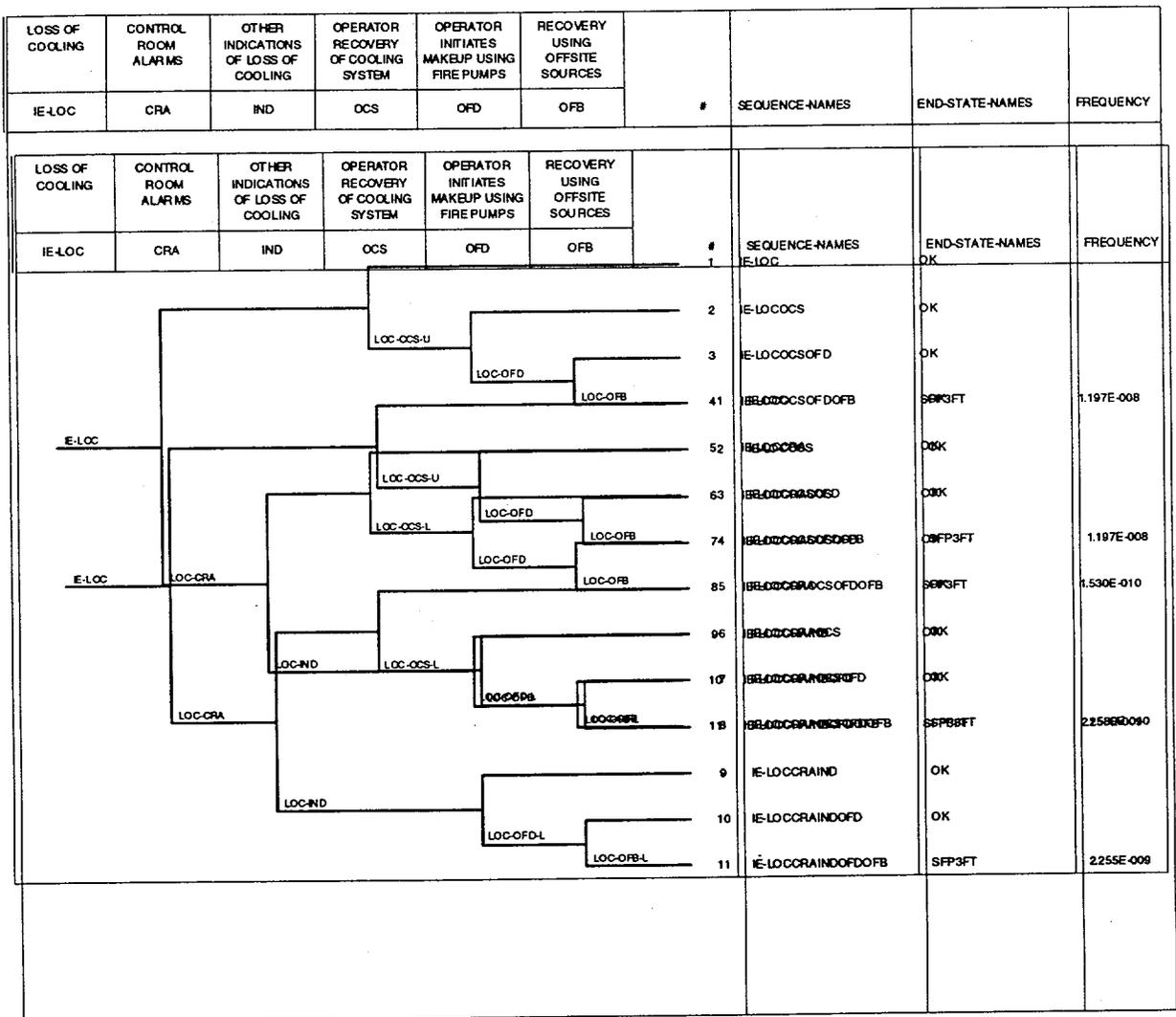


Figure 4.1 Loss of spent fuel pool cooling system event tree

4.1.3.3 Quantification

Human Error Probabilities

The functional fault trees include two human failure events, depending on whether the control room alarms have failed, or whether there was a failure to respond to the initial alarm (it is assumed that the alarm was canceled). If the operator failed to respond to control room alarms, then event HEP-WLKDOWN-DEPEN models subsequent operating crews' failures to recognize the loss of cooling during walk-downs, taking into account the dependence on event HEP-DIAG-ALARM. A specific mechanism for dependence can only be identified on a plant and event specific basis, but could result, for example, from an organizational failure that leads to poor adherence to plant procedures. Because this is considered unlikely, and because the conditions in the pool area change significantly over the time scale defined by the success criterion for this event, the degree of dependence is assumed to be low.

If the alarms failed, then event HEP-WLKDOWN-LSFPC models subsequent crews' failures to recognize the loss of cooling during walk-downs, with no dependence on previous HEPs. However, because the control room readouts could share a dependency with the alarms, the assumption of local temperature measurements becomes important. The failure probabilities for these events were developed using THERP, and are based upon three individual failures: failure to carry out an inspection, missing a step in a written procedure, and misreading a measuring device. Because there are on the order of 33 - 43 hours before the spent fuel pool cooling system becomes irrecoverable without pool make-up, it is assumed that multiple crews would have to fail. However, the probability is truncated at 1E-05.

4.1.3.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-WLKDOWN-LSFPC	1.0E-5
HEP-WLKDOWN-DEPEN	5.0E-2

4.1.4 Top Event OCS – Operator Recovery of Cooling System

4.1.4.1 Event Description and Timing

Once the operators recognize loss of spent fuel pool cooling, they will likely focus their attention on recovery of the SFP cooling system. It is assumed that only after bulk boiling begins and the water level drops below the cooling system suction that the operator will inject water from other makeup systems (e.g., firewater). Therefore, the time available to recover the SFP cooling system could be as long as 43 hours, given an immediate response to an alarm. However, it has assumed that the operating staff has only until shortly after bulk boiling begins (assumed to be 33 hours) to restore the SFP cooling system. This assumption is based on concerns about volume reduction due to cooling and whether the makeup system capacity is sufficient to overcome that volume reduction.

The initial cause of the loss of cooling could be the failure of a running pump in either the primary or the secondary system, in which case the response required is simply to start the

redundant pump. However, it could also be a more significant failure, such as a pipe break or a heat exchanger blockage. To simplify the model, it has been assumed that a repair is necessary. While this is conservative, it is not considered that this unduly biases the conclusions of the overall study.

If the loss of cooling was detected via the control room alarms, the staff has the full 33 hours in which to repair the system. Assuming that it takes at least 16 hours before parts and technical help arrive, then the operator has 17 hours (33 hours less 16 hours) to repair the system. Failure to repair the SFPC system event is modeled as HEP-COOL-REP-E. This case is modeled by fault tree LOC-OCS-U.

If the loss of cooling was discovered during walkdowns, it has been conservatively assumed the operator has only 9 hours available (allowing 24 hours before loss of cooling was noticed). Since it is assumed that it takes at least 16 hours before technical help and parts arrive, it is not possible that the SFPC system can be repaired before the bulk boiling would begin. Failure to repair the SFPC system event is modeled as HEP-COOL-REP-L. This case is modeled by fault tree LOC-OCS-L.

4.1.4.2 Relevant Assumptions

- The operators will avoid using raw water (e.g., water not chemically controlled) if possible. Therefore, the operators are assumed to focus solely on restoration of the SFP cooling system in the initial stages of the event.
- If the loss of cooling was detected through shift walk-downs, then 24 hours are (conservatively) assumed to have passed before discovery.
- It takes 16 hours to contact maintenance personnel, diagnose the cause of failure, and get new parts.
- Mean time to repair the SFP cooling system is 10 hours.
- Operating staff has received formal training and there are administrative procedures to guide them in initiating repair (NEI commitment no. 8).
- Repair crew is different than the on-site operators.

4.1.4.3 Quantification

Human Error Probabilities

The probability of failure to repair SFPC system is represented by the exponential repair model:

$$e^{-\lambda t}$$

where

λ = (inverse of mean time to repair)

t = available time

In the case where discovery was from the control room, probability of failure to repair SFPC system event, HEP-COOL-REP-E, would be 0.18 based on 17 hours available to repair. In the case that the discovery was due to operator walk-down (HEP-COOL-REP-L), it is assumed that there is not enough time available to repair and restart the SFP makeup system in time to prevent bulk boiling, and has been assigned a value of 1.0.

4.1.4.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-COOL-REP-E	1.8E-1
HEP-COOL-REP-L	1.0

4.1.5 Top Event OFD – Operator Recovery Using On-site Sources

4.1.5.1 Event Description and Timing

On the two upper branches of the event tree, the operators have recognized the loss of the SFPC system, and have tried unsuccessfully to restore the system. After 43 hours, the level of the pool has dropped below the suction of the SFP cooling system (see below), so that repair of that system will not have any effect until pool level is restored. The operating staff now has 88 hours to provide makeup to the pool using firewater (or other available on-site sources) to prevent fuel uncover (131 hours less 43 hours). This event represents failure to provide makeup to the SFP. The operators have both an electric and a diesel-driven firewater pump available to perform this function. If both pumps were to fail, there may be time to repair one of the pumps. This event has been modeled by the fault tree LOC-OFD.

Given the operators were not successful in detecting the loss of cooling early enough to allow recovery of the normal cooling system, this event is modeled by functional fault tree LOC-OFD-L. At this stage, even though the operators have failed over several shifts to detect the need to respond, there would be several increasingly compelling cues available to the operators performing walk-downs, including a visibly lowered pool level and a hot and humid atmosphere. Since there are on the order of 88 hours before the level drops to 3 feet above the fuel, some credit has been taken for subsequent crews to recognize the loss of cooling and take corrective action.

4.1.5.2 Relevant Assumptions

- The operators have 88 hours to provide makeup.
- The operators will avoid using raw water (e.g., water not chemically controlled) if possible.
- The boil-off rate is assumed to be higher than the SFP makeup system capacity.
- The operators are aware that they must use raw water to refill the pool once the level drops to below the suction of the cooling system and the pool begins boiling, since the makeup system cannot compensate for the boiling.

- For repair of failed pumps, it is assumed that it takes 16 hours to contact maintenance personnel, identify the problem, and get new parts.
- There is a means to remotely align a makeup source to the spent fuel pool without entry to the refuel floor, so that makeup can be provided even when the environment is uninhabitable due to steam and/or high radiation (NEI commitment no.8).
- Repair crew is different than on-site operators.
- Mean time to repair the firewater pump is 10 hours.
- Operators have received formal training and there are procedures that include clear guidance on the use of the firewater system as a makeup system (NEI commitment no. 2).
- Firewater pumps are maintained and tested on a regular schedule (NEI commitment no. 10).

4.1.5.3 Quantification

Human Error Probabilities

Three human failure events are modeled in functional fault tree LOC-OFD
HEP-RECG-FWSTART represents the operator's failure to recognize the need to initiate the firewater system. The conditions under which the firewater system is to be used are assumed to be explicit in a written procedure. This event was quantified using the SPAR HRA technique. The assumptions include expansive time (> 24 hours), a high level of stress, diagnostic type procedures, good ergonomic interface, and good quality of work process. This diagnosis task provides the diagnosis for the subsequent actions taken to re-establish cooling to the pool.

HEP-FW-START represents failure to start the electric or diesel firewater pump within 88 hours after the onset of bulk boiling, given that the decision to start a firewater pump was made. No difficult valve alignment is required. This event was quantified using SPAR HRA technique. An expansive time (> 50 times the required time), high stress, highly complex task because of its non-routine nature, quality procedures available, as well as good ergonomics including equipment and tools matched to procedure, and crews that are conversant with the procedures and one another through training were assumed .

HEP-FW-REP-DEPEN represents the failure of the repair crew to repair a firewater pump. Note that the repair crew had failed to restore the SFPC system. Therefore, dependency was modeled in the failure to repair firewater system. We assume that the operator will focus his recovery efforts on only one pump. Assuming that it takes another two shifts (16 hours) before technical help and parts arrive, then the operator has 72 hours (88 hours less 16 hours) to repair the pump. Assuming a 10-hour mean time to repair, the probability of failure to repair the pump would be $\text{Exp}[-(1/10) * 72] = 1.0\text{E-}3$. For HEP-FW-REP-DEPEN a low level of dependence was applied modifying the nominal failure probability of $1.0\text{E-}3$ to $5.0\text{E-}2$ using the THERP formulation for low dependence.

Functional fault tree LOC-OFD-L is similar except that basic event HEP-RECG-FWSTART is replaced by HEP-RECG-FWSTART-L. The probability of this event is 5E-2, representing a low level of dependence due to the fact that a failure to detect the condition during the first few shifts may be indicative of a more serious underlying problem.

Hardware Failure Probabilities

Basic event FP-2PUMPS-FTF represents the failure of both firewater pumps. The pump may be required to run 8 to 10 hours at the most (250 gpm capacity), given that the water inventory drops by 20 ft (i.e., 3 ft from the top of the fuel). A failure probability of 3.7E-3 for failure to start and run for the electric pump and 0.18 for the diesel driven pump are used from INEL-96/0334 (Ref. 12). Note that the relatively high unavailability assumed for the diesel driven firewater pump may be conservative if it is subject to a maintenance and testing program, and there are controls on availability. These individual pump failures result in a value of 6.7E-4 for event FP-2PUMPS-FTF.

4.1.5.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-RECG-FWSTART	2.0E-5
HEP-RECG-FWSTART-L	5.0E-2
HEP-FW-START	1.0E-5
HEP-FW-REP-DEPEN	5.0E-2
FP-2PUMPS-FTF	6.7E-4

4.1.6 Top Event OFB – Operator Recovery Using Off-site Sources

4.1.6.1 Event Description and Timing

This event accounts for recovery of coolant makeup using off-site sources given the failure of recovery actions using on-site sources. Adequate time is available for this action, provided that the operating staff recognizes that recovery of cooling using on-site sources will not be successful, and that off-site sources are the only viable alternatives. This top event is quantified using fault tree LOC-OFB, for the upper two branches, and LOC-OFB-L for the lowest branch. Note that in this fault tree event HEP-INV-OFFSITE is ORed with the failure of the operator to recognize the need to start the firewater system (event HEP-RECG-FWSTART or HEP-RECG-FWSTART-L, described in Section 4.1.5.3). In essence, if the operators fail to recognize the need for firewater, it is assumed they will fail to recognize the need for other off-site sources of makeup.

4.1.6.2 Relevant Assumptions

- The operators have 88 hours to provide makeup and inventory cooling.
- Procedures and training are in place that ensure that off-site resources can be brought to bear (NEI commitment no. 2 and 4), and that preparation for this contingency is made when it is realized that it may be necessary to supplement the pool makeup.

- Procedures explicitly state that if the water level drops below a certain level (e.g., 15 ft below normal level) operator must initiate recovery using off-site sources.
- Operators have received formal training in the procedures.
- Off-site resources are familiar with the facility.

4.1.6.3 Quantification

Human Error Probabilities

The event HEP-INV-OFFSITE represents failure to recognize that it is necessary to take the extreme measure of using off-site sources, given that even though there has been ample time up to this point to attempt recovery of both the SFP cooling system and both firewater pumps it has not been successful. This top event should include contributions from failure of both the diagnosis of the need to provide inventory from off-site sources, and of the action itself. The availability of off-site resources is assumed not to be limiting on the assumption of an expansive preparation time. However, rather than use a calculated HEP directly, a low level of dependence to account for the possible detrimental effects of the failure to complete prior tasks successfully.

4.1.6.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-INV-OFFSITE	5.0E-2

4.1.7 Summary

Table 4.1 presents a summary of basic event probabilities used in the event tree quantification.

Based on the assumptions made, the frequency of core uncover can be seen to be very low. A careful and thorough adherence to NEI commitments 2, 5, 8 and 10 is crucial to establishing the low frequency. In addition, however, the assumption that walkdowns are performed on a regular, (once per shift) basis is important to compensate for potential failures to the instrumentation monitoring the status of the pool. The analysis has also assumed that the procedures and/or training are explicit in giving guidance on the capability of the fuel pool makeup system, and when it becomes essential to supplement with alternate higher volume sources. The analysis also assumed that the procedures and training are sufficiently clear in giving guidance on early preparation for using the alternate makeup sources.

Table 4.1 Basic Event Summary for the Loss of Cooling Event Tree

Basic Event Name	Description	Basic Event Probability
IE-LOC	Loss of SFP cooling initiating event	3.0E-3
HEP-DIAG-ALARM	Operators fail to respond to a signal indication in the control room	3.0E-4
HEP-WLKDOWN-LSFPC	Operators fail to observe the loss of cooling in walk-downs (independent case)	1.0E-5
HEP-WLKDOWN-DEPEN	Operators fail to observe the loss of cooling in walk-downs (dependent case)	5.0E-2
HEP-COOL-REP-E	Repair crew fails to repair SFPC system	1.8E-1
HEP-COOL-REP-L	Repair crew fails to repair SFPC system	1.0
HEP-RECG-FWSTART	Operators fail to diagnose need to start the firewater system	2.0E-5
HEP-FW-START	Operators fail to start firewater pump and provide alignment	1.0E-5
HEP-FW-REP-DEPEN	Repair crew fails to repair firewater system	5.0E-2
HEP-INV-OFFSITE	Operators fail to provide alternate sources of cooling from off-site	5.0E-2
FP-2PUMPS-FTF	Failure of firewater pump system	6.7E-4
SPC-LVL-LOF	Failure of control room alarm channel	1.0E-5
SPC-LVL-LOP	Electrical faults leading to alarm channel failure	2.0E-3

4.2 Internal Fire Event Tree

This event tree models the loss of SFP cooling caused by internal fires. Given a fire alarm, the operator will attempt to suppress the fire, and then attempt to re-start SFP cooling given that the SFP cooling system and off-site power feeder system have not been damaged by the fire. In the unlikely event that the operator fails to respond to the alarms or is unsuccessful in suppressing the fire, it is assumed that the SFPC system will be damaged to the extent where repair will not be possible. The operator then has to provide alternate cooling and inventory makeup – either using the site firewater system or by calling upon off-site resources. Figure 4.2 shows the Internal Fire event tree sequence progression.

4.2.1 Initiating Event FIR – Internal Fire

4.2.1.1 Event Description and Timing

The fire initiator includes those fires of sufficient magnitude, that if not suppressed, would cause a loss of cooling to the SFP. This loss of cooling could either result from damage to the SFPC system or the off-site power feeder system.

4.2.1.2 Relevant Assumptions

- Fire ignition frequencies from operating plants are assumed to be applicable at the SFP facility.
- Ignition sources from welding and cutting are expected to be insignificant. The facility configuration is expected to be stable, negating the need for modification and fabrication work requiring welding and cutting.

4.2.1.3 Quantification

Data compiled from historical fires at nuclear power plants is summarized in the Fire-Induced Vulnerability Evaluation (FIVE) methodology document (Ref. 13). This document identifies fire ignition sources and associated frequencies and is segregated by plant location and ignition type. Of the plant locations identified in the FIVE document, the intake structure was considered to most closely approximate the conditions and equipment associated with the spent fuel pool facilities considered in this analysis.

FIVE identifies specific frequencies associated with “electrical cabinets,” “fire pumps,” and ‘others’ in the intake structure. In addition to these frequencies associated with specific equipment normally located in the intake structure, ignition sources from equipment (plant-wide) that may be located in the intake structure is also apportioned.

The largest ignition frequency contribution identified for intake structures is from fire pumps. In the plant configuration assumed in this study, the firewater pumps are located in an unattached structure and thus can be eliminated as ignition sources. FIVE also identifies electrical cabinets as significant ignition sources in the intake structure with an average frequency of $2.4E-3/\text{yr}$. Because the number of electrical cabinets (breakers) in the spent fuel facility is expected to be less than those in the typical intake structure, a scaling factor was used to estimate the electrical cabinet contribution. Typically there are five motor-driven pumps (4 cooling pumps, 1 makeup pump) and related support equipment associated with the SPF facility. The number of electrical cabinets (breakers) was therefore estimated to be less than ten in a typical SFP facility. The number of electrical cabinets in the intake structure was estimated to be 25 (engineering judgement based on plant walkdowns). Therefore, the fire ignition frequency contribution from electrical cabinets at the spent fuel pool facility is estimated to be $(10/25)(2.4E-3/\text{yr}) = 9.6E-4/\text{yr}$.

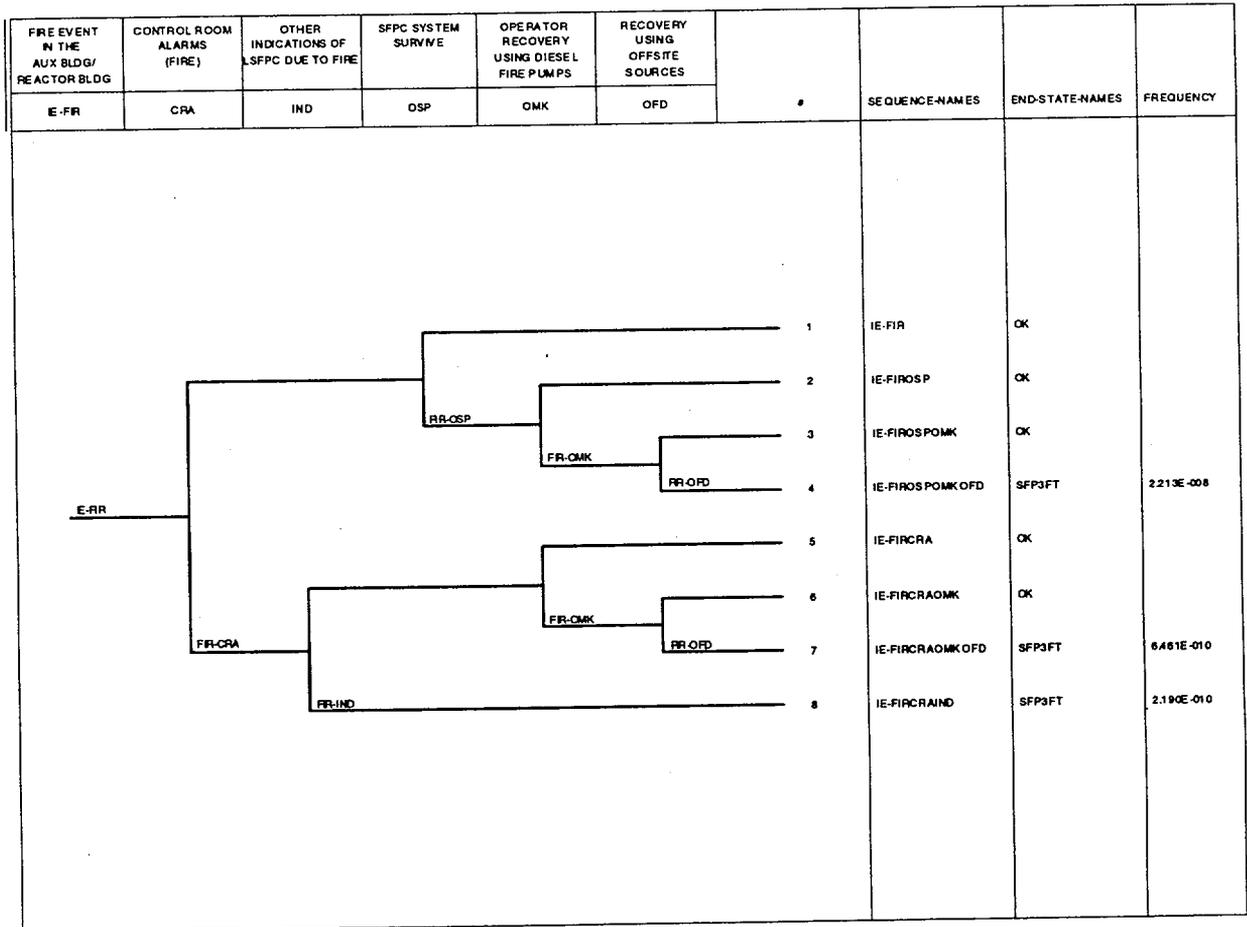


Figure 4.2 Fire initiating event tree

A similar approach was used to correlate the ignition frequency for "other" to a value appropriate for the SFP facility. Intake structures typically have several pumps (e.g., circulating water, service water, screen wash, fire, etc.) as well as peripheral equipment. For this analysis, all ignition frequency associated with the "other" category was apportioned to pumps. The number of pumps in the typical intake structure was estimated to be 10 (again, engineering judgement based on plant walkdowns). Therefore, the fire ignition frequency for "other" equipment at the spent fuel pool facility is estimated to be $(5/10)(3.2E-3/yr) = 1.6E-3/yr$.

The contribution of ignition sources, identified as "plant-wide" sources in the FIVE document, to the ignition frequency of the SFP facility is considered to be negligible. Large ignition source contributors such as elevator motors, dryers, and MG sets do not exist in the spent fuel facility. Additionally, spontaneous cable fires are expected to be a negligible contributor because of the minimal amount of energized electrical cable. The facility configuration is expected to be stable, negating the need for modification and fabrication work requiring welding and cutting.

The fire ignition frequency for the SFP facility is therefore estimated to be $9.6E-4/yr + 1.6E-3/yr = 2.6E-3/yr$. A fire frequency value of $3E-3/yr$ will be used in the analysis to provide additional margin and to account for any uncertainties in equipment configuration.

4.2.1.4 Basic Event Probability

Basic Event	Basic Event Probability
IE-FIRE	3E-3

4.2.2 Top Event CRA – Control Room Alarms

4.2.2.1 Event Description and Timing

This event represents fire detection system failure to alarm in the control room or operator failure to respond to the alarm. The proper conditions for an alarm are assumed to exist within a few minutes of fire initiation. Failure to respond could be due to operator error (failure to respond), failure of the detectors, or loss of indication due to electrical faults. Success for this event is defined as the operator recognizing the alarm and responding to the fire. Failure of this event is assumed to lead to a fire damage state where there is a loss of the SFPC system and a loss of the plant power supply system. This event is quantified by fault tree FIR-CRA and includes hardware and human failures.

4.2.2.2 Relevant Assumptions

- The SFP area is equipped with fire detectors which are alarmed in the control room. However, the area is not equipped with an automatic fire suppression system.
- Fire alarms will be activated in the control room within a few minutes of the initiation of a fire.
- Regular maintenance and testing is performed on the fire detection system and on the control room annunciators.

- Procedures are available to guide operator response to a fire, and plant operators are trained in these procedures (NEI commitment no. 2).

4.2.2.3 Quantification

Human Error Probabilities

One human failure event is modeled for this event (basic event HEP-DIAG-ALARM). The operator may fail to respond to a signal or indication in the control room. The source for this error rate is THERP (Table 20-23).

Hardware Failure Probabilities

The value used for failure of the detectors, SFP-FIRE-DETECT (5.0E-3), was taken from OREDA-92 (Ref. 14). The value used for local electrical faults leading to alarm channel failure, SFP-FIRE-AOL (2.0E-3), was estimated based on information in reference 11.

4.2.2.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-DIAG-ALARM	3.0E-4
SFP-FIRE	2.0E-3
SFP-FIRE-DETECT	5.0E-3

4.2.3 Top Event IND – Other Indications of Loss of Cooling

4.2.3.1 Event Description and Timing

This event models the failure of the operators to recognize the loss of SFP cooling resulting from a fire, given that either the fire alarm system failed or was not attended to. Since the assumed consequences of not attending to the alarm are a fire large enough to cause loss of power to the facility, the indications available to the operator during a walk-down include clear effects of the fire, both from visible evidence and the smell of burning, as well as the lack of power. Ultimately, if no action is taken to restore cooling, the high area temperature and humidity, and low water level from boiloff will become increasingly evident. The operators have more than 10 shifts (about 131 hours) to discover the loss of SFP cooling. Success for this event is defined as the operators recognizing the abnormal condition and understanding the need to take action within this time. This event is modeled by fault tree FIR-IND.

4.2.3.2 Relevant Assumptions

- Operators perform walk-downs once per shift (every 8 to 12 hours) and walk-downs are required to be logged.
- If the fire is discovered during the walk-down, the SFPC system is assumed to be damaged to the extent where repair will not be feasible within a few days.

- Local instrumentation and alarms are destroyed in a fire which is not extinguished within 20 minutes.
- Procedures are available to guide plant operators for off-normal conditions, and operators are trained in these procedures (NEI commitment no. 2).

4.2.3.3 Quantification

Human Error Probability

This event is represented by the basic event HEP-WLKDOWN-LSFPC which models the operators failure to recognize the loss of cooling during walk-downs. The failure rate was developed using THERP, and is based upon three individual failures: failure to carry out an inspection, missing a step in a written procedure, and misreading a measuring device. Multiple opportunities for recovery were assumed.

Note that no dependency on the previous HEP was modeled. While it could be argued that, in the case where the operator has already failed to respond to control room alarms, there may be a dependence between the event HEP-DIAG-ALARM and HEP-WLKDOWN-LSFPC. However, the cues for this event are quite different. There will be obvious physical changes in the plant (e.g., loss of off-site power, a burnt out area, smoke, etc.). The only source of dependency is one where a situation would result in the operator failing to respond to control room alarms and also result in a total abandonment of plant walk-downs.

4.2.3.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-WLKDOWN-LSFPC	1.0E-5

4.2.4 Top Event OSP – Fire Suppression

4.2.4.1 Event Description and Timing

This top event represents operator failure to suppress the fire before the SFP cooling system is damaged given that he responds to fire alarms. If the SFP cooling and makeup system pumps and plant power supply system are damaged to a point that they cannot be repaired in time to prevent fuel uncover, the operator must provide cooling using available on-site (i.e., diesel fire pumps) and off-site water sources. If the fire is suppressed in time to prevent damage to SFP components, then the SFP cooling system can be restored in time to prevent fuel uncover. The top event is represented by fault tree FIR-OSP.

4.2.4.2 Relevant Assumptions

- The automatic fire suppression system is unavailable.
- If the fire is not extinguished within 20 minutes, it is assumed that SFP cooling will be lost due either to damage of SFPC equipment, or to the plant's power supply system.

- No credit is taken for the firewater system in the suppression of the fire.
- Fire suppression extinguishers are located strategically in the SFP area, and these extinguishers are tested periodically.

4.2.4.3 Quantification

Failure of fire suppression is represented by basic event HEP-RES-FIRE. The modeling of fire growth and propagation and the determination of the effects of a fire on equipment in a room would optimally take into account the combustible loading in the room, the presence of intervening combustibles, the room size and geometry, and other characteristics such as ventilation rates and the presence of openings in the room. Because detailed inputs such as these are not applicable for a generic study such as this, fire growth and propagation was determined based on best estimate assumptions. It is assumed that the operator has 20 minutes to suppress the fire, otherwise, it is assumed that SFP cooling will be lost (due either to damage of SFPC equipment, or to the plant's power supply system).

HEP-RES-FIRE was modeled using THERP. Due to the level of uncertainty about the size of the fire, its location, and when it is discovered, the approach taken was to model this error as a dynamic task requiring a higher level of human interaction, including keeping track of multiple functions. In addition little experience in fighting fires was assumed. Table 20-16 in THERP provides modifications of estimated HEPs for the effects of stress and experience. Using the performance shaping factors of extremely high stress (as fighting a fire would be), a dynamic task, and an operator experienced in fighting fires, this table provides an HEP of 2.5E-1.

- Notes: (1) It can be argued that damage time (to disable the SFP cooling function) could be in excess of 20 minutes because typical SFP facilities are relatively large and because equipment within such facilities is usually spread out. However, in this analysis, the SFP pumps are assumed to be located in the same general vicinity with no fire barriers between them.
- (2) Scenarios can be postulated where the fire damage state is less severe than that described above (e.g., fire damage to the running cooling pump, with the other pump undamaged, and with off-site power available). These scenarios can be subsumed into the "Loss of Cooling" event, and SFP cooling "recovery" in these cases would be by use of the undamaged pump train.

4.2.4.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-RES-FIRE	2.5E-1

4.2.5 Top Event OMK – Operator Recovery Using On-site Sources

4.2.5.1 Event Description and Timing

At this point in the event tree, the SFP cooling has been lost as a result of the fire, and the operators are unable to restore the cooling system. Also, the fire has damaged the electrical system such that the motor-driven firewater pump is unavailable. If no actions are taken, SFP water level would drop to 3 ft above the top of fuel in 131 hours from the time the loss of SFP cooling occurred. This event represents failure of the operators to start the diesel-driven firewater pump and provide makeup to the SFP. If the diesel firewater pump fails, the operators have time to attempt repair. This event is modeled by fault tree FIR-OMK.

4.2.5.2 Relevant Assumptions

- There is a means to remotely align a makeup source to the spent fuel pool without entry to the refuel floor, so that makeup can be provided even when the environment is uninhabitable due to steam and/or high radiation (NEI commitment no.8).
- Inventory makeup using the firewater system is initiated by on-site operators.
- In modeling the repair of a failed firewater pump, it is assumed that it takes 16 hours to contact maintenance personnel, make a diagnosis, and get new parts.
- Mean time to repair the firewater pump is 10 hours.
- Inventory makeup using the firewater pumps are proceduralized, and the operators are trained in these procedures (NEI commitment no. 2).
- Firewater pumps are tested and maintained on a regular schedule (NEI commitment no. 10).

4.2.5.3 Quantification

Human Error Probabilities

The fault trees used to quantify this top event include three human failure events.

HEP-RECG-FWSTART represents the operators' failure to recognize the loss of SFP cooling and the need to initiate the firewater system. This event was quantified using the SPAR HRA technique. The assumptions include expansive time (> 24 hours), a high level of stress, diagnostic type procedures, good ergonomic interface, and good quality of work process. This diagnosis task provides the diagnosis for the subsequent actions taken to re-establish cooling to the pool. Although this diagnosis and subsequent actions follow a fire, no dependence between response to the fire and subsequent actions is assumed, because of the large time lag.

HEP-FW-START represents failure to start the diesel firewater pump within 88 hours after the onset of bulk boiling, given that the decision to start a firewater pump was made. No difficult valve alignment is required, but the operator may have to position a hose in the pool area. This event HEP-FW-START was quantified using SPAR HRA technique. The following PSFs were assumed: expansive time (> 50 times the required time), high stress, highly complex task because of the multiple steps, its non-routine nature, quality procedures available, as well as good ergonomics including equipment and tools matched to procedure, and finally a crew who had executed these tasks before, conversant with the procedures and one another.

HEP-FW-REP-NODEP represents the failure of the repair crew to repair a firewater pump. It is assumed that the operators will focus their recovery efforts on only the diesel driven pump. Assuming that it takes 16 hours before technical help and parts arrive, then the operators have 72 hours (88 hours less 16 hours) to repair the pump. Assuming a 10-hour mean time to repair, the probability of failure to repair the pump would be $\text{Exp}[-(1/10) \times 72] = 1.0\text{E-}3$.

Hardware Failure Probabilities

Basic event FP-DGPUMP-FTF represents the failure of the diesel driven firewater pump. The pump may be required to run 8 to 10 hours at the most (250 gpm capacity), given that the water inventory drops by 20 ft (i.e., 3 ft from the top of the fuel). A failure probability of 1.8E-1 for failure to start and run for the diesel driven pump is used from INEL-96/0334 (Ref. 12).

4.2.5.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-RECG-FWSTART	2.0E-5
HEP-FW-START	1.0E-5
HEP-FW-REP-NODEP	1.0E-3
FP-DGPUMP-FTF	1.8E-1

4.2.6 Top Event OFD – Operator Recovery Using Off-site Sources

4.2.6.1 Event Description and Timing

Given the failure of recovery actions using on-site sources, this event accounts for recovery of coolant makeup using off-site sources. Adequate time is available for this action, provided that the operators recognize that recovery of cooling using on-site sources will not be successful, and that off-site sources are the only viable alternatives. This top event is quantified using fault tree FIR-OFD. This event is represented by a basic event HEP-INV-OFFSITE.

4.2.6.2 Relevant Assumptions

- The operators have 88 hours to provide makeup and inventory cooling.
- Procedures and training are in place that ensure that off-site resources can be brought to bear (NEI commitment no. 2 and 4), and that preparation for this contingency is made when it is realized that it may be necessary to supplement the pool makeup.

- Procedures explicitly state that if the water level drops below a certain level (e.g., 15 ft below normal level) operator must initiate recovery using off-site sources.
- Operators have received formal training in the procedures.
- Off-site resources are familiar with the facility.

4.2.6.3 Quantification

Human Error Probabilities

The event HEP-INV-OFFSITE represents failure to recognize that it is necessary to take the extreme measure of using off-site sources, given that even though there has been ample time up to this point to attempt recovery of the firewater pump, it has not been successful. This top event should include failures of both the diagnosis of the need to provide inventory from off-site sources, and of the action itself. The availability of off-site resources is assumed not to be limiting on the assumption of an expansive preparation time. However, rather than use a calculated HEP directly, a low level of dependence to account for the possible detrimental effects of the failure to complete prior tasks successfully.

4.2.6.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-INV-OFFSITE	5.0E-2

4.2.7 Summary

Table 4.2 presents a summary of basic event probabilities used in the event tree quantification.

As in the case of the loss of cooling event, the frequency of core uncover, based on the assumptions made in the analysis, is very low. The assumptions that support this low value include: careful and thorough adherence to NEI commitments 2, 5, 8 and 10; walk-downs are performed on a regular, (once per shift) (important to compensate for potential failures to the instrumentation monitoring the status of the pool); procedures and/or training are explicit in giving guidance on the capability of the fuel pool makeup system, and when it becomes essential to supplement with alternate higher volume sources; procedures and training are sufficiently clear in giving guidance on early preparation for using the alternate makeup sources.

Table 4.2 Basic Event Summary for the Internal Fire Event Tree

Basic Event Name	Description	Basic Event Probability
HEP-DIAG-ALARM	Operators fail to respond to a signal indication in the control room	3.0E-4
HEP-RES-FIRE	Operators fail to suppress fire	2.5E-1
HEP-WLKDWN-LSFPC	Operators fail to observe the loss of cooling in walk-downs (independent case)	1.0E-5
HEP-WLKDWN-DEPEN	Operators fail to observe the loss of cooling in walk-downs (dependent case)	5.0E-2
HEP-RECG-FWSTART	Operators fail to diagnoses need to start the firewater system	2.0E-5
HEP-FW-START	Operators fail to start firewater pump and provide alignment	1.0E-5
HEP-FW-REP-NODEP	Repair crew fails to repair firewater system	1.0E-3
HEP-INV-OFFSITE	Operators fail to provide alternate sources of cooling from off-site	5.0E-2
FP-DGPUMP-FTF	Failure of firewater pump system	0.18
SFP-FIXE-LOA	Electrical faults causing loss of alarms	2E-3
SFP-FIRE-DETECT	Failure of fire detectors	5E-3

4.3 Plant-centered and Grid-related Loss of Off-site Power Event Tree

This event tree represents the loss of SFP cooling resulting from a loss of off-site power from plant-centered and grid-related events. Until off-site power is recovered, the electrical pumps would be unavailable, and only the diesel fire pump would be available to provide makeup.

Figure 4.3 shows the Plant-centered and Grid-related Loss of Off-site Power (LOSP) event tree sequence progression.

4.3.1

Initiating Event LP1 – Plant-centered and Grid-related Loss of Off-site Power

4.3.1.1 Event Description

Initiating event IE-LP1 represents plant-centered and grid-related losses of off-site power. Plant-centered events typically involve hardware failures, design deficiencies, human errors (in

maintenance and switching), localized weather-induced faults (e.g., lightning), or combinations of these. Grid-related events are those in which problems in the off-site power grid cause the loss of off-site power.

4.3.1.2 Quantification

For plant-centered LOSP events, NUREG/CR-5496 (Ref. 16) estimates a frequency of .04/critical year for plant centered loss of off-site power for an operating plant, and .18/unit shutdown year for a shutdown plant. For grid-related LOSP events, a frequency of $4E-3$ /site yr was estimated. The frequency of grid-related losses is assumed to be directly applicable. However, neither of the plant centered frequencies is directly applicable. At a decommissioning plant there will no longer be the necessity to have the multiplicity of incoming lines typical of operating plants, which could increase the frequency of loss of off-site power from mechanical failures. On the other hand, the plant will be a normally operating facility, and it would be expected that there will be less activity and operations in the switchyard than would be expected at a shutdown plant, which would decrease the frequency of loss from human error, the dominant cause of losses for shutdown plants. For purposes of this analysis, the LOSP initiating event frequency of 0.08/yr, assumed in INEL-96/0334 (Ref. 13), is assumed for the combined losses from plant-centered and grid-related events.

4.3.2 Top Event OPR – Off-site Power Recovery

4.3.2.1 Event Description and Timing

The fault tree for this top event (LP1-OPR) is a single basic event that represents the non-recovery probability of off-site power.

NUREG-1032 (Ref. 17) classified LOSP events into plant-centered, grid-related, and severe-weather-related categories, because these categories involved different mechanisms and also seemed to have different recovery times. Similarly, NUREG/CR-5496 (Ref. 16) divides LOSP events into three categories and estimates different values of non-recovery as functions of time.

4.3.2.2 Relevant Assumptions

- Trained electricians may not be present at the site for the quick recovery.
- Operators have received formal training and there are procedures to guide them (NEI commitment no. 2).

LOSS OF OFF-SITE POWER FROM PLANT CENTERED AND GRID RELATED EVENTS	OFFSITE POWER RECOVERY PRIOR TO SFP/C SYSTEM LOSS	COOLING SYSTEM RESTART AND RERUN	OPERATOR RECOVERY USING MAKEUP SYSTEM	RECOVERY FROM OFFSITE SOURCES					
E-LP1	OPR	OCS	OMK	OFD	#	SEQUENCE NAMES	END-STATE-NAMES	FREQUENCY	
						1	IE-LP1	OK	
						2	IE-LP1OCS	OK	
						3	IE-LP1OCSOMK	OK	
						4	IE-LP1OCSOMKOFD	SFP3FT	5.673E-009
						5	IE-LP1OPR	OK	
						6	IE-LP1OPROMK	OK	
						7	IE-LP1OPROMKOFD	SFP3FT	2.360E-008

Figure 4.3 Plant centered and grid related loss of off-site power event tree

4.3.2.3 Quantification

The basic event that represents recovery of off-site power for plant-centered and grid-related LOSPs is REC-OSP-PC. The data in NUREG/CR-5496 indicates that one event in 102 plant centered events resulted in a loss for greater than 24 hours, and all 6 of the grid centered events were recovered in a relatively short time. Therefore a non-recovery probability of 1E-02 is assumed.

4.3.2.4 Basic Event Probability

Basic Event	Basic Event Probability
REC-OSP-PC	1E-02

4.3.3 Top Event OCS – Cooling System Restart and Run

4.3.3.1 Event Description and Timing

This top event represents restarting the SFP cooling system, given that off-site power has been recovered within 24 hours. There are two electrically operated pumps and the operator can start either one. If the operator starts the pump that was in operation, no valve alignment would be required. However, if the operator starts the standby pump, some valve alignment may be required.

Fault tree LP1-OCS has several basic events: an operator action representing the failure to establish SFP cooling, and several hardware failures of the system. If power is recovered within 24 hours, the operator has 9 hours to start the system before boil-off starts.

4.3.3.2 Relevant Assumptions

- The operators have 9 hours to start the SFP cooling system.
- The SFP has at least one SFP water temperature monitor, with either direct indication or a trouble light in the control room (there could also be indications or alarms associated with pump flow and pressure) (NEI commitment no. 5).
- Procedures exist for response to and recovery from a loss of power, and the operators are trained in their use (NEI commitment no. 2).

4.3.3.3 Quantification

Human Error Probabilities

Event HEP-SFP-STR-LP1 represents operator failure to restart/realign the SFP cooling system in 9 hours. The operator can restart the previously running pump and may not have to make any valve alignment. If he decides to restart the standby pump he may have to make some valve alignment. The response part of the error was quantified using SPAR. The relevant performance shaping factors for this event included expansive time, high stress due to previous

failures, moderately complex task due to potential valve lineups, highly trained staff, good ergonomics (well laid out and labeled matching procedures), and good work process.

A diagnosis error HEP-DIAG-SFPLP1, representing failure of the operators to recognize the loss of SFP cooling was also included. Success would most likely result from recognition that the electric pumps stop running once power is lost and require restart following recovery of power. If the operator fails to make an early diagnosis of loss of SFP cooling, then success could still be achieved during walk-downs following the loss of off-site power. Alternatively, if power is restored, the operator will have alarms available as well. Therefore this value consists of two errors. The diagnosis error was calculated using SPAR, and the walk-down error was calculated using THERP. The relevant performance shaping factors included greater than 24 hours for diagnosis, high stress, well-trained operators, diagnostic procedures, and good work processes. A low dependence for the walk-down error was applied.

Because it is assumed that at most 9 hours are available, no credit was given for repair of the SFP cooling system.

Non-HEP Probabilities

Fault tree LP1-OCS represents failure of the SFP cooling system to restart and run. Hardware failure rates have been taken from INEL-96/0334 (Ref. 13). It is assumed that SFPC system will be maintained since it is required to be running all the time.

4.3.3.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-DIAG-SFPLP1	1.0E-06
HEP-SFP-STR-LP1	5.0E-6
SPC-CKV-CCF-H	1.9E-5
SPC-CKV-CCF-M	3.2E-5
SPC-HTX-CCF	1.9E-5
SPC-HTX-FTR	2.4E-4
SPC-HTX-PLG	2.2E-5
SPC-PMP-CCF	5.9E-4
SPC-PMP-FTF-1	3.9E-3
SPC-PMP-FTF-2	3.9E-3

4.3.4 Top Event OMK – Operator Recovery Using Makeup Systems

4.3.4.1 Event Description and Timing

This top event represents the failure to provide makeup using the firewater pumps. If off-site power is recovered then the fault tree LP1-OMK-U represents this top event. In this case, the operator has both electric and diesel firewater pumps available. If off-site power is not

recovered then fault tree LP1-OMK-L represents this top event. In this case, the operator has only the diesel firewater pump available.

4.3.4.2 Relevant Assumptions

- It is assumed that the procedures guide the operators to wait until it is clear that spent fuel pool cooling cannot be reestablished (e.g., using cues such as the level drops to below the suction of the cooling system or the pool begins boiling) before using alternate makeup sources. Therefore, they have 88 hours to start a firewater pump.
- There is a means to remotely align a makeup source to the spent fuel pool without entry to the refuel floor, so that makeup can be provided even when the environment is uninhabitable due to steam and/or high radiation (NEI commitment no.8).
- Repair crew is different than on-site operators.
- Repair crew will focus recovery efforts only on one pump.
- On average, it takes 10 hours to repair a pump if it fails to start and run.
- It takes 16 hours to contact maintenance personnel, make a diagnosis, and get new parts.
- Both firewater pumps are located in a separate structure or protected from the potential harsh environment in case of pool bulk boiling.
- Maintenance is performed per schedule on diesel and electric firewater pumps to maintain operable status.
- Operators have received formal training on relevant procedures.

4.3.4.3 Quantification

Human Error Probabilities

The fault tree LPI-OMK-U includes five human failure events and LPI-OMK-L has three.

Two events are common. HEP-RECG-FWSTART represents the failure of the operator to recognize the need to initiate firewater as an inventory makeup system, given that a loss of fuel pool cooling has been recognized. This event was quantified using the SPAR HRA technique. The assumptions included expansive time (> 24 hours), a high level of stress, diagnostic type procedures, good ergonomic interface, and good quality of work process.

HEP-FW-START represents failure to start either the electric or diesel firewater pump (depending upon availability) within 88 hours after the onset of bulk boiling, given that the decision to start a firewater pump was made. No difficult valve alignment is required, but the operator may have to position a hose in the pool area. This event was quantified using the SPAR HRA technique. The PSFs included expansive time (> 50 times the required time), high

stress, highly complex task because of the multiple steps, its non-routine nature, quality procedures available, as well as good ergonomics including equipment and tools matched to procedure, and finally a crew who had executed these tasks before, conversant with the procedures and one another.

HEP-FW-REP-NODEP represents the failure of the repair crew to repair a firewater pump for the scenario where power is not recovered. Note that it has been assumed that since power is not recovered, the repair crew did not make any attempt to repair the SFPC system, and therefore no dependency was modeled in the failure to repair the firewater system. Assuming that it takes another 16 hours before technical help and parts arrive, then the operator has 72 hours (88 hours less 16 hours) to repair the pump. Assuming a 10-hour mean time to repair, the probability of failure to repair the pump would be $\text{Exp}[-(1/10) (72)] = 1.0\text{E-}3$. This event is modeled in the fault tree, LP1-OMK-L.

HEP-FW-REP-DEPEN represents the failure of the repair crew to repair a firewater pump. Note that repair was not credited for top event OCS; however, it has been assumed that the repair crew would have made an attempt to restore the SFPC system, and so dependency was modeled in the failure to repair the firewater system. A probability of failure to repair a pump in 88 hrs is estimated to be $1.0\text{E-}3$. For HEP-FW-REP-DEPEN a low level of dependence was applied modifying the failure rate of $1.0\text{E-}3$ to $5.0\text{E-}2$ using the THERP formulation for low dependence. This event is modeled in the fault tree, LP1-OMK-U.

In addition, in fault tree LP1-OMK-U, the possibility that no action is taken has been included by incorporating an AND gate with basic events HEP-DIAG-SFPLPI and HEP-RECG-DEPEN. The latter is quantified on the assumption of a low dependency.

Hardware Failure Probabilities

In the case of LP1-OMK-U, both firewater pumps are available. Failure of both firewater pumps is represented by basic event FP-2PUMPS-FTF. In the case of LP1-OMK-L, only the diesel-driven firewater pump is available, and its failure is represented by basic event FP-DGPUMP-FTF.

The pump may be required to run 8 to 10 hours at the most (250 gpm capacity), given that the water inventory drops by 20 ft (i.e., 3 ft above the top of the fuel). A failure probability of $3.7\text{E-}3$ for failure to start and run for the electric pump and 0.18 for the diesel driven pump are used from INEL-96/0334. These individual pump failures result in a value of 0.18 for event FP-DGPUMP-FTF and $6.7\text{E-}4$ for event FP-2PUMPS-FTF.

4.3.4.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-RECG-DEPEN	5E-02
HEP-RECG-FWSTART	2.0E-5

Basic Event	Basic Event Probability
HEP-FW-START	1.0E-5
HEP-FW-REP-DEPEN	5.0E-2
FP-2PUMPS-FTF	6.7E-4
FP-DGPUMP-FTF	1.8E-1

4.3.5 Top Event OFD – Operator Recovery Using Off-site Sources

4.3.5.1 Event Description and Timing

Given the failure of recovery actions using on-site sources, this event accounts for recovery of coolant makeup using off-site sources such as procurement of a fire engine. Adequate time is available for this action, provided that the operator recognizes that recovery of cooling using on-site sources will not be successful, and that off-site sources are the only viable alternatives. Fault tree LP1-OFD represents this top event for the lower branch, and LP1-OFD-U for the upper branch. These fault trees contains those basic events from the fault trees LP1-OMK-U and LP1-OMK-L that relate to recognition of the need to initiate the fire water system; if OMK fails because the operator failed to recognize the need for firewater makeup, then it is assumed that the operator will fail here for the same reason.

4.3.5.2 Relevant Assumptions

- The operators have 88 hours to provide makeup and inventory cooling.
- Procedures and training are in place that ensure that off-site resources can be brought to bear (NEI commitment no. 2 and 4), and that preparation for this contingency is made when it is realized that it may be necessary to supplement the pool makeup.
- Procedures explicitly states that if the water level drops below a certain level (e.g., 15 ft below normal level) operator must initiate recovery using off-site sources.
- Operators have received formal training in the procedures.
- Off-site resources are familiar with the facility.

4.3.5.3 Quantification

Human Error Probabilities

The event HEP-INV-OFFSITE represents failure to recognize that it is necessary to take the extreme measure of using off-site sources, given that even though there has been ample time up to this point to attempt recovery of both the SFP cooling system and both firewater pumps it has not been successful. This top event should include failures of both the diagnosis of the need to provide inventory from off-site sources, and the action itself. The availability of off-site

resources is assumed not to be limiting on the assumption of an expansive preparation time. However, rather than use a calculated HEP directly, a low level of dependence is used to account for the possible detrimental effects of the failure to complete prior tasks successfully.

4.3.5.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-INV-OFFSITE	5.0E-2

4.3.6 Summary

Table 4.3 presents a summary of basic event probabilities used in the quantification of the Plant-centered and Grid-related Loss of Off-site Power event tree.

As in the case of the loss of cooling, and fire initiating events, based on the assumptions made, the frequency of core uncover can be seen to be very low. Again, a careful and thorough adherence to NEI commitments 2, 5, 8 and 10, the assumption that walk-downs are performed on a regular, (once per shift) basis is important to compensate for potential failures to the instrumentation monitoring the status of the pool, the assumption that the procedures and/or training are explicit in giving guidance on the capability of the fuel pool makeup system, and when it becomes essential to supplement with alternate higher volume sources, the assumption that the procedures and training are sufficiently clear in giving guidance on early preparation for using the alternate makeup sources, are crucial to establishing the low frequency.

Table 4.3 Basic Event Summary for Plant-centered and Grid-related Loss of Off-site Power

Basic Event Name	Description	Probability
IE-LP1	Loss of off-site power due to plant-centered or grid-related causes	8.0E-2
REC-OSP-PC	Recovery of off-site power within 24 hours	1.0E-2
HEP-DIAG-SFPLP1	Operators fail to diagnose loss of SFP cooling due to loss of off-site power	1.0E-6
HEP-SFP-STR-LP1	Operators fail to restart and align the SFP cooling system once power is recovered	5.0E-6
HEP-RECG-FWSTART	Operators fail to diagnose need to start the firewater system	2.0E-5
HEP-DIAG-DEPEN	Operators fail to recognize need to cool pool given prior failure	5E-02
HEP-FW-START	Operators fail to start firewater pump and provide alignment	1.0E-5
HEP-FW-REP-NODEP	Repair crew fails to repair firewater system	1E-3
SPC-PMP-CCF	SFP cooling pumps – common cause failure	5.9E-4
SPC-PMP-FTF-1	SFP cooling pump 1 fails to start and run	3.9E-3
SPC-PMP-FTF-2	SFP cooling pump 2 fails to start and run	3.9E-3
FP-2PUMPS-FTF	Failure of firewater pump system	6.7E-4
FP-DGPUMP-FTF	Failure of the diesel-driven firewater pump	1.8E-1

4.4 Severe Weather Loss of Off-site Power Event Tree

This event tree represents the loss of SFP cooling resulting from a loss of off-site power from severe-weather-related events. Until off-site power is recovered, the electrical pumps would be unavailable, and only the diesel fire pump would be available to provide makeup.

Figure 4.4 shows the Severe Weather Loss of Off-site Power (LOSP) event tree sequence progression.

4.4.1 Initiating Event LP2 – Severe Weather Loss of Off-site Power

4.4.1.1 Event Description

Initiating event IE-LP2 represents severe-weather-related losses of off-site power. Severe weather threatens the safe operation of a SFP facility by simultaneously causing loss of off-site power and potentially draining regional resources or limiting their access to the facility. This event tree also differs from the plant-centered and grid-related LOSP event tree in that the probability of off-site power recovery is reduced.

4.4.1.2 Quantification

The LOSP frequency from severe weather events is $1.1E-2$ /yr, taken from NUREG/CR-5496 (Ref. 16). This includes contributions from hurricanes, snow and wind, ice, wind and salt, wind, and one tornado event, and occurred at a relatively small number of plants. Because of their potential for severe localized damage, tornados were analyzed separately in Appendix 2e.

4.4.2 Top Event OPR – Off-site Power Recovery

4.4.2.1 Event Description and Timing

The fault tree for this top event (LP2-OPR) is a single basic event that represents the non-recovery probability of off-site power. It is assumed that if power is recovered before boil-off starts (33 hours), the operator has a chance to reestablish cooling using the SFP cooling system.

4.4.2.2 Relevant Assumptions

- See section 4.4.2.3 below.

4.4.2.3 Quantification

Non-HEP Probability

NUREG-1032 (Ref. 17) classified LOSP events into plant-centered, grid-related, and severe-weather-related categories, because these categories involved different mechanisms and also seemed to have different recovery times. Similarly, NUREG/CE-5496 divides LOSP events into three categories and estimates different values of non-recovery as functions of time. A non-recovery probability within 24 hrs for the off-site power from the severe weather event was estimated to be $2.0E-2$ to $<1.0E-4$ depending on the location of the plant. In the operating plant, recovery of off-site power may be very efficient due to presence of skilled electricians. In the decommissioned plant, the skilled electricians may not be present at the site. Therefore, for the purpose of this analysis, a non-recovery probability for off-site power due to severe weather event (REC-OSP-SW) of $2.0E-2$ is used.

Figure 4.4 Severe weather related loss of off-site power event tree

LOSS OF OFF-SITE POWER FROM SEVERE WEATHER EVENTS	OFF-SITE POWER RECOVERY PRIOR TO SFP3 SYSTEM LOSS	COOLING SYSTEM RE-START AND RUN	OPERATOR RECOVERY USING MAKEUP SYSTEM	RECOVERY FROM OFF-SITE SOURCES				
IE-LP2	OPR	OCS	OMK	OFD	#	SEQUENCE-NAMES	END-STATE-NAME	FREQUENCY
					1	IE-LP2	OK	
					2	IE-LP2OCS	OK	
					3	IE-LP2OCSOMK	OK	
					4	IE-LP2OCSOMKOFD	SFP3FT	1.395E-008
					5	IE-LP2OPR	OK	
					6	IE-LP2OPROMK	OK	
					7	IE-LP2OPROMKOFD	SFP3FT	1.188E-007

4.4.2.4 Basic Event Probability

Basic Event	Basic Event Probability
REC-OSP-SW	2.0E-2

4.4.3 Top Event OCS – Cooling System Restart and Run

4.4.3.1 Event Description and Timing

This top event represents restarting the SFP cooling system, given that off-site power has been recovered within 24 hours. There are two electrically operated pumps and the operator can start either one. If the operator starts the pump that was in operation, no valve alignment would be required. However, if operator starts the standby pump, some valve alignment may be required.

Fault tree LP2-OCS has several basic events: an event representing failure of the operators to realize they need to start the spent fuel pool cooling system, an operator action representing the failure to establish SFP cooling, and several hardware failures of the system. If power is recovered within 24 hours, the operator has 9 hours to start the system before boil-off starts. If he fails to initiate SFP cooling before boil-off begins, the operator must start a firewater pump to provide makeup.

4.4.3.2 Relevant Assumptions

- The operators have 9 hours to start the SFP cooling system before boil-off starts.
- Operators have received formal training and there are procedures to guide them (NEI commitment no. 2).

4.4.3.3 Quantification

Human Error Probabilities

HEP-DIAG-SFPLP2 represents failure of the operator to recognize the loss of SFP cooling. Success could result from recognition that the electric pumps stop running once power is lost and require restart following recovery of power. If the operator fails to make an early diagnosis of loss of SFP cooling, then success could still be achieved during walkdowns following the loss of off-site power. Alternatively, if power is restored, the operator will have alarms available as well. Therefore this value consists of two errors. The diagnosis error was calculated using SPAR, and the walkdown error was calculated using THERP. The relevant performance shaping factors included greater than 24 hours for diagnosis, extreme stress, moderately complex task (due to potential complications from severe weather), diagnostic procedures, and good work processes. A low dependence was applied to the walk-down error.

Event HEP-SFP-STR-LP2 represents operator failure to restart/realign the SFP cooling system in 9 hours. The operators can restart the previously running pump and may not have to make

any valve alignment. If they decide to restart the standby pump they may have to make some valve alignment. This error was quantified using SPAR. The relevant performance shaping factors included expansive time, extreme stress due to severe weather, moderately complex task due to potential valve lineups and severe weather, poor ergonomics due to severe weather, and good work process.

If the system fails to start and run for a few hours then the operators would try to get the system repaired. Assuming that it takes another two shifts (16 hours) to contact maintenance personnel, make a diagnosis, and get new parts, and assuming an average repair time of 10 hours, there is not sufficient time to fix the system. Therefore, no credit was given for repair of the SFP cooling system.

Non-HEP Probabilities

Fault tree LP2-OCS represents failure of the SFP cooling system to restart and run. Hardware failure rates have been taken from INEL-96/0334. It is assumed that the SFPC system will be maintained since it is required to be running all the time.

4.4.3.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-DIAG-SFPLP2	2.0E-5
HEP-SFP-STR-LP2	5.0E-4
SPC-CKV-CCF-H	1.9E-5
SPC-CKV-CCF-M	3.2E-5
SPC-HTX-CCF	1.9E-5
SPC-HTX-FTR	2.4E-4
SPC-HTX-PLG	2.2E-5
SPC-PMP-CCF	5.9E-4
SPC-PMP-FTF-1	3.9E-3
SPC-PMP-FTF-2	3.9E-3

4.4.4 Top Event OMK – Operator Recovery Using Makeup Systems

4.4.4.1 Event Description and Timing

This top event represents the failure probability of the firewater pumps. If off-site power is recovered then the fault tree LP2-OMK-U represents this top event. In this case, the operators have both electric and diesel firewater pumps available. If off-site power is not recovered then

fault tree LP2-OMK-L represents this top event. In this case, the operator has only the diesel firewater pump available.

4.4.4.2 Relevant Assumptions

- It is assumed that the procedures guide the operators to wait until it is clear that spent fuel pool cooling cannot be reestablished (e.g., using cues such as the level drops to below the suction of the cooling system or the pool begins boiling) before using alternate makeup sources. Therefore, they have 88 hours to start a firewater pump.
- Because of the severe weather, if one or both pumps fail to start or run, it is assumed that it takes another four to five shifts (48 hours) to contact maintenance personnel, perform the diagnosis, and get new parts. Therefore, the operator would have 40 hours (88 hours less 48 hours) to perform repairs.
- There is a means to remotely align a makeup source to the spent fuel pool without entry to the refuel floor, so that makeup can be provided even when the environment is uninhabitable due to steam and/or high radiation (NEI commitment no.8).
- Repair crew is different than on-site operators.
- Repair crew will focus his recovery efforts on only one pump
- On average, it takes 10 hours to repair a pump if it fails to start and run.
- It would take two days (48 hours) to contact maintenance personnel, make a diagnosis, and get new parts due to severe weather.
- Both firewater pumps are located in a separate structure or protected from the potential harsh environment in case of pool bulk boiling.
- Maintenance is performed per schedule on diesel and electric firewater pumps to maintain operable status.
- Operators have received formal training on relevant procedures.

4.4.4.3 Quantification

Human Error Probabilities

The fault tree LP2-OMK-U has five operator actions, and LP2-OMK-I has three. Two of the events are common. HEP-RECG-FWST-SW represents the failure of the operator to recognize the need to initiate firewater as an inventory makeup system. This event was quantified using the SPAR HRA technique. The assumptions included expansive time (> 24 hours), extreme stress, highly trained staff, diagnostic type procedures, and good quality of work process. This diagnosis task provides the diagnosis for the subsequent actions taken to re-establish cooling to the pool.

HEP-FW-START-SW represents failure to start either the electric or diesel firewater pump (depending upon availability) within 88 hours after the onset of bulk boiling, given that the decision to start a firewater pump was made. No difficult valve alignment is required, but the operator may have to position a hose in the pool area. This event was quantified using the SPAR HRA technique. The PSFs chosen were; expansive time (> 50 times the required time), high stress, highly complex task because of the multiple steps and severe weather and its non-routine nature, quality procedures, poor ergonomics due to severe weather, and finally a crew who had executed these tasks before, conversant with the procedures and one another.

HEP-FW-REP-NODSW represents the failure of the repair crew to repair a firewater pump for the scenario where power is not recovered. Note that we have assumed that since power is not recovered, the repair crew did not make any attempt to repair the SFPC system, and therefore no dependency was modeled in the failure to repair the firewater system. We assume that the operator will focus his recovery efforts on only one pump. Assuming that it takes two days (48 hours) before technical help and parts arrive, then the operator has 40 hours (88 hours less 48 hours) to repair the pump. Assuming a 10-hour mean time to repair, the probability of failure to repair the pump would be $\text{Exp} [-(1/10) (40)] = 2.5\text{E-}2$. This event is modeled in the fault tree, LP2-OMK-L.

HEP-FW-REP-DEPSW represents the failure of the repair crew to repair a firewater pump for the scenario where power is recovered. Note that repair was not credited for top event OCS; however, we have assumed that the repair crew did make an attempt to restore the SFPC system, and so dependency was modeled in the failure to repair the firewater system. For HEP-FW-REP-DEPSW a low level of dependence was applied modifying the failure rate of $2.5\text{E-}2$ to $7.0\text{E-}2$ using the THERP formulation for low dependence.

In addition, in fault tree LP2-OMK-U, the possibility that no action is taken has been included by incorporating an OR gate with basic events HEP-DIAG-SFPLP2 and HEP-RECG-DEPEN. The latter is quantified on the assumption of a low dependency.

Non-HEP Probabilities

In the case of LP2-OMK-U, both firewater pumps are available. Failure of both firewater pumps is represented by basic event FP-2PUMPS-FTF.

In the case of LP2-OMK-L, only the diesel-driven firewater pump is available, and its failure is represented by basic event FP-DGPUMP-FTF.

The pump may be required to run 8 to 10 hours at the most (250 gpm capacity), given that the water inventory drops by 20 ft (i.e., 3 ft above the top of the fuel). A failure probability of $3.7\text{E-}3$ for failure to start and run for the electric pump and 0.18 for the diesel driven pump are used from INEL-96/0334. These individual pump failures result in a value of 0.18 for event FP-DGPUMP-FTF and $6.7\text{E-}4$ for event FP-2PUMPS-FTF.

The dependency between makeup water supply (e.g., fragility of the fire water supply tank) to events that may have caused the loss of offsite power (such as for high winds) is assumed to be bounded by the dependency modeled in the HEPs.

4.4.4.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-RECG-FWST-SW	1.0E-4
HEP-RECG-DEPEN	5.0E-2
HEP-FW-START-SW	1.0E-3
HEP-FW-REP-DEPSW	7.0E-2
HEP-FW-REP-NODSW	2.5E-2
FP-2PUMPS-FTF	6.7E-4
FP-DGPUMP-FTF	1.8E-1
FP-DGPUMP-SW	5.0E-1

4.4.5 Top Event OFD – Operator Recovery Using Off-site Sources

4.4.5.1 Event Description and Timing

Given the failure of recovery actions using on-site sources, this event accounts for recovery of coolant makeup using off-site sources such as procurement of a fire engine. Adequate time is available for this action, provided that the operator recognizes that recovery of cooling using on-site sources will not be successful, and that off-site sources are the only viable alternatives. Fault tree LP2-OFD represents this top event for the lower branch (off-site power not recovered), and LP2-OFD-U for the upper branch. These fault trees contains those basic events from the fault trees LP2-OMK-U and LP2-OMK-L that relate to recognition of the need to initiate the firewater system; if OMK fails because the operator failed to recognize the need for firewater makeup, then it is assumed that the operator will fail here for the same reason.

4.4.5.2 Relevant Assumptions

- The operators have 88 hours to provide makeup and inventory cooling.
- Procedures and training are in place that ensure that off-site resources can be brought to bear (NEI commitment no. 2, 3 and 4), and that preparation for this contingency is made when it is realized that it may be necessary to supplement the pool makeup.
- Procedure explicitly states that if the water level drops below a certain level (e.g., 15 ft below normal level) operator must initiate recovery using off-site sources.
- Off-site resources are familiar with the facility.

4.4.5.3 Quantification

Human Error Probability

The event HEP-INV-OFFSITE represents failure to take the extreme measure of using off-site sources, given that even though there has been ample time up to this point to attempt recovery of both the SFP cooling system and both firewater pumps it has not been successful. This top event includes failures of both the diagnosis of the need to provide inventory from off-site sources, and the action itself. The contribution from the failure to diagnose is assessed by assuming a low level of dependence to account for the possible detrimental effects of the failure to complete prior tasks successfully. A relatively low contribution of 3E-02 is assumed for failure to complete the task, based on the fact that there are between five and six days for recovery of the infrastructure following a severe weather event. This results in a total HEP of 8E-02. NEI commitments 3 and 4 provide a basis for this relatively low number.

4.4.5.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-INV-OFFSITE	8.0E-2

4.4.6 Summary

Table 4.4 presents a summary of basic events used in the event tree for Loss of Off-site Power from severe weather events.

As in the case of the loss of off-site power from plant centered and grid related events, based on the assumptions made, the frequency of core uncover can be seen to be very low. Again, a careful and thorough adherence to NEI commitments 2, 5, 8 and 10, the assumption that walk-downs are performed on a regular, (once per shift) basis is important to compensate for potential failures to the instrumentation monitoring the status of the pool, the assumption that the procedures and/or training are explicit in giving guidance on the capability of the fuel pool makeup system, and when it becomes essential to supplement with alternate higher volume sources, the assumption that the procedures and training are sufficiently clear in giving guidance on early preparation for using the alternate makeup sources, are crucial to establishing the low frequency. NEI commitment 3, related to establishing communication between on site and off site organizations during severe weather, is also important, though its importance is somewhat obscured by the assumption of dependence between the events OMK and OFD. However, if no such provision were made, the availability of off-site resources could become more limiting.

Table 4.4 Basic Event Summary for Severe Weather Loss of Off-site Power

Basic Event Name	Description	Basic Event Probability
IE-LP2	LOSP event due to severe-weather-related causes	1.1E-02
HEP-DIAG-SFPLP2	Operators fail to diagnose loss of SFP cooling due to loss of off-site power	2.0E-5
HEP-RECG-DEPEN	Failure to recognize need to cool pool given prior failure	5.0E-2
HEP-SFP-STR-LP2	Operators fail to restart and align the SFP cooling system once power is recovered	5.0E-4
HEP-RECG-FWST-SW	Operators fail to diagnose need to start the firewater system	1.0E-4
HEP-FW-START-SW	Operators fail to start firewater pump and provide alignment	1.0E-3
HEP-FW-REP-DEPSW	Repair crew fails to repair firewater system	7.0E-2
HEP-FW-REP-NODSW	Repair crew fails to repair firewater system	2.5E-2
HEP-INV-OFFST-SW	Operators fail to provide alternate sources of cooling from off-site	8.0E-2
REC-OSP-SW	Recovery of off-site power within 24 hours	2.0E-2
SPC-CKV-CCF-H	Heat exchanger discharge check valves – CCF	1.9E-5
SPC-CKV-CCF-M	SFP cooling pump discharge check valves - CCF	3.2E-5
SPC-HTX-CCF	SFP heat exchangers – CCF	1.9E-5
SPC-HTX-FTR	SFP heat exchanger cooling system fails	2.4E-4
SPC-HTX-PLG	Heat exchanger plugs	2.2E-5
SPC-PMP-CCF	SFP cooling pumps – common cause failure	5.9E-4

Basic Event Name	Description	Basic Event Probability
SPC-PMP-FTF-1	SFP cooling pump 1 fails to start and run	3.9E-3
SPC-PMP-FTF-2	SFP cooling pump 2 fails to start and run	3.9E-3
FP-2PUMPS-FTF	Failure of firewater pump system	6.7E-4
FP-DGPUMP-FTF	Failure of the diesel-driven firewater pump	1.8E-1

4.5 Loss of Inventory Event Tree

This event tree (Figure 4.5) models general loss of inventory events, that are not the result of catastrophic failures that could result from events such as dropped loads, tornado missiles, or seismic events. The following assumption was made in the development of the event tree.

- Maximum depth of siphon path is assumed to be 15 ft. below the normal pool water level (related to NEI commitments 6 and 7). Once the water level drops 15 ft below the normal pool water level, the losses would be only from the boil-off. This assumption may be significant, and potentially non-conservative for sites that do not adopt NEI commitments 6 and 7.

4.5.1 Initiating Event LOI – Loss of Inventory

4.5.1.1 Event Description and Timing

This initiator (IE–LOI) includes loss of coolant inventory from events such as those resulting from configuration control errors, siphoning, piping failures, and gate and seal failures. Operational data provided in NUREG-1275 (Ref. 12), show that the frequency of loss of inventory events in which the level decreased more than one foot can be estimated to be less than one event per 100 reactor years. Most of these events were the result of operator error and were recoverable. NUREG-1275 shows that, except for one event that lasted for 72 hours, there were no events that lasted more than 24 hours. Eight events resulted in a level decrease of between one and five feet and another two events resulted in an inventory loss of between five and 10 feet.

4.5.1.2 Relevant Assumption

- NEI commitments 6 and 7 will reduce the likelihood of a significant initiating event.

4.5.1.3 Quantification

The data reviewed during the development of NUREG-1275 (Ref. 12) indicated fewer than one event per 100 years in which level decreased over one foot. This would give a frequency of

1E-02. However, it is assumed that the NEI commitments 6 and 7 when implemented will reduce this frequency by an order of magnitude or more. Thus the frequency is estimated as 1E-03 per year.

4.5.2 Top Event NLL – Loss Exceeds Normal Makeup Capacity

4.5.2.1 Event Description and Timing

This phenomenological event divides the losses of inventory into two categories: those for which the leak size exceeds the capacity of the SFP makeup and therefore require isolation of the leak, and those for which the SFP makeup system's capacity is sufficient to prevent fuel uncover without isolation of the leak.

4.5.2.2 Relevant Assumptions

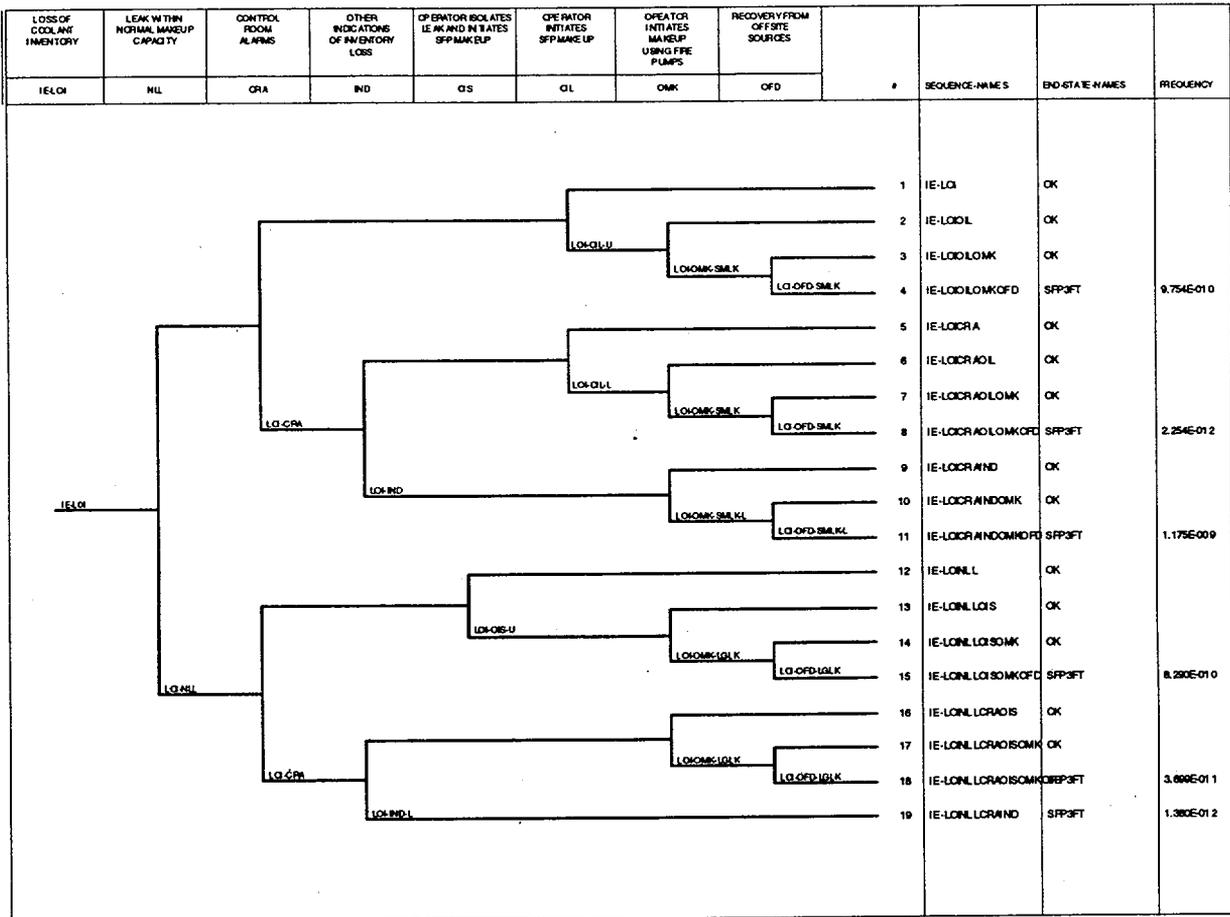
- In the case of a large leak, a leak rate is assumed to be twice the capacity of the SFP makeup system, i.e., 60 gpm. Although a range of leak rates is possible, the larger leak rates are postulated to be from failures in gates, seals, or from large siphoning events, and NEI commitments 6 and 7 will go a considerable way toward minimizing these events.
- The small leak is assumed for analysis purposes to be at the limit of the make-up system capacity, i.e., 30 gpm.

4.5.2.3 Quantification

Non-HEP Probabilities

This top event is quantified by a single basic event, LOI-LGLK. From Table 3.2 of NUREG-1275, there were 38 events that lead to a loss of pool inventory. If we do not consider the load drop event (because this is treated separately), we have 37 events. Of these, 2 events involved level drops greater than 5 feet. Therefore, a probability of large leak event would be $2/37 \approx 0.06$ (6%). For the other 94% of the cases, operation of the makeup pump is sufficient to prevent fuel uncover.

Figure 4.5 Loss of inventory event tree



4.5.3 Top Event CRA – Control Room Alarms

4.5.3.1 Event description and Timing

This top event represents the failure of the control room operators to respond to the initial loss of inventory from the spent fuel pool. This top event is represented by fault tree LOI-CRA. Depending on the leak size, the timings for the water level to drop below the level alarm set point (assumed 1 ft below the normal level) would vary. It is estimated that water level would drop below the low-level alarm set point in about 4 hours in the case of a small leak and in the case of a large leak, it would take 1 to 2 hours. Failure to respond could be due to operator failure to respond to an alarm, or loss of instrumentation system. Success for this event is defined as the operators recognizing the alarm as indicating a loss of inventory.

4.5.3.2 Relevant Assumptions

- Regular test and maintenance is performed on instrumentation (NEI commitment no. 10).
- Procedures are available to guide the operators on response to off-normal conditions, and the operators are trained on the use of these procedures (NEI commitment no. 2).
- System drawings are revised as needed to reflect current plant configuration.
- SFP water level indicator is provided in the control room (NEI commitment no. 5).
- SFP low-water level alarm (narrow range) is provided in the control room (NEI commitment no. 5).
- Low level alarm set point is set to one foot below the normal level.

4.5.3.3 Quantification

Human Error Probabilities

One operator error, HEP-DIAG-ALARM is modeled under this top event. This event represents operator failure to respond after receiving a low-level alarm. Success is defined as the operator investigating the alarm and identifying the cause. This failure was quantified using The Technique for Human Error Prediction (THERP) Table 20-23. No distinction is made between the two leak sizes because this is treated as a simple annunciator response.

Non-HEP Probabilities

The value used for local faults leading to alarm channel failure, SPC-LVL-LOF (2.0E-3), was estimated based on information in NUREG-1275, Volume 12. This includes both local electrical faults and instrumentation faults.

4.5.3.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-DIAG-ALARM	3.0E-4
SPC-LVL-LOF	2.0E-3

4.5.4 Top Event IND – Other Indications of Inventory Loss

4.5.4.1 Event Description and Timing

This top event models operator failure to recognize the loss of inventory during walk-downs over subsequent shifts. Indications available to the operators include read-outs in the control room, and a visibly decreasing water level. Eventually, when pool cooling is lost the environment would become noticeably hot and humid. Success for this event, in the context of the event tree, is treated differently for the small and large leaks.

For the small leak, it is defined as the operator recognizing the abnormal condition and understanding its cause in sufficient time to allow actions to prevent pool cooling from being lost. Failure of this top event does not lead to fuel uncover. This top event is represented by the functional fault tree LOI-IND. Following an alarm, the operators would have in excess of 8 hrs before the water level would drop below the SFP cooling suction level. Therefore, for this event, only one shift is credited for recognition.

For the large leak, success is defined as recognizing there is a leak in sufficient time to allow make-up from alternate sources (fire water and off-site sources) before fuel uncover. This top event is represented by the basic event LOI-IND-L. Based on the success criterion, there are many more opportunities for successive crews to recognize the need to take action. If the leakage is in the SFP cooling system, the leak would be isolated automatically once the water level drops below the SFP suction level. In this case, it would take more than 88 hrs (heatup plus boil-off) for the water level to reach 3 ft above the top fuel and the event would be similar to loss of spent fuel pool cooling. For the purpose of this analysis, it is assumed that leakage path is assumed to be below SFP cooling system suction level. It is assumed that once the water level drops 15 ft below normal pool level the leak is isolated automatically, and the inventory losses would be only due to boil-off. Time needed to boil-off to 3 ft above the top fuel is estimated to be 25 hours. Therefore, depending on the size of the leak and location and heatup rate, the total time available for operator actions after the first alarm before the water level drops below the SFP suction level to the 3 ft above the top of fuel would be more than 40 hrs. Furthermore, the indications become increasingly more compelling; with a large leak it would be expected that the water would be clearly visible, the level in the pool is obviously decreasing, and as the pool boils the environment in the pool area becomes increasingly hot and humid. Because of these very obvious physical changes, no dependence is assumed between the event IND and the event CRA. This lack of dependence is however, contingent on the fact that the operating crews performing walkdowns on a regular basis.

4.5.4.2 Relevant assumptions

- Operators have more than 40 hrs in the case of a large leak to take actions after the first alarm before the water level drops to the 3 ft above the top of fuel.

- SFP water level indicator is provided in the control room e.g., camera or digital readout.
- SFP low-water level alarm (narrow range) is provided in the control room.
- System drawings are revised as needed to reflect current plant configuration.
- Procedure/guidance exist for the operators to recognize and respond to indications of loss of inventory, and they are trained in the use of these procedures (NEI commitment no. 2).
- Water level measurement stick with clear marking is installed in the pool at a location that is easy to observe
- Operators are required to make a round per shift and document walkdowns in a log
- Training plans are revised as needed to reflect the changes in equipment configuration as they occur

4.5.4.3 Quantification

Human Error Probabilities

The top event LOI-IND, for small leaks, includes two HEPs, depending on whether the control room alarms have failed, or the operators failed to respond to the alarms. If the operators failed to respond to control room alarms, then event HEP-WLKDOWN-DEPEN models the failure of the next shift to recognize the loss of cooling during a walkdown or during a control room review, taking into account a potential dependence on event HEP-DIAG-ALARM. A low dependence is assumed. If the alarms failed, then event HEP-WLKDOWN-LOI models operator's failure to recognize the loss of inventory during walkdowns, with no dependence on previous HEPs. Because only one crew is credited, the HEP is estimated as 5E-03.

This failure probability is developed using THERP, and is based upon three individual failures: failure to carry out an inspection, missing a step in a written procedure, and misreading a measuring device.

The top event LOI-IND-L is modeled taking into account several opportunities for recovery by consecutive crews, and because the indications are so compelling no dependency is assumed between this HEP and the prior event.

4.5.4.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-WLKDOWN-DEPEN	5.0E-2
HEP-WLKDOWN-LOI-L	1.0E-5
HEP-WLKDOWN-LOI	5.0E-3

4.5.5 Top Event OIS – Operator Isolates Leak and Initiates SFP Makeup

4.5.5.1 Event Description and Timing

This top event represents the operator's failure to isolate a large leak and initiate the SFP makeup system before the pool level drops below the SFP cooling system suction, and is represented by the fault tree LOI-OIS-U. Failure requires that the operators must provide the inventory using the firewater system or off-site resources.

The critical action is the isolation of the leak. With the leak size assumed, and on the assumption that the low level alarm is set at 1 foot below the normal level, the operators have 4 hours to isolate the leak. Once the leak has been isolated, there would be considerable time available to initiate the normal make-up, since pool heat up to the point of initiation of boiling takes several hours.

If the loss of inventory is discovered through walkdowns, it is assumed that there is not enough time available to isolate the leak in time to provide for SFP makeup system success, and this event does not appear on the failure branch of event CRA.

4.5.5.2 Relevant Assumptions

- System drawings are kept up to date and training plans are revised as needed to reflect changes in plant configuration.
- With an assumed leak rate of 60 gpm, the operator has in excess of 4 hrs to isolate the leak and provide makeup.
- There are procedures to guide the operators in how to deal with loss of inventory, and the operators are trained in their use (NEI commitment no. 2).
- Spent fuel pool operations that have the potential to rapidly drain the pool will be under strict administrative controls (NEI commitment no. 9). This increases the likelihood of the operators successfully terminating a leak should one occur.

4.5.5.3 Quantification

Human Error Probabilities

Two human failure events are included in the functional fault tree LOI-OIS, one for failure to start the SFP makeup pump, HEP-MKUP-START, and one for failure to successfully isolate the leak, HEP-LEAK-ISO.

SPAR HRA worksheets were used to quantify each of these errors. For HEP-MKUP-START, it was assumed that the operator is experiencing a high stress level, he is highly trained, the equipment associated with the task is well labeled and matched to a quality procedure, and the crew has effective interactions in a quality facility.

For HEP-LEAK-ISO, it was assumed that the operators would be experiencing a high level of stress, the task is highly complex due to the fact that it is necessary to identify the source of the leak and it may be difficult to isolate, the operators are highly trained, have all the equipment available, and all components are well labeled and correspond to a procedure, and the crew has effective interactions in a quality facility.

Hardware Failure Probabilities

Unavailability of a SFP makeup system, SFP-REGMKUP-F, was assigned a value of 5.0E-2 from INEL-96/0334. It is assumed that the SFP makeup system is maintained since it is required often to provide makeup.

4.5.5.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-LEAK-ISO	1.3E-3
HEP-MKUP-START	2.5E-4
SFP-REGMKUP-F	5.0E-2

4.5.6 Top Event OIL – Operator Initiates SFP Makeup System

4.5.6.1 Event Description and Timing

This top event represents the failure to initiate the SFP makeup system in time to prevent loss of spent fuel pool cooling, for a small leak. This top event is represented by the fault trees LOI-OIL-U and LOI-OIL-L, which include contributions from operator error and hardware failure. The leak is small enough that isolation is not required for success. If the operators respond to the initiator early (i.e., CRA is successful), they would have more than 8 hours to terminate the event using the SFP makeup system before the water level drops below the SFP suction level. If operators respond late (i.e., IND success), it is assumed that they would have on the order of 4 hours, based on the leak initiating at the start of one shift and the walkdown taking place at shift turnover.

4.5.6.2 Relevant Assumptions

- There are procedures to guide the operators in how to deal with loss of inventory, and the operators are trained in their use (NEI commitment no. 2).
- The manipulations required to start the make-up system can be achieved in less than 10 minutes.

4.5.6.3 Quantification

Human Error Probabilities

In the case of an early response, the operator would have more than 8 hours available to establish SFP makeup and the failure is represented by the basic event HEP-MKUP-START (see fault tree L OI-OIL-U). In the case of a late response, the operator is assumed to have

4 hours available to establish SFP makeup and is represented by the basic event HEP-MKUP-START-L (see fault tree L OI-OIL-L). Success is defined as the operator starting the makeup pump and performing valve manipulation as needed.

SPAR HRA worksheets were used to quantify each of these errors. For HEP-MKUP-START it was assumed that the 8 hour time window will allow more than 50 times the time required to complete this task, the operators are under high stress, are highly trained, have equipment that is well labeled and matched to a procedure, and the crew has effective interactions in a quality facility. For HEP-MKUP-START-L, the time available is not as extensive, and is considered nominal, all other PSFs being equal.

Hardware Failure Probabilities

Unavailability of a SFP makeup system, SFP-REGMKUP-F, was assigned a value of 5.0E-2 from INEL-96/0334. It is assumed that the SFP makeup system is maintained since it is required often to provide makeup.

4.5.6.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-MKUP-START-E	2.5E-4
HEP-MKUP-START	2.5E-6
SFP-REGMKUP-F	5.0E-2

4.5.7 Top Event OMK – Operator Initiates Makeup Using Fire Pumps

4.5.7.1 Event Description and Timing

This top event represents failure to provide make-up using the firewater pumps. The case of a large leak is represented by a fault tree LOI-OMK-LGLK. In this case the operators have 40 hours to start firewater system. The case of a small leak is represented by two functional fault trees, LOI-OMK-SMLK, and LOI-OMK-SMLK-L. The difference between the two trees is that in the first, the operators are aware of the problem and are attempting to solve it, whereas in the second, the operators will need to first recognize the problem. In both small leak cases, the operator has more than 65 hrs to start firewater system. In all cases both the firewater pumps would be available.

4.5.7.2 Relevant Assumptions

- The operators have 40 to 65 hours to start a firewater pump depending on the leak size.
- There is a means to remotely align a makeup source to the spent fuel pool without entry to the refuel floor so that makeup can be provided even when the environment is uninhabitable due to steam and/or high radiation (NEI commitment no.8).
- Repair crew is different than on-site operators.
- On average, it takes 10 hours to repair a pump if it fails to start and run.

Formatted Version, Rev. 5 2/1/00 1100 hours

- It takes 16 hours to contact maintenance personnel, make a diagnosis, and get new parts.
- Both firewater pumps are located in a separate structure and are protected from the potential harsh environment in the case of pool bulk boiling.
- Maintenance and testing are performed on diesel and electric firewater pumps to maintain operable status (NEI commitment no. 10).
- There are procedures to guide the operators in how to deal with loss of inventory, and the operators are trained in their use. The guidance on when to begin addition of water from alternate sources is clear and related to a clearly identified condition, such as pool level or onset of boiling (NEI commitment no. 2).

4.5.7.3 Quantification

Human Error Probabilities

Each fault tree includes three human failure events. In the case of a functional fault tree LOI-OMK-SMLK, a basic event EP-RECG-FWSTART represents the failure of the operator to recognize the need to initiate firewater as an inventory makeup system; a basic event HEP-FW-START represents failure to start either the electric or diesel firewater pump; and a basic event HEP-FW-REP-NODSM represents the failure of the repair crew to repair a firewater pump.

For functional fault tree LOI-OMK-SMLK-L, the basic event EP-RECG-FWSTART is replaced by EP-RECG-FWSTART-L. This event requires that the operators recognize that the deteriorating conditions in the spent-fuel pool are due to an inventory loss. The cues will include pool heat up due to the loss of spent fuel pool cooling which should be alarmed in the control room, as well as other physical indications such as increasing temperature and humidity, and a significant loss of level. Because of the nature of the sequence, the failure to recognize the need for action will be modeled by assuming a low dependence between this event and the prior failures.

For functional fault tree LOI-OMK-LGLK, a basic event HEP-RECG-FW-LOI represents the failure of the operator to recognize the need to initiate firewater as an inventory makeup system; a basic event HEP-FW-START-LOI represents failure to start either the electric or diesel firewater pump; and a basic event HEP-FW-REP-NODLG represents the failure of the repair crew to repair a firewater pump.

SPAR HRA worksheets were also used to quantify the HEPs.

HEP-FW-START represents failure to start either the electric or diesel firewater pump (depending upon availability), given that the decision to start a firewater pump was made. No difficult valve alignment is required, but the operator may have to position a hose in the pool area, therefore, expansive time is assumed, with all other OSFs being the same as the other HEPs below.

For HEP-RECG-FWSTART it was assumed that extensive time is available to the operators for diagnosis, that the operators are under high stress, are highly trained, have a diagnostic procedure, have good instrumentation in the form of alarms, and are part of a crew that interacts well in a quality facility.

For HEP-RECG-FW-LOI it was assumed that extra time (>60 minutes) is available to the operators for diagnosis, that the operators are under high stress, are highly trained, have a diagnostic procedure, have good instrumentation in the form of alarms, and are part of a crew that interacts well in a quality facility.

For HEP-FW-START-LOI it was assumed that the operators are under high stress, are engaged in a highly complex task due to its non-routine nature, have a high level of training, have a diagnostic procedure, and are a part of a crew that interacts well in a quality facility.

Basic event HEP-FW-REP-NODS (see fault tree, OIL-OMK-SMLKL) represents the failure of the repair crew to repair a firewater pump for the small leak scenarios. Note that repairing the SFP regular makeup system is not modeled, as there would not be enough time to get help before the SFP makeup would be ineffectual and therefore no dependency was modeled in the failure to repair the firewater system. It is assumed that the operators will focus their recovery efforts on only one pump. Assuming that it takes another 16 hours before technical help and parts arrive, the operators have about 50 hours (65 hours less 16 hours) to repair the pump. Therefore, assuming a 10-hour mean time to repair, the probability of failure to repair the pump would be $\text{Exp}(-(1/10) * 49) = 7.5\text{E-}3$ in the case of a small break scenario.

Basic event HEP-FW-REP-NODLG represents the failure of the repair crew to repair a firewater pump for the large leak scenarios. For this case there would only be 24 hours to repair the pump. Therefore, assuming a 10-hour mean time to repair, the probability of failure to repair the pump would be $\text{Exp}(-(1/10) * 24) = 9.0\text{E-}2$ in the case of a large break scenario.

Hardware Failure Probabilities

Failure of both firewater pumps is represented by basic event FP-2PUMPS-FTF. The pump may be required to run 8 to 10 hours at the most (250 gpm capacity), given that the water inventory drops by 20 ft (i.e., 3 ft from the top of the fuel). A failure probability of $3.7\text{E-}3$ for failure to start and run for the electric pump and 0.18 for the diesel driven pump are used from INEL-96/0334. These individual pump failures result in a value $6.7\text{E-}4$ for basic event FP-2PUMPS-FTF.

4.5.7.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-RECG-FWSTART	2.0E-5
HEP-RECG-FWSTART-L	5E-02
HEP-FW-START	1.0E-5
HEP-FW-REP-NODSM	7.5E-3
HEP-FW-REP-NODLG	9.0E-2

FP-2PUMPS-FTF	6.7E-4
HEP-RECG-FW-LOI	2.0E-4
HEP-FW-START-LOI	1.3E-3

4.5.8 Top Event OFD – Recovery From Off-site Sources

4.5.8.1 Event Description and Timing

Given the failure of recovery actions using on-site sources, this event accounts for recovery of coolant makeup using off-site sources such as procurement of a fire engine. This event is represented by the fault trees LOI-OFD-LGLK, LOI-OFD-SMLK and LOI-OFD-SMLK-L for the large break and two small break scenarios, respectively.

4.5.8.2 Relevant Assumptions

- The operator has 40 to 65 hours depending on the break size to provide makeup inventory and cooling.
- Procedure explicitly states that if the water level drops below a certain level (e.g., 15 ft below normal level) operator must initiate recovery using off-site sources.
- Operator has received formal training and there are procedures to guide him.
- Off-site resources are familiar with the facility.

4.5.8.3 Quantification

Human Error Probabilities

The only new basic events in these functional fault trees are HEP-INV-OFFST-LK and HEP-INV-OFFST. They were quantified using SPAR HRA worksheets. The diagnosis of the need to initiate the action is considered totally dependent on the recognition of the need to initiate inventory makeup with the fire water system. The PSFs are as follows: extreme stress (it's the last opportunity for success), high complexity because of the involvement of off-site personnel, highly trained staff with good procedures, good ergonomics (equipment is available to make off-site support straightforward) and good work processes. For both cases, a low level of dependence was assumed on the failure of prior tasks.

4.5.8.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-INV-OFFST-LK	5.0E-2
HEP-INV-OFFSITE	5.0E-2

4.5.9 Summary

Table 4.5 presents a summary of basic events.

As in the previous cases, the frequency of core uncovering can be seen to be very low. Again, a careful and thorough adherence to NEI commitments 2, 4, 5, 8 and 10, the assumption that walk-downs are performed on a regular, (once per shift) basis is important to compensate for potential failures to the instrumentation monitoring the status of the pool, the assumption that the procedures and/or training are explicit in giving guidance on the capability of the fuel pool makeup system, and when it becomes essential to supplement with alternate higher volume sources, the assumption that the procedures and training are sufficiently clear in giving guidance on early preparation for using the alternate makeup sources, are crucial to establishing the low frequency. NEI commitments 6, 7 and 9 have been credited with lowering the initiating event frequency.

Table 4.5 Basic Event Summary for the Loss of Inventory Event Tree

Basic Event Name	Description	Basic Event Probability
IE-LOI	Loss of inventory initiating event	1.0E-3
HEP-DIAG-LGLK	Operators fail to respond to a signal indication in the control room (large leak)	4.0E-4
HEP-DIAG-ALARM	Operators fail to respond to a signal indication in the control room	3.0E-4
HEP-WLKDOWN-LOI	Operators fail to observe the LOI/loss of cooling in walk-downs, given failure to prevent loss of SFP cooling	5.0E-3
HEP-WLKDOWN-LOI-L	Operators fail to observe the LOI/loss of cooling in walk-downs (independent case)	1.0E-5
HEP-WLKDOWN-DEPEN	Operators fail to observe the LOI event walk-downs (dependent case)	5.0E-2
HEP-RECG-FW-LOI	Operators fail to diagnose need to start the firewater system	2.0E-4
HEP-RECG-FWSTART	Operators fail to diagnose need to start the firewater system	2.0E-5
HEP-RECG-FWSTART-L	Operators fail to diagnose need to start the firewater system given he failed to prevent loss of SFP cooling	5.0E-2
HEP-LEAK-ISO	Operators fail to isolate leak	1.3E-3
HEP-FW-START-LOI	Fails to start firewater pumps	1.3E-3
HEP-FW-START	Operators fail to start firewater pump and provide alignment	1.0E-5
HEP-FW-REP-NODLG	Fails to repair firewater pump (20 hrs)	9.0E-2
HEP-FW-REP-NODSM	Fails to repair firewater pump (49 hrs)	7.5E-3
HEP-INV-OFFST-LK	Operators fail to recover via off-site sources	5.0E-2
HEP-INV-OFFSITE	Operators fail to provide alternate sources of cooling from off-site	5.0E-2
FP-2PUMPS-FTF	Failure of firewater pump system	6.7E-4
LOI-LGLK	Loss exceeds normal makeup normal	6.0E-2
HEP-MKUP-START	Operators fail to start makeup (small leak)	2.5E-6
HEP-MKUP-START-E	Operators fail to start makeup (Early Respond)	2.5E-4
HEP-MKUP-START-L	Operators fail to start makeup (Late Respond)	1.0
SFP-REGMKUP-F	Regular SFP makeup system fails	5.0E-2
SPC-LVL-LOF	Failure of control room alarm channel	1.0E-5
SPC-LVL-LOP	Electrical faults leading to alarm channel failure	2.0E-3

5.0 Summary of Results

The results of this analysis provide insight into the risks associated with storage of spent nuclear fuel in fuel pools at decommissioned nuclear power plants. The five accident initiators that were analyzed consist of: 1) internal fires, 2) Loss of cooling, 3) loss of inventory, 4) plant/grid centered losses of off-site power, and 5) severe weather induced losses of off-site power. The total frequency for the endstate is estimated to be $2.3E-7$ /year. Table 5.1 summarizes the fuel uncover frequency for each initiator. The frequencies are point estimates, based on the use of point estimates for the input parameters. For the most part these input parameter values would be used as the mean values of the probability distributions that would be used in a calculation to propagate parameter uncertainty. Because the systems are essentially single train systems, the point estimates closely correlate to the mean values that would be obtained from a full propagation of parameter uncertainty.

The numerical results are a function of the assumptions made and in particular, the model used to evaluate the human error probabilities. The results represent a reasonable assessment of the levels of risk that are achievable, given an appropriate level of attention to managing the facility with a view to ensuring the health and safety of the public. Alternate HRA models could result in frequencies that differ by an order of magnitude. However, given the time scales involved, and the simplicity of the systems, we believe that the conclusions of this study, namely that the risks are low, and that the NEI commitments play an important role in determining that low level, are robust.

Certain assumptions may be identified as having the potential for significantly influencing the results. For example, the calculated time windows associated with the loss of inventory event tree are sensitive to the assumptions about the leak size. The SPAR HRA method is, however, not highly sensitive to the time windows assumed, primarily making a distinction between time windows that represent an inadequate time, barely adequate, nominal, extra time, and expansive time. The precise definitions of these terms can be found in Reference 9. Consequently, the assumption of the large leak rate as 60 gpm is not critical. For the loss of inventory event tree, the assumption that the leak is self-limiting after a drop in level of 15 feet, may be a more significant assumption that, on a site specific basis may be non-conservative. The assumption that the preparation time of several days is adequate to bring offsite sources to bear may be questioned in the case of extreme conditions. However, the very conservative assumption that this is guaranteed to fail would change the corresponding event sequences by about an order of magnitude.

The analysis show that, based on the assumptions made, the frequency of fuel uncover from the loss of cooling, loss of inventory, loss of off-site power and fire initiating events is very low. The assumptions that have been made include that the licensee has adhered to NEI commitments 2, 4, 5, 8 and 10. In order to take full credit for these commitments, additional assumptions concerning how these commitments will be implemented have been made. These include: procedures and/or training are explicit in giving guidance on the capability of the fuel pool makeup system, and when it becomes essential to supplement with alternate higher volume sources; procedures and training are sufficiently clear in giving guidance on early preparation for using the alternate makeup sources; walk-downs are performed on a regular, (once per shift) basis. The latter is important to compensate for potential failures to the instrumentation monitoring the status of the pool.

NEI commitment 3, related to establishing communication between on site and off site organizations during severe weather, is also important, though its importance is somewhat obscured in the analysis by the assumption that there is some degree of dependence between the decision to implement supplemental makeup to the spent fuel pool from on-site sources such as fire water pumps, and that from off-site sources. However, if no such provision were made, the availability of off-site resources could become more limiting.

NEI commitments 6, 7 and 9 have been credited with lowering the initiating event frequency for the loss of inventory events from its historical levels.

This analysis has, demonstrated to the staff that, given an appropriate implementation of the NEI commitments, the risk is indeed low, and would warrant consideration of granting exemptions. Without credit for these commitments, the risk will be more than an order of magnitude higher.

Table 5.1 Summary of Results

Initiating Event	Core Uncovery Frequency (per/yr)
Internal Fires	4.5E-08
Loss of Cooling	1.4E-08
Loss of Inventory	3.1E-09
Loss of Offsite Power (plant centered & grid-related events)	3.0E-8
Loss of Offsite Power (severe weather events)	1.3E-7
TOTAL =	2.3E-007

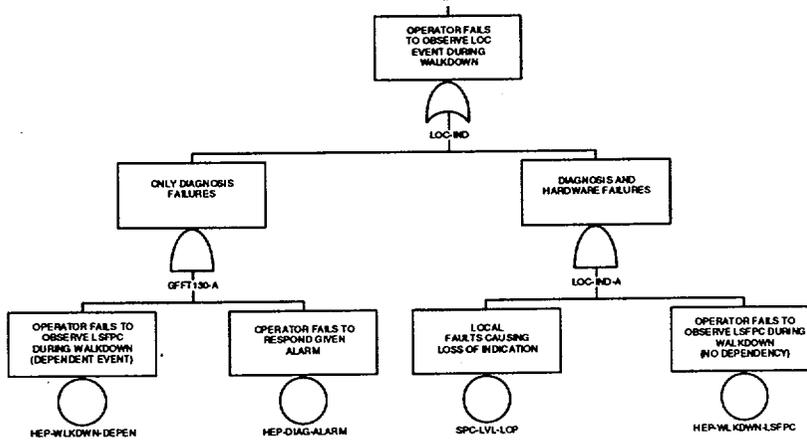
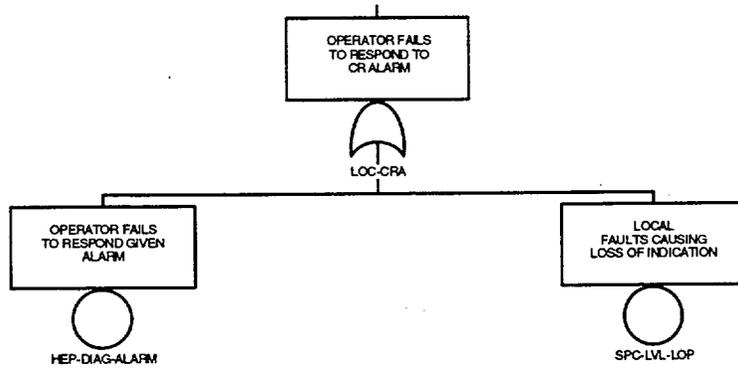
6.0 REFERENCES

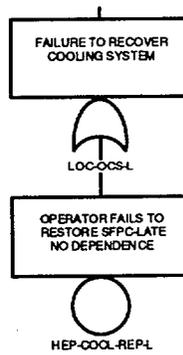
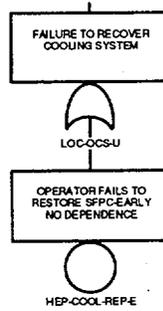
1. Memorandum, G. M. Holahan (NRC) to J. A. Zwolinski (NRC), "Preliminary Draft Technical Study of Spent Fuel Pool Accidents for Decommissioning Plants," June 16, 1999.
2. Letter from L. Hendricks of the Nuclear Energy Institute (NEI) to R. Barrett of the USNRC, dated November 12, 1999.
3. Letter, J. A. Lake (INEEL) to G. B. Kelly (NRC), "Details for the Spent Fuel Pool Operator Dose Calculations," CCN# 00-000479, October 20, 1999.
4. K. D. Russell, et al., "Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE), Version 5.0: Technical Reference Manual," NUREG/CR-6116, July 1994.
5. Williams, J. C., "A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance", in Proceedings of the 1988 IEEE Conference on Human Factors and Poer PLants, Monterey, Ca., June 5-9, 1988, pp 436-450, Institute of Electrical and Electronics Engineers, New York, NY, 1988.
6. Hollnagel, E., "Cognitive Reliability and Error Analysis Method - CREAM" Elsevier, 1998.
7. Cooper, S. E., et al, "A Technique for Human Error Analysis (ATHEANA), NUREG/CR-6350, May 1996, USNRC.
8. Swain, A. D., and Guttman, H. E., "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", (THERP), NUREG/CR-1278, August 1983, USNRC.
9. Byers, J.C., et al., "Revision of the 1994 ASP HRA Methodology (Draft)", INEEL/EXT-99-00041, January 1999.
10. Sailor, et. al., "Severe Accidents in Spent Fuel Pools in Support of Generic Issue 82", NUREG/CR-4982 (BNL-NUREG-52093), July 1987.
11. U.S. Nuclear Regulatory Commission, "Control of Heavy Loads at Nuclear Power Plants, Resolution of Generic Technical Activity A-36," NUREG-0612, July 1980.
12. U.S. Nuclear Regulatory Commission, "Operating Experience Feedback Report - Assessment of Spent Fuel Cooling," NUREG-1275, Volume 12, February 1997.
13. Idaho National Engineering and Environmental Laboratory, "Loss of Spent Fuel Pool Cooling PRA: Model and Results," INEL-96/0334, September 1996.
14. Electric Power Research Institute, "Fire-Induced Vulnerability Evaluation (FIVE)," EPRI TR-100370s, April 1992.

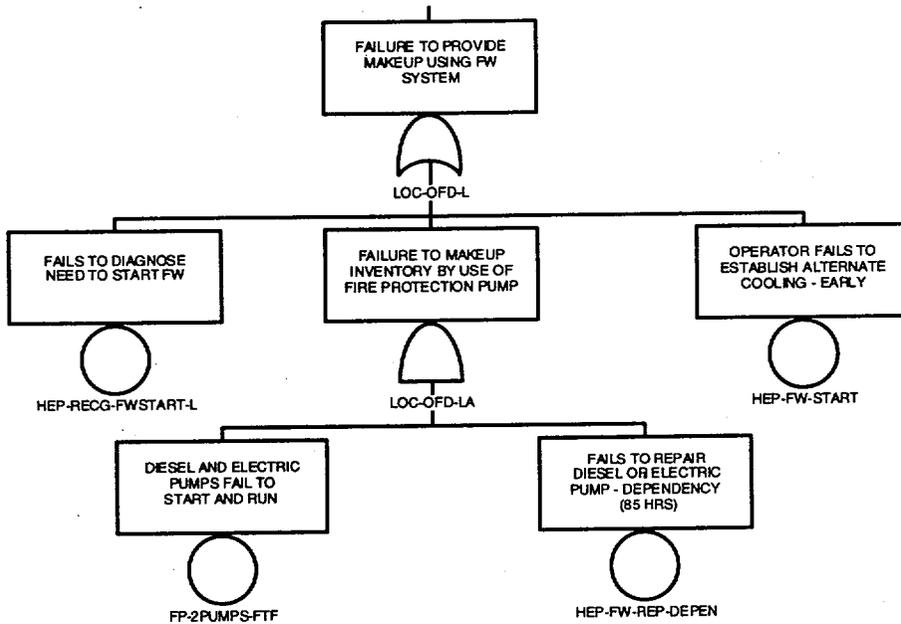
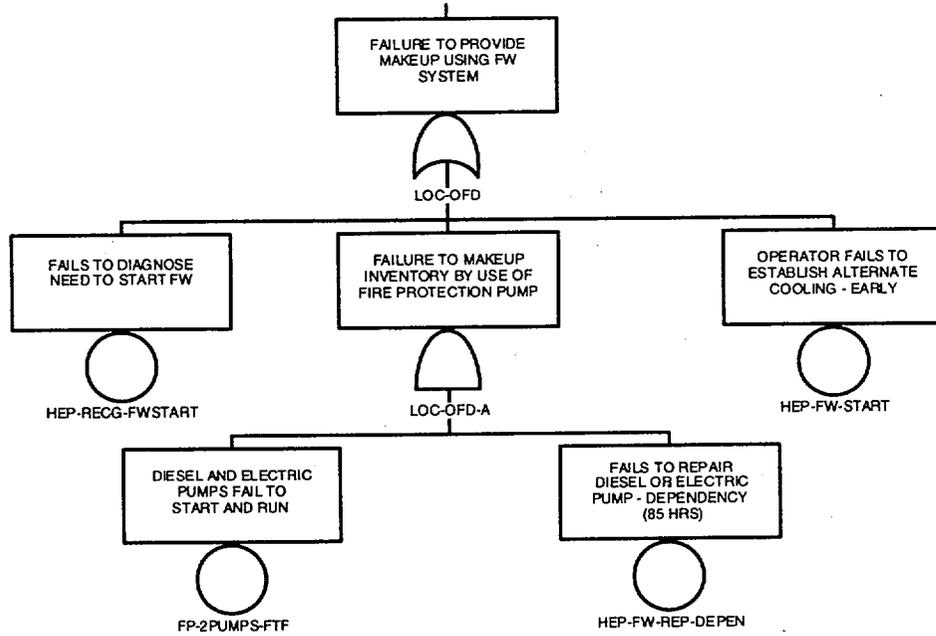
Formatted Version, Rev. 5 2/1/00 1100 hours

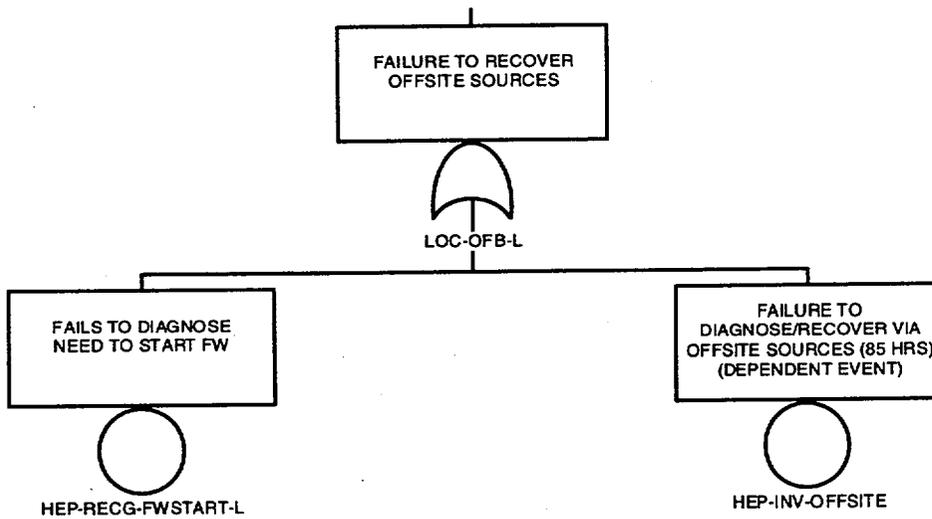
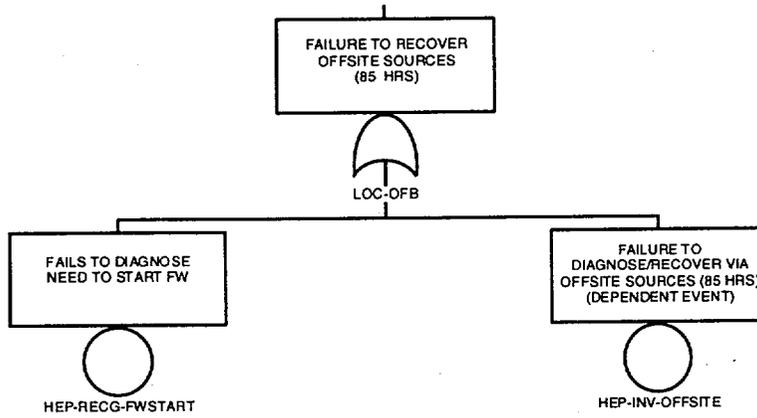
15. OREDA-92 Offshore Reliability Data Handbook, 2nd Edition, 1992.
16. Atwood, et. al., "Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980 - 1996," NUREG/CR-5486, November 1998.
17. U.S. Nuclear Regulatory Commission, "Evaluation of Station Blackout Accidents at Nuclear Power Plants," NUREG-1032, June 1988.
18. U.S. Nuclear Regulatory Commission, "Single-Failure-Proof Cranes for Nuclear Power Plants," USNRC Report NUREG-0554, May 1979.

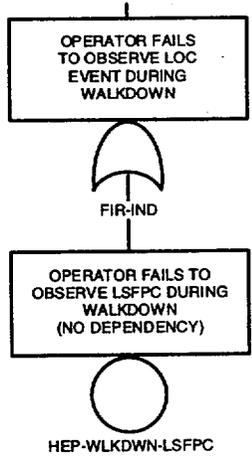
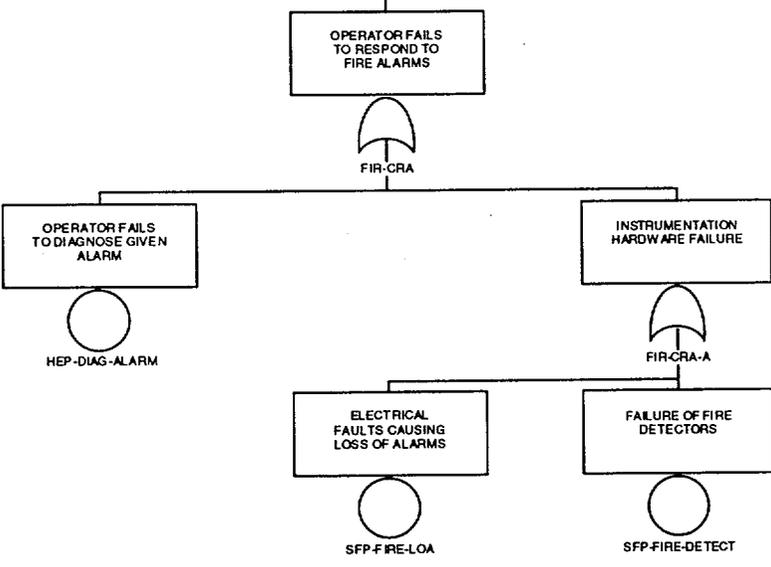
ATTACHMENT A
FAULT TREES USED IN THE RISK ANALYSIS

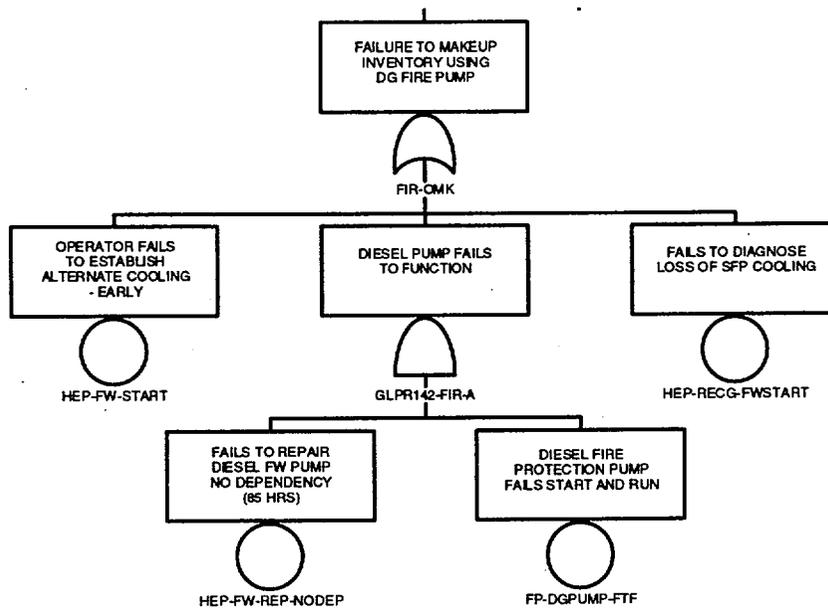
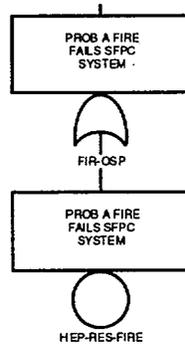


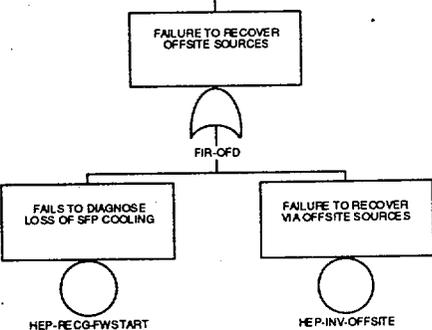


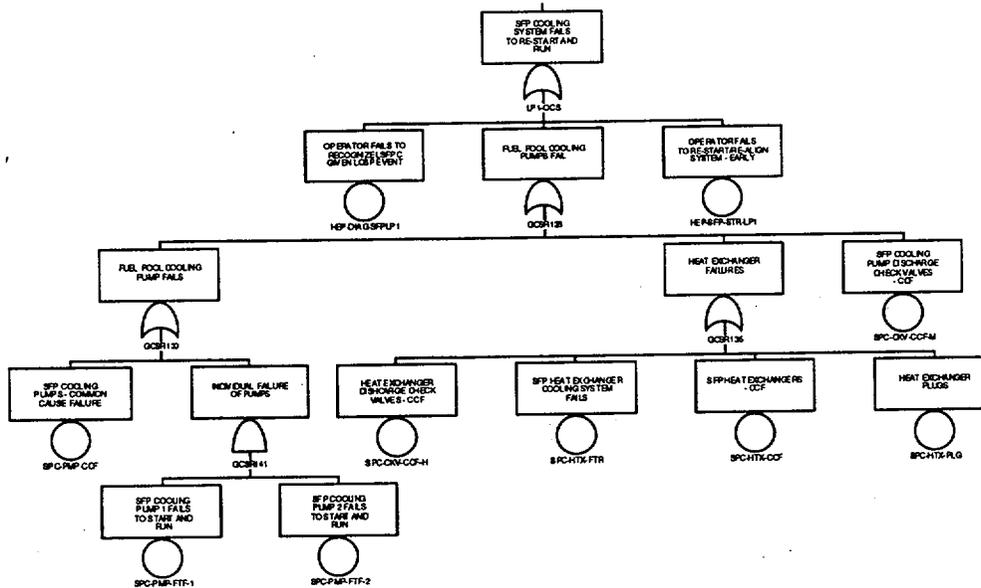
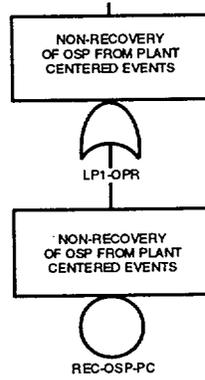


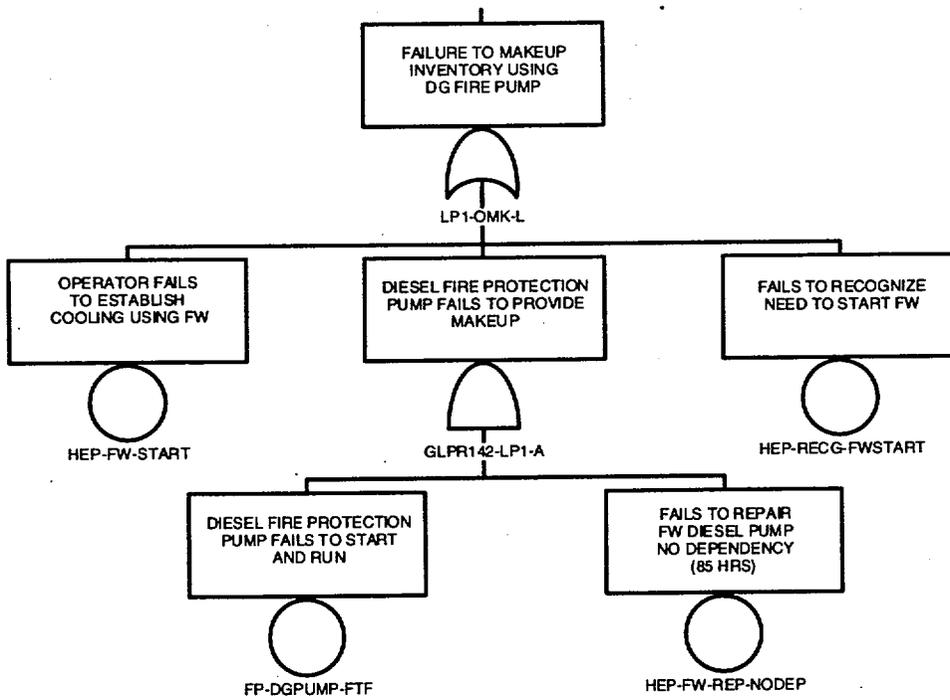
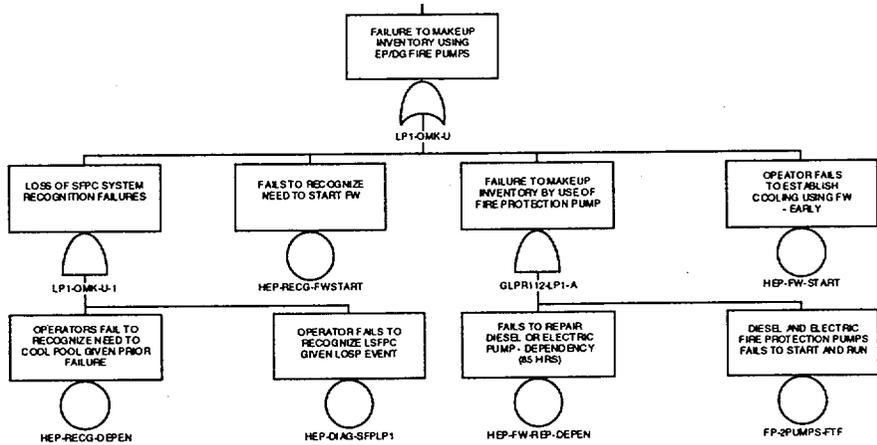


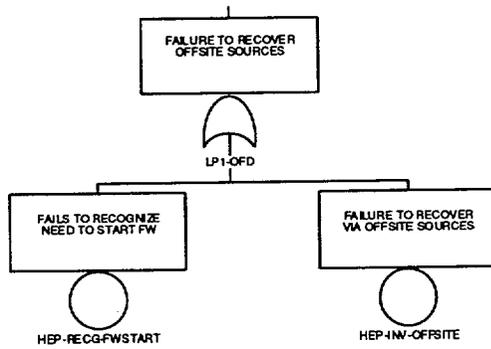
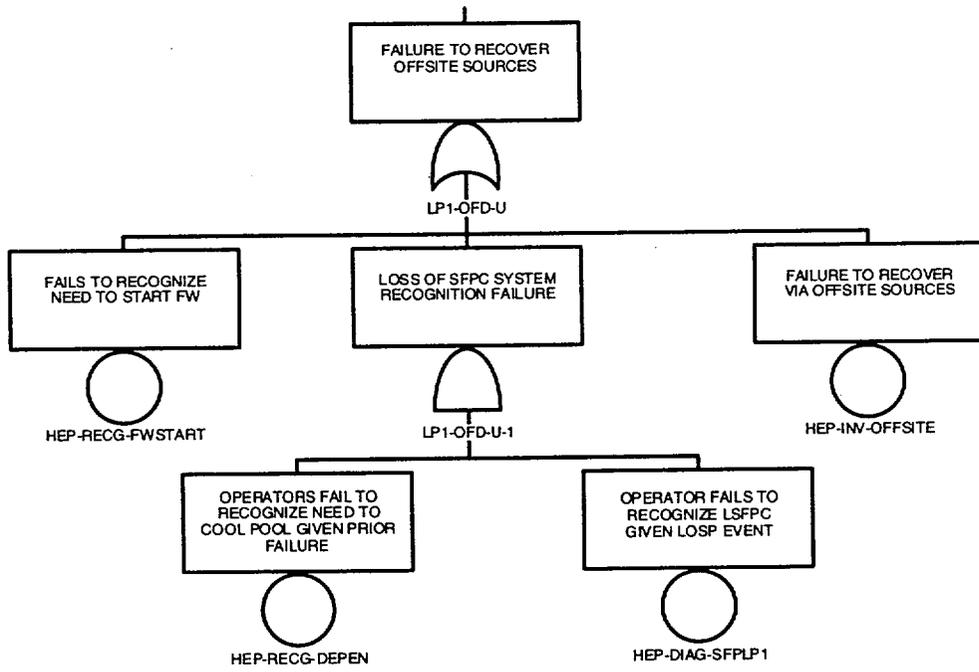


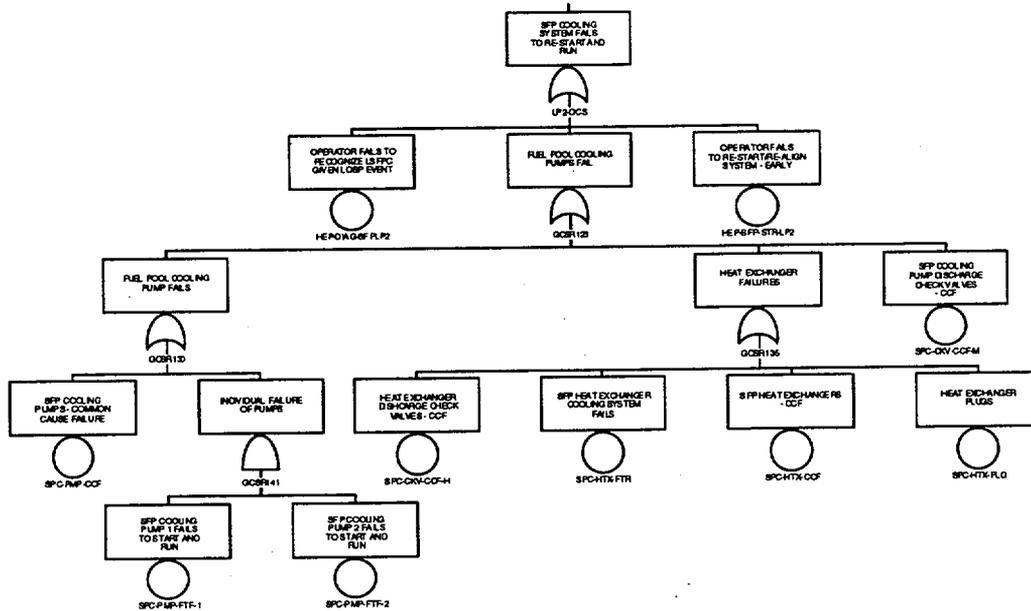
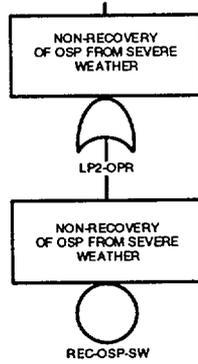


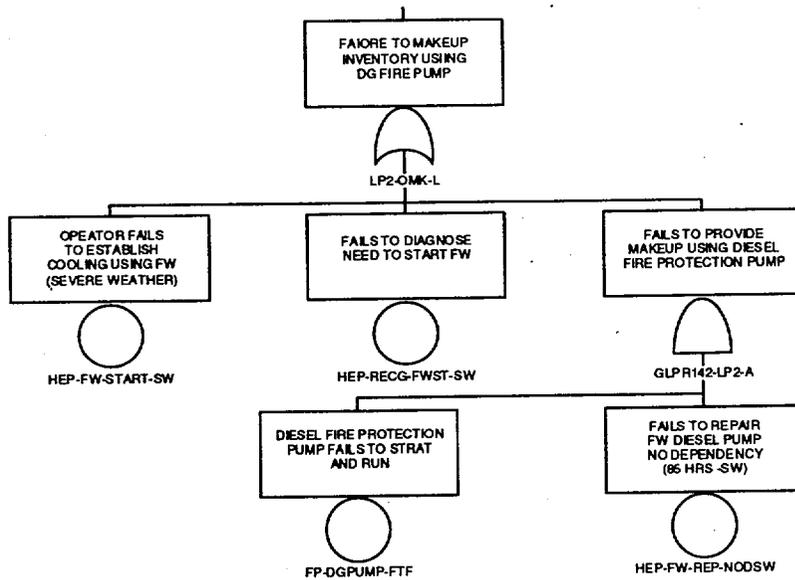
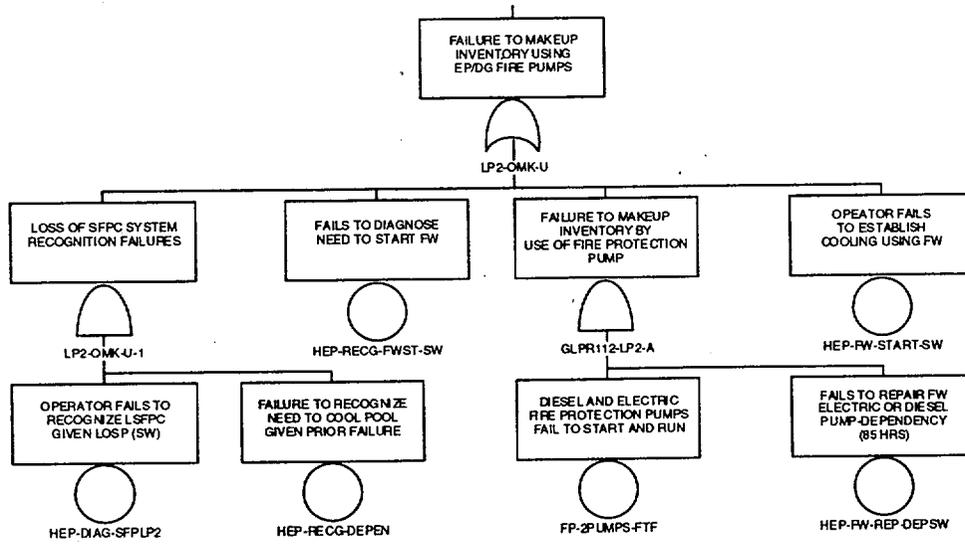


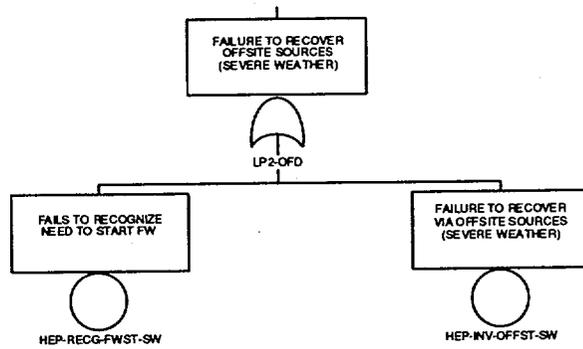
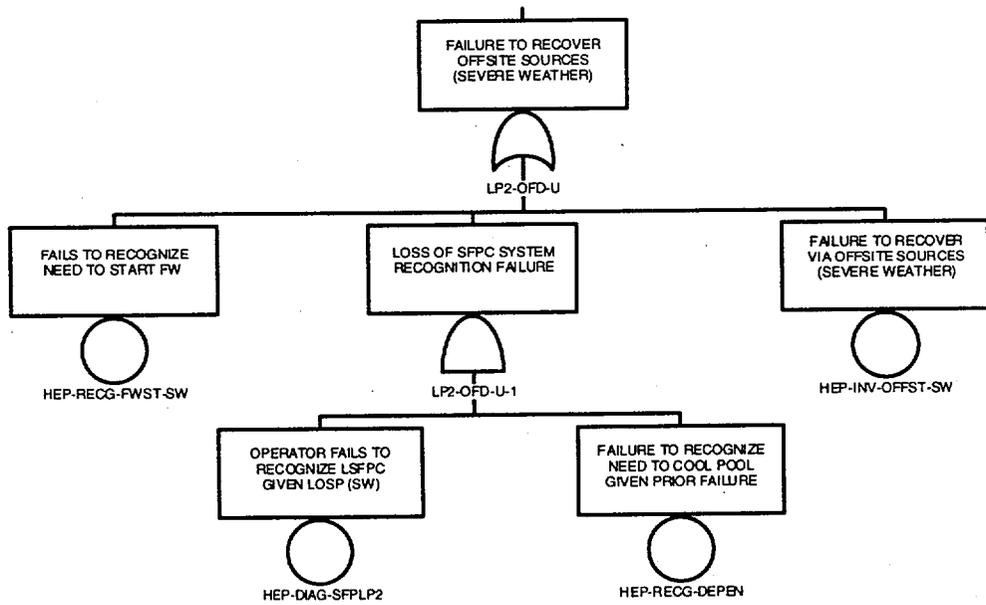


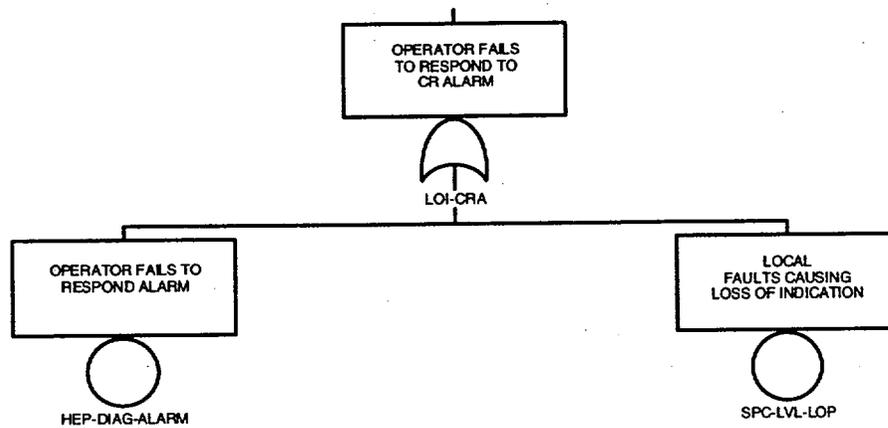
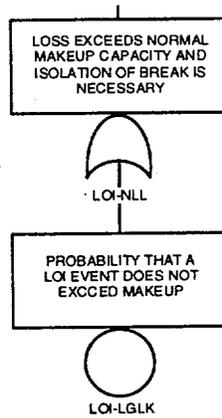


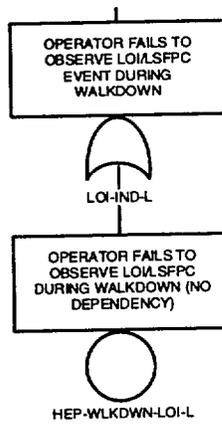
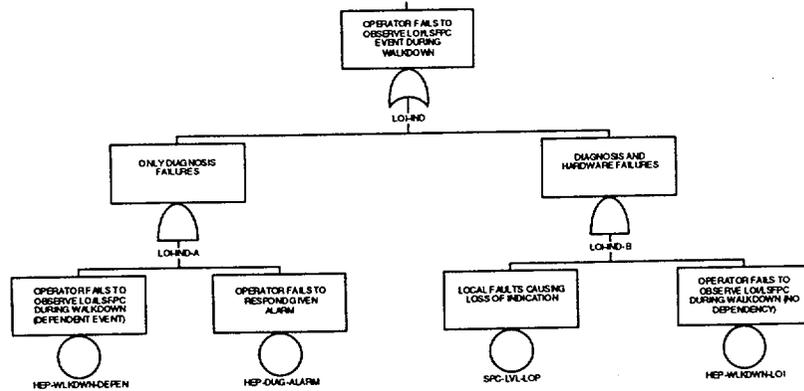


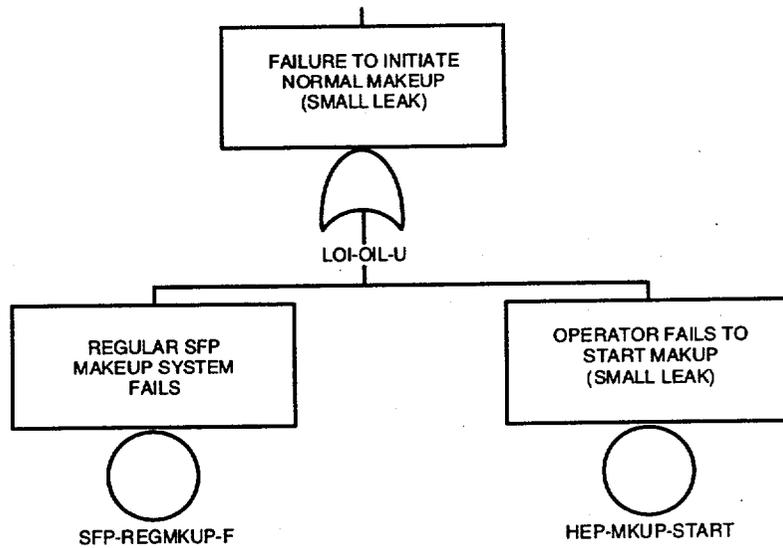
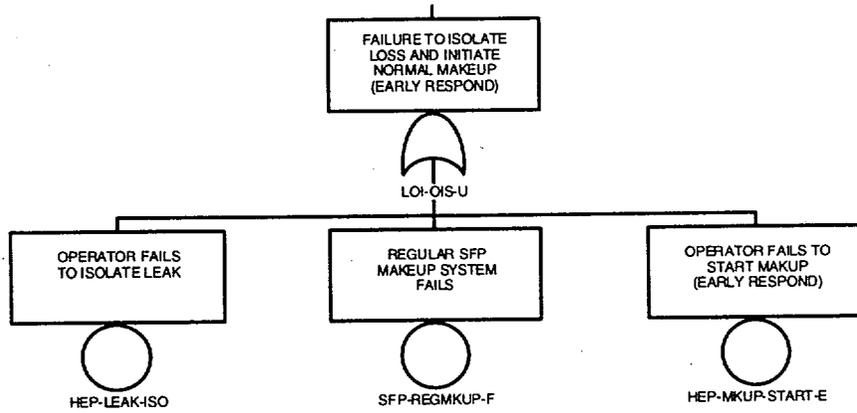


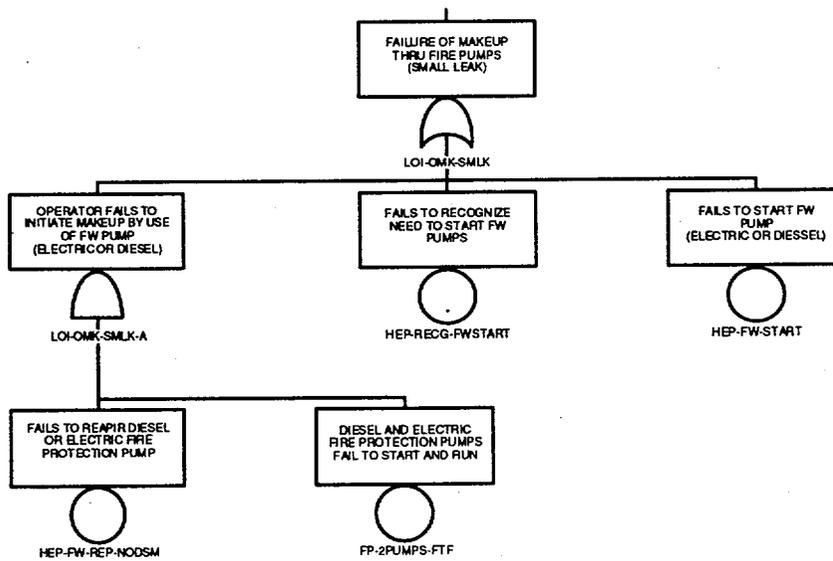
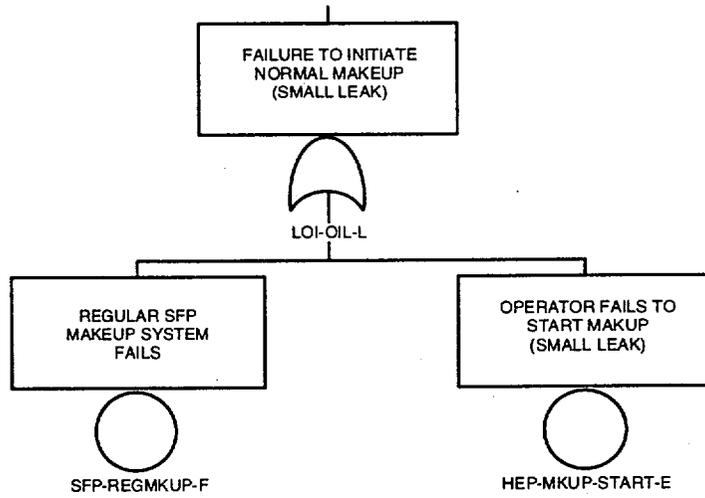


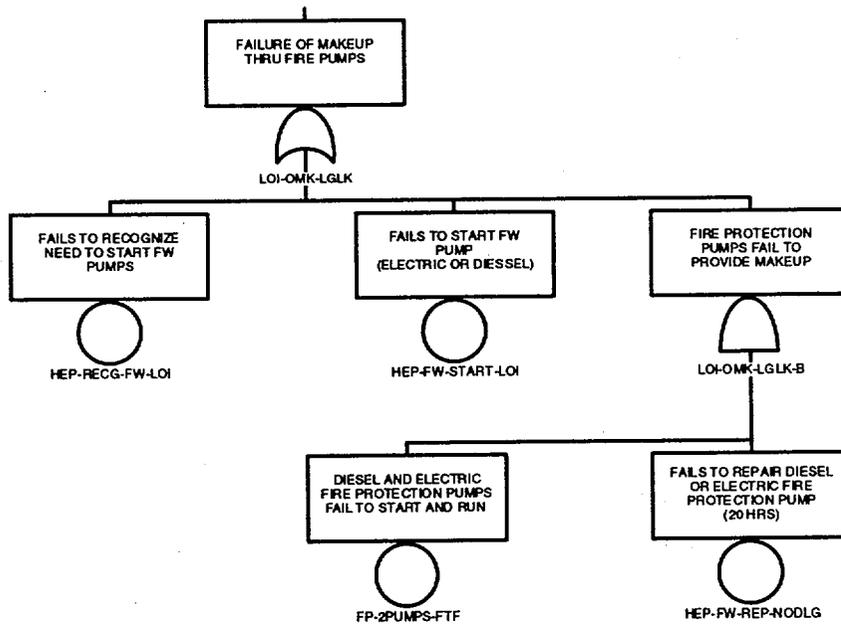
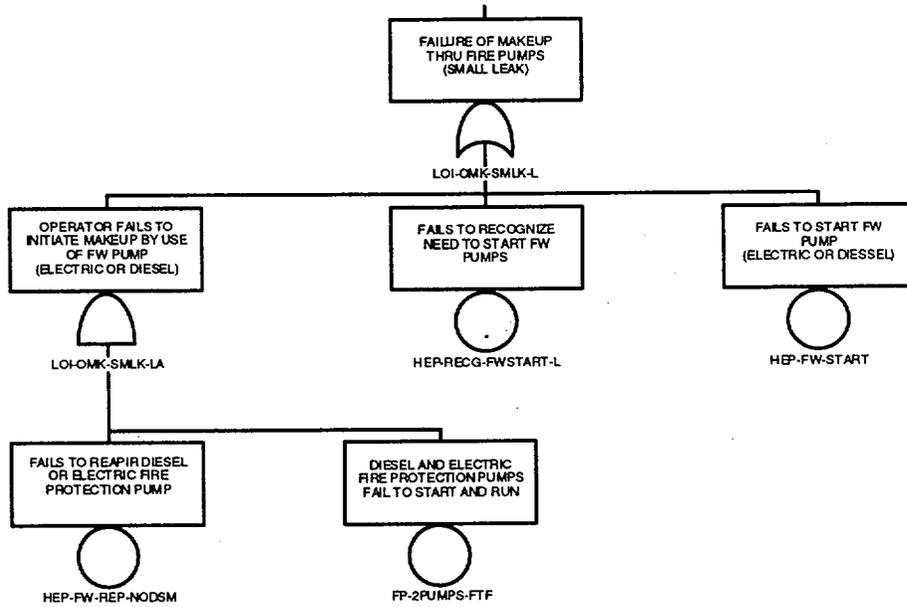


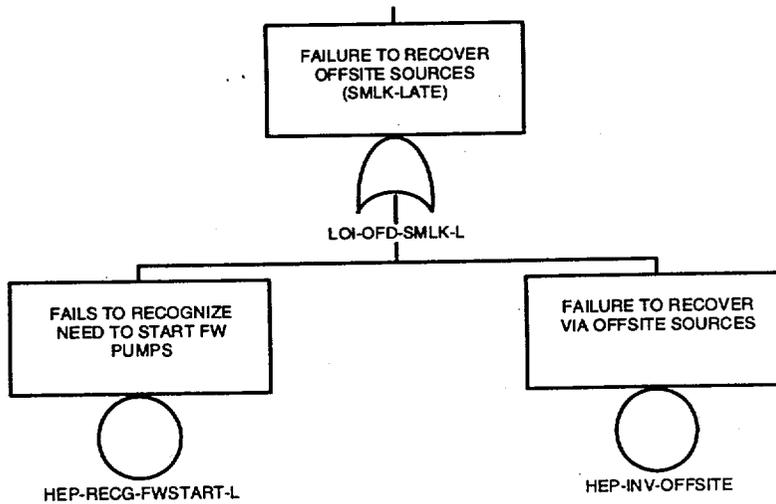
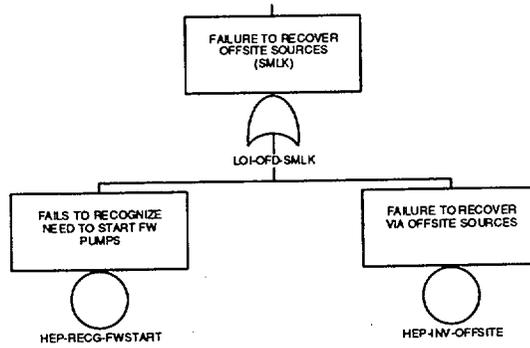


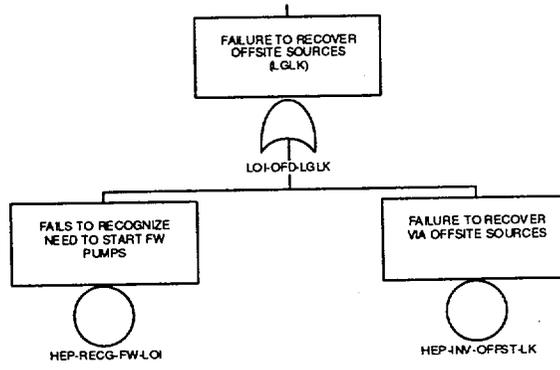












ATTACHMENT B
SPAR HRA Worksheet

SPAR HRA Human Error Worksheet (Page 1 of 3)

Plant: _____ Initiating Event: _____ Sequence Number: _____ Basic Event Code: _____

Basic Event Context: _____

Basic Event Description: _____

Does this task contain a significant amount of diagnosis activity? YES (start with Part I, p. 1) NO (skip Part I, p. 1; start with Part II, p. 2) Why? _____

Part I. DIAGNOSIS

A. Evaluate PSFs for the diagnosis portion of the task.

PSFs	PSF Levels	Multiplier for Diagnosis	If non-nominal PSF levels are selected, please note specific reasons in this column
Available Time	Inadequate time	P(failure) = 1.0	
	Barely adequate time <20 min	10	
	Nominal time . 30 min	1	
	Extra time >60 min	0.1	
	Expansive time >24 hrs	0.01	
Stress	Extreme	5	
	High	2	
	Nominal	1	
Complexity	Highly complex	5	
	Moderately complex	2	
	Nominal	1	
	Obvious diagnosis	0.1	
Experience/Training	Low	10	
	Nominal	1	
	High	0.5	
Procedures	Not available	50	
	Available, but poor	5	
	Nominal	1	
	Diagnostic/symptom oriented	0.5	
Ergonomics	Missing/Misleading	50	
	Poor	10	
	Nominal	1	
	Good	0.5	
Fitness for Duty	Unfit	P(failure) = 1.0	
	Degraded Fitness	5	
	Nominal	1	
Work Processes	Poor	2	
	Nominal	1	
	Good	0.8	

SPAR HRA Human Error Worksheet (Page 2 of 3)

Plant: _____ Initiating Event: _____ Sequence Number: _____ Basic Event Code: _____

Basic Event Context: _____

Basic Event Description: _____

Part II. ACTION

A. Evaluate PSFs for the action portion of the task.

PSFs	PSF Levels	Multiplier for Action	If non-nominal PSF levels are selected, please note specific reasons in this column
Available Time	Inadequate time	P(failure) = 1.0	
	Time available . time required	10	
	Nominal time	1	
	Time available > 50 x time required	0.01	
Stress	Extreme	5	
	High	2	
	Nominal	1	
Complexity	Highly complex	5	
	Moderately complex	2	
	Nominal	1	
Experience/Training	Low	3	
	Nominal	1	
	High	0.5	
Procedures	Not available	50	
	Available, but poor	5	
	Nominal	1	
Ergonomics	Missing/Misleading	50	
	Poor	10	
	Nominal	1	
	Good	0.5	
Fitness for Duty	Unfit	P(failure) = 1.0	
	Degraded Fitness	5	
	Nominal	1	
Work Processes	Poor	5	
	Nominal	1	
	Good	0.5	

B. Calculate the Action Failure Probability

(1) If all PSF ratings are nominal, then the Action Failure Probability = 10E-3

(2) Otherwise,	Time	Stress	Complexity	Experience/ Training	Procedures	Ergonomics	Fitness for Duty	Work Processes	=
Action: 10E-3 _____	x__	x__	x__	x__	x__	x__	x__	x__	=__

Action

Failure Probability

SPAR HRA Human Error Worksheet (Page 3 of 3)

Plant: _____ Initiating Event: _____ Sequence Number: _____ Basic Event Code: _____

PART III. CALCULATE THE TASK FAILURE PROBABILITY WITHOUT FORMAL DEPENDENCE ($P_{w/od}$)

Calculate the Task Failure Probability Without Formal Dependence ($P_{w/od}$) by adding the Diagnosis Failure Probability (from Part I, p.1) and the Action Failure Probability (from Part II, p. 2).

If all PSFs are nominal, then

Diagnosis Failure Probability: _____
10E-2

Diagnosis Failure Probability:

Action Failure Probability: + _____
+10E-3

Action Failure Probability:

Task Failure Without
Formal Dependence ($P_{w/od}$) = _____
= 1.1x10E-2

$P_{(w/od)}$

Part IV. DEPENDENCY

For all tasks, except the first task in the sequence, use the table and formulae below to calculate the Task Failure Probability With Formal Dependence (P_{wd}).

If there is a reason why failure on previous tasks should not be considered, explain here:

Dependency Condition Table

Crew (same or different)	Time (close in time or not close in time)	Location (same or different)	Cues (additional or not additional)	Dependency	Number of Human Action Failures Rule - Not Applicable. Why? _____
Same	Close	Same	-	complete	<p>If this error is the 3rd error in the sequence, then the dependency is at least moderate.</p> <p>If this error is the 4th error in the sequence, then the dependency is at least high.</p> <p>This rule may be ignored only if there is compelling evidence for less dependence with the previous tasks. Explain above.</p>
		Different	-	high	
	Not Close	Same	No Additional	high	
		Additional	moderate		
		Different	No Additional	moderate	
		Additional	low		
Different	Close	-	-	moderate	
	Not Close	-	-	low	

Using P_{wod} = Probability of Task Failure Without Formal Dependence (calculated in Part III, p. 3):

For Complete Dependence the probability of failure is 1.

For High Dependence the probability of failure is $(1 + P_{wod})/2$

For Moderate Dependence the probability of failure is $(1 + 6 \times P_{wod})/7$

For Low Dependence the probability of failure is $(1 + 19 \times P_{wod})/20$

For Zero Dependence the probability of failure is P_{wod}

Calculate P_{wd} using the appropriate values:

$(1 + (*)) / =$ Task Failure Probability With Formal Dependence (P_{wd})

1.0 INTRODUCTION

In reference 1, the NRC performed a preliminary study of spent fuel pool risk at decommissioning plants to: examine the full scope of potentially risk-significant issues; identify credible accident scenarios; document the assessment for public review; and to elicit feedback from all stakeholders regarding analysis assumptions and design and operational features expected at decommissioning plants. In this current analysis, Ref. 1 was updated based on:

- stakeholder feedback on the original analysis
- NEI commitments as documented in Ref. 2
- a revised human reliability analysis (HRA) approach
- peer review of the technical analysis by the Idaho National Engineering and Environmental Laboratory (INEEL).

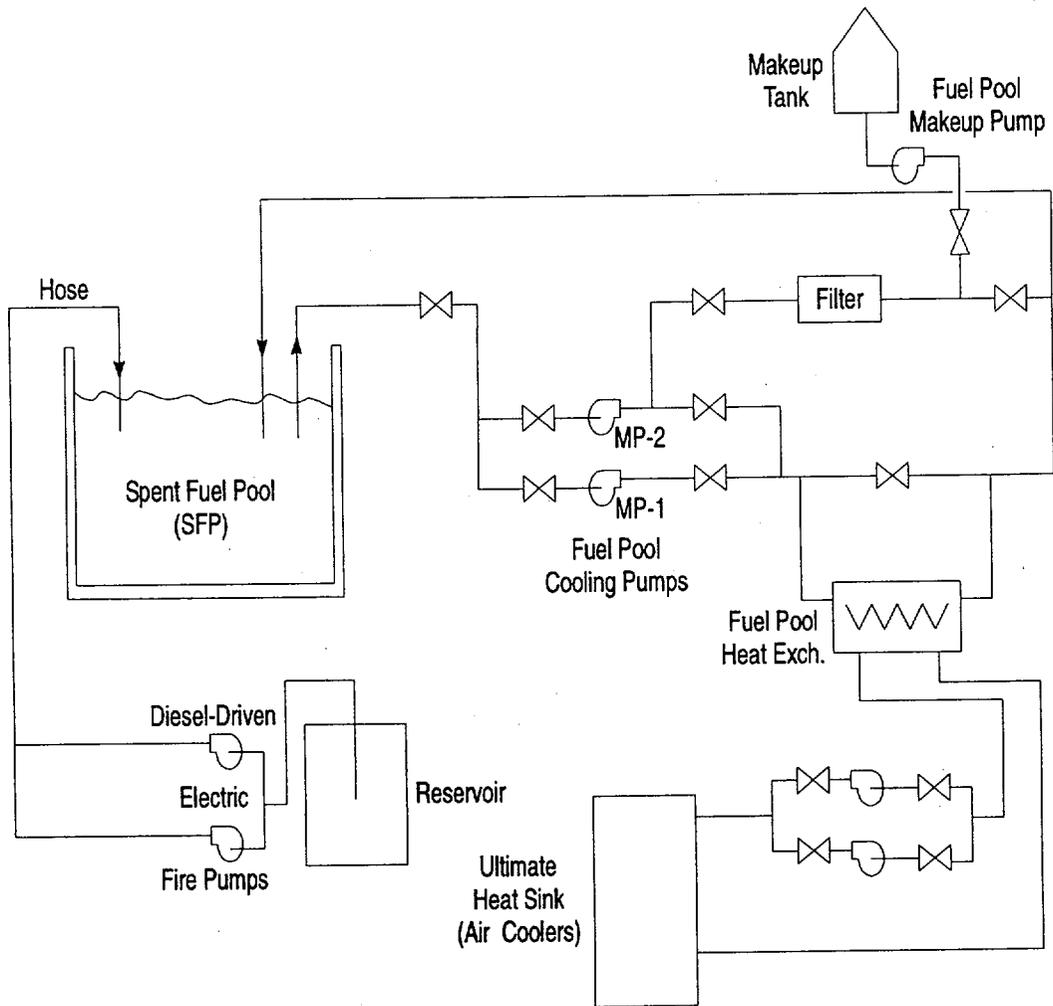
This updated PRA, performed by a combination of INEEL and NRC staff, addresses the following initiating events:

- loss of spent fuel pool cooling
- fire leading to loss of spent fuel pool cooling
- loss of offsite power due to plant centered and grid related causes
- loss of offsite power due to severe weather
- non-catastrophic loss of spent fuel pool inventory

Those low frequency events such as earthquakes, aircraft crashes, heavy load drops, and tornado strikes that could lead to catastrophic pool failure are dealt with elsewhere. The analysis is based on the following input. The assumed system configuration is typical of the sled-mounted systems that are used at many current decommissioned plants. Information about existing decommissioned plants was gathered by decommissioning project managers (NRC Staff) during visits to four sites covering all four major nuclear steam supply system vendors (General Electric, Westinghouse, Babcock & Wilcox, and Combustion Engineering). The assumptions made about the operation of the facility are based in part on a set of commitments made by NEI (Ref. 2), supplemented by an interpretation of how some of those commitments might be applied.

2.0 SYSTEM DESCRIPTION

Figure 2.1 is a simplified drawing of the system assumed for the development of the model. The spent fuel pool cooling (SFPC) system is located in the SFP area and consists of motor-driven pumps, a heat exchanger, an ultimate heat sink, a makeup tank, filtration system and isolation valves. Suction is taken via one of the two pumps on the primary side from the spent



GC99 0672

Figure 2.1 Simplified Diagram of Spent Fuel Pool Cooling and Inventory Makeup Systems

fuel pool and is passed through the heat exchanger and returned back to the pool. One of the two pumps on the secondary side rejects the heat to the ultimate heat sink. A small amount of water from the suction line is diverted to the filtration process and is returned back to the discharge line. A regular makeup system supplements the small losses due to evaporation. In the case of prolonged loss of SFPC system or loss of inventory events, the inventory in the pool can be made up using the firewater system. There are two firewater pumps, one motor-driven (electric) and one diesel-driven, which provide firewater throughout the plant. A firewater hose station is provided in the SFP area. The firewater pumps are located in a separate structure.

3.0 METHODOLOGY

3.1 Logic Model

This section summarizes the spent fuel pool PRA model developed in this study. The description of the modeling approach and key assumptions is intended to provide a basis for interpreting the results in Sections 4 and 5. The detailed model documentation is provided in Attachments A and B. The event trees and fault trees presented in this report are meant to be generic enough to apply to many different configurations.

The endstate for this analysis is defined as loss of coolant inventory to the point of fuel uncover from either leakage or boil-off. Dose calculations (Ref. 3) show that less than 3 feet of water above the top of the fuel results in an environment that is rapidly lethal to anyone at the edge of the pool. For accident scenarios in which coolant inventory level has dropped to less than 3 feet above the top of fuel, recovery may require operators to approach the pool. Therefore, 3 feet has been adopted as an effective limit for recovery purposes. In other words, the endstate for this analysis is effectively defined as loss of coolant inventory to a point 3 feet above the top of the fuel. One of the NEI commitments is that there should be a provision for remote alignment of the makeup source to the pool, which would make this assumption conservative. However, the impact of this conservatism on the conclusions of this analysis is minor.

The event tree and fault tree models were developed and quantified using Version 6 of the SAPHIRE software package (Ref. 4), using a fault tree linking approach. Event trees were developed for each of the initiators identified in Section 1.

3.2 HRA Methodology

3.2.1 Introduction

One of the key issues in performing a probabilistic risk assessment (PRA) for the spent fuel pool during the decommissioning phase of a nuclear power plant's lifecycle is how much credit can be given to the operating staff to respond to an incident that impacts the spent fuel pool that would, if not attended to, lead to a loss of cooling of the spent fuel and eventually to a zirconium fire.

The objective of the HRA analysis in this PRA is to assess whether the design features and

operational practices assumed can be argued to suggest that the non-response probabilities should be low. The design features include the physical plant characteristics (e.g., nature and number of alarms, available mitigation equipment) and the operational practices include operational and management practices (including crew structure and individual responsibilities), procedures, contingency plans, and training. Since the details will vary from plant to plant, the focus is on general features and operational practices that can support low non-response probabilities.

Section 3.2.2 discusses the differences between the full power and decommissioning modes of operation as they impact human reliability analysis, and the issues that need to be addressed in the analysis of the decommissioning mode are identified. Section 3.2.3 discusses the factors that recent studies have shown to be significant in establishing adequacy of human performance.

3.2.2 Analysis Approach

The human reliability analysis (HRA) approaches that have been developed over the past few years have primarily been for use in PRAs of nuclear power plants at full power. Methods have been developed for assessing the likelihood of errors associated with routine processes such as restoration of systems to operation following maintenance, and those errors in responding to plant transients or accidents from full power. For spent fuel pool operation during the decommissioning phase, there are unique conditions not typical of those found during full-power operation. Thus the human reliability methods developed for full power operation PRAs, and their associated error probabilities, are not directly applicable. However, some of the methods can be adapted to provide insights into the likelihood of failures in operator performance for the spent fuel pool analysis by accommodating the differences in conditions that might impact operating crew performance in the full power and decommissioning phases. There are both positive and negative aspects of the difference in conditions with respect to the reliability of human performance.

Examples of the positive aspects are:

- For most scenarios, the time-scale for changes to plant condition to become significant are protracted. This is in contrast to full power transients or accidents in which response is required in a relatively short time, ranging from a few minutes to a few hours. In the staff's analysis, times ranging from 50 to greater than 120 hours were estimated for heat up and boil off following loss of spent fuel pool cooling. Thus, there are many opportunities for different plant personnel to recognize off-normal conditions, and a long time to take corrective action, such as making repairs, hooking up alternate cooling or inventory make-up systems, or even bringing in help from off site.
- There is only one function to be maintained, namely decay heat removal, and the systems available to perform this function are relatively simple. By contrast, in the full power case there are several functions that have to be maintained, including criticality, pressure control, heat removal, containment integrity.
- With respect to the last point, it is also expected that the number of controls and indications that are required in the control room are considerably fewer than for an

operating plant, and therefore, there is less cause for confusion or distraction.

Examples of the negative aspects are:

- The plant operation is not as constrained by regulatory tools (technical specifications are not as comprehensive and restrictive as they are for operating plants), and there is no requirement for emergency procedures.
- Because the back-up systems are not automatically initiated, operator action is essential to successful response to failures of the cooling function.
- There is expected to be little or no redundancy in the on-site mitigating capability as compared with the operating plant mode of operation. (In the staff's initial evaluation, because little redundant onsite equipment was assumed to be available, the failure to bring on offsite equipment was one of the most important contributors.) This implies that repair of failed functions is relatively more significant in the risk analysis for the spent fuel pool case.

In choosing an approach for developing the estimates documented in this report, the following issues were considered to be important:

- Because of the long time scales, it is essential to address the potential for recovery of failures on the part of one crew or individual by other plant staff, including subsequent shifts.
- However, potential sources of dependency that could lead to a failure of the organization as a whole to respond adequately should be taken into account.
- The approach should be consistent with current understanding of human performance issues (see for example, Refs. 5, 6, and 7).
- Those factors that the industry has suggested that will help ensure adequate response (instrumentation, monitoring strategies, procedures, contingency plans) should be addressed (Ref. 2).
- Where possible, any evaluations of human error probabilities (HEPs) should be calibrated against currently acceptable ranges for HEPs.
- The reasoning behind the assumptions made should be transparent.

3.2.3 Human Performance Issues

In order to be successful in coping with an incident at the facility, there are three basic functions that are required of the operating staff, and these are either explicit (awareness) or implicit (situation assessment and response planning and response implementation) in the definitions of the human failure events in the PRA model.

- plant personnel must be able to detect and recognize when the spent fuel cooling function is deteriorating or pool inventory is being lost (Awareness).
- plant personnel must be able to interpret the indications (identify the source of the problem) and formulate a plan that would mitigate the situation (Situation Assessment and Response Planning).
- plant personnel must be able to perform the actions required to maintain cooling of and/or add water to the spent fuel pool (Response Implementation).

In the following sections, factors that are relevant to determining effective operator responses are discussed. While not minimizing the importance of such factors as the establishment of a safety culture and effective intra-crew communication, the focus is on factors which can be determined to be present on a relatively objective basis. A review of LERs associated with human performance problems involved in response to loss of fuel pool cooling revealed a variety of contributing factors, including crew inexperience, poor communication, and inadequate administrative controls. In addition, there were some instances of design peculiarities that made operator response more complex than necessary.

The factors discussed below were used to identify additional assumptions made in the analysis that the Staff considered would provide for an effective implementation of the NEI commitments.

3.2.3.1 Awareness/Detection of Deviant Conditions

There are two types of monitoring that can be expected to be used in alerting the plant staff to deviant conditions: a) passive monitoring in which alarms and annunciators are used to alert operators; b) active monitoring in which operators, on a routine basis, make observations to detect off-normal behavior. In practice both would probably be used to some extent. The amount of credit that can be assumed depends on the detailed design and application of the monitoring scheme.

- a) In assessing the effectiveness of alarms there are several factors that could be taken into account, for example:
- alarms (including control room indications) are maintained and checked/calibrated on a regular basis
 - the instruments that activate instruments and alarms measure, as directly as possible, the parameters they purport to measure
 - alarm set-point is not too sensitive, so that there are few false alarms
 - alarms cannot be permanently canceled without taking action to clear the signal
 - alarms have multiple set-points corresponding to increasing degradation
 - the importance of responding to the alarms is stressed in plant operating procedures

and training

- the existence of independent alarms that measure different primary parameters (e.g., level, temperature, airborne radiation), or provide indirect evidence (sump pump alarms, secondary side cooling system trouble alarms)

The first and last of these factors may be reflected in the reliability assumed for the alarm and in the structure of the logic model (fault tree) for the event tree function CRA, respectively. The other factors may be taken into account in assessing the reliability of the operator response.

b) For active monitoring, examples of the factors used in assessing the effectiveness of the monitoring include:

- scheduled walkdowns required within areas of concern, with specific items to check (particularly to look for indications not annunciated in, or monitored from, the control room, for example, indications of leakage, operation of sump pumps if not monitored, steaming over the pool, humidity level)
- plant operating procedures that require the active measurement of parameters (e.g., temperature, level) rather than simply observing the condition of the pool
- requirement to log, check, and trend results of monitoring
- alert levels specified and noted on measurement devices

These factors can all be regarded as performance shaping factors (PSFs) that affect the reliability of the operators.

An important factor that should mitigate against not noticing a deteriorating condition is the time scale of development, which allows the opportunity for several shifts to notice the problem. The requirement for a formal shift turnover meeting should be considered.

3.2.3.2 Situation Assessment and Response Planning

The principal operator aids for situation assessment and response planning are procedures and training in their use.

The types of procedures that might be available are:

- annunciator/alarm response procedure that is explicit in pointing towards potential problems
- detailed procedures for use of alternate systems indicating primary and back up sources, recovery of power, etc..

The response procedures may have features that enhance the likelihood of success, for example:

- guidance for early action to establish contingency plans (e.g., alerting offsite agencies such as fire brigades) in parallel with a primary response such as carrying out repairs or lining up an on-site alternate system.
- clearly and unambiguously written, with an understanding of a variety of different scenarios and their timing.

In addition:

- training for plant staff to provide an awareness of the time scales of heat up to boiling and fuel uncovering as a function of the age of the fuel would enhance the likelihood of successful response.

3.2.3.3 Response Implementation

Successful implementation of planned responses may be influenced by several factors, for example:

- accessibility/availability of equipment
- staffing levels that are adequate for conducting each task and any parallel contingency plans, or plans to bring in additional staff
- training
- timely feedback on corrective action

3.2.4 Quantification Method

Three quantification methods were applied, and each is briefly described below.

- The Technique for Human Error Prediction (THERP, Ref. 8). This method was used to quantify the initial recognition of the problem. Specifically, the annunciator response model (Table 20-23) was used for response to alarms. The THERP approach was also used to assess the likelihood of failure to detect a deviant condition during a walkdown, and also the failure to respond to a fire.
- The Exponential Repair Model (while not strictly a human reliability model) was applied to calculate the probability of failure associated with the repair of systems and components in this analysis. This method is described in the main body of the report. In cases where dependency exists with prior repair tasks, the dependency model used in THERP was used to assess the impact of that dependency.
- The Simplified Plant Analysis Risk Human Error Analysis Method (SPAR HRA, Ref. 9) this method was employed for all other HEPs. This method separately evaluates the diagnosis or response planning errors and the execution errors.

3.3 Other Inputs to the Risk Model

A variety of other inputs were required for this PRA, including generic configuration data used in the fault tree models, radiological calculations, and timing calculations. Initiating event frequencies and generic reliability data, were derived from other studies sponsored by the NRC. The times available for operator actions are based on calculations of the time it would take for bulk boiling to begin in the pool, or on the time it takes for the level in the pool to fall to the level of the fuel pool cooling system suction, or to a height of approximately 3 ft above the fuel, as appropriate to the definition of the corresponding human failure event.

It takes a relatively long time to uncover the fuel if inventory is lost in this manner due to the large amount of water in a spent fuel pool, the large specific heat of water, and the large latent heat of vaporization for water. Simple calculations for a typical-sized spent fuel pool yield the results in Table 3.1. These results are based on the following assumptions:

- no heat losses
- atmospheric pressure
- Heat of vaporization $h_{fg} \approx 2258$ kJ/kg
- base pool heat load for a full pool of 2 MW
- core thermal power of 3293 MW
- typical pool size (based on Tables 2.1 and 2.2 of NUREG/CR-4982, Ref. 10)
 typical BWR pool is 40' deep by 26' by 39'
 typical PWR pool is 43' deep by 22' by 40'

Table 3.1 Time to Bulk Boiling, and Boil-off Rates

Time after discharge (days)	Decay power from last core (MW)	Total heat load (MW)	Time to bulk boiling (hr)	Boil-off rate (gpm)	Level decrease (ft/hr) ¹
2	16.4	18.4	5.6	130	1.0
10	8.6	10.6	9.8	74	0.6
30	5.5	7.5	14	52	0.42
60	3.8	5.8	18	41	0.33
90	3.0	5.0	21	35	0.28
180	1.9	3.9	27	27	0.22
365	1.1	3.1	33	22	0.18 ~ 0.2

Notes: (1) using typical pool sizes, it is estimated that for BWRs, we have 1040 ft³/ft depth, and for PWRs, we have 957 ft³/ft depth. Assume ≈ 1000 ft³/ft depth for level decreases resulting from boil-off.

In a SFP, the depth of water above the fuel is typically 23 to 25 feet. Subtracting 3 feet to account for shielding requirements, it is estimated that approximately 20 feet of water will have to boil-off before the start of fuel uncovering. Therefore, using the above table, the available time for operator actions for the loss of cooling type accidents is estimated as follows:

For one-year-old fuel, the total time available equals the time to bulk boiling plus the time to boil-down to 3 ft above the top of the fuel. Therefore, the total time available for operator action is as follows:

$$\begin{aligned} \text{Total Time} &= 33 \text{ hr} + (20 \text{ ft}) / (0.2 \text{ ft/hr}) \\ &= 131 \text{ hours} \end{aligned}$$

It is assumed that the operator will not use alternate systems (e.g., firewater) until after bulk boiling begins and the level drops to below the suction of the cooling system. It is assumed that the suction of the cooling system is 2 ft below the nominal pool level. Therefore, if bulk boiling begins at 33 hours, and the boil-off rate is 0.2 ft/hr, then the total time available to provide makeup using the firewater system to prevent fuel uncovering is as follows:

$$131 \text{ hrs} - \text{Time to Bulk Boiling} + \text{Time for Boil-off} = 33 \text{ hrs} + \frac{2 \text{ ft}}{0.2 \text{ ft/hr}} = 131 - 43 \text{ hrs} = 88 \text{ hrs}$$

3.4 General Assumptions

This analysis is based on the assumption that the commitments for procedures and equipment proposed by NEI in their November 12, 1999 letter to Richard J. Barrett (Ref. 2) are adopted. These are reproduced below:

1. Cask drop analyses will be performed or single failure proof cranes will be in use for handling of heavy loads, (i.e., phase II of NUREG 0612 (Ref. 11) will be implemented).
2. Procedures and training of personnel will be in place to ensure that on site and off site resources can be brought to bear during an event.
3. Procedures will be in place to establish communication between on site and off site organizations during severe weather and seismic events.
4. An off site resource plan will be developed which will include access to portable pumps and emergency power to supplement on site resources. The plan would principally identify organizations or suppliers where off site resources could be obtained in a timely manner.
5. Spent fuel pool instrumentation will include readouts and alarms in the control room (or where personnel are stationed) for spent fuel pool temperature, water level, and area radiation levels.
6. Spent fuel pool boundary seals that could cause leakage leading to fuel uncovering in the event of seal failure shall be self limiting to leakage or otherwise engineered so that drainage cannot occur.
7. Procedures or administrative controls to reduce the likelihood of rapid drain down events will include (1) prohibitions on the use of pumps that lack adequate siphon protection; or (2) controls for pump suction and discharge points. The functionality of anti-siphon devices will be periodically verified.
8. An on site restoration plan will be in place to provide for repair of the spent fuel pool cooling systems or to provide access for makeup water to the spent fuel pool. The plan

will provide for remote alignment of the makeup source to the spent fuel pool without requiring entry to the refuel floor.

9. Procedures will be in place to control spent fuel pool operations that have the potential to rapidly decrease spent fuel pool inventory. These administrative controls may require additional operations or administrative limitations such as restrictions on heavy load movements.
10. Routine testing of the alternative fuel pool makeup system components will be performed and administrative controls for equipment out of service will be implemented to provide added assurance that the components would be available if needed.

Since the commitments are stated at a relatively high level, additional assumptions have been made as detailed below.

- It is assumed that the operators (through procedures and training) are aware of the available backup sources that can be used to replenish the SFP inventory (i.e., the fire protection pumps, or offsite sources such as from fire engines). Arrangements have been made in advance with fire stations including what is required from the fire department including equipment and tasks.
- The site has two operable firewater pumps, one diesel-driven and one electrically driven from offsite power.
- The makeup capability (with respect to volumetric flow) is assumed as follows:

Make-up pump:	20 - 30 gpm
Firewater pump:	100 - 200 gpm
Fire engine:	100 - 250 gpm [depending on hose size: 1-½" (100 gpm) or 2-½" (250 gpm)]
- It is therefore assumed that, for the larger loss of coolant inventory accidents, makeup through the makeup pumps is not feasible unless the source of inventory loss can be isolated.
- The operators perform walkdowns of the SFP area once per shift (8- to 12-hour shifts). A different crew member is assumed for the next shift. It is also assumed that the SFP water is clear and pool level is observable via a measuring stick in the pool that can alert operators to level changes.
- Requirements for fire detection and suppression may be reduced (when compared to those for an operating plant) and it is assumed that automatic detection and suppression capability may not be present.
- All equipment, including external sources (fire department), are available and in good working order.

- The emergency diesel generators and support systems such as residual heat removal and service water (that could provide SFP cooling or makeup prior to the plant being decommissioned) have been removed from service.
- The SFP cooling system, its support systems, and the electric driven fire protection pump are fed off the same electrical bus.
- Procedures exist to mitigate small leaks from the SFP or for loss of the SFP cooling system.
- The only significant technical specification applicable to SFPs is the requirement for radiation monitors to be operable when fuel is being moved. There are no technical specifications requirements for the cooling pumps, makeup pumps, firewater pumps, or any of the support systems.
- Generic industry data was used for initiating event frequencies for the loss of offsite power, the loss of pool cooling, and the loss of coolant inventory.
- For the purposes of timing, the transfer of the last fuel from the reactor to the SFP is assumed to have occurred one year previously.

4.0 MODEL DEVELOPMENT

This section describes the risk models that were developed to assess the likelihood of core uncover from spent fuel pool loss of cooling events, fire events, loss-of-off-site power, loss of inventory events.

4.1 Loss of Cooling Event Tree

This event tree (Figure 4.1) models generic loss of cooling events (i.e., those not related to other causes such as fire or loss of power, which are modeled in later sections). The top events and the supporting functional fault trees are discussed in the following sections.

4.1.1 Initiating Event LOC – Loss of Cooling

4.1.1.1 Event Description

This initiating event includes conditions arising from loss of coolant system flow due to the failure of the operating pumps or valves, from piping failures, from an ineffective heat sink (e.g., loss of heat exchangers), or from a local loss of power (e.g., failure of electrical connections).

4.1.1.2 Quantification

This initiating event is modeled by a single basic event, IE-LOC. An initiation frequency of $3.0E-3/\text{yr}$ is taken from NUREG-1275 Volume 12 (Ref. 12). This represents the frequency of loss of cooling events in which temperatures rise more than 20°F.

4.1.2 Top Event CRA – Control Room Alarms

4.1.2.1 Event Description and Timing

This event represents a failure to respond to conditions in the pool that are sufficient to trigger an alarm. Failure could be due to operator error (failure to respond), or loss of indication due to equipment faults. Success for this event is defined as the operator recognizing the alarm and understanding the need to investigate its cause. This event is quantified by fault tree LOC-CRA and includes hardware and human failures basic events that represent failure of control room instrumentation to alarm given that SFP cooling has been lost, and the operators fail to respond to the alarm, respectively.

4.1.2.2 Relevant Assumptions

- Within 8 to 12 hours of the loss of cooling, one or more alarms or indications will reflect an out-of-tolerance condition to the operators in the control room (there may be level indication available locally or remotely, but any change in level is not likely to be significant until later in the sequence of events).
- The SFP has at least one water temperature measuring device, with an alarm and a readout in the control room (NEI commitment no. 5). There could also be indications or alarms associated with pump flow and pressure, but no credit is taken here.
- The instrumentation is tested on a routine basis and maintained operable.
- Procedures are available to guide the operators in their response to off-normal conditions, and the operators are trained on the use of these procedures (NEI commitment no. 2).

4.1.2.3 Quantification

Human Error Probabilities

The basic event HEP-DIAG-ALARM models operator failure to respond to an indication in the control room and diagnose a loss of cooling event. Such an alarm would likely be the first indication of trouble, so the operator would not be under any heightened state of alertness. On the other hand, it is not likely that any other signals or alarms for any other conditions would be present to distract the operator. The error rate is taken from THERP (Table 20-23).

Hardware Failure Probabilities

The value used for local faults leading to alarm channel failure (event SPC-LVL-LOF, 2.0E-3) was estimated based on information in reference 11. This event includes failure of instrumentation and local electrical faults.

4.1.2.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-DIAG-ALARM	3.0E-4
SPC-LVL-LOF	2.0E-3

4.1.3 Top Event IND – Other Indications of Loss of Cooling

4.1.3.1 Event Description and Timing

This top event models subsequent operator failures to recognize the loss of cooling during walkdowns over multiple shifts. Indications available to the operators include: temperature readouts in the control room (NEI commitment no. 5), local temperature measurements, and

eventually, increasing area temperature and humidity, low water level from boil-off, and local alarms. Success for this event is defined as the operator recognizing the abnormal condition and understanding the need to investigate its cause, leaving sufficient time to attempt to correct the problem before the pool level drops below the spent fuel pool cooling system suction. The event is modeled by fault tree LOC-IND.

4.1.3.2 Relevant Assumptions

- The loss of cooling may not be noticeable during the first two shifts but conditions are assumed to be sufficient to trigger high temperature alarms locally and in the control room
- Operators perform walkdowns and control room readouts once per shift (every 8 to 12 hours) and document observations in a log
- Regular test and maintenance is performed on instrumentation (NEI commitment no. 10)
- During walkdowns, level changes in the SFP can be observed on a large, graduated level indicator in the pool
- Procedures are available to guide the operators on response to off-normal conditions, and the operators are trained on the use of these procedures (NEI commitment no. 2)

Figure 4.1 Loss of spent fuel pool cooling system event tree

LOSS OF COOLING	CONTROL ROOM ALARMS	OTHER INDICATIONS OF LOSS OF COOLING	OPERATOR RECOVERY OF COOLING SYSTEM	OPERATOR INITIATES MAKEUP USING FIRE PUMPS	RECOVERY USING OFFSITE SOURCES				
IE-LOC	CRA	IND	OCS	OFD	OFB	#	SEQUENCE-NAMES	END-STATE-NAMES	FREQUENCY
						1	IE-LOC	OK	
						2	IE-LOC OCS	OK	
						3	IE-LOC OCS OFD	OK	
						4	IE-LOC OCS OF DOFB	SFP3FT	1.197E-008
						5	IE-LOC CRA	OK	
						6	IE-LOC CRA OCS	OK	
						7	IE-LOC CRA OCS OFD	OK	
						8	IE-LOC CRA OCS OF DOFB	SFP3FT	1.530E-010
						9	IE-LOC CRA IND	OK	
						10	IE-LOC CRA IND OFD	OK	
						11	IE-LOC CRA IND OF DOFB	SFP3FT	2.255E-009

4.1.3.3 Quantification

Human Error Probabilities

The functional fault trees includes two human failure events, depending on whether the control room alarms have failed, or whether there was a failure to respond to the initial alarm (it is assumed that the alarm was canceled). If the operator failed to respond to control room alarms, then event HEP-WLKDOWN-DEPEN models subsequent operating crews' failures to recognize the loss of cooling during walkdowns, taking into account the dependence on event HEP-DIAG-ALARM. A specific mechanism for dependence can only be identified on a plant and event specific basis, but could result, for example, from an organizational failure that leads to poor adherence to plant procedures. Because this is considered unlikely, and because the conditions in the pool area change significantly over the time scale defined by the success criterion for this event, the degree of dependence is assumed to be low.

If the alarms failed, then event HEP-WLKDOWN-LSFPC models subsequent crews' failures to recognize the loss of cooling during walkdowns, with no dependence on previous HEPs. However, because the control room readouts could share a dependency with the alarms, the assumption of local temperature measurements becomes important. The failure probabilities for these events were developed using THERP, and are based upon three individual failures: failure to carry out an inspection, missing a step in a written procedure, and misreading a measuring device. Because there are on the order of 33 - 43 hours before the spent fuel pool cooling system becomes irrecoverable without pool make-up, it is assumed that multiple crews would have to fail. However, the probability is truncated at 1E-05.

4.1.3.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-WLKDOWN-LSFPC	1.0E-5
HEP-WLKDOWN-DEPEN	5.0E-2

4.1.4 Top Event OCS – Operator Recovery of Cooling System

4.1.4.1 Event Description and Timing

Once the operators recognize loss of spent fuel pool cooling, they will likely focus their attention on recovery of the SFP cooling system. It is assumed that only after bulk boiling begins and the water level drops below the cooling system suction that the operator will inject water from other makeup systems (e.g., firewater). Therefore, the time available to recover the SFP cooling system could be as long as 43 hours, given an immediate response to an alarm. However, it has assumed that the operating staff has only until shortly after bulk boiling begins (assumed to be 33 hours) to restore the SFP cooling system. This assumption is based on concerns about volume reduction due to cooling and whether the makeup system capacity is sufficient to overcome that volume reduction.

The initial cause of the loss of cooling could be the failure of a running pump in either the primary or the secondary system, in which case the response required is simply to start the redundant pump. However, it could also be a more significant failure, such as a pipe break or a heat exchanger blockage. To simplify the model, it has been assumed that a repair is necessary. While this is conservative, it is not considered that this unduly biases the conclusions of the overall study.

If the loss of cooling was detected via the control room alarms, the staff has the full 33 hours in which to repair the system. Assuming that it takes at least 16 hours before parts and technical help arrive, then the operator has 17 hours (33 hours less 16 hours) to repair the system. Failure to repair the SFPC system event is modeled as HEP-COOL-REP-E. This case is modeled by fault tree LOC-OCS-U.

If the loss of cooling was discovered during walkdowns, it has been conservatively assumed the operator has only 9 hours available (allowing 24 hours before loss of cooling was noticed). Since it is assumed that it takes at least 16 hours before technical help and parts arrive, it is not possible that the SFPC system can be repaired before the bulk boiling would begin. Failure to repair the SFPC system event is modeled as HEP-COOL-REP-L. This case is modeled by fault tree LOC-OCS-L.

4.1.4.2 Relevant Assumptions

- The operators will avoid using raw water (e.g., water not chemically controlled) if possible. Therefore, the operators are assumed to focus solely on restoration of the SFP cooling system in the initial stages of the event
- If the loss of cooling was detected through shift walkdowns, then 24 hours are (conservatively) assumed to have passed before discovery
- It takes 16 hours to contact maintenance personnel, diagnose the cause of failure, and get new parts
- Mean time to repair the SFP cooling system is 10 hours
- Operating staff has received formal training and there are administrative procedures to guide them in initiating repair (NEI commitment no. 8)
- Repair crew is different than the onsite operators

4.1.4.3 Quantification

Human Error Probabilities

The probability of failure to repair SFPC system is represented by the exponential repair model:

$$e^{-\lambda t}$$

where

λ = (inverse of mean time to repair)

t = available time

In the case where discovery was from the control room, probability of failure to repair SFPC system event, HEP-COOL-REP-E, would be 0.18 based on 17 hours available to repair. In the case that the discovery was due to operator walkdown (HEP-COOL-REP-L), it is assumed that there is not enough time available to repair and restart the SFP makeup system in time to prevent bulk boiling, and has been assigned a value of 1.0.

4.1.4.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-COOL-REP-E	1.8E-1
HEP-COOL-REP-L	1.0

4.1.5 Top Event OFD – Operator Recovery Using Onsite Sources

4.1.5.1 Event Description and Timing

On the two upper branches of the event tree, the operators have recognized the loss of the SFPC system, and have tried unsuccessfully to restore the system. After 43 hours, the level of the pool has dropped below the suction of the SFP cooling system (see below), so that repair of that system will not have any effect until pool level is restored. The operating staff now has 88 hours to provide makeup to the pool using firewater (or other available onsite sources) to prevent fuel uncover (131 hours less 43 hours). This event represents failure to provide makeup to the SFP. The operators have both an electric- and a diesel-driven firewater pump available to perform this function. If both pumps were to fail, there may be time to attempt to repair one of the pumps. This event has been modeled by the fault tree LOC-OFD.

Given the operators were not successful in detecting the loss of cooling early enough to allow recovery of the normal cooling system, this event is modeled by functional fault tree LOC-OFD-L. At this stage, even though the operators have failed over several shifts to detect the need to respond, there would be several increasingly compelling cues available to the operators performing walkdowns, including a visibly lowered pool level and a hot and humid atmosphere. Since there are on the order of 88 hours before the level drops to 3 feet above the fuel, some credit has been taken for subsequent crews to recognize the loss of cooling and take corrective action.

4.1.5.2 Relevant Assumptions

- The operators have 88 hours to provide makeup
- The operators will avoid using raw water (e.g., water not chemically controlled) if possible
- The boil-off rate is assumed to be higher than the SFP makeup system capacity

- The operators are aware that they must use raw water to refill the pool once the level drops to below the suction of the cooling system and the pool begins boiling, since the makeup system cannot compensate for the boiling
- For repair of failed pumps, it is assumed that it takes 16 hours to contact maintenance personnel, identify the problem, and get new parts
- There is a means to remotely align a makeup source to the spent fuel pool without entry to the refuel floor, so that makeup can be provided even when the environment is uninhabitable due to steam and/or high radiation (NEI commitment no.8)
- Repair crew is different than onsite operators
- Mean time to repair the firewater pump is 10 hours
- Operators have received formal training and there are procedures that include clear guidance on the use of the firewater system as a makeup system (NEI commitment no. 2)
- Firewater pumps are maintained and tested on a regular schedule (NEI commitment no. 10)

4.1.5.3 Quantification

Human Error Probabilities

Three human failure events are modeled in functional fault tree LOC-OFD.

HEP-RECG-FWSTART represents the operator's failure to recognize the need to initiate the firewater system. The conditions under which the firewater system is to be used are assumed to be explicit in a written procedure. This event was quantified using the SPAR HRA technique. The assumptions include expansive time (> 24 hours), a high level of stress, diagnostic type procedures, good ergonomic interface, and good quality of work process. This diagnosis task provides the diagnosis for the subsequent actions taken to re-establish cooling to the pool.

HEP-FW-START represents failure to start the electric or diesel firewater pump within 88 hours after the onset of bulk boiling, given that the decision to start a firewater pump was made. No difficult valve alignment is required. This event was quantified using SPAR HRA technique. An expansive time (> 50 times the required time), high stress, highly complex task because of its non-routine nature, quality procedures available, as well as good ergonomics including equipment and tools matched to procedure, and crews that are conversant with the procedures and one another through training were assumed.

HEP-FW-REP-DEPEN represents the failure of the repair crew to repair a firewater pump. Note that the repair crew had failed to restore the SFPC system. Therefore, dependency was modeled in the failure to repair firewater system. We assume that the operator will focus his recovery efforts on only one pump. Assuming that it takes another two shifts (16 hours) before

technical help and parts arrive, then the operator has 72 hours (88 hours less 16 hours) to repair the pump. Assuming a 10-hour mean time to repair, the probability of failure to repair the pump would be $\text{Exp} [-(1/10) * 72] = 1.0\text{E-}3$. For HEP-FW-REP-DEPEN a low level of dependence was applied modifying the nominal failure probability of $1.0\text{E-}3$ to $5.0\text{E-}2$ using the THERP formulation for low dependence.

Functional fault tree LOC-OFD-L is similar except that basic event HEP-RECG-FWSTART is replaced by HEP-RECG-FWSTART-L. The probability of this event is $5\text{E-}2$, representing a low level of dependence due to the fact that a failure to detect the condition during the first few shifts may be indicative of a more serious underlying problem.

Hardware Failure Probabilities

Basic event FP-2PUMPS-FTF represents the failure of both firewater pumps. The pump may be required to run 8 to 10 hours at the most (250 gpm capacity), given that the water inventory drops by 20 ft (i.e., 3 ft from the top of the fuel). A failure probability of $3.7\text{E-}3$ for failure to start and run for the electric pump and 0.18 for the diesel driven pump are used from INEL-96/0334 (Ref. 12). Note that the relatively high unavailability assumed for the diesel driven firewater pump may be conservative if it is subject to a maintenance and testing program, and there are controls on availability. These individual pump failures result in a value of $6.7\text{E-}4$ for event FP-2PUMPS-FTF.

4.1.5.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-RECG-FWSTART	$2.0\text{E-}5$
HEP-RECG-FWSTART-L	$5.0\text{E-}2$
HEP-FW-START	$1.0\text{E-}5$
HEP-FW-REP-DEPEN	$5.0\text{E-}2$
FP-2PUMPS-FTF	$6.7\text{E-}4$

4.1.6 Top Event OFB – Operator Recovery Using Offsite Sources

4.1.6.1 Event Description and Timing

This event accounts for recovery of coolant makeup using offsite sources given the failure of recovery actions using onsite sources. Adequate time is available for this action, provided that the operating staff recognizes that recovery of cooling using onsite sources will not be successful, and that offsite sources are the only viable alternatives. This top event is quantified using fault tree LOC-OFB, for the upper two branches, and LOC-OFB-L for the lowest branch. Note that in this fault tree event HEP-INV-OFFSITE is ORed with the failure of the operator to recognize the need to start the firewater system (event HEP-RECG-FWSTART or HEP-RECG-FWSTART-L, described in Section 4.1.5.3). In essence, if the operators fail to recognize the need for firewater, it is assumed they will fail to recognize the need for other offsite sources of makeup.

4.1.6.2 Relevant Assumptions

- The operators have 88 hours to provide makeup and inventory cooling
- Procedures and training are in place that ensure that offsite resources can be brought to bear (NEI commitment no. 2 and 4), and that preparation for this contingency is made when it is realized that it may be necessary to supplement the pool makeup
- Procedures explicitly states that if the water level drops below a certain level (e.g., 15 ft below normal level) operator must initiate recovery using offsite sources
- Operators have received formal training in the procedures
- Offsite resources are familiar with the facility

4.1.6.3 Quantification

Human Error Probabilities

The event HEP-INV-OFFSITE represents failure to recognize that it is necessary to take the extreme measure of using offsite sources, given that even though there has been ample time up to this point to attempt recovery of both the SFP cooling system and both firewater pumps it has not been successful. This top event should include contributions from failure of both the diagnosis of the need to provide inventory from offsite sources, and of the action itself. The availability of offsite resources is assumed not to be limiting on the assumption of an expansive preparation time. However, rather than use a calculated HEP directly, a low level of dependence to account for the possible detrimental effects of the failure to complete prior tasks successfully.

4.1.6.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-INV-OFFSITE	5.0E-2

4.1.7 Summary

Table 4.1 presents a summary of basic event probabilities used in the event tree quantification.

Based on the assumptions made, the frequency of core uncovering can be seen to be very low. A careful and thorough adherence to NEI commitments 2, 5, 8 and 10 is crucial to establishing the low frequency. In addition, however, the assumption that walkdowns are performed on a regular, (once per shift) basis is important to compensate for potential failures to the instrumentation monitoring the status of the pool. The analysis has also assumed that the procedures and/or training are explicit in giving guidance on the capability of the fuel pool

makeup system, and when it becomes essential to supplement with alternate higher volume sources. The analysis also assumed that the procedures and training are sufficiently clear in giving guidance on early preparation for using the alternate makeup sources.

Table 4.1 Basic Event Summary for the Loss of Cooling Event Tree

Basic Event Name	Description	Basic Event Probability
IE-LOC	Loss of SFP cooling initiating event	3.0E-3
HEP-DIAG-ALARM	Operators fail to respond to a signal indication in the control room	3.0E-4
HEP-WLKDOWN-LSFPC	Operators fail to observe the loss of cooling in walkdowns (independent case)	1.0E-5
HEP-WLKDOWN-DEPEN	Operators fail to observe the loss of cooling in walkdowns (dependent case)	5.0E-2
HEP-COOL-REP-E	Repair crew fails to repair SFPC system	1.8E-1
HEP-COOL-REP-L	Repair crew fails to repair SFPC system	1.0
HEP-RECG-FWSTART	Operators fail to diagnose need to start the firewater system	2.0E-5
HEP-FW-START	Operators fail to start firewater pump and provide alignment	1.0E-5
HEP-FW-REP-DEPEN	Repair crew fails to repair firewater system	5.0E-2
HEP-INV-OFFSITE	Operators fail to provide alternate sources of cooling from offsite	5.0E-2
FP-2PUMPS-FTF	Failure of firewater pump system	6.7E-4
SPC-LVL-LOF	Failure of control room alarm channel	1.0E-5
SPC-LVL-LOP	Electrical faults leading to alarm channel failure	2.0E-3

4.2 Internal Fire Event Tree

This event tree models the loss of SFP cooling caused by internal fires. Given a fire alarm, the operator will attempt to suppress the fire, and then attempt to re-start SFP cooling given that the SFP cooling system and offsite power feeder system have not been damaged by the fire. In the unlikely event that the operator fails to respond to the alarms or is unsuccessful in suppressing the fire, it is assumed that the SFPC system will be damaged to the extent where repair will not be possible. The operator then has to provide alternate cooling and inventory

makeup – either using the site firewater system or by calling upon offsite resources. Figure 4.2 shows the Internal Fire event tree sequence progression.

4.2.1 Initiating Event FIR – Internal Fire

4.2.1.1 Event Description and Timing

The fire initiator includes those fires of sufficient magnitude, that if not suppressed, would cause a loss of cooling to the SFP. This loss of cooling could either result from damage to the SFPC system or the offsite power feeder system.

4.2.1.2 Relevant Assumptions

- Fire ignition frequencies from operating plants are assumed to be also applicable at the SFP facility.
- Ignition sources from welding and cutting are expected to be insignificant. The facility configuration is expected to be stable, negating the need for modification and fabrication work requiring welding and cutting.

4.2.1.3 Quantification

Data compiled from historical fires at nuclear power plants is summarized in the Fire-Induced Vulnerability Evaluation (FIVE) methodology document (Ref. 13). This document identifies fire ignition sources and associated frequencies and is segregated by plant location and ignition type. Of the plant locations identified in the FIVE document, the intake structure was considered to most closely approximate the conditions and equipment associated with the spent fuel pool facilities considered in this analysis.

FIVE identifies specific frequencies associated with 'electrical cabinets,' 'fire pumps,' and 'others' in the intake structure. In addition to these frequencies associated with specific equipment normally located in the intake structure, ignition sources from equipment (plant-wide) that may be located in the intake structure is also apportioned.

The largest ignition frequency contribution identified for intake structures is from fire pumps. In the plant configuration assumed in this study, the firewater pumps are located in an unattached structure and thus can be eliminated as ignition sources. FIVE also identifies electrical cabinets as significant ignition sources in the intake structure with an average frequency of $2.4E-3$ /yr. Because the number of electrical cabinets (breakers) in the spent fuel facility is expected to be less than those in the typical intake structure, a scaling factor was used to estimate the electrical cabinet contribution. Typically there are five motor-driven pumps (4 cooling pumps, 1 makeup pump) and related support equipment associated with the SPF facility. The number of electrical cabinets (breakers) was therefore estimated to be less than ten in a typical SFP facility. The number of electrical cabinets in the intake structure was estimated to be 25 (engineering judgement based on plant walkdowns). Therefore, the fire ignition frequency

contribution from electrical cabinets at the spent fuel pool facility is estimated to be $(10/25)(2.4E-3/\text{yr}) = 9.6E-4/\text{yr}$.

Figure 4.2 Fire initiating event tree

FIRE EVENT IN THE AUX BLDG/ REACTOR BLDG	CONTROL ROOM ALARMS (FIRE)	OTHER INDICATIONS OF LSFC DUE TO FIRE	SFC SYSTEM SURVIVE	OPERATOR RECOVERY USING DIESEL FIRE PUMPS	RECOVERY USING OFFSITE SOURCES		SEQUENCE-NAMES	END-STATE-NAMES	FREQUENCY	
E-FR	CRA	IND	OSP	OMK	OFD	#				
							1	IE-FIR	OK	
							2	IE-FIROSP	OK	
							3	IE-FIROS POMK	OK	
							4	IE-FIROS POMK OFD	SFP3FT	2.213E-008
							5	IE-FIRCRA	OK	
							6	IE-FIRCRAOMK	OK	
							7	IE-FIRCRAOMK OFD	SFP3FT	6.461E-010
							8	IE-FIRCRAIND	SFP3FT	2.190E-010

A similar approach was used to correlate the ignition frequency for "other" to a value appropriate for the SFP facility. Intake structures typically have several pumps (e.g., circulating water, service water, screen wash, fire, etc.) as well as peripheral equipment. For this analysis, all of the ignition frequency associated with the "other" category was apportioned to pumps. The number of pumps in the typical intake structure was estimated to be 10 (again, engineering judgement based on plant walkdowns). Therefore, the fire ignition frequency for "other" equipment at the spent fuel pool facility is estimated to be $(5/10)(3.2E-3/yr) = 1.6E-3/yr$.

The contribution of ignition sources, identified as 'plant-wide' sources in the FIVE document, to the ignition frequency of the SFP facility is considered to be negligible. Large ignition source contributors such as elevator motors, dryers, and MG sets do not exist in the spent fuel facility. Additionally, spontaneous cable fires are expected to be a negligible contributor because of the minimal amount of energized electrical cable. The facility configuration is expected to be stable, negating the need for modification and fabrication work requiring welding and cutting.

The fire ignition frequency for the SFP facility is therefore estimated to be $9.6E-4/yr + 1.6E-3/yr = 2.6E-3/yr$. A fire frequency value of $3E-3/yr$ will be used in the analysis to provide additional margin and to account for any uncertainties in equipment configuration.

4.2.1.4 Basic Event Probability

Basic Event	Basic Event Probability
IE-FIRE	3E-3

4.2.2 Top Event CRA – Control Room Alarms

4.2.2.1 Event Description and Timing

This event represents fire detection system failure to alarm in the control room or operator failure to respond to the alarm. The proper conditions for an alarm are assumed to exist within a few minutes of fire initiation. Failure to respond could be due to operator error (failure to respond), failure of the detectors, or loss of indication due to electrical faults. Success for this event is defined as the operator recognizing the alarm and responding to the fire. Failure of this event is assumed to lead to a fire damage state where there is a loss of the SFPC system and a loss of the plant power supply system. This event is quantified by fault tree FIR-CRA and includes hardware and human failures.

4.2.2.2 Relevant Assumptions

- The SFP area is equipped with fire detectors which are alarmed in the control room. However, the area is not equipped with an automatic fire suppression system.
- Fire alarms will be activated in the control room within a few minutes of the initiation of a fire.

- Regular maintenance and testing is performed on the fire detection system and on the control room annunciators.
- Procedures are available to guide operator response to a fire, and plant operators are trained in these procedures (NEI commitment no. 2).

4.2.2.3 Quantification

Human Error Probabilities

One human failure event is modeled for this event (basic event HEP-DIAG-ALARM). The operator may fail to respond to a signal or indication in the control room. The source for this error rate is THERP (Table 20-23).

Hardware Failure Probabilities

The value used for failure of the detectors, SFP-FIRE-DETECT (5.0E-3), was taken from OREDA-92 (Ref. 14). The value used for local electrical faults leading to alarm channel failure, SFP-FIRE-AOL (2.0E-3), was estimated based on information in reference 11.

4.2.2.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-DIAG-ALARM	3.0E-4
SFP-FIRE	2.0E-3
SFP-FIRE-DETECT	5.0E-3

4.2.3 Top Event IND – Other Indications of Loss of Cooling

4.2.3.1 Event Description and Timing

This event models the failure of the operators to recognize the loss of SFP cooling resulting from a fire, given that either the fire alarm system failed or was not attended to. Since the assumed consequences of not attending to the alarm are a fire large enough to cause loss of power to the facility, the indications available to the operator during a walkdown include clear effects of the fire, both from visible evidence and the smell of burning, as well as the lack of power. Ultimately, if no action is taken to restore cooling, the high area temperature and humidity, and low water level from boil-off will become increasingly evident. The operators have more than 10 shifts (about 131 hours) to discover the loss of SFP cooling. Success for this event is defined as the operators recognizing the abnormal condition and understanding the need to take action within this time. This event is modeled by fault tree FIR-IND.

4.2.3.2 Relevant Assumptions

- Operators perform walkdowns once per shift (every 8 to 12 hours) and walkdowns are required to be logged
- If the fire is discovered during the walkdown, the SFPC system is assumed to be damaged to the extent where repair will not be feasible within a few days.
- Local instrumentation and alarms are destroyed in a fire which is not extinguished within 20 minutes.
- Procedures are available to guide plant operators for off-normal conditions, and operators are trained in these procedures (NEI commitment no. 2).

4.2.3.3 Quantification

Human Error Probability

This event is represented by the basic event HEP-WLKDOWN-LSFPC which models the operators' failure to recognize the loss of cooling during walkdowns. The failure rate was developed using THERP, and is based upon three individual failures: failure to carry out an inspection, missing a step in a written procedure, and misreading a measuring device. Multiple opportunities for recovery were assumed.

Note that no dependency on the previous HEP was modeled. While it could be argued that, in the case where the operator has already failed to respond to control room alarms, there may be a dependence between the event HEP-DIAG-ALARM and HEP-WLKDOWN-LSFPC. However, the cues for this event are quite different. There will be obvious physical changes in the plant (e.g., loss of offsite power, a burnt out area, smoke, etc.). The only source of dependency is one where a situation would result in the operator failing to respond to control room alarms and also result in a total abandonment of plant walkdowns.

4.2.3.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-WLKDOWN-LSFPC	1.0E-5

4.2.4 Top Event OSP – Fire Suppression

4.2.4.1 Event Description and Timing

This top event represents operator failure to suppress the fire before the SFP cooling system is damaged given that he responds to fire alarms. If the SFP cooling and makeup system pumps and plant power supply system are damaged to a point that they cannot be repaired in time to

prevent fuel uncover, the operator must provide cooling using available onsite (i.e., diesel fire pumps) and offsite water sources. If the fire is suppressed in time to prevent damage to SFP components, then the SFP cooling system can be restored in time to prevent fuel uncover. The top event is represented by fault tree FIR-OSP.

4.2.4.2 Relevant Assumptions

- The automatic fire suppression system is unavailable.
- If the fire is not extinguished within 20 minutes, it is assumed that SFP cooling will be lost due either to damage of SFPC equipment, or to the plant's power supply system.
- No credit is taken for the firewater system in the suppression of the fire.
- Fire suppression extinguishers are located strategically in the SFP area, and these extinguishers are tested periodically.

4.2.4.3 Quantification

Failure of fire suppression is represented by basic event HEP-RES-FIRE. The modeling of fire growth and propagation and the determination of the effects of a fire on equipment in a room would optimally take into account the combustible loading in the room, the presence of intervening combustibles, the room size and geometry, and other characteristics such as ventilation rates and the presence of openings in the room. Because detailed inputs such as these are not applicable for a generic study such as this, fire growth and propagation was determined based on best estimate assumptions. It is assumed that the operator has 20 minutes to suppress the fire, otherwise, it is assumed that SFP cooling will be lost (due either to damage of SFPC equipment, or to the plant's power supply system).

HEP-RES-FIRE was modeled using THERP. Due to the level of uncertainty about the size of the fire, its location, and when it is discovered, the approach taken was to model this error as a dynamic task requiring a higher level of human interaction, including keeping track of multiple functions. In addition little experience in fighting fires was assumed. Table 20-16 in THERP provides modifications of estimated HEPs for the effects of stress and experience. Using the performance shaping factors of extremely high stress (as fighting a fire would be), a dynamic task, and an operator experienced in fighting fires, this table provides an HEP of $2.5E-1$.

Notes: (1) It can be argued that damage time (to disable the SFP cooling function) could be in excess of 20 minutes because typical SFP facilities are relatively large and because equipment within such facilities is usually spread out. However, in this analysis, the SFP pumps are assumed to be located in the same general vicinity with no fire barriers between them.

(2) Scenarios can be postulated where the fire damage state is less severe than that described above (e.g., fire damage to the running cooling pump, with the other pump undamaged, and with offsite power available). These scenarios can

be subsumed into the "Loss of Cooling" event, and SFP cooling "recovery" in these cases would be by use of the undamaged pump train.

4.2.4.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-RES-FIRE	2.5E-1

4.2.5 Top Event OMK – Operator Recovery Using Onsite Sources

4.2.5.1 Event Description and Timing

At this point in the event tree, the SFP cooling has been lost as a result of the fire, and the operators are unable to restore the cooling system. Also, the fire has damaged the electrical system such that the motor-driven firewater pump is unavailable. If no actions are taken, SFP water level would drop to 3 ft above the top of fuel in 131 hours from the time the loss of SFP cooling occurred. This event represents failure of the operators to start the diesel-driven firewater pump and provide makeup to the SFP. If the diesel firewater pump fails, the operators have time to attempt repair. This event is modeled by fault tree FIR-OMK.

4.2.5.2 Relevant Assumptions

- There is a means to remotely align a makeup source to the spent fuel pool without entry to the refuel floor, so that makeup can be provided even when the environment is uninhabitable due to steam and/or high radiation (NEI commitment no.8)
- Inventory makeup using the firewater system is initiated by onsite operators.
- In modeling the repair of a failed firewater pump, it is assumed that it takes 16 hours to contact maintenance personnel, make a diagnosis, and get new parts.
- Mean time to repair the firewater pump is 10 hours.
- Inventory makeup using the firewater pumps are proceduralized, and the operators are trained in these procedures (NEI commitment no. 2).
- Firewater pumps are tested and maintained on a regular schedule (NEI commitment no. 10).

4.2.5.3 Quantification

Human Error Probabilities

The fault trees used to quantify this top event include three human failure events.

HEP-RECG-FWSTART represents the operators' failure to recognize the loss of SFP cooling and the need to initiate the firewater system. This event was quantified using the SPAR HRA technique. The assumptions include expansive time (> 24 hours), a high level of stress, diagnostic type procedures, good ergonomic interface, and good quality of work process. This diagnosis task provides the diagnosis for the subsequent actions taken to re-establish cooling to the pool. Although this diagnosis and subsequent actions follow a fire, no dependence between response to the fire and subsequent actions is assumed, because of the large time lag.

HEP-FW-START represents failure to start the diesel firewater pump within 88 hours after the onset of bulk boiling, given that the decision to start a firewater pump was made. No difficult valve alignment is required, but the operator may have to position a hose in the pool area. This event HEP-FW-START was quantified using SPAR HRA technique. The following PSFs were assumed: expansive time (> 50 times the required time), high stress, highly complex task because of the multiple steps, its non-routine nature, quality procedures available, as well as good ergonomics including equipment and tools matched to procedure, and finally a crew who had executed these tasks before, conversant with the procedures and one another.

HEP-FW-REP-NODEP represents the failure of the repair crew to repair a firewater pump. It is assumed that the operators will focus their recovery efforts on only the diesel driven pump. Assuming that it takes 16 hours before technical help and parts arrive, then the operators have 72 hours (88 hours less 16 hours) to repair the pump. Assuming a 10-hour mean time to repair, the probability of failure to repair the pump would be $\text{Exp}[-(1/10) \times 72] = 1.0\text{E-}3$.

Hardware Failure Probabilities

Basic event FP-DGPUMP-FTF represents the failure of the diesel driven firewater pump. The pump may be required to run 8 to 10 hours at the most (250 gpm capacity), given that the water inventory drops by 20 ft (i.e., 3 ft from the top of the fuel). A failure probability of 1.8E-1 for failure to start and run for the diesel driven pump is used from INEL-96/0334 (Ref. 12).

4.2.5.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-RECG-FWSTART	2.0E-5
HEP-FW-START	1.0E-5
HEP-FW-REP-NODEP	1.0E-3
FP-DGPUMP-FTF	1.8E-1

4.2.6 Top Event OFD – Operator Recovery Using Offsite Sources

4.2.6.1 Event Description and Timing

Given the failure of recovery actions using onsite sources, this event accounts for recovery of coolant makeup using offsite sources. Adequate time is available for this action, provided that the operators recognize that recovery of cooling using onsite sources will not be successful,

and that offsite sources are the only viable alternatives. This top event is quantified using fault tree FIR-OFD. This event is represented by a basic event HEP-INV-OFFSITE.

4.2.6.2 Relevant Assumptions

- The operators have 88 hours to provide makeup and inventory cooling
- Procedures and training are in place that ensure that offsite resources can be brought to bear (NEI commitment no. 2 and 4), and that preparation for this contingency is made when it is realized that it may be necessary to supplement the pool makeup
- Procedures explicitly states that if the water level drops below a certain level (e.g., 15 ft below normal level) operator must initiate recovery using offsite sources
- Operators have received formal training in the procedures
- Offsite resources are familiar with the facility

4.2.6.3 Quantification

Human Error Probabilities

The event HEP-INV-OFFSITE represents failure to recognize that it is necessary to take the extreme measure of using offsite sources, given that even though there has been ample time up to this point to attempt recovery of the firewater pump, it has not been successful. This top event should include failures of both the diagnosis of the need to provide inventory from offsite sources, and of the action itself. The availability of offsite resources is assumed not to be limiting on the assumption of an expansive preparation time. However, rather than use a calculated HEP directly, a low level of dependence to account for the possible detrimental effects of the failure to complete prior tasks successfully.

4.2.6.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-INV-OFFSITE	5.0E-2

4.2.7 Summary

Table 4.2 presents a summary of basic event probabilities used in the event tree quantification.

As in the case of the loss of cooling event, the frequency of core uncover, based on the assumptions made in the analysis, is very low. The assumptions that support this low value include: careful and thorough adherence to NEI commitments 2, 5, 8 and 10; walkdowns are performed on a regular, (once per shift) (important to compensate for potential failures to the instrumentation monitoring the status of the pool); procedures and/or training are explicit in

giving guidance on the capability of the fuel pool makeup system, and when it becomes essential to supplement with alternate higher volume sources; procedures and training are sufficiently clear in giving guidance on early preparation for using the alternate makeup sources.

Table 4.2 Basic Event Summary for the Internal Fire Event Tree

Basic Event Name	Description	Basic Event Probability
HEP-DIAG-ALARM	Operators fail to respond to a signal indication in the control room	3.0E-4
HEP-RES-FIRE	Operators fail to suppress fire	2.5E-1
HEP-WLKDWN-LSFPC	Operators fail to observe the loss of cooling in walkdowns (independent case)	1.0E-5
HEP-WLKDWN-DEPEN	Operators fail to observe the loss of cooling in walkdowns (dependent case)	5.0E-2
HEP-RECG-FWSTART	Operators fail to diagnoses need to start the firewater system	2.0E-5
HEP-FW-START	Operators fail to start firewater pump and provide alignment	1.0E-5
HEP-FW-REP-NODEP	Repair crew fails to repair firewater system	1.0E-3
HEP-INV-OFFSITE	Operators fail to provide alternate sources of cooling from offsite	5.0E-2
FP-DGPUMP-FTF	Failure of firewater pump system	0.18
SFP-FIXE-LOA	Electrical faults causing loss of alarms	2E-3
SFP-FIRE-DETECT	Failure of fire detectors	5E-3

4.3 Plant-centered and Grid-related Loss of Offsite Power Event Tree

This event tree represents the loss of SFP cooling resulting from a loss of offsite power from plant-centered and grid-related events. Until offsite power is recovered, the electrical pumps would be unavailable, and only the diesel fire pump would be available to provide makeup.

Figure 4.3 shows the Plant-centered and Grid-related Loss of Offsite Power (LOSP) event tree sequence progression.

4.3.1 Initiating Event LP1 – Plant-centered and Grid-related Loss of Offsite Power

4.3.1.1 Event Description

Initiating event IE-LP1 represents plant-centered and grid-related losses of offsite power. Plant-centered events typically involve hardware failures, design deficiencies, human errors (in maintenance and switching), localized weather-induced faults (e.g., lightning), or combinations of these. Grid-related events are those in which problems in the offsite power grid cause the loss of offsite power.

4.3.1.2 Quantification

For plant-centered LOSP events, NUREG/CR-5496 (Ref. 16) estimates a frequency of .04/critical year for plant centered loss of offsite power for an operating plant, and .18/unit shutdown year for a shutdown plant. For grid-related LOSP events, a frequency of 4E-3/site yr was estimated. The frequency of grid-related losses is assumed to be directly applicable. However, neither of the plant centered frequencies is directly applicable. At a decommissioning plant there will no longer be the necessity to have the multiplicity of incoming lines typical of operating plants, which could increase the frequency of loss of offsite power from mechanical failures. On the other hand, the plant will be a normally operating facility, and it would be expected that there will be less activity and operations in the switchyard than would be expected at a shutdown plant, which would decrease the frequency of loss from human error, the dominant cause of losses for shutdown plants. For purposes of this analysis, the LOSP initiating event frequency of 0.08/yr, assumed in INEL-96/0334 (Ref. 13), is assumed for the combined losses from plant-centered and grid-related events.

4.3.2 Top Event OPR – Offsite Power Recovery

4.3.2.1 Event Description and Timing

The fault tree for this top event (LP1-OPR) is a single basic event that represents the non-recovery probability of offsite power.

NUREG-1032 (Ref. 17) classified LOSP events into plant-centered, grid-related, and severe-weather-related categories, because these categories involved different mechanisms and also seemed to have different recovery times. Similarly, NUREG/CR-5496 (Ref. 16) divides LOSP events into three categories and estimates different values of non-recovery as functions of time.

4.3.2.2 Relevant Assumptions

- Trained electricians may not be present at the site for the quick recovery.
- Operators have received formal training and there are procedures to guide them (NEI commitment no. 2).

Figure 4.3 Plant centered and grid related loss of offsite power event tree

LOSS OF OFFSITE POWER FROM PLANT CENTERED AND GRID RELATED EVENTS	OFFSITE POWER RECOVERY PRIOR TO SFP C SYSTEM LOSS	COOLING SYSTEM RESTART AND RERUN	OPERATOR RECOVERY USING MAKEUP SYSTEM	RECOVERY FROM OFFSITE SOURCES				
E-LP1	OPR	OCS	OMK	OFD	#	SEQUENCE-NAMES	END-STATE-NAMES	FREQUENCY
					1	IE-LP1	OK	
					2	IE-LP1OCS	OK	
					3	IE-LP1OCSOMK	OK	
					4	IE-LP1OCSOMKOFD	SFP3FT	5.673E-009
					5	IE-LP1OPR	OK	
					6	IE-LP1OPROMK	OK	
					7	IE-LP1OPROMKOFD	SFP3FT	2.360E-008