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

411

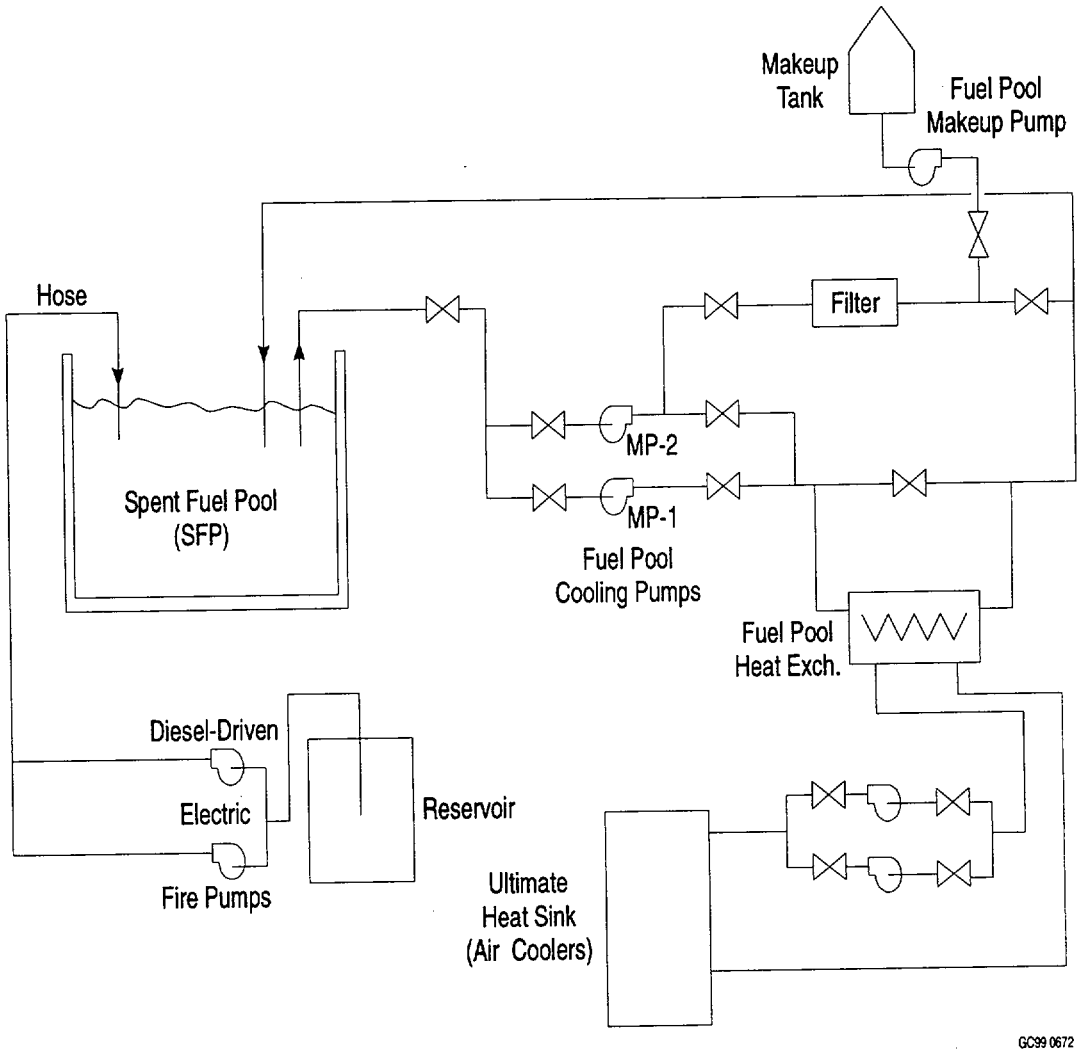


Figure 2.1 Simplified Diagram of Spent Fuel Pool Cooling and Inventory Makeup Systems

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 uncovery 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 uncovery 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 ft^3/ft depth, and for PWRs, we have 957 ft^3/ft depth. Assume ≈ 1000 ft^3/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 uncovery. 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 boildown to 3 ft above the top of the fuel. Therefore, the total time available for operator action is as follows:

Total Time = 33 hr + (20 ft)/(0.2 ft/hr)
= 131 hours

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 uncovery is as follows:

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

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 uncovery 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 uncovery 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/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

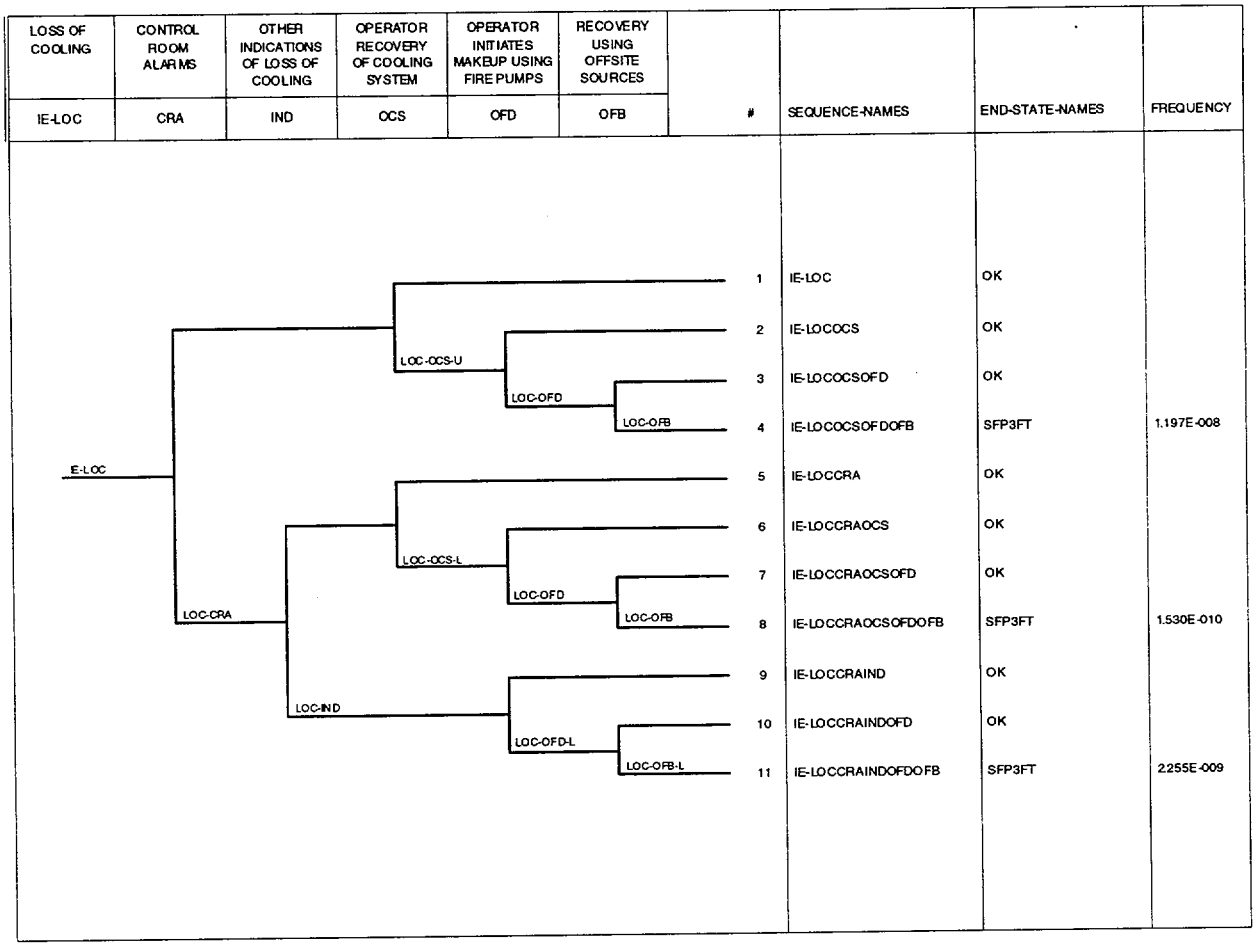
This top event models subsequent operator failures to recognize the loss of cooling during walkdowns over multiple shifts. Indications available to the operators include: temperature readouts in the control room (NEI commitment no. 5), local temperature measurements, and

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



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-WLKDWN-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-WLKDWN-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-WLKDWN-LSFPC	1.0E-5
HEP-WLKDWN-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 uncovery (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 Exp [-(1/10) * 72] = 1.0E-3. For HEP-FW-REP-DEPEN a low level of

dependence was applied modifying the nominal failure probability of 1.0E-3 to 5.0E-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 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 uncovery 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-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-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.

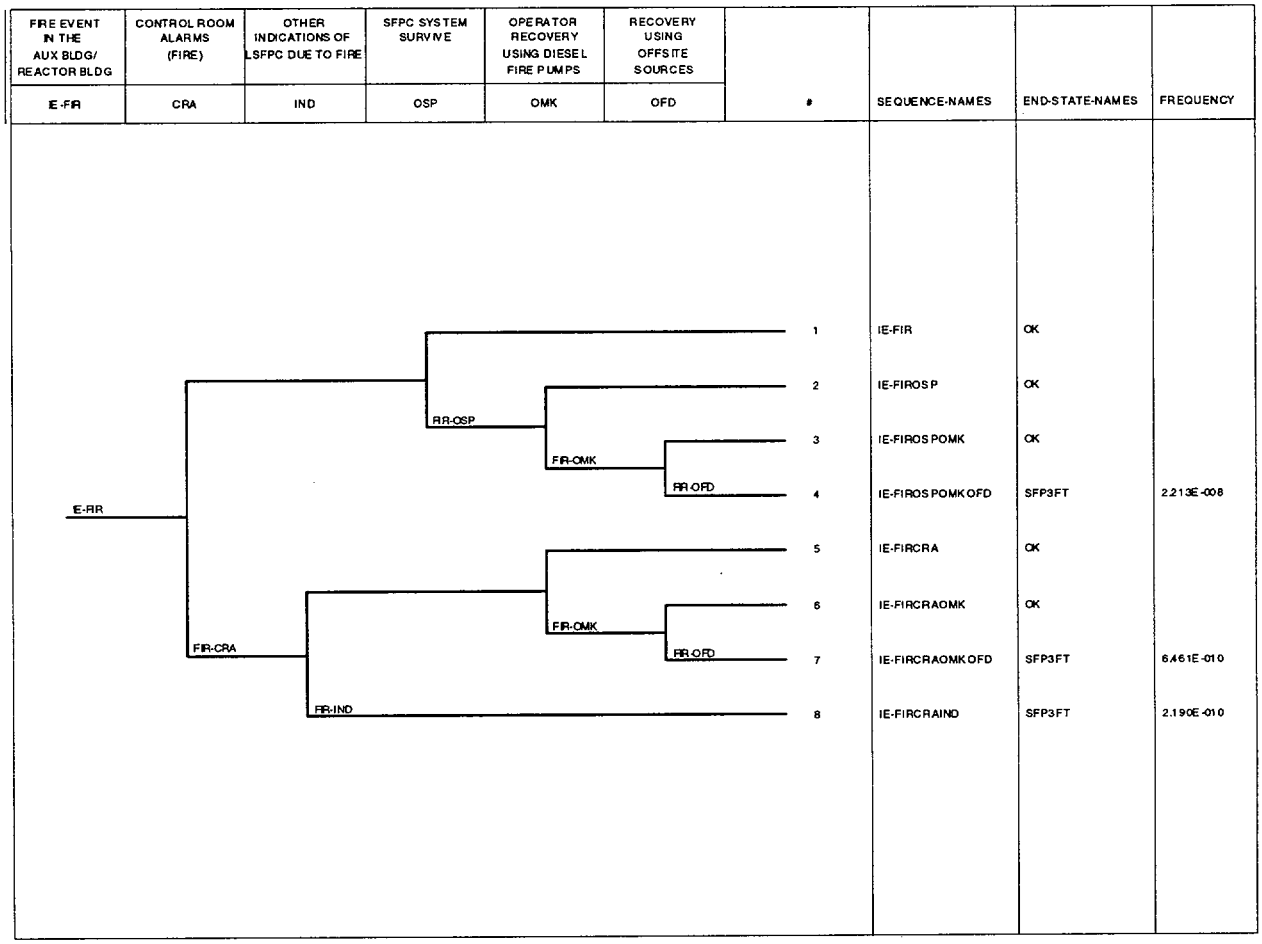
4.2.1.3 Quantification

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/yr) = 9.6E-4/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 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-WLKDWN-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-WLKDWN-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-WLKDWN-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 uncovery, 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 uncovery. 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 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 assume 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 Exp [-(1/10)x72] = 1.0E-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 uncovery, 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

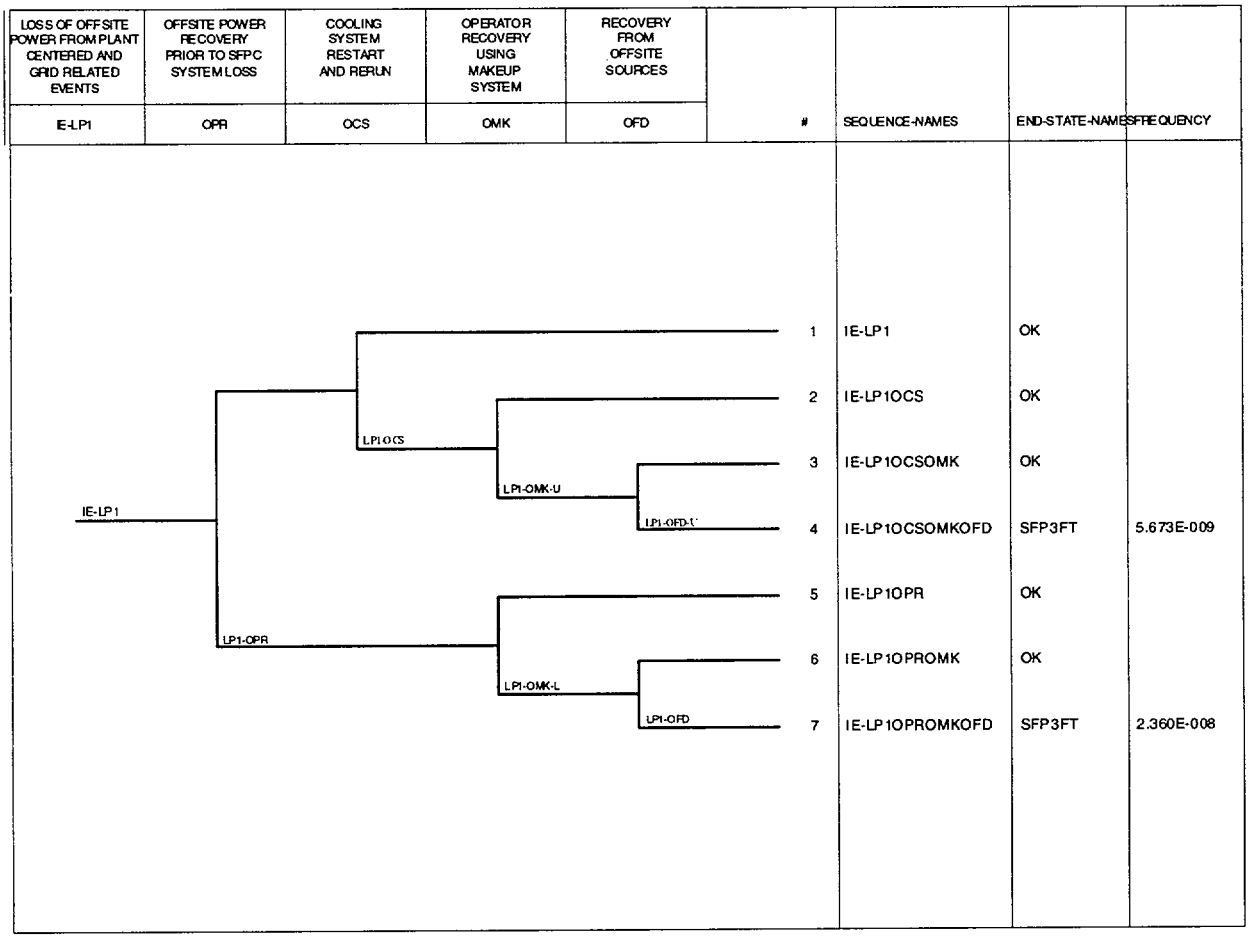
The fault tree for this top event (LP1-OPR) is a single basic event that represents the non-recovery probability of offsite power.

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



4.3.2.3 Quantification

The basic event that represents recovery of offsite 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 offsite 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 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 walkdowns following the loss of offsite 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, high stress, well-trained operators, diagnostic procedures, and good work processes. A low dependence for the walkdown 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 offsite 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 offsite 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 onsite 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 since 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 Exp [-(1/10) (72] = 1.0E-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 1.0E-3. For HEP-FW-REP-DEPEN a low level of dependence was applied modifying the failure rate of 1.0E-3 to 5.0E-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 3.7E-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. These individual pump failures result in a value of 0.18 for event FP-DGPUMP-FTF and 6.7E-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
HEP-FW-START	1.0E-5
HEP-FW-REP-DEPEN	5.0E-2

Basic Event	Basic Event Probability
FP-2PUMPS-FTF	6.7E-4
FP-DGPUMP-FTF	1.8E-1

4.3.5 Top Event OFD – Operator Recovery Using Offsite Sources

4.3.5.1 Event Description and Timing

Given the failure of recovery actions using onsite sources, this event accounts for recovery of coolant makeup using offsite sources such as procurement of a fire engine. Adequate time is available for this action, provided that the operator recognizes that recovery of cooling using onsite sources will not be successful, and that offsite 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 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

4.3.5.3 Quantification

Human Error Probabilities

The event HEP-INV-OFFSITE represents failure to recognize that it is necessary to take the extreme measure of using 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 failures of both the diagnosis of the need to provide inventory from offsite sources, and 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.

4.3.5.4 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 Offsite 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 uncovery can be seen to be very low. Again, a careful and thorough adherence to NEI commitments 2, 5, 8 and 10, 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 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 Offsite Power

Basic Event Name	Description	Probability
IE-LP1	Loss of offsite power due to plant-centered or grid-related causes	8.0E-2
REC-OSP-PC	Recovery of offsite power within 24 hours	1.0E-2
HEP-DIAG-SFPLP1	Operators fail to diagnose loss of SFP cooling due to loss of offsite 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 Offsite Power Event Tree

This event tree represents the loss of SFP cooling resulting from a loss of offsite power from severe-weather-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 4.4 shows the Severe Weather Loss of Offsite Power (LOSP) event tree sequence progression.

4.4.1 Initiating Event LP2 – Severe Weather Loss of Offsite Power

4.4.1.1 Event Description

Initiating event IE-LP2 represents severe-weather-related losses of offsite power. Severe weather threatens the safe operation of a SFP facility by simultaneously causing loss of offsite

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 offsite 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).

4.4.2 Top Event OPR – Offsite 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 offsite 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

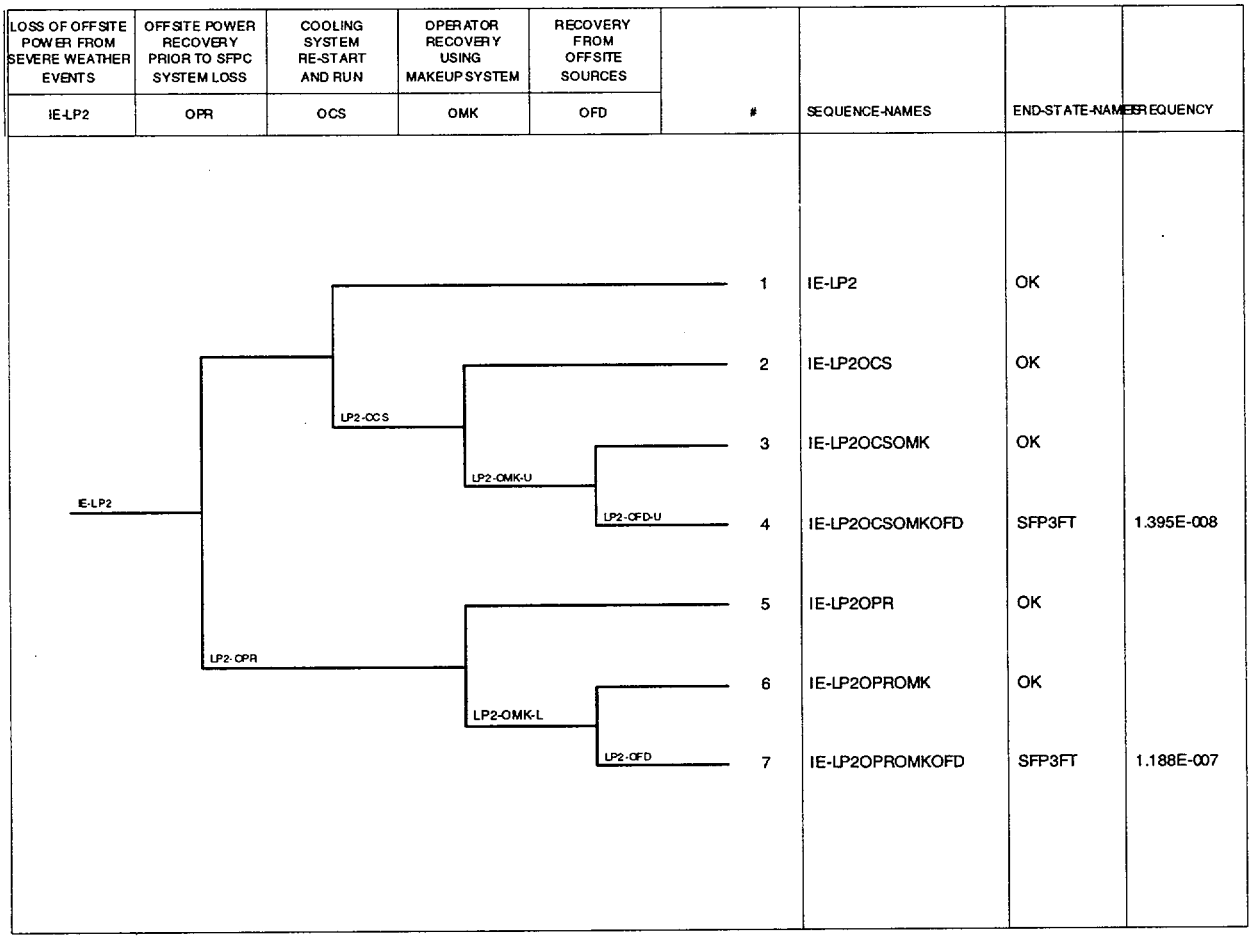
- See section 4.4.2.3 below.

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 offsite 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 offsite 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 offsite power due to severe weather event (REC-OSP-SW) of 2.0E-2 is used.

Figure 4.4 Severe weather related loss of offsite power event tree



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 offsite 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 offsite 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 walkdown 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 offsite 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 offsite 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 onsite 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 haves 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 Exp [-(1/10) (40)] = 2.5E-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 2.5E-2 to 7.0E-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 3.7E-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. These individual pump failures result in a value of 0.18 for event FP-DGPUMP-FTF and 6.7E-4 for event FP-2PUMPS-FTF.

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 Offsite Sources

4.4.5.1 Event Description and Timing

Given the failure of recovery actions using onsite sources, this event accounts for recovery of coolant makeup using offsite sources such as procurement of a fire engine. Adequate time is available for this action, provided that the operator recognizes that recovery of cooling using onsite sources will not be successful, and that offsite sources are the only viable alternatives. Fault tree LP2-OFD represents this top event for the lower branch (offsite 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 offsite 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 offsite sources
- Offsite resources are familiar with the facility

4.4.5.3 Quantification

Human Error Probability

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 failures of both the diagnosis of the need to provide inventory from offsite sources, and 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.

4.4.5.4 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 Offsite Power from severe weather events.

As in the case of the loss of offsite power from plant centered and grid related events, based on the assumptions made, the frequency of core uncovery can be seen to be very low. Again, a careful and thorough adherence to NEI commitments 2, 5, 8 and 10, 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 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 communivation 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 offsite resources could become more limiting.

Table 4.4 Basic Event Summary for Severe Weather Loss of Offsite 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 offsite 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

Basic Event Name	Description	Basic Event Probability
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 offsite	8.0E-2
REC-OSP-SW	Recovery of offsite 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
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 dropped loads or seismic events. The following assumptions have been 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 boiloff

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 uncovery 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

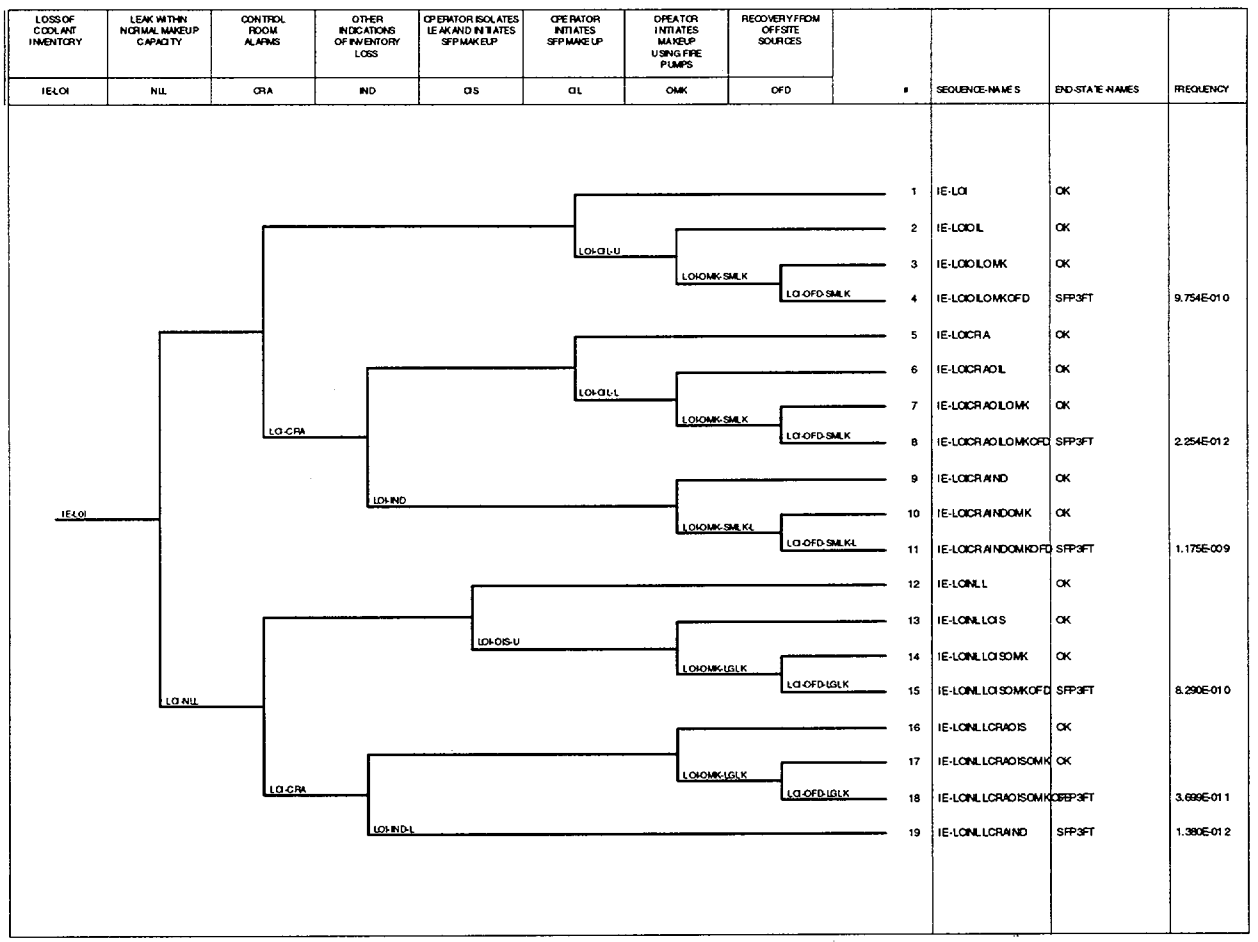
- The small leak is assumed for analysis purposes to be at the limit of the make-up system capacity, i.e., 30 gpm

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 uncovery.

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 walkdowns over subsequent shifts. Indications available to the operators include readouts 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 uncovery. 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 offsite sources) before fuel uncovery. 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-WLKDWN-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-WLKDWN-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-WLKDWN-DEPEN	5.0E-2
HEP-WLKDWN-LOI-L	1.0E-5
HEP-WLKDWN-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 here 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 on the order of 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
- 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 would be 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 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 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 Proabability

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 onsite operators
- 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 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, then 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 Exp (-(1/10) * 49) = 7.5E-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 Exp (-(1/10) * 24) = 9.0E-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 3.7E-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. These individual pump failures result in a value 6.7E-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 Offsite Sources

4.5.8.1 Event Description and Timing

Given the failure of recovery actions using onsite sources, this event accounts for recovery of coolant makeup using offsite sources 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 offsite sources
- Operator has received formal training and there are procedures to guide him
- Offsite 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 offsite personnel, highly trained staff with good procedures, good ergonomics (equipment is available to make offsite 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 uncovery 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 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 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-WLKDWN-LOI	Operators fail to observe the LOI/loss of cooling in walkdowns, given failure to prevent loss of SFP cooling	5.0E-3
HEP-WLKDWN-LOI-L	Operators fail to observe the LOI/loss of cooling in walkdowns (independent case)	1.0E-5
HEP-WLKDWN-DEPEN	Operators fail to observe the LOI event walkdowns (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 offsite sources	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
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 Offsite Power, 5) Severe Weather Induced Losses of Offsite Power. The total frequency for the endstate is estimated to be 2.3E-7/year. Table 5.1 summarizes the core uncovery frequency for each accident sequence. 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 system, the point estimates therefore closely correlate to the mean values that would be obtained from a full propagation of parameter uncertainty.

The analysis has shown that, based on the assumptions made, the frequency of core uncovery from the loss of cooling, loss of inventory, loss of offsite 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; walkdowns 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 onsite sources such as fire water pumps, and that from offsite sources. However, if no such provision were made, the availability of offsite resources could become more limiting.

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

The worth of each individual commitment in achieving the low level of risk has not evaluated. The analysis has, however, demonstrated to the staff that, given an appropriate implementation of the commitments, the risk is indeed low, and would warrant consideration of granting exemptions.

Table 5.1 Summary of results

Sequence ID	**Core Uncovery Frequency (1/yr)**
IE-FIR-4	2.2E-008
IE-FIR-7	6.5E-010
IE-FIR-8	2.2E-008
IE-LOC-4	1.2E-008
IE-LOC-8	1.5E-010
IE-LOC-11	2.2E-009
IE-LOI-04	9.8E-010
IE-LOI-08	2.3E-012
IE-LOI-011	1.2E-009
IE-LOI-15	8.3E-010
IE-LOI-18	3.7E-011
IE-LOI-19	1.4E-012
IE-LP1-4	5.7E-009
IE-LP1-7	2.4E-008
IE-LP2-4	1.4E-008
IE-LP2-7	1.2E-007
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, date November 9, 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, Instituite 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. Blackman, H. S., SPAR HRA

10. Sailor, et. al., "Severe Accidents in Spent Fuel Pools in Support of Generic Safety 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

15. OREDA-92 Offshore Reliability Data Handbook, 2nd Edition, 1992.

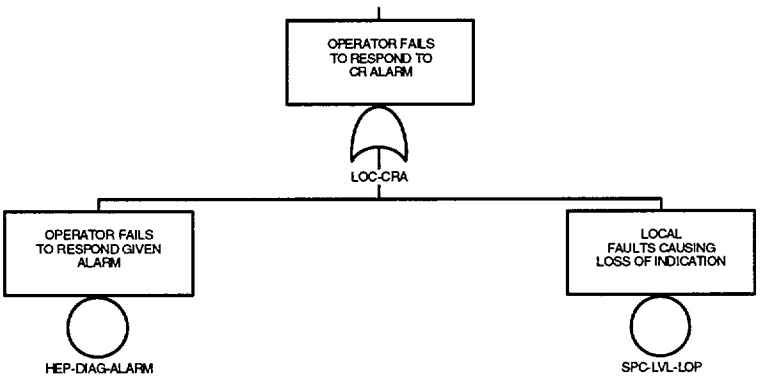
16. Atwood, et. al., "Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980 - 1996," NUREG/CR-5486, November 1998

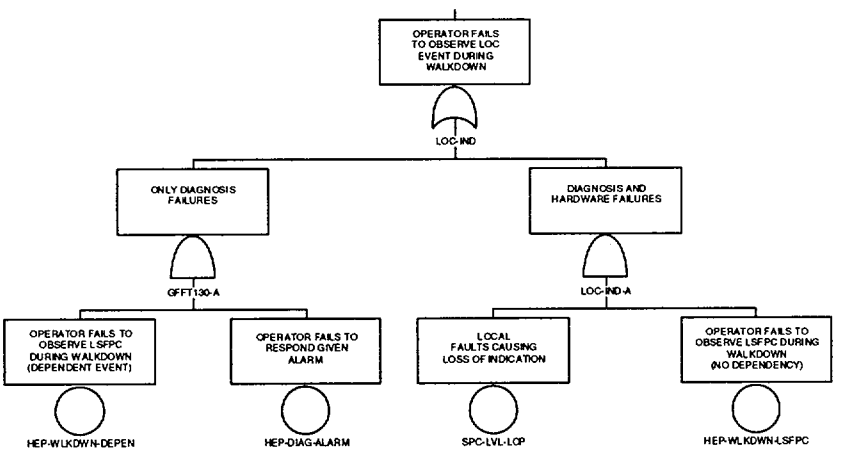
17. U.S. Nuclear Regulatory Commission, "Evaluation of Station Blackout Accidents at Nuclear Power Plants," NUREG-1032, June 1988

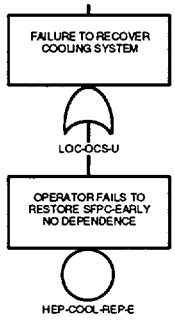
18. U.S. Nuclear Regulatory Commission, "Single-Failure-Proof Cranes for Nuclear Power Plants," USNRC Report NUREG-0554, May 1979

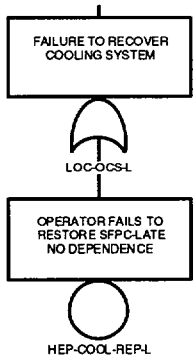
ATTACHMENT A

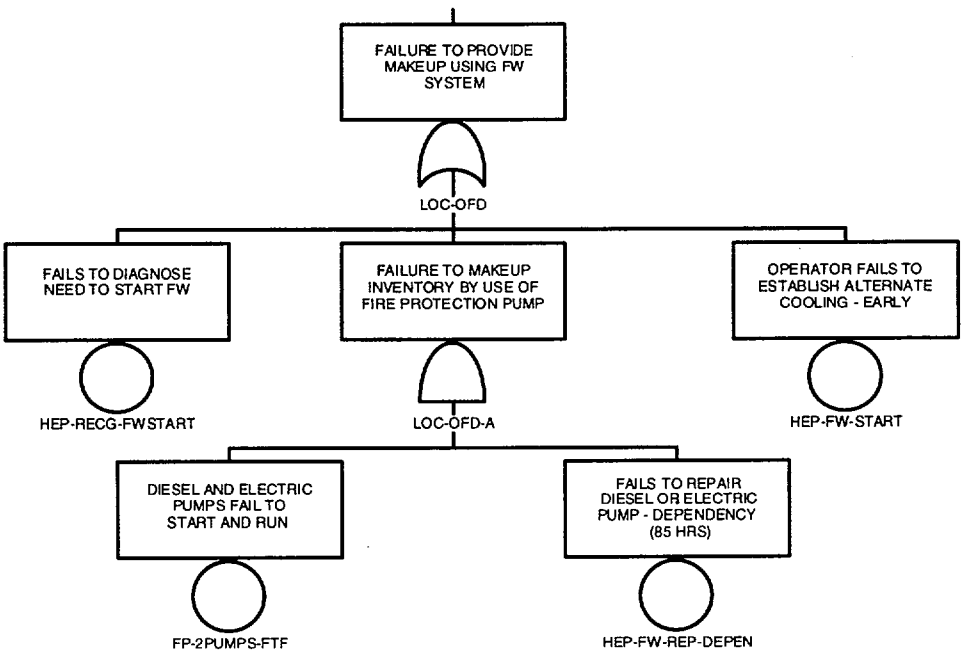
FAULT TREES USED IN THE RISK ANALYSIS

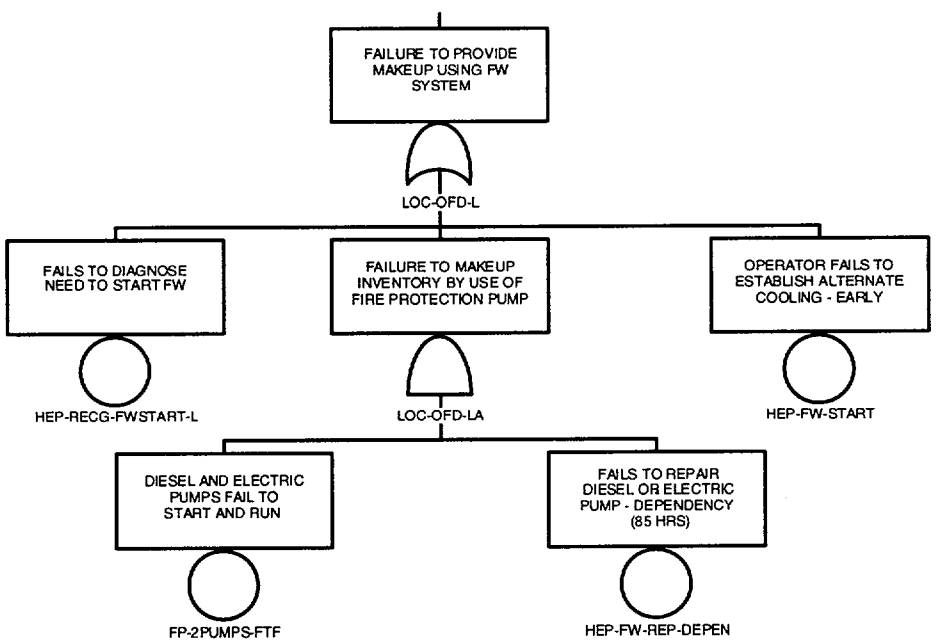

OPERATOR FAILS TO RESPOND TO CR ALARM
LOC-CRA
OPERATOR FAILS TO RESPOND GIVEN ALARM
LOCAL FAULTS CAUSING LOSS OF INDICATION
HEP-DIAG-ALARM
SPC-LVL-LOP

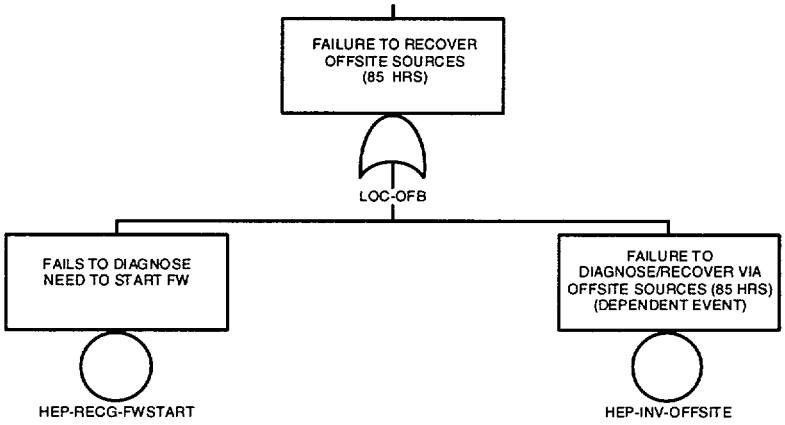

OPERATOR FAILS TO OBSERVE LOC EVENT DURING WALKDOWN
LOC-IND
ONLY DIAGNOSIS FAILURES
DIAGNOSIS AND HARDWARE FAILURES
GFFT130-A
LOC-IND-A
OPERATOR FAILS TO OBSERVE LSFPC DURING WALKDOWN (DEPENDENT EVENT)
OPERATOR FAILS TO RESPOND GIVEN ALARM
LOCAL FAULTS CAUSING LOSS OF INDICATION
OPERATOR FAILS TO OBSERVE LSFPC DURING WALKDOWN (NO DEPENDENCY)
HEP-WLKDWN-DEPEN
HEP-DIAG-ALARM
SPC-LVL-LOP
HEP-WLKDWN-LSFPC

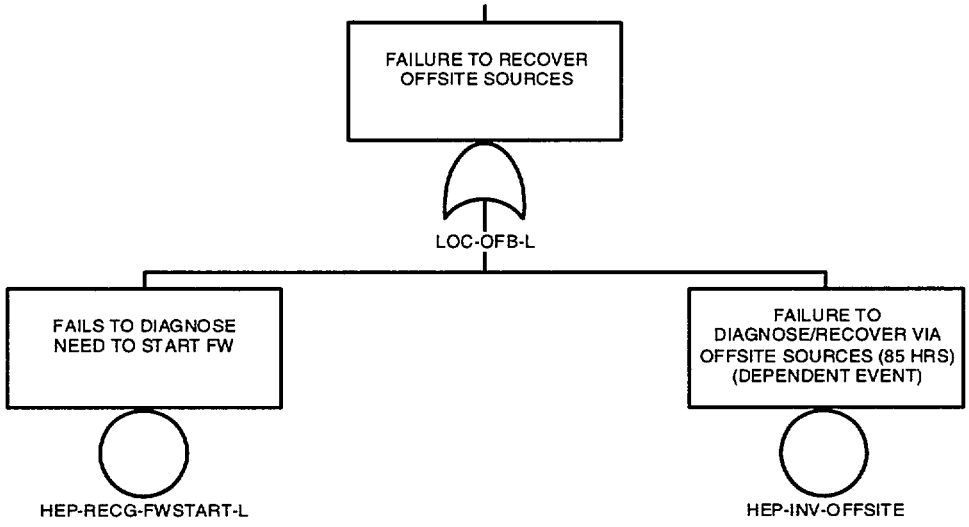

FAILURE TO RECOVER COOLING SYSTEM
LOC-OCS-U
OPERATOR FAILS TO RESTORE SFPC-EARLY NO DEPENDENCE
HEP-COOL-REP-E

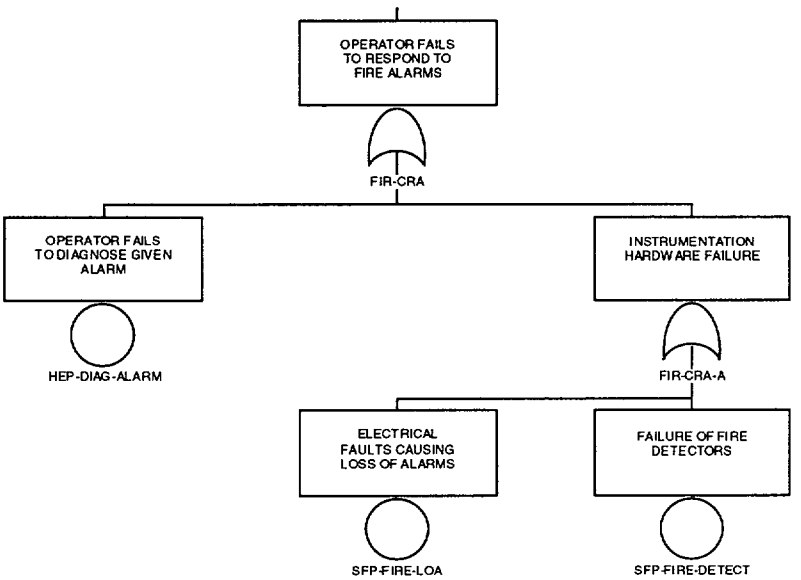

FAILURE TO RECOVER COOLING SYSTEM
LOC-OCS-L
OPERATOR FAILS TO RESTORE SFPC-LATE NO DEPENDENCE
HEP-COOL-REP-L

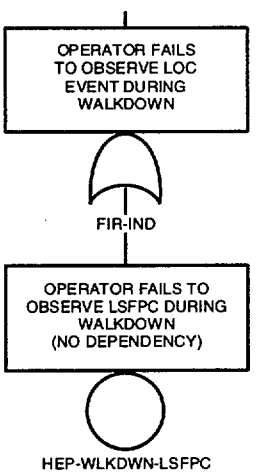

FAILURE TO PROVIDE MAKEUP USING FW SYSTEM
LOC-OFD
FAILS TO DIAGNOSE NEED TO START FW
FAILURE TO MAKEUP INVENTORY BY USE OF FIRE PROTECTION PUMP
OPERATOR FAILS TO ESTABLISH ALTERNATE COOLING - EARLY
HEP-RECG-FWSTART
LOC-OFD-A
HEP-FW-START
DIESEL AND ELECTRIC PUMPS FAIL TO START AND RUN
FAILS TO REPAIR DIESEL OR ELECTRIC PUMP - DEPENDENCY (85 HRS)
FP-2PUMPS-FTF
HEP-FW-REP-DEPEN

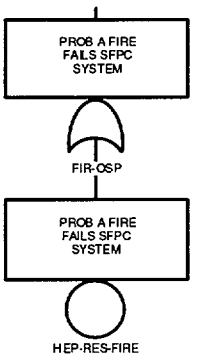

FAILURE TO PROVIDE MAKEUP USING FW SYSTEM
LOC-OFD-L
FAILS TO DIAGNOSE NEED TO START FW
FAILURE TO MAKEUP INVENTORY BY USE OF FIRE PROTECTION PUMP
OPERATOR FAILS TO ESTABLISH ALTERNATE COOLING - EARLY
HEP-RECG-FWSTART-L
LOC-OFD-LA
HEP-FW-START
DIESEL AND ELECTRIC PUMPS FAIL TO START AND RUN
FAILS TO REPAIR DIESEL OR ELECTRIC PUMP - DEPENDENCY (85 HRS)
FP-2PUMPS-FTF
HEP-FW-REP-DEPEN

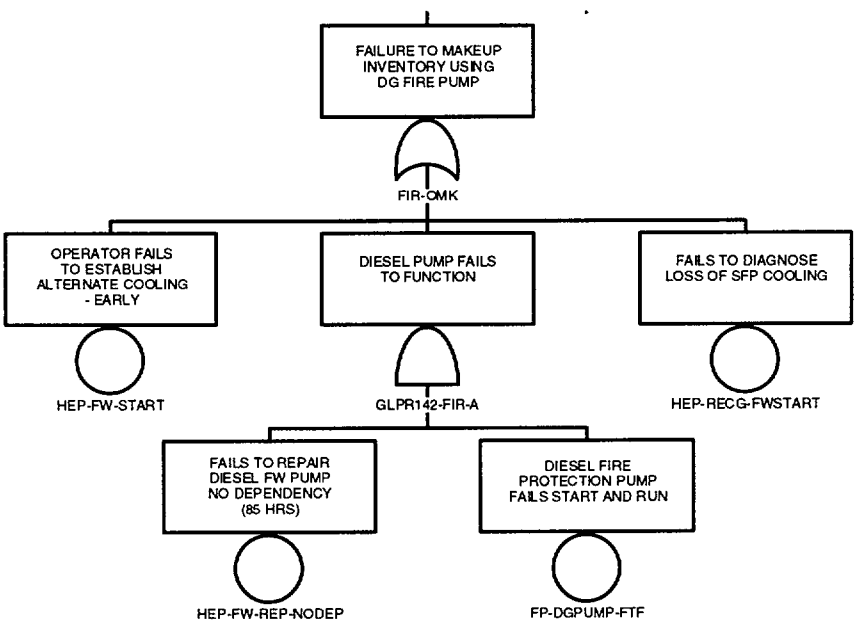

FAILURE TO RECOVER OFFSITE SOURCES (85 HRS)
LOC-OFB
FAILS TO DIAGNOSE NEED TO START FW
FAILURE TO DIAGNOSE/RECOVER VIA OFFSITE SOURCES (85 HRS) (DEPENDENT EVENT)
HEP-RECG-FWSTART
HEP-INV-OFFSITE

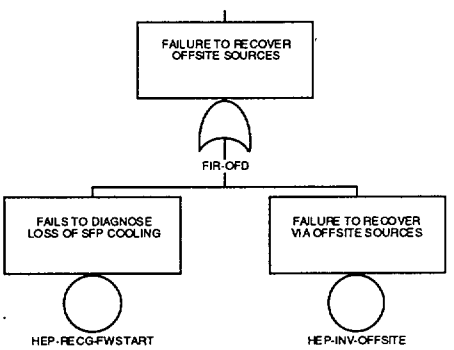

FAILURE TO RECOVER OFFSITE SOURCES
LOC-OFB-L
FAILS TO DIAGNOSE NEED TO START FW
FAILURE TO DIAGNOSE/RECOVER VIA OFFSITE SOURCES (85 HRS) (DEPENDENT EVENT)
HEP-RECG-FWSTART-L
HEP-INV-OFFSITE

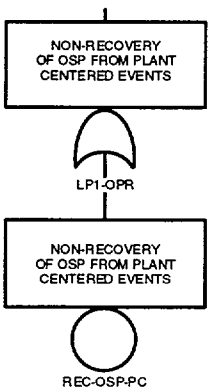

OPERATOR FAILS TO RESPOND TO FIRE ALARMS
FIR-CRA
OPERATOR FAILS TO DIAGNOSE GIVEN ALARM
HEP-DIAG-ALARM
INSTRUMENTATION HARDWARE FAILURE
FIR-CRA-A
ELECTRICAL FAULTS CAUSING LOSS OF ALARMS
SFP-FIRE-LOA
FAILURE OF FIRE DETECTORS
SFP-FIRE-DETECT

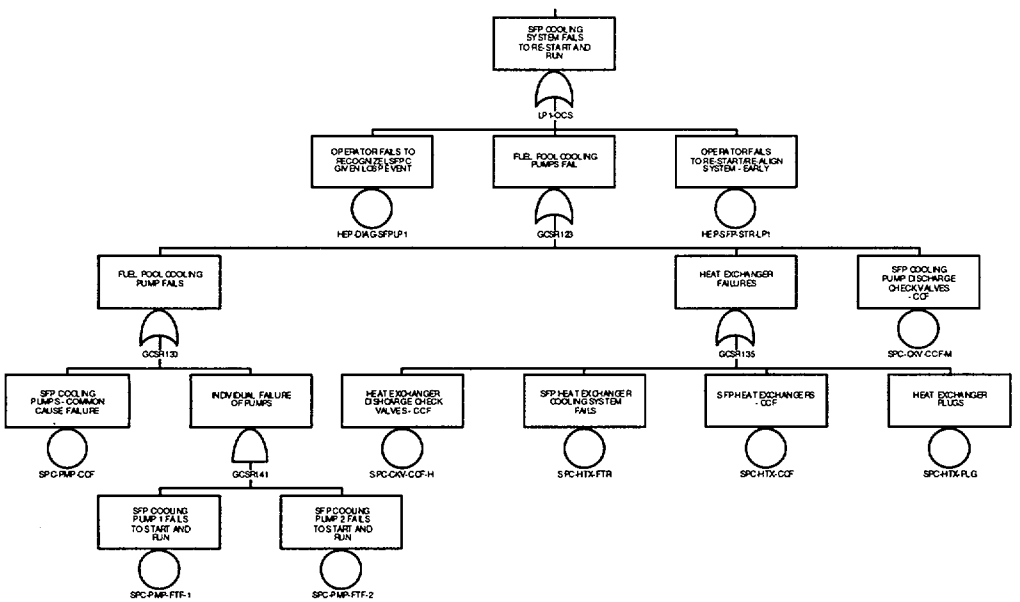

OPERATOR FAILS TO OBSERVE LOC EVENT DURING WALKDOWN
FIR-IND
OPERATOR FAILS TO OBSERVE LSFPC DURING WALKDOWN (NO DEPENDENCY)
HEP-WLKDWN-LSFPC

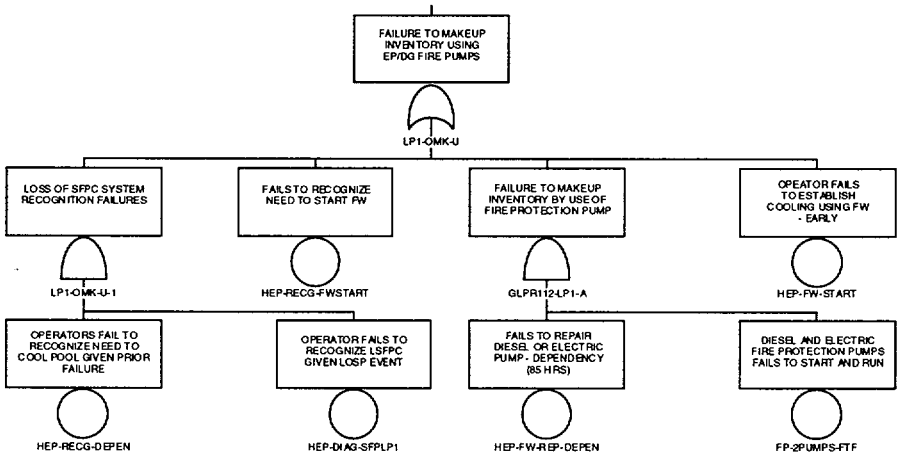

PROB A FIRE
FAILS SFPC
SYSTEM
FIR-OSP
PROB A FIRE
FAILS SFPC
SYSTEM
HEP-RES-FIRE

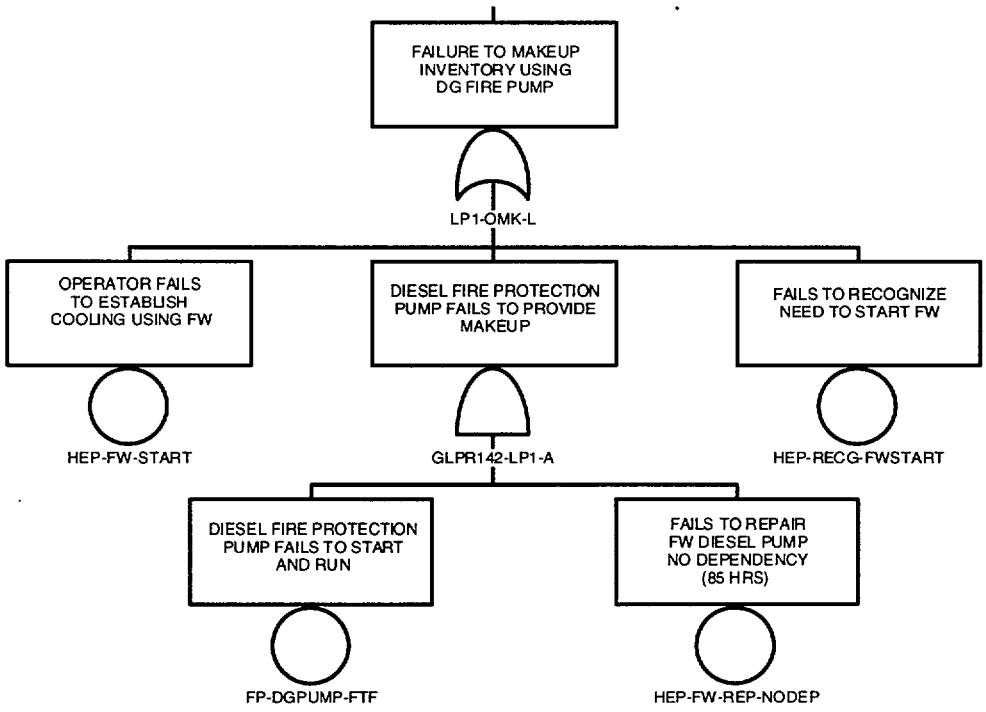

FAILURE TO MAKEUP
INVENTORY USING
DG FIRE PUMP
FIR-OMK
OPERATOR FAILS
TO ESTABLISH
ALTERNATE COOLING
- EARLY
DIESEL PUMP FAILS
TO FUNCTION
FAILS TO DIAGNOSE
LOSS OF SFP COOLING
HEP-FW-START
GLPR142-FIR-A
HEP-RECG-FWSTART
FAILS TO REPAIR
DIESEL FW PUMP
NO DEPENDENCY
(85 HRS)
DIESEL FIRE
PROTECTION PUMP
FAILS START AND RUN
HEP-FW-REP-NODEP
FP-DGPUMP-FTF

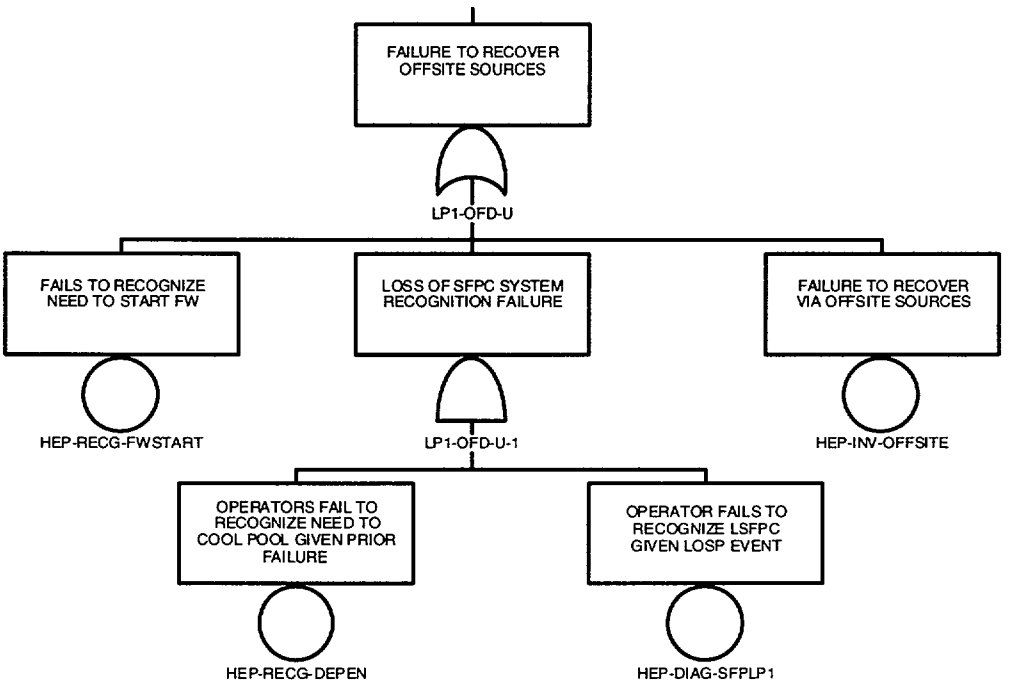

FAILURE TO RECOVER OFFSITE SOURCES
FIR-OFD
FAILS TO DIAGNOSE LOSS OF SFP COOLING
FAILURE TO RECOVER VIA OFFSITE SOURCES
HEP-RECG-FWSTART
HEP-INV-OFFSITE

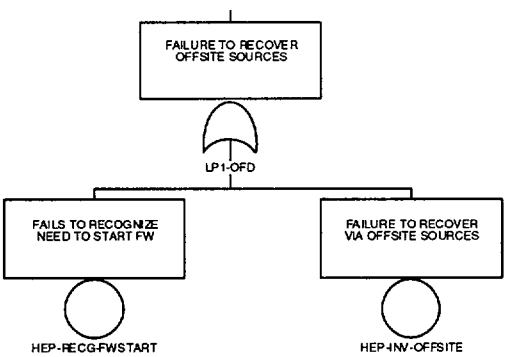

NON-RECOVERY OF OSP FROM PLANT CENTERED EVENTS
LP1-OPR
NON-RECOVERY OF OSP FROM PLANT CENTERED EVENTS
REC-OSP-PC

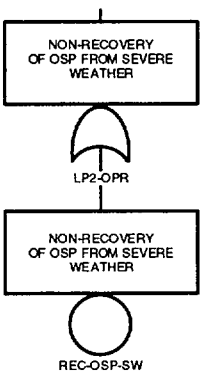

SFP COOLING SYSTEM FAILS TO RE-START AND RUN
LP1-OCS
OPERATOR FAILS TO RECOGNIZE LOSFPC GIVEN LOSP EVENT
FUEL POOL COOLING PUMPS FAIL
OPERATOR FAILS TO RE-START/RE-ALIGN SYSTEM - EARLY
HEP-DIAG-SFPLP1
GCSR128
HEP-SFP-STR-LP1
FUEL POOL COOLING PUMP FAILS
HEAT EXCHANGER FAILURES
SFP COOLING PUMP DISCHARGE CHECK VALVES - CCF
GCSR130
GCSR135
SPC-CKV-CCF-M
SFP COOLING PUMPS - COMMON CAUSE FAILURE
INDIVIDUAL FAILURE OF PUMPS
HEAT EXCHANGER DISCHARGE CHECK VALVES - CCF
SFP HEAT EXCHANGER COOLING SYSTEM FAILS
SFP HEAT EXCHANGERS - CCF
HEAT EXCHANGER PLUGS
SPC-PMP-CCF
GCSR141
SPC-CKV-CCF-H
SPC-HTX-FTR
SPC-HTX-CCF
SPC-HTX-PLG
SFP COOLING PUMP 1 FAILS TO START AND RUN
SFP COOLING PUMP 2 FAILS TO START AND RUN
SPC-PMP-FTF-1
SPC-PMP-FTF-2

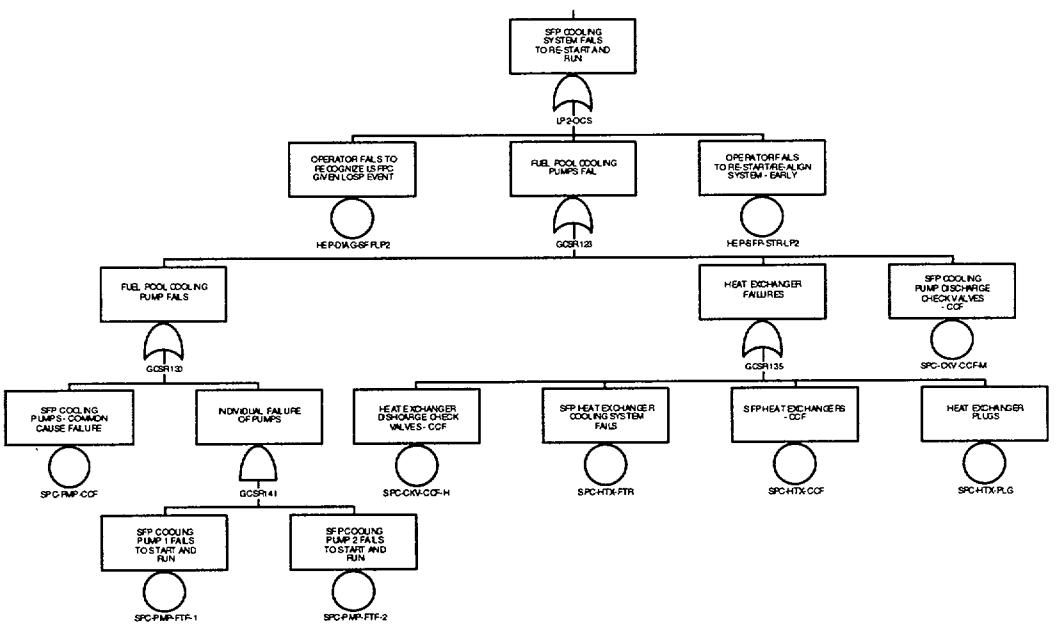

FAILURE TO MAKEUP INVENTORY USING EP/DG FIRE PUMPS
LP1-OMK-U
LOSS OF SFPC SYSTEM RECOGNITION FAILURES
FAILS TO RECOGNIZE NEED TO START FW
FAILURE TO MAKEUP INVENTORY BY USE OF FIRE PROTECTION PUMP
OPEATOR FAILS TO ESTABLISH COOLING USING FW - EARLY
LP1-OMK-U-1
HEP-RECG-FWSTART
GLPR112-LP1-A
HEP-FW-START
OPERATORS FAIL TO RECOGNIZE NEED TO COOL POOL GIVEN PRIOR FAILURE
OPERATOR FAILS TO RECOGNIZE LSFPC GIVEN LOSP EVENT
FAILS TO REPAIR DIESEL OR ELECTRIC PUMP - DEPENDENCY (85 HRS)
DIESEL AND ELECTRIC FIRE PROTECTION PUMPS FAILS TO START AND RUN
HEP-RECG-DEPEN
HEP-DIAG-SFPLP1
HEP-FW-REP-DEPEN
FP-2PUMPS-FTF

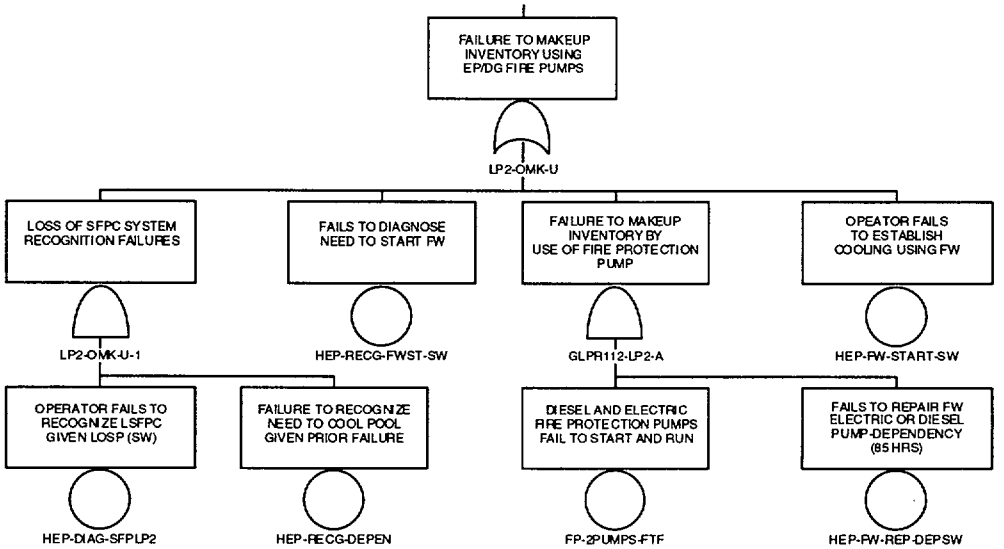

FAILURE TO MAKEUP INVENTORY USING DG FIRE PUMP
LP1-OMK-L
OPERATOR FAILS TO ESTABLISH COOLING USING FW
DIESEL FIRE PROTECTION PUMP FAILS TO PROVIDE MAKEUP
FAILS TO RECOGNIZE NEED TO START FW
HEP-FW-START
GLPR142-LP1-A
HEP-RECG-FWSTART
DIESEL FIRE PROTECTION PUMP FAILS TO START AND RUN
FAILS TO REPAIR FW DIESEL PUMP NO DEPENDENCY (85 HRS)
FP-DGPUMP-FTF
HEP-FW-REP-NODEP

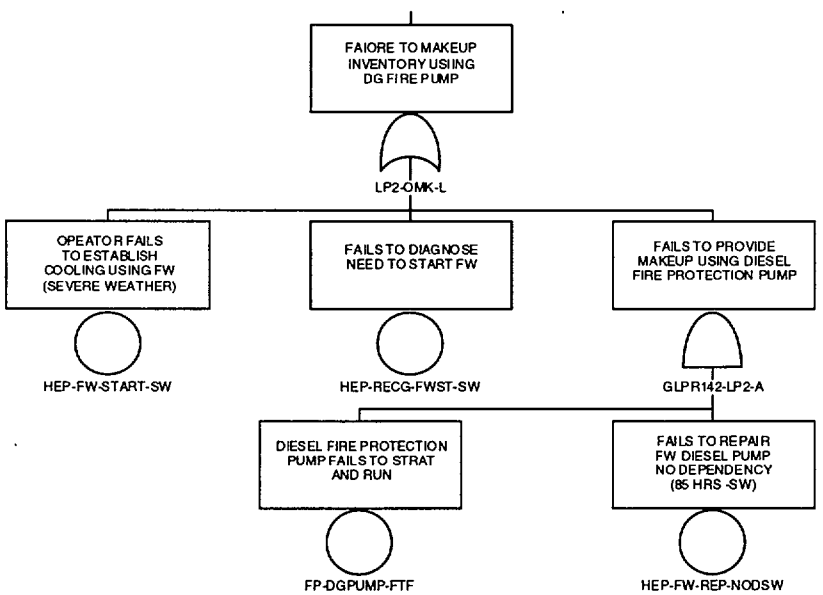

FAILURE TO RECOVER OFFSITE SOURCES
LP1-OFD-U
FAILS TO RECOGNIZE NEED TO START FW
LOSS OF SFPC SYSTEM RECOGNITION FAILURE
FAILURE TO RECOVER VIA OFFSITE SOURCES
HEP-RECG-FWSTART
LP1-OFD-U-1
HEP-INV-OFFSITE
OPERATORS FAIL TO RECOGNIZE NEED TO COOL POOL GIVEN PRIOR FAILURE
OPERATOR FAILS TO RECOGNIZE LSFPC GIVEN LOSP EVENT
HEP-RECG-DEPEN
HEP-DIAG-SFPLP1

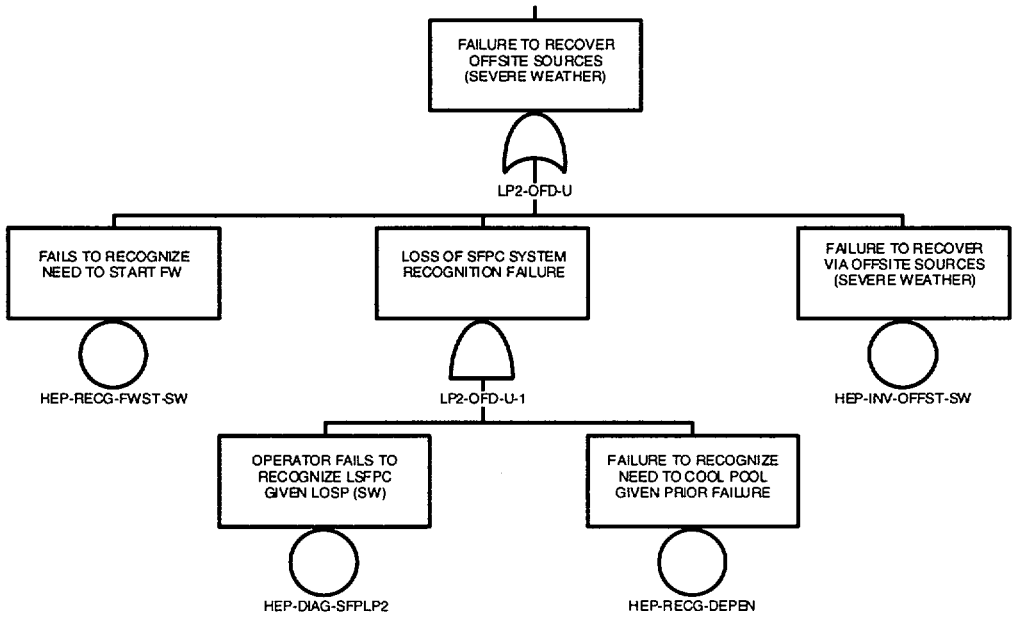

FAILURE TO RECOVER OFFSITE SOURCES
LP1-OFD
FAILS TO RECOGNIZE NEED TO START FW
FAILURE TO RECOVER VIA OFFSITE SOURCES
HEP-RECG-FWSTART
HEP-INV-OFFSITE

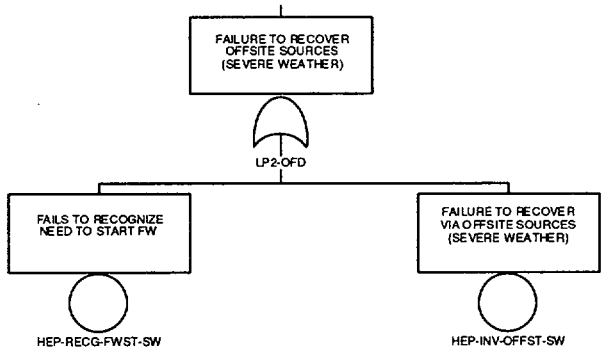

NON-RECOVERY OF OSP FROM SEVERE WEATHER
LP2-OPR
NON-RECOVERY OF OSP FROM SEVERE WEATHER
REC-OSP-SW

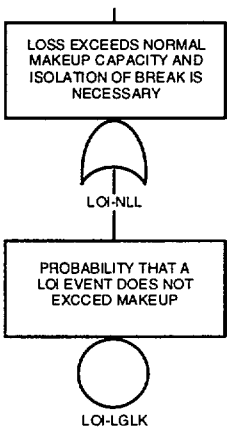

SFP COOLING SYSTEM FAILS TO RE-START AND RUN
LP2-OCS
OPERATOR FAILS TO RECOGNIZE LS PPC GIVEN LOSP EVENT
FUEL POOL COOLING PUMPS FAIL
OPERATOR FAILS TO RE-START/RE-ALIGN SYSTEM - EARLY
HEP-DIAG-SFP-LP2
GCSR128
HEP-SFR-STR-LP2
FUEL POOL COOLING PUMP FAILS
HEAT EXCHANGER FAILURES
SFP COOLING PUMP DISCHARGE CHECK VALVES - CCF
GCSR130
GCSR135
SPC-CKV-CCF-M
SFP COOLING PUMPS - COMMON CAUSE FAILURE
INDIVIDUAL FAILURE OF PUMPS
HEAT EXCHANGER DISCHARGE CHECK VALVES - CCF
SFP HEAT EXCHANGER COOLING SYSTEM FAILS
SFP HEAT EXCHANGERS - CCF
HEAT EXCHANGER PLUGS
SPC-PMP-CCF
GCSR141
SPC-CKV-CCF-H
SPC-HTX-FTR
SPC-HTX-CCF
SPC-HTX-PLG
SFP COOLING PUMP 1 FAILS TO START AND RUN
SFP COOLING PUMP 2 FAILS TO START AND RUN
SPC-PMP-FTF-1
SPC-PMP-FTF-2

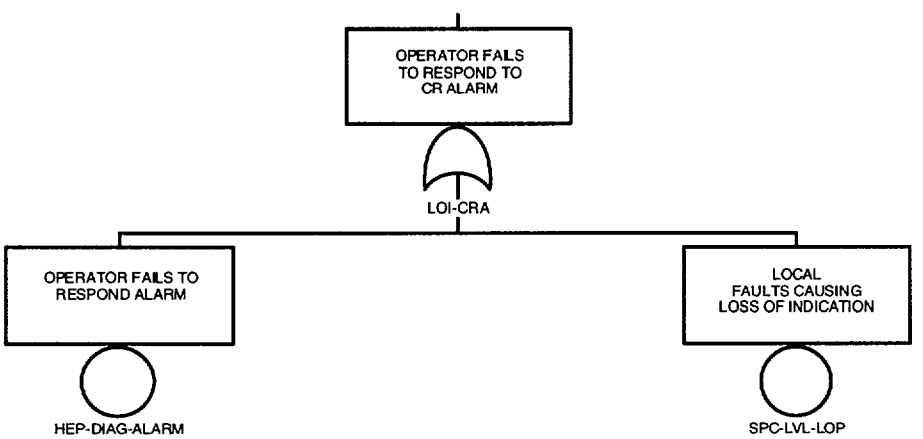

FAILURE TO MAKEUP INVENTORY USING EP/DG FIRE PUMPS
LP2-OMK-U
LOSS OF SFPC SYSTEM RECOGNITION FAILURES
FAILS TO DIAGNOSE NEED TO START FW
FAILURE TO MAKEUP INVENTORY BY USE OF FIRE PROTECTION PUMP
OPEATOR FAILS TO ESTABLISH COOLING USING FW
LP2-OMK-U-1
HEP-RECG-FWST-SW
GLPR112-LP2-A
HEP-FW-START-SW
OPERATOR FAILS TO RECOGNIZE LSFPC GIVEN LOSP (SW)
FAILURE TO RECOGNIZE NEED TO COOL POOL GIVEN PRIOR FAILURE
DIESEL AND ELECTRIC FIRE PROTECTION PUMPS FAIL TO START AND RUN
FAILS TO REPAIR FW ELECTRIC OR DIESEL PUMP-DEPENDENCY (85 HRS)
HEP-DIAG-SFPLP2
HEP-RECG-DEPEN
FP-2PUMPS-FTF
HEP-FW-REP-DEPSW

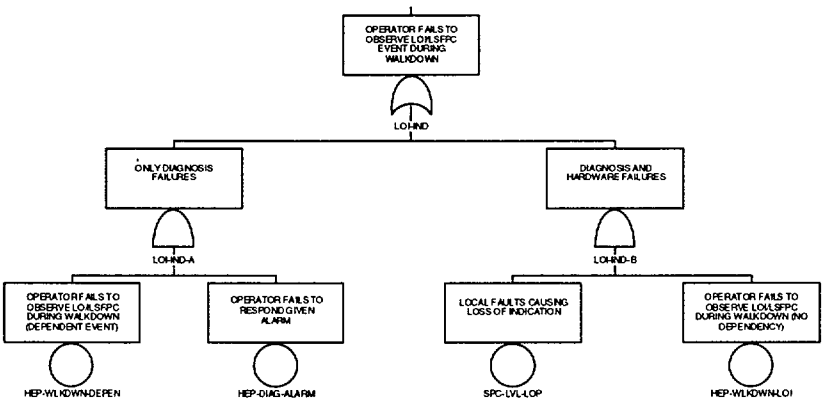

FAIORE TO MAKEUP INVENTORY USIING DG FIRE PUMP
LP2-OMK-L
OPEATOR FAILS TO ESTABLISH COOLING USING FW (SEVERE WEATHER)
FAILS TO DIAGNOSE NEED TO START FW
FAILS TO PROVIDE MAKEUP USING DIESEL FIRE PROTECTION PUMP
HEP-FW-START-SW
HEP-RECG-FWST-SW
GLPR142-LP2-A
DIESEL FIRE PROTECTION PUMP FAILS TO STRAT AND RUN
FAILS TO REPAIR FW DIESEL PUMP NO DEPENDENCY (85 HRS -SW)
FP-DGPUMP-FTF
HEP-FW-REP-NODSW

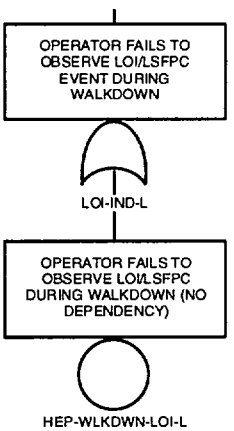

FAILURE TO RECOVER OFFSITE SOURCES (SEVERE WEATHER)
LP2-OFD-U
FAILS TO RECOGNIZE NEED TO START FW
LOSS OF SFPC SYSTEM RECOGNITION FAILURE
FAILURE TO RECOVER VIA OFFSITE SOURCES (SEVERE WEATHER)
HEP-RECG-FWST-SW
LP2-OFD-U-1
HEP-INV-OFFST-SW
OPERATOR FAILS TO RECOGNIZE LSFPC GIVEN LOSP (SW)
FAILURE TO RECOGNIZE NEED TO COOL POOL GIVEN PRIOR FAILURE
HEP-DIAG-SFPLP2
HEP-RECG-DEPEN

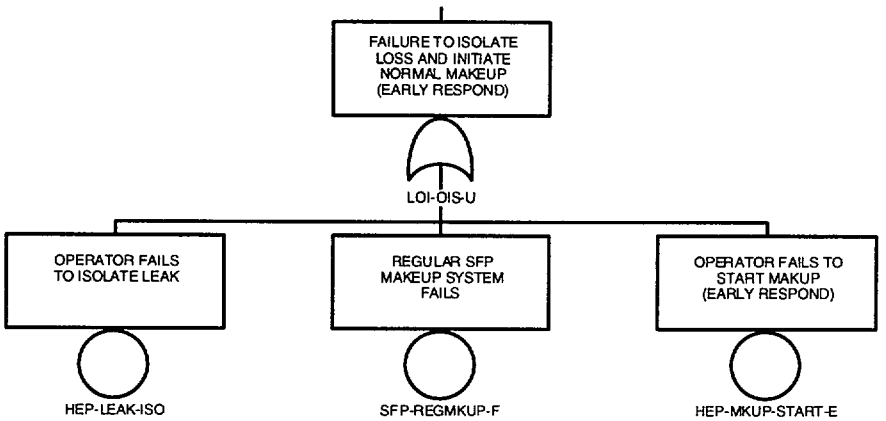

FAILURE TO RECOVER OFFSITE SOURCES (SEVERE WEATHER)
LP2-OFD
FAILS TO RECOGNIZE NEED TO START FW
FAILURE TO RECOVER VIA OFFSITE SOURCES (SEVERE WEATHER)
HEP-RECG-FWST-SW
HEP-INV-OFFST-SW

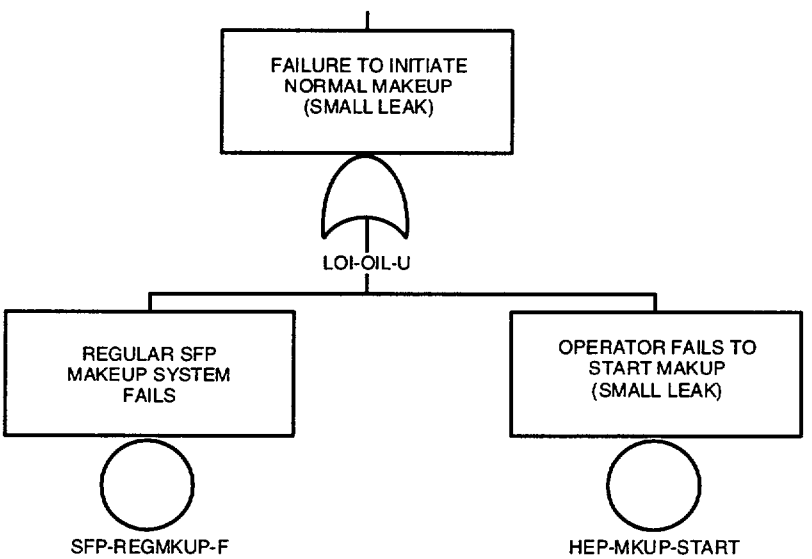

LOSS EXCEEDS NORMAL MAKEUP CAPACITY AND ISOLATION OF BREAK IS NECESSARY
LOI-NLL
PROBABILITY THAT A LOI EVENT DOES NOT EXCCED MAKEUP
LOI-LGLK

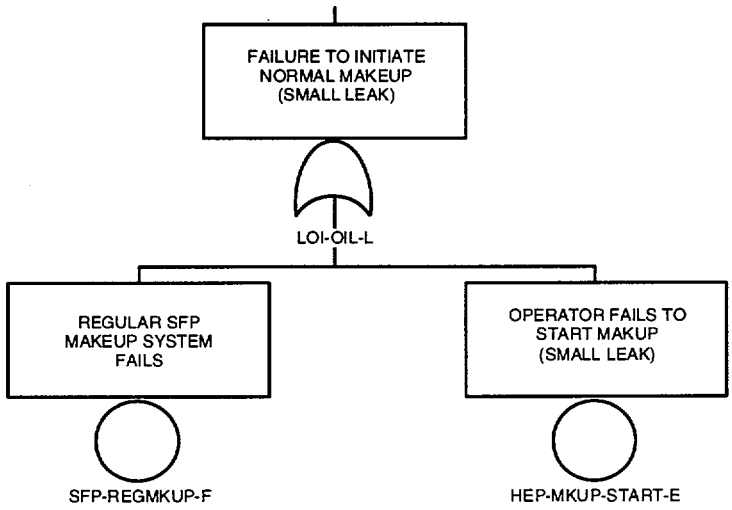

OPERATOR FAILS TO RESPOND TO CR ALARM
LOI-CRA
OPERATOR FAILS TO RESPOND ALARM
HEP-DIAG-ALARM
LOCAL FAULTS CAUSING LOSS OF INDICATION
SPC-LVL-LOP

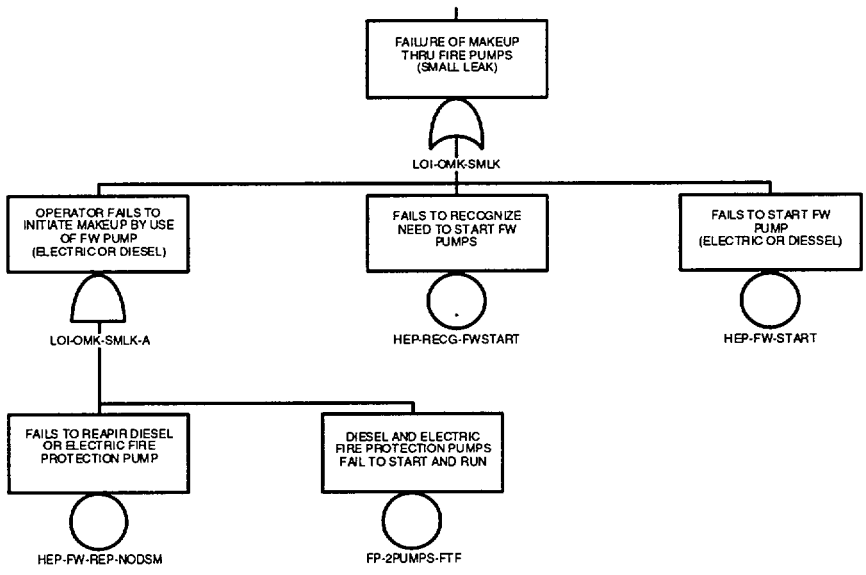

OPERATOR FAILS TO OBSERVE LOI/LSFPC EVENT DURING WALKDOWN
LOI-IND
ONLY DIAGNOSIS FAILURES
DIAGNOSIS AND HARDWARE FAILURES
LOI-IND-A
LOI-IND-B
OPERATOR FAILS TO OBSERVE LOI/LSFPC DURING WALKDOWN (DEPENDENT EVENT)
OPERATOR FAILS TO RESPOND GIVEN ALARM
LOCAL FAULTS CAUSING LOSS OF INDICATION
OPERATOR FAILS TO OBSERVE LOI/LSFPC DURING WALKDOWN (NO DEPENDENCY)
HEP-WLKDWN-DEPEN
HEP-DIAG-ALARM
SPC-LVL-LOP
HEP-WLKDWN-LOI

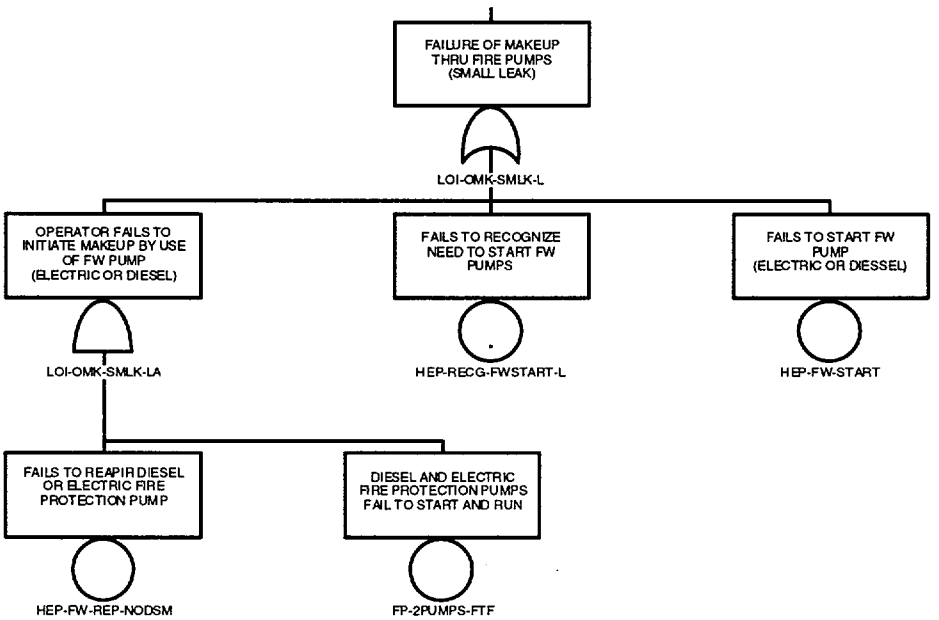

OPERATOR FAILS TO OBSERVE LOI/LSFPC EVENT DURING WALKDOWN
LOI-IND-L
OPERATOR FAILS TO OBSERVE LOI/LSFPC DURING WALKDOWN (NO DEPENDENCY)
HEP-WLKDWN-LOI-L

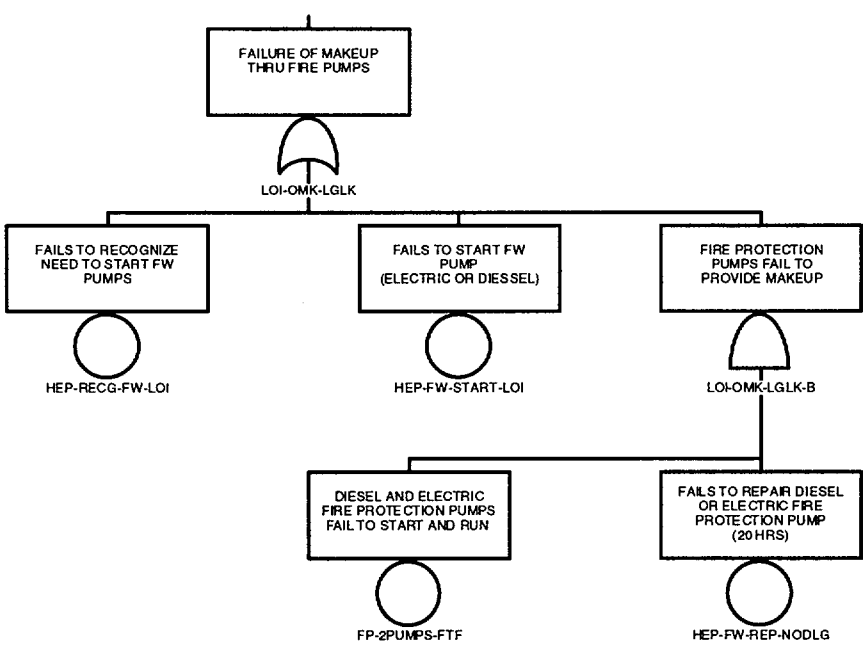

FAILURE TO ISOLATE LOSS AND INITIATE NORMAL MAKEUP (EARLY RESPOND)
LOI-OIS-U
OPERATOR FAILS TO ISOLATE LEAK
REGULAR SFP MAKEUP SYSTEM FAILS
OPERATOR FAILS TO START MAKUP (EARLY RESPOND)
HEP-LEAK-ISO
SFP-REGMKUP-F
HEP-MKUP-START-E

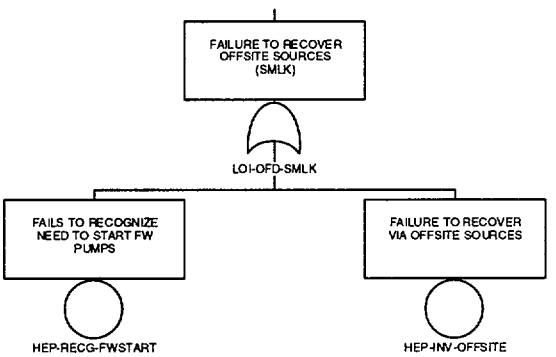

FAILURE TO INITIATE NORMAL MAKEUP (SMALL LEAK)
LOI-OIL-U
REGULAR SFP MAKEUP SYSTEM FAILS
OPERATOR FAILS TO START MAKUP (SMALL LEAK)
SFP-REGMKUP-F
HEP-MKUP-START

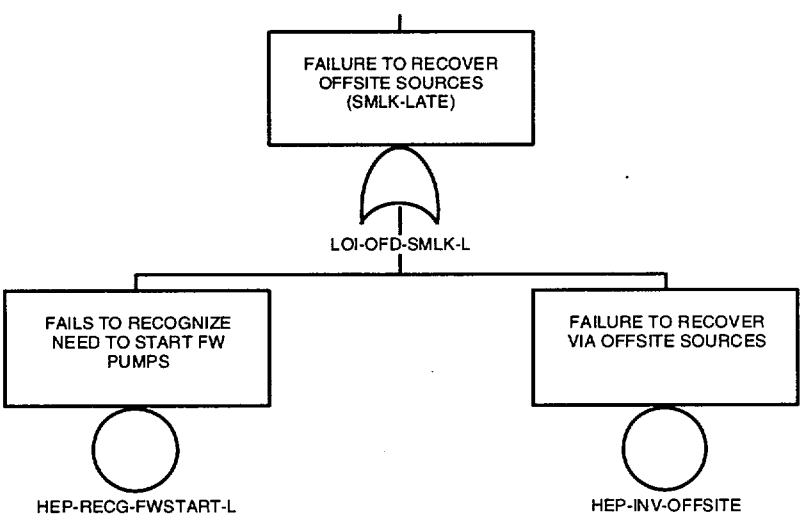

FAILURE TO INITIATE NORMAL MAKEUP (SMALL LEAK)
LOI-OIL-L
REGULAR SFP MAKEUP SYSTEM FAILS
OPERATOR FAILS TO START MAKUP (SMALL LEAK)
SFP-REGMKUP-F
HEP-MKUP-START-E

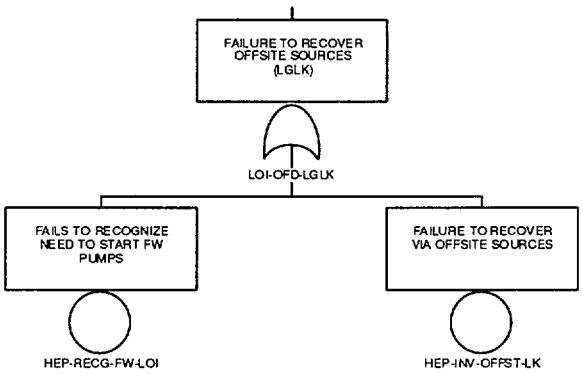

FAILURE OF MAKEUP THRU FIRE PUMPS (SMALL LEAK)
LOI-OMK-SMLK
OPERATOR FAILS TO INITIATE MAKEUP BY USE OF FW PUMP (ELECTRIC OR DIESEL)
FAILS TO RECOGNIZE NEED TO START FW PUMPS
FAILS TO START FW PUMP (ELECTRIC OR DIESSEL)
LOI-OMK-SMLK-A
HEP-RECG-FWSTART
HEP-FW-START
FAILS TO REAPIR DIESEL OR ELECTRIC FIRE PROTECTION PUMP
DIESEL AND ELECTRIC FIRE PROTECTION PUMPS FAIL TO START AND RUN
HEP-FW-REP-NODSM
FP-2PUMPS-FTF


FAILURE OF MAKEUP THRU FIRE PUMPS (SMALL LEAK)
LOI-OMK-SMLK-L
OPERATOR FAILS TO INITIATE MAKEUP BY USE OF FW PUMP (ELECTRIC OR DIESEL)
FAILS TO RECOGNIZE NEED TO START FW PUMPS
FAILS TO START FW PUMP (ELECTRIC OR DIESSEL)
LOI-OMK-SMLK-LA
HEP-RECG-FWSTART-L
HEP-FW-START
FAILS TO REAPIR DIESEL OR ELECTRIC FIRE PROTECTION PUMP
DIESEL AND ELECTRIC FIRE PROTECTION PUMPS FAIL TO START AND RUN
HEP-FW-REP-NODSM
FP-2PUMPS-FTF


FAILURE OF MAKEUP THRU FIRE PUMPS
LOI-OMK-LGLK
FAILS TO RECOGNIZE NEED TO START FW PUMPS
FAILS TO START FW PUMP (ELECTRIC OR DIESSEL)
FIRE PROTECTION PUMPS FAIL TO PROVIDE MAKEUP
HEP-RECG-FW-LOI
HEP-FW-START-LOI
LOI-OMK-LGLK-B
DIESEL AND ELECTRIC FIRE PROTECTION PUMPS FAIL TO START AND RUN
FAILS TO REPAIR DIESEL OR ELECTRIC FIRE PROTECTION PUMP (20 HRS)
FP-2PUMPS-FTF
HEP-FW-REP-NODLG


FAILURE TO RECOVER OFFSITE SOURCES (SMLK)
LOI-OFD-SMLK
FAILS TO RECOGNIZE NEED TO START FW PUMPS
FAILURE TO RECOVER VIA OFFSITE SOURCES
HEP-RECG-FWSTART
HEP-INV-OFFSITE


FAILURE TO RECOVER OFFSITE SOURCES (SMLK-LATE)
LOI-OFD-SMLK-L
FAILS TO RECOGNIZE NEED TO START FW PUMPS
FAILURE TO RECOVER VIA OFFSITE SOURCES
HEP-RECG-FWSTART-L
HEP-INV-OFFSITE


FAILURE TO RECOVER OFFSITE SOURCES (LGLK)
LOI-OFD-LGLK
FAILS TO RECOGNIZE NEED TO START FW PUMPS
FAILURE TO RECOVER VIA OFFSITE SOURCES
HEP-RECG-FW-LOI
HEP-INV-OFFST-LK

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	

B. Calculate the Diagnosis Failure Probability

(1) If all PSF ratings are nominal, then the Diagnosis Failure Probability = 10E-2

(2) Otherwise,

	Time	Stress	Complexity	Experience/ Training	Procedures	Ergonomics	Fitness for Duty	Work Processes	
Diagnosis:	10E-2x__	x__	x__	x__	x__	x__	x__	x__	=__

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

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:	_____	Diagnosis Failure Probability:	10E-2
Action Failure Probability:	+_____	Action Failure Probability:	+10E-3
Task Failure Without Formal Dependence ($P_{w/od}$)	=_____	$P_{(w/od)}$	= 1.1x10E-2

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	If this error is the **3rd error in the sequence**, then the dependency is at least **moderate.** If this error is the **4th error in the sequence**, then the dependency is at least **high.** This rule may be ignored only if there is compelling evidence for less dependence with the previous tasks. Explain above.
		Different	-	high	
	Not Close	Same	No Additional	high	
			Additional	moderate	
		Different	No Additional	moderate	
			Additional	low	
Different	Close	-	-	moderate	
	Not Close	-	-	low	

Using $P_{w/od}$ = 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 $(1+ P_{w/od})/2$

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

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

For Zero Dependence the probability of failure is $P_{w/od}$

Calculate $P_{w/d}$ using the appropriate values:

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