11/16/99

1. MODEL DEVELOPMENT

This section describes the event trees, fault trees, and basic events used to perform the analysis. Section 1.1 describes the assumptions that apply to all event trees in the analysis. The remaining sections describe each event tree in the model.

1.1. General Assumptions

This analysis is based on the assumptions listed for Case 1 of the NRC draft report. Additional assumptions specific to each scenario are listed in the appropriate section.

Other significant assumptions, such as the definition of the event tree end states (i.e., pool level less than 3 ft above the top of the fuel), and the time to bulk boiling, have also been adopted from the NRC draft report.

1.2. Loss of Cooling Event Tree

This event tree 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). Figure 1 shows the Loss of Cooling event tree sequence progression.

1.2.1. Initiating Event LOC – Loss of Cooling

1.2.1.1. Event Description and Timing

This initiating event includes conditions arising from loss of coolant system flow due to the failure of 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).

1.2.1.2. Relevant Assumptions

None.

1.2.1.3. Quantification

This initiator is represented by basic event IE-LO-POOL-COOL. The NRC draft report uses an initiation frequency of 3.0E-3/yr taken from NUREG-1275, "Operating Experience Feedback Report – Assessment of Spent Fuel Cooling" (Ref 1). This represents loss of cooling events in which temperatures rose more than 20°F, and which resulted from failures of pumps, valves, piping, or from loss of heat sink (heat exchangers), or from local losses of power (e.g., electrical connections).

1.2.2. Top Event CRA – Control Room Alarms

1.2.2.1. Event Description and Timing

This event represents the probability that control room instrumentation will fail to alarm given that SFP cooling has been lost, or that the operator fails to respond to that alarm. The proper conditions for an alarm are assumed to exist within the first 8 to 12 hours of the loss of cooling (i.e., one shift). Failure could be due to operator error (failure to respond), failure of the signal channel, or loss of indication due to electrical 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 GCRA112.

1.2.2.2. Relevant Assumptions

- The SFP has at least one 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)

B|21|7

- Within 8 to 12 hours of the loss of cooling, one or more of these 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)

1.2.2.3. Quantification

Human Error Probabilities

One operator failure is modeled under this top event (basic event HEP-RES-ALARM). The operator may fail to respond to a signal or indication in the control room. Such a signal 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 probability of operator failure was determined using THERP, assuming only two independent shift walkdowns (3.0E-3).

Non-HEP Probabilities

The value used for failure of the alarm channel (1.0E-5) was taken from NUREG-1740 (Ref 2). The value used for local electrical faults leading to alarm channel failure (2.0E-3) was estimated based on information in NUREG-1275, Volume 12 (Ref 1).

1.2.2.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-RES-ALARM	3.0E-3	3.0E-3

1.2.3. Top Event IND – Other Indications of Loss of Cooling

1.2.3.1. Event Description and Timing

This top event models the probability that the operators fail to recognize the loss of cooling during walkdowns over multiple shifts. Indications available to the operator during a walkdown include high area temperature and humidity, low water level from boil-off, and local alarms. After pool heatup begins, the operator has more than 10 shifts (about 128 hours) to discover the loss of SFP cooling. Success for this event is defined as the operator recognizing the abnormal condition and understanding the need to investigate its cause. This event is modeled by fault tree GFFT130.

1.2.3.2. Relevant Assumptions

- Operators perform walkdowns once per shift (every 8 to 12 hours)
- The loss of cooling may not be noticeable during the first two shifts (this is conservative because conditions are assumed to be sufficient to trigger local and control room alarms)
- After bulk boiling begins, level changes in the SFP will be indicated on a large, graduated level indicator in the pool
- About 128 hours are available to recover from the initiating event before water level reaches 3 ft above the fuel

1.2.3.3. Quantification

Human Error Probabilities

This top event is modeled by a single HEP (basic event REC-WLKDWN-LOC). At this point in the event tree, the control room alarms have failed, or the operator has failed to recognize their importance. The operator then fails to observe the loss of cooling during subsequent walkdowns. Note that during the first two or three shifts, water level may not drop significantly. After two shifts, however, the environment in the pool area would be hot and humid. After pool heatup begins, operator has more than 10 shifts (about

128 hours) to discover the loss of SFP cooling. The probability of failure was determined using THERP (1.0E-5).

1.2.3.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
REC-WLKDWN-LOC	1.0E-5	1.0E-2

1.2.4. Top Event OCS – Operator Recovery of Cooling System

1.2.4.1. Event Description and Timing

Once the loss of cooling has been recognized, either by control room alarms or by walkdowns, the operators will likely focus their attention on repair of the SFP cooling system. It is only after bulk boiling begins and the water level drops below the cooling system suction that the operator will consider injection of 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 (see top event OFD, Section 1.2.5.1). However, we have assumed that the operator has only until bulk boiling begins (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.

If the loss of cooling was detected via the control room alarms, the operator has the full 33 hours in which to repair the system. This case is modeled by fault tree GLCR121. If discovered during walkdowns, we've assumed he has only 9 hours available (33 hours less 24 hours before loss of cooling was noticed). This case is modeled by fault tree GLCR161.

1.2.4.2. Relevant Assumptions

- The operator will avoid using raw water (e.g., water not chemically controlled) if possible
- The operator 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
- The boil-off rate is assumed to be higher than the SFP makeup system capacity
- Time to bulk boiling is 33 hours from the time cooling is lost
- The boil-off rate is 0.2 ft/hr
- If the loss of cooling was detected through shift walkdowns, then we assume 24 hours has passed before discovery
- It takes two shifts (16 hours) to contact maintenance personnel, make a diagnosis, and get new parts
- Mean time to repair for the SFP cooling system was assumed to be 10 hours

1.2.4.3. Quantification

Human Error Probabilities

This top event includes the operator actions required to recognize the failure of the SFP cooling system and to act to restart it, both diagnosis and action. Failure to diagnose or recognize the need for action is represented by event HEP-SFPC-DIAGNOS, which has a value of 1.0E-5 (from the ASP method).

The probability of failure to repair/restart the SFP cooling system depends on the time available. In the case when the operator action is initiated by control room alarms (HEP-COOL-LOC-E), the time available is 33 hours. Assuming that it takes another two shifts (16 hours) before parts and technical help arrive, then the operator has 17 hours (33 hours less 16 hours) to repair the pump. Therefore, the probability of failure, given a 10-hour mean time to repair, is as follows:

$$e^{-\lambda t} = e^{-(1/10)\times 17} = 1.8E\text{-}1$$

where

λ mean time to repair

t available time

In the case when discovery was due to operator walkdown (HEP-COOL-LOC-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.

1.2.4.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-SFPC-DIAGNOS	1.0E-5	N/A
HEP-COOL-LOC-E	1.8E-1	1.0E-4
HEP-COOL-LOC-L	1.0	2.2E-4

1.2.5. Top Event OFD – Operator Recovery Using Onsite Sources

1.2.5.1. Event Description and Timing

At this point in the event tree, the operator has discovered the loss of cooling, but has been unable to restore the SFP cooling system to operation. 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 operator now has 85 hours to provide some form of external makeup to the pool to prevent fuel uncovery (128 hours less 43 hours). This event represents failure of the operator to start a firewater pump and provide makeup to the SFP. He has both electric- and diesel-driven firewater pumps available to perform this function. Furthermore, given failure of both pumps, the operator has time to attempt repair of one of the pumps.

Note that there is a difference in timing depending on whether the loss of cooling was discovered early (via instrumentation) or late (via walkdowns). The NRC draft report used two fault trees to represent these two cases: GLCR123 (early detection) and GLCR163 (late detection). However, so much time is available to provide some form of external makeup to the pool to prevent fuel uncovery that the distinction between early and late identification of the loss of cooling has been ignored. We assume that the discovery of loss of cooling occurred prior to the level dropping below the SFP cooling system intake. Also, the quantification of event IND only considered two shift walkdowns, which would occur much earlier than 43 hours. Therefore, this event has been modeled by the single fault tree GLCR163.

We assume 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 is as follows:

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

Refilling time is estimated to be more than 2 ft/hr for a 250-gpm capacity pump (1 ft/hr for a 100-gpm capacity pump). There is a possibility that the operator may wait until the SFP cooling system is available before he starts a firewater pump.

1.2.5.2. Relevant Assumptions

- The operator has 128 hours from the onset of the initiator to provide makeup and inventory cooling
- The operator will avoid using raw water (e.g., water not chemically controlled) if possible

- The operator 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
- The boil-off rate is assumed to be higher than the SFP makeup system capacity
- The suction of the cooling system is 2 ft below the nominal pool level
- The operator must travel to the firewater pumps to start them locally
- Firewater pumps are maintained on a regular schedule
- It takes two shifts (16 hours) to contact maintenance personnel, make a diagnosis, and get new parts
- There is a means of fixing a fire hose in place, so that the operator is not required to stand in a hot, humid, and possibly radiologically hazardous area for the period of time required to refill the SFP

1.2.5.3. Quantification

Human Error Probabilities

The operator was unable to fix the SFPC system within the first 43 hours. He must diagnose the need for alternate makeup, and then successfully start a firewater pump and provide alignment to the SFP. The fault tree used to quantify this top event (GLCR163) comprises both the following operator actions:

> Failure to recognize the need to start a firewater pump within 85 hours after the onset of bulk boiling, given the operator has failed to diagnose the need to restart the SFP cooling system (HEP-FW-DIAGNOSE)
>
> Failure to start the electric or diesel firewater pump within 85 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. (HEP-FW-START)

Analysis using the ASP methodology resulted in a conditional probability of 0.05 for the diagnosis (HEP-FW-DIAGNOSE is conditional on event HEP-SFPC-DIAGNOS), and a probability of 1.0E-5 for the failure to start (HEP-FW-START).

Non-HEP Probabilities

The failure probability used for electric pump failure to start and run in the NRC draft report (FP-MKUP-FTF) seemed high (its unavailability was 6.0E-2). The pump may be required to run 8 to 10 hours at the most, given that the water inventory drops by 20 ft (i.e., 3 ft from the top of the fuel). We recommend 3.7E-3 for failure to start and run, taken from INEL-96/0334 (Ref 3).

Further, the possibility of repair of one pump has been added to the model. If the operator starts the electric firewater pump after 43 hours but the pump fails to start and run (with a probability of 3.7E-3), then the operator would try to start the diesel-driven firewater pump. If it also failed (with a probability of 0.18), then the operator would try to get one of the pumps repaired. We assume that the operator will focus his recovery efforts on only one pump. Assuming that it takes another two shifts (16 hours) before parts and technical help arrive, then the operator has 69 hours (85 hours less 16 hours) to repair the pump. Assuming a 10-hour mean time to repair, the probability of failure to repair the pump would be $\text{Exp}[-(1/10) \times 69] = 1.0\text{E-}3$. Therefore, the unavailability of both firewater pumps would be $3.7\text{E-}3 \times 0.18 \times 1.0\text{E-}3 < 1.0\text{E-}5$.

1.2.5.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-FW-DIAGNOSE	5.0E-2	N/A
HEP-FW-START	1.0E-5	2.0E-2 (HEP-ALTCL-L)
FP-MKUP-FTF	1.0E-5	1.0E-2

1.2.6. Top Event OFB – Operator Recovery Using Offsite Sources

1.2.6.1. Event Description and Timing

Given the failure of recovery actions using onsite sources, this event accounts for recovery of coolant makeup using offsite sources 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. This top event is quantified using fault tree GFFT111.

1.2.6.2. Relevant Assumptions

- The operator has 128 hours from the onset of the initiator to provide makeup and inventory cooling
- He has sufficient time to recognize the need for and provide external sources of makeup

1.2.6.3. Quantification

Human Error Probabilities

The operator must recognize that extreme measures must be taken to provide makeup to the SFP, and he has had ample time up to this point to attempt recovery of both the SFP cooling system and both firewater pumps. This top event includes operator actions for both the diagnosis of the need to provide inventory from offsite, and the action itself. The conditional probability of failure to diagnose the need for action (HEP-OFFSITE-DIAG) was assigned a probability of 1.0, based on the fact that two earlier diagnoses failed. Note that if earlier diagnoses succeeded, then diagnosis for this top event is not required.

Event REC-INV-OFFSITE1 represents the failure of the operator to bring in offsite resources to mitigate the event. Success implies that offsite resources are brought to bear on the situation, but no effort is made to quantify specific hardware failures. The ASP methodology generated a failure probability for this action of 1.0E-4.

1.2.6.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-OFFSITE-DIAG	1.0	N/A
REC-INV-OFFSITE1	1.0E-4	1.0E-2

1.2.7. Summary

Table 1 presents a summary of basic event changes relative to the NRC draft report.

Table 1 Basic Event Changes from the NRC Draft Report for the Loss of Cooling Event Tree

Basic Event Name	Description	INEEL	NRC	Remarks and Assumptions in INEEL Analysis
HEP-RES-ALARM	Operator fails to respond to a signal indication in the control room	3.0E-3	3.0E-3	Single alarm, procedures and training
REC-WLKDWN-LOC	Operator fails to observe the loss of cooling in walkdowns	1.0E-5	1.0E-2	Active monitoring, procedures, training, shift change over discussion
HEP-SFPC-DIAGNOS	Operator fails to diagnoses need to restart SFPC	1.0E-5	—	Procedures and training provided
HEP-COOL-LOC-E	Operator fails to repair SFPC system	1.8E-1	1.0E-4	Based on 10 hrs MTTR and 33 hrs to repair (early)
HEP-COOL-LOC-L	Operator fails to repair SFPC system	1.0	2.2E-4	Procedures and training provided
HEP-FW-DIAGNOS	Operator fails to diagnoses need for alternate makeup (dependency on HEP-SFPC-DIAGNOS)	5.0E-2	—	Procedures and training provided.
HEP-FW-START	Operator fails to start FW pump and provide alignment	1.0E-5	1.0E-2	Procedures, training, and equipment provided. Extra staff available. (NRC draft report basic event names HEP-ALTCL-E or HEP-ALTCL-L)
FP-MKUP-FTF	Failure of diesel FW pump system Failure of electric FW pump system Operator fails to repair FW system	1.8E-1 3.7E-3 1.0E-3	1.8E-1 6.0E-2 —	Based on INEL-96/0334 Based on 10 hrs MTTR and 84 hrs to repair
HEP-OFFSITE-DIAG	Operator fails to diagnoses need for offsite resources (dependency on HEP-FW-DIAGNOS)	1.0	—	Procedures and training provided.
REC-INV-OFFSITE1	Operator fails to provide alternate sources of cooling from offsite	1.0E-4	1.0E-2	Procedures, training, and equipment provided. Extra staff available.

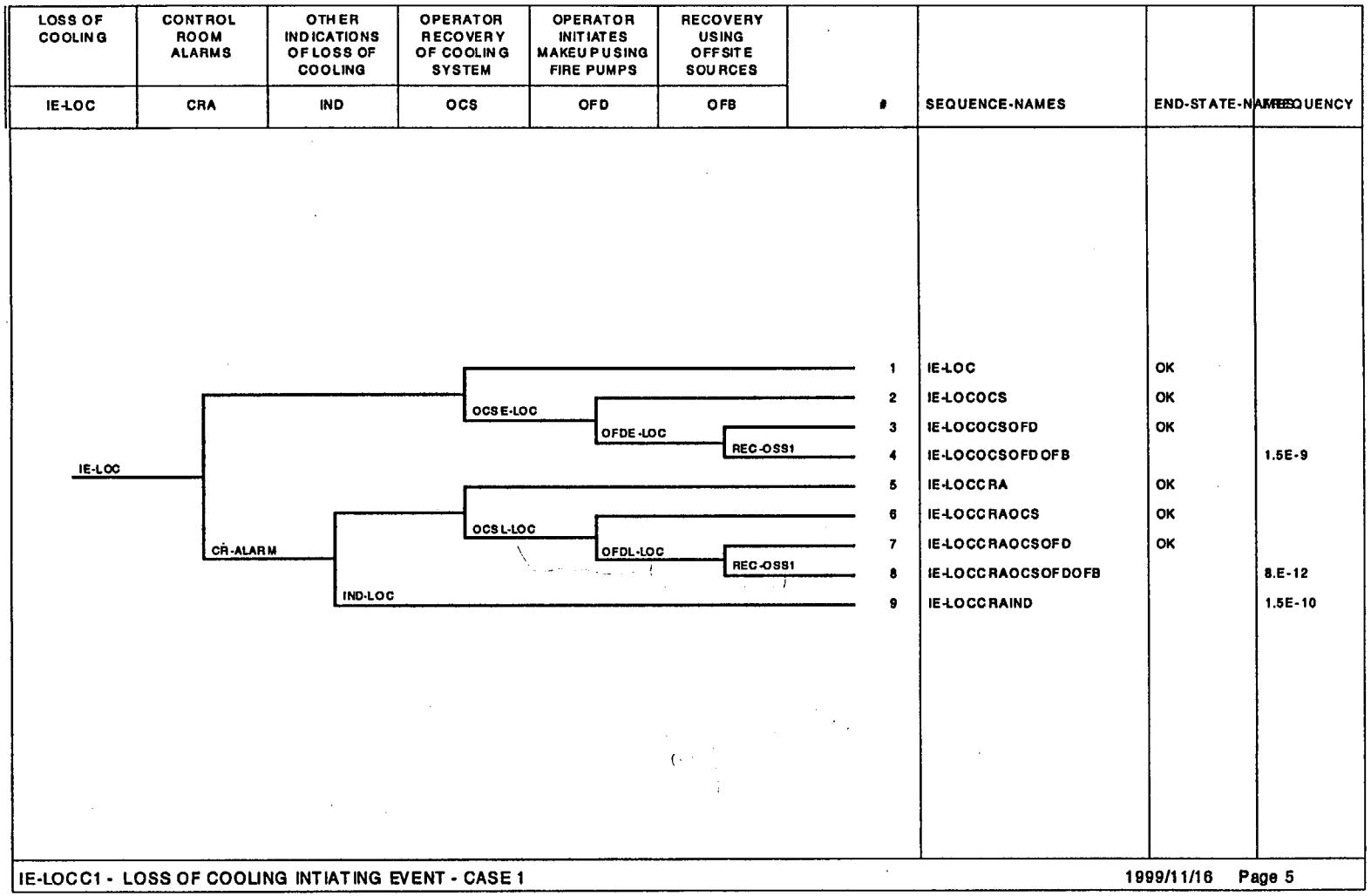

Figure 1 Loss of Cooling Event Tree

1.3. Internal Fire Event Tree

This event tree models the loss of SFP cooling caused by internal fires. The postulated fire event is assumed to incapacitate the SFP cooling and makeup system pumps (via electrical supplies) if suppression is not successful. The operator may initially attempt to recover the damaged SFP cooling system, although no credit is given for success. Once the inventory level drops below the SFP cooling system suction level, the operator has about 85 hours to provide some sort of alternate makeup – either using the site firewater system or by calling upon offsite resources. Note that this event tree assumes that there has been some damage to the site electrical system such that the electrical firewater pump is not available.

Figure 2 shows the Internal Fire event tree sequence progression.

1.3.1. Initiating Event FIR – Internal Fire

1.3.1.1. Event Description and Timing

The fire initiator (IE-INT-FIRE) includes those fires of sufficient magnitude and location to cause a loss of cooling to the SFP. It is similar to the Loss of Cooling event tree, except for the specific differences listed in the following section.

1.3.1.2. Relevant Assumptions

- The operator has discovered the fire in time to attempt suppression and prevent loss of cooling to the SFP
- Recovery of the SFP cooling system is not possible if fire suppression efforts fail
- The motor-driven firewater pump is assumed to be unavailable due to the fire

1.3.1.3. Quantification

The NRC draft report estimates the fire initiating event frequency using EPRI's Fire-Induced Vulnerability Evaluation (FIVE) document (Ref 4). The NRC draft report uses 9.0E-3/yr, which is the result derived for two areas analyzed in the EPRI report: intake structures and radwaste areas.

Activities in radwaste areas during normal operation are not expected to be similar to the activities in a fuel handling building of decommissioned plant. During normal operation, a large amount of transient combustibles (i.e., oil, flammable liquids, etc.) would be present in a radwaste area.

Fire initiators in intake structures are divided into fires initiated by pumps, electrical cabinets, and "other." This analysis will derive an overall fire initiation frequency from the contribution of pumps and electrical cabinets.

Frequencies for the different buildings listed in the EPRI report are based on the average loading in each building. For example, the pump fire frequency for an intake building is based on factors such as the total number of operating pumps in the building, and on a severity factor, which is a measure of the potential of a fire to spread. The severity factor depends on the surroundings, housekeeping, and presence of other combustible loads. Both of these factors could be significantly different for a SFP facility.

The EPRI report gives a frequency of 4.0E-3/yr for pump fires in an intake structure. That estimate is based on pumps that require lubrication (lubrication fluid is the source of most pump fires). The EPRI Fire Implementation Guide report recommends a severity factor of 0.2. It is assumed that the severity factor is embedded in the frequency of fire for intake structures. We can also assume that four pumps are running in the intake building. Using this information, we can estimate a single pump fire frequency by dividing the given pump fire frequency by the number of pumps and the severity factor;
i.e., $4.0E\text{-}3/(4 \times 0.2) = 5E\text{-}3/yr$.

For this analysis, we assume that the cooling system includes one SFP pump and one heat exchanger pump, both rated 480 volts. (In normal operating plants, SFP cooling pumps are 480 volts.) For 480-volt pumps with no significant combustibles (no oil reservoir or large amount of lubricant), the severity factor would be smaller than 0.2. In the case of the SFP facility, the potential for poor housekeeping could result in a potential for fire to spread. Therefore, assuming a severity factor of 0.01, the contribution of pumps to the facility fire frequency is $2 \times 5E\text{-}3/yr \times 0.01 = 1.0E\text{-}4/yr$.

Note that the pump failure to run probability includes a contribution from localized pump fire and is included in of the loss of SFP cooling initiating event.

Similarly, the contribution of electrical cabinets to the facility fire frequency is based on the total number of cabinets. The EPRI ignition frequency of 2.4E-3/yr for electrical cabinets in the intake structure is based on 480-volt and higher cabinets. Note that probability of the SFP cooling system being an ignition source is less likely because it does not draw much load. Also, most intake structures have a minimum of ten cabinets (based on discussions with a former operator and an NRC examiner). Assuming there are four 480-volt cabinets supplying power to the SFP cooling components, and that the severity factor does not change, the contribution of electrical cabinets to the facility fire initiation frequency would be $4 \times (2.4E\text{-}3/yr)/10 = 9.6E\text{-}4/yr$.

Therefore, the total frequency for fires from both pumps and electrical cabinets is 1.1E-3/yr.

1.3.1.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
IE-INT-FIRE	1.1E-3	9.0E-3

1.3.2. Top Event OSP – Fire Suppression

1.3.2.1. Event Description and Timing

This top event represents failure to suppress the fire before the SFP cooling system is damaged. There is an underlying assumption that if the fire is not suppressed then the SFP cooling and makeup system pumps and their power supplies are damaged to a point that they can not be repaired in time to prevent fuel uncovery. If the fire is suppressed in time to prevent damage to SFP components, then the SFP cooling system will be restored in time. The top event is represented by fault tree GFFT150.

1.3.2.2. Relevant Assumptions

- The operator has discovered the fire in time to prevent loss of cooling to the SFP
- If suppression efforts fail, recovery of the SFP cooling system is not possible
- A damage time of 20 minutes is assumed; that is, it is assumed that it will take at least 20 minutes before a fire will either fail both of the cooling pumps or fail power to the pumps

1.3.2.3. Quantification

Failure of fire suppression is represented by basic event REC-FIRE-EVT, and its probability is obtained from EPRI report NSAC-181 (Ref 5). That report gives the probabilities of failing to suppress a fire for three damage times as follows:

Probability of Failure of Fire Suppression (from NSAC-181)

Damage Time	Automatic Actuation	Manual Recovery	Manual Suppression	Total
3	0.05	1.0	0.7	0.035
13	0.05	0.33	0.4	0.007
20	0.05	0.33	0.33	0.005

The above probabilities were estimated based on information on operating reactors. For decommissioned plants, the fire protection program may be changed (Ref 6). Depending on changing plant conditions, features such as automatic fire suppression systems or an onsite fire brigade may no longer be required.

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 input such as these are not applicable for a generic study such as this, fire growth and propagation will have to be determined based on best estimate assumptions. A damage time in excess of 20 minutes is assumed because typical SFP facilities are relatively large and because equipment within such facilities is usually spread out. That is, it is assumed that it will take at least 20 minutes before a fire will either fail both of the cooling pumps or fail offsite power feed to the pumps. Therefore, from the table, the probability of failure of fire suppression is 0.005. However, given the discussion in the above paragraph, the NRC draft report assumed that suppression is not as effective in a decommissioned plant as it would be in an operating reactor, so the failure probability was increased by a factor of 10. Thus, the probability of failure of fire suppression, and the probability that this unsuppressed fire will fail the SFP cooling function, is 0.05.

1.3.3. Top Event OMK – Operator Recovery Using Onsite Sources

1.3.3.1. Event Description and Timing

At this point in the event tree, the SFP has lost cooling because of the fire, and the operator is unable to restore the SFP cooling system. Also, the fire has damaged the electrical system such that the motor-driven firewater pump is unavailable. The operator now has 128 hours to provide some form of external makeup to the pool to prevent fuel uncovery. This event represents failure of the operator to start the diesel-driven firewater pump and provide makeup to the SFP. If the diesel firewater pump fails, the operator has time to attempt repair. This event is represented by fault tree GLPR142.

Refilling time is estimated to be more than 2 ft/hr for a 250-gpm capacity pump (1 ft/hr for a 100-gpm capacity pump).

1.3.3.2. Relevant Assumptions

- The fire damage time is assumed to be about 20 minutes
- The operator must travel to the firewater pump to start it locally
- Firewater pumps are maintained on a regular schedule
- It takes two shifts (16 hours) to contact maintenance personnel, make a diagnosis, and get new parts
- There is a means of fixing a fire hose in place, so that the operator is not required to stand in a hot, humid, and possibly radiologically hazardous area for the period of time required to refill the SFP

1.3.3.3. Quantification

Human Error Probabilities

Given that the fire disables the SFP cooling system early in the sequence, the operator must diagnose the need for alternate makeup, and then successfully start the diesel firewater pump and provide alignment to the SFP. The human actions include the following:

> Failure to recognize the need to start a firewater pump within 85 hours after the onset of bulk boiling (HEP-FW-DIAGNOSE)
>
> Failure to start the electric or diesel firewater pump within 85 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. (HEP-FW-START)

The ASP analysis provides a probability of 1.0E-5 for each of these actions. There is no earlier diagnosis event for which dependency must be considered.

Non-HEP Probabilities

A single basic event (FP-DGPUMP-FTF) represents failure of the diesel firewater pump, and it includes the possibility of repair. If the diesel firewater pump fails to start and run (with a probability of 0.18), then the operator would try to repair it. Assuming that it takes another two shifts (16 hours) before parts and technical help arrive, then the operator has 69 hours (85 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) x 69] = 1.0E-3. Therefore, the unavailability of the diesel firewater pump would be 0.18 x 1.0E-3 = 1.8E-4.

1.3.3.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-FW-DIAGNOSE	1.0E-5	N/A
HEP-FW-START	1.0E-5	1.0E-2 (HEP-ALTCL-LP-E)
FP-DGPUMP-FTF	1.8E-4	1.8E-1

1.3.4. Top Event OFD – Operator Recovery Using Offsite Sources

1.3.4.1. 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. This top event is quantified using fault tree GFFT111.

1.3.4.2. Relevant Assumptions

- The operator has 128 hours from the onset of the initiator to provide makeup and inventory cooling
- The SFP cooling system and the electric firewater pump were damaged in the fire, and the operator has attempted to start the diesel firewater pump
- He has sufficient time to recognize the need for external sources of makeup

1.3.4.3. Quantification

Human Error Probabilities

The operator must recognize that extreme measures must be taken to provide makeup to the SFP, and he has had ample time up to this point to attempt recovery of both the SFP cooling system and both firewater pumps. This top event includes operator actions for both the diagnosis of the need to provide inventory from offsite, and the action itself. The conditional probability of failure to diagnose the need for action (HEP-OFFSITE-DIAG) was assigned a probability of 5.0E-2, based on the fact that an earlier diagnosis failed (HEP-FW-DIAGNOSE). Note that if the earlier diagnosis succeeded, then diagnosis for this top event is not required.

Event REC-INV-OFFSITE1 represents the failure of the operator to bring in offsite resources to mitigate the event. Success implies that offsite resources are brought to bear on the situation, but no effort is made to quantify specific hardware failures. The ASP methodology generated a failure probability for this action of 1.0E-4.

1.3.4.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-OFFSITE-DIAG	5.0E-2	N/A
REC-INV-OFFSITE1	1.0E-4	1.0E-2

1.3.5. Summary

Table 2 presents a summary of basic event changes relative to the NRC draft report.

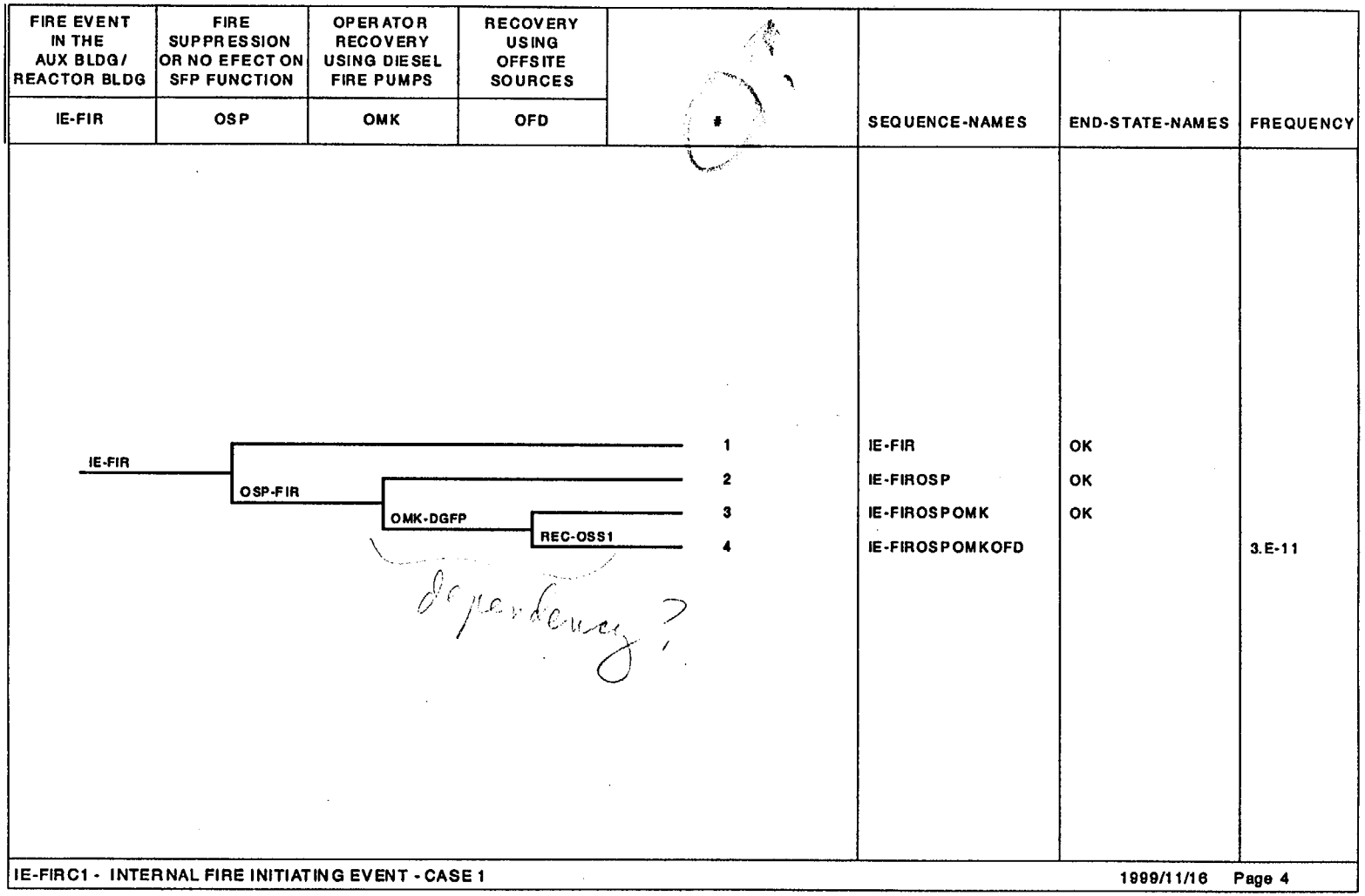

Figure 2 Internal Fire Event Tree

Table 2 Basic Event Changes from the NRC Draft Report for the Internal Fire Event Tree

Basic Event Name	Description	INEEL	NRC	Remarks and Assumptions in INEEL analysis
IE-INT-FIRE	Initiating event frequency of fire	1.1E-3	9.0E-3	Frequency of pump initiated fire, 1.E-4/yr and electrical cabinet initiated fire, 9.6E-4/yr.
HEP-FW-DIAGNOS	Operator fails to diagnoses need for alternate makeup	1.0E-5	—	Procedures and training provided.
HEP-FW-START	Operator fails to start FW pump and provide alignment	1.0E-5	1.0E-2	Procedures, training, and equipment provided. Extra staff available. (NRC draft report basic event name HEP-ALTCL-LP-E)
FP-DGPUMP-FTF Operator fails to repair FW system	Failure of diesel FW pump system	1.8E-1 1.0E-3	1.8E-1 —	Based on INEL-96/0334 Based on 10 hrs MTTR and 37 hrs to repair
HEP-OFFSITE-DIAG	Operator fails to diagnoses need for offsite resources (dependency on HEP-FW-DIAGNOS)	5.0E-2	—	Procedures and training provided.
REC-INV-OFFSITE1	Operator fails to provide alternate sources of cooling from offsite	1.0E-4	1.0E-2	Procedures, training, and equipment provided. Extra staff available.

1.4. 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. The order of the top events has been modified when compared to the NRC draft report to represent the expected sequence of events (i.e., given a LOSP event, the first thing operator would do is to attempt to recover power), and to evaluate properly the dependency between operator errors.

Also note that diagnosis errors are not considered for this event tree. It is assumed that the loss of power is obvious to the operator, and that he is aware of the need to take actions if the outage extends beyond several hours.

Figure 3 shows the Plant-centered and Grid-related Loss of Offsite Power event tree sequence progression.

1.4.1. Initiating Event LP1 – Plant-centered and Grid-related Loss of Offsite Power*

1.4.1.1. Event Description and Timing

Initiating event IE-LOOP-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.

1.4.1.2. Relevant Assumptions

None.

1.4.1.3. Quantification

The NRC draft report uses a LOSP frequency of 0.08/yr for plant-centered events, taken from INEL-96/0334 (Ref 3), and 1.9E-3/yr for grid-related events, taken from NUREG/CR-5496 (Ref 8). For the purpose of this analysis, the LOSP IE frequency from plant-centered and grid-related events is assigned a value of 0.08/yr. This number may be slightly high because relative to a decommissioned plant, a higher proportion of LOSP events at an operating plant would be caused by maintenance and operations activity performed by the utility. The same high level of activities would not be present at a decommissioned plant.

1.4.2. Top Event OPR – Offsite Power Recovery

1.4.2.1. Event Description and Timing

The fault tree for this top event (GFFT170) is a single basic event that represents the non-recovery probability of offsite power. The draft report assumes that if the power is not recovered in first 50 hours, the probability of recovering offsite power in 128 hours is negligible.

---

* The use of initiating event frequency estimated in the NUREG/CR-5496 (Ref 8) is conservative. In the NUREG/CR, the events that failed only the safety (vital) buses without LOSP event (did not fail non-vital buses) but required the AC generators to start and power the respective buses were also included as LOSP events in the estimation of the IE frequency.

A decommissioned plant would be similar to non-power utility industries. For a non-power generating plant, the plant-centered LOSP event frequency is estimated to be 0.02/yr (Ref 7)

Baranowsky (Ref 9) 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 (Ref 8) divides LOSPs into three categories and estimates different values of non-recovery as functions of time. For the purpose of this analysis, a weighted non-recovery probability is used.

1.4.2.2. Relevant Assumptions

If power is not recovered within the first 33 hours, it is assumed that problem is significant and the probability of recovering power within 128 hours is very small.

1.4.2.3. Quantification

Non-HEP Probabilities

The basic event that represents recovery of offsite power for plant-centered and grid-related LOSPs is REC-OSP-PC. Based on the ASP analysis from ORNL/NRC/LTR-89/11 (Ref 10) for plant-centered LOSP events, the non-recovery probability within 24 hours is less than 1.0E-5. In the case of grid-related LOSP events, the non-recovery probability within 24 hours is 1.0E-3. Therefore, the weighted non-recovery probability of offsite power, from both plant-centered and grid-related events is as follows:

$$\frac{(0.08/\text{yr} \times 1.0\text{E}{-5} + 1.9\text{E}{-3}/\text{yr} \times 1.0\text{E}{-3})}{0.08/\text{yr} + 1.9\text{E}{-3}/\text{yr}} = 3.3\text{E}{-5}$$

The draft report provides only one estimate (1.0E-3) for non-recovery of power for more than 50 hours, derived from NUREG/CR-5032 (Ref 11).

1.4.2.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
REC-OSP-PC	3.3E-5	1.0E-3

1.4.3. Top Event OCS – Cooling System Restart and Run

1.4.3.1. 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 GCSR112 has several basic events: one operator error to establish SFP cooling, and several hardware failures of the system. This top event is dominated by the operator error to restart/realign the SFP cooling 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.

1.4.3.2. Relevant Assumptions

- The operator has 9 hours to start the SFP cooling system (this is equivalent to the conservative assumption that offsite power is recovered at exactly 24 hours)
- Task completion time 1 hour
- Well-written procedures exist
- It takes two shifts (16 hours) to contact maintenance personnel, make a diagnosis, and get new parts
- Operator has received the necessary training
- Potential harsh environment (hot and humid)

1.4.3.3. Quantification

Human Error Probability

One operator error is modeled under this top event (HEP-COOL-LOP-E). In the NRC draft report, a probability of 3.5E-3 was assigned to the operator error to restart/realign the SFP cooling system, based on event SFP-XHE-XE-LP from INEL-96/0334 (Ref 3). This event represents operator failure to restart/realign the SFP cooling system in 9 hours given that power is recovered. 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 ASP methodology provides a failure probability of 5.0E-4 for this event.

Non-HEP Probabilities

In the NRC draft report, a probability of 9.4E-4 was estimated for the hardware failures of the system. If the system fails to start and run for a few hours then the operator 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 to repair the SFP cooling system.

1.4.3.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-COOL-LOP-E	5.0E-4	3.5E-3

1.4.4. Top Event OMK – Operator Recovery Using Onsite Sources

1.4.4.1. Event Description and Timing

This top event represents the unavailability of the firewater pumps. If offsite power is recovered then the fault tree GLPR112 represents this top event. In this case, the operator has both electric and diesel firewater pumps available. The top event has two basic events: an operator error to start any firewater pump, and failure of electric and diesel firewater pumps to start and run.

If offsite power is not recovered then fault tree GLPR142 represents this top event. In this case, the operator has only the diesel firewater pump available. The top event has two basic events: an operator error to start the diesel firewater pump and failure of the diesel firewater pump to start and run. (Note that if power is recovered later in the event, operator has an option of starting the electrical firewater pump.)

It is assumed that the operator will first try to reestablish the SFP cooling system, and will wait some time for offsite power to be restored before resorting to the firewater system as a source of makeup. Failure to restore power or failure to restart/realign the SFP cooling system would eventually result in pool boiling and loss of inventory. Once the pool level drops below the SFP cooling system suction level (assumed to occur at about 43 hours – see Section 1.2.5.1), the operator would have to provide makeup using the firewater system. Therefore, the operator would have about 85 hours to provide firewater makeup (128 hours less 43 hours). If one or both pumps fail to start or run, we assume that it takes another two shifts (16 hours) to contact maintenance personnel, to perform the diagnosis, and to get new parts; therefore, the operator would have 69 hours (85 hours less 16 hours) to perform repairs.

1.4.4.2. Relevant Assumptions

- Maintenance is performed per schedule on diesel and electric firewater pumps to maintain operable status
- The operator has 85 hours to start a firewater pump
- On average, it takes 10 hours to repair a pump if it fails to start and run
- It takes two shifts (16 hours) to contact maintenance personnel, make a diagnosis, and get new parts
- The hose in the SFP area can be secured in less than 1 hour

- Both firewater pumps are located in a separate structure or protected from the potential harsh environment in case of pool bulk boiling

1.4.4.3. Quantification

Human Error Probabilities

This top event includes two operator actions. One represents the operator's failure to establish firewater makeup given that power was recovered and the operator failed to restart/realign the SFP cooling system before boil-off began. The action is identical to basic event HEP-FW-START described in Section 1.2.5.3. Success is defined as the operator starting one of two firewater pumps and securing a firewater hose in the spent fuel pool area. There are multiple shifts available to start the pump. The ASP methodology produced a value of 1.0E-5 for this event.

The second event represents the operator's failure to establish makeup given that power was not recovered, and is identical to basic event HEP-FW-START described in Section 1.3.3.3. Success is defined as the operator starting the diesel firewater pump and securing a firewater hose in the spent fuel pool area. There are multiple shifts available to start the pump. It is assumed the task requires 1 hour. The ASP methodology produced a value of 1.0E-5 for this event.

Non-HEP Probabilities

In the NRC draft report, the failure probabilities (including both failure to start and failure to run) for electric and diesel firewater pumps are 6.0E-2 and 0.18, respectively. Either pump may be required to run at the most 8 hours, given that the water inventory drops by 20 feet (i.e., 3 feet from the top of the fuel). For the electric firewater pump, we recommend 3.7E-3 failure probability for the pump to start and run for 10 hours, from INEL-96/0334 (Ref 3).

The operator would first try to start all available pumps. If he fails to do so, he would try to fix one pump. Therefore, credit for repairing a pump is given to only one pump. Given that the operator will not initiate firewater until the water level in the pool drops below the SFP cooling system suction level, he would have about 85 hours to provide makeup (128 hours less 43 hours). Assuming that it takes another two shifts (16 hours) to contact maintenance personnel, make a diagnosis, and get new parts, then the operator has 69 hours (85 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 1.0E-3 (Exp [-(1/10) × 69]). Therefore, the probability of the diesel and electric firewater pumps failing to start and run (basic event FP-MKUP-FTF) would be $0.18 \times 3.7E\text{-}3 \times 1.0E\text{-}3 < 1.0E\text{-}5$.

Similarly, given that offsite power is not recovered, the probability of the diesel firewater pump failing to start and run (basic event FP-DGPUMP-FTF) would be $0.18 \times 1.0E\text{-}3 = 1.8E\text{-}4$.

1.4.4.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-FW-START	1.0E-5	2.0E-2 (HEP-ALTCL-L)
HEP-FW-START	1.0E-5	1.0E-2 (HEP-ALTCL-LP-E)
FP-MKUP-FTF	1.0E-5	1.0E-2
FP-DGPUMP-FTF	1.8E-4	0.18

1.4.5. Top Event OFD – Operator Recovery Using Offsite Sources

1.4.5.1. 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 GFFT~~111~~ represents this top event, and it is quantified twice to account for whether or not power has been recovered

1.4.5.2. Relevant Assumptions

- The operator has 128 hours from the onset of the initiator to provide makeup and inventory cooling
- He has sufficient time to recognize the need for external sources of makeup

1.4.5.3. Quantification

Human Error Probabilities

The operator must recognize that extreme measures must be taken to provide makeup to the SFP. He has had ample time up to this point to attempt recovery of both the SFP cooling system and both firewater pumps. This event (REC-INV-OFFSITE1) represents the failure of the operator to recognize that he must bring in offsite resources to mitigate the event. Success implies that offsite resources are brought to bear on the situation, but no effort is made to quantify hardware failures or human errors related to execution of any actions. It is assumed that once the operator is no longer acting alone, once regional authorities are aware of the situation, the sequence will be successfully terminated.

The ASP methodology generated a failure probability for this action of 1.0E-4 (with no difference between the cases where offsite power was recovered or not).

1.4.5.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
REC-INV-OFFSITE1	1.0E-4	1.0E-2

1.4.6. Summary

Table 3 presents a summary of basic event changes relative to the NRC draft report.

Table 3 Basic Event Changes from the NRC Draft Report for the Plant-centered and Grid-related LOSP Event Tree

Basic Event Name	Description	INEEL	NRC	Remarks and Assumptions in INEEL analysis
REC-OSP-PC	Failure to recover offsite power	3.3E-5	1.0E-3	Weighted on frequency of plant-centered and grid-related LOSP events
HEP-COOL-LOP-E	Operator fails to restart SFPC system	5.0E-4	3.5E-3	Procedures and training provided
HEP-FW-START	Operator fails to start FW pump and provide alignment	1.0E-5	1.0E-2	Procedures, training, and equipment provided. Extra staff available. (NRC draft report basic event name HEP-ALTCL-LP-E)
FP-MKUP-FTF (Power Recovered)	Failure of diesel FW pump system Failure of electric FW pump system Operator fails to repair FW system	1.8E-1 3.7E-3 1.0E-3	1.8E-1 6.0E-2 —	Based on INEL-96/0334 Based on 10 hrs MTTR and 69 hrs to repair
FP-DGPUMP-FTF (Power not recovered)	Failure of diesel FW pump system Operator fails to repair FW system	1.8E-1 1.0E-3	1.8E-1 —	Based on INEL-96/0334 Based on 10 hrs MTTR and 69 hrs to repair
REC-INV-OFFSITE1	Operator fails to provide alternate sources of cooling from offsite	1.0E-4	5.0E-2	Procedures, training, and equipment provided. Extra staff available.

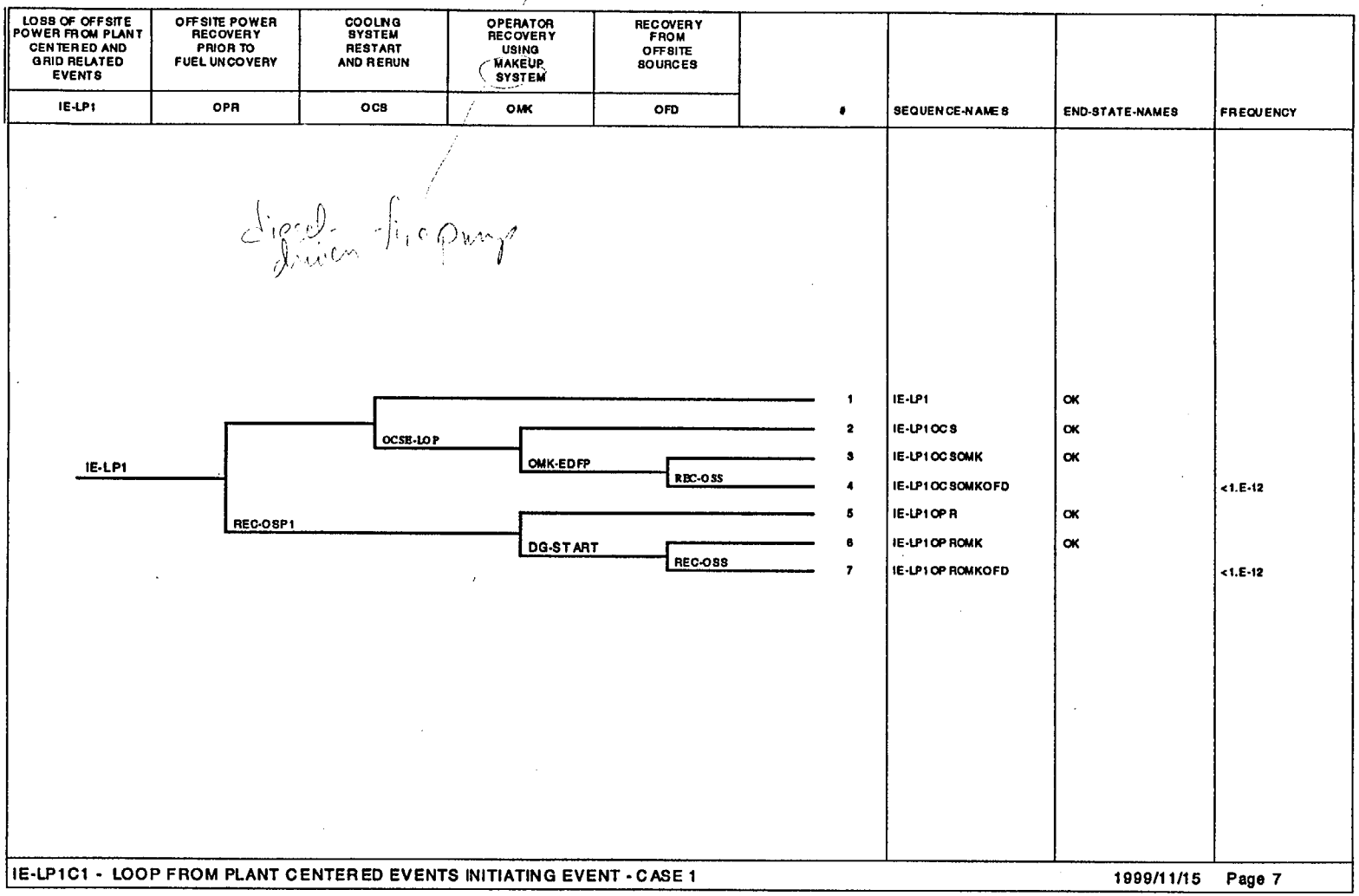

Figure 3 Plant Centered and Grid -related Loss of Offsite Power Event Tree

1.5. 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. The order of the top events has been modified when compared to the NRC draft report to represent the expected sequence of events (i.e., given a LOSP event, the first thing operator would do is to attempt to recover power), and to evaluate properly the dependency between operator errors.

Also note that diagnosis errors are not considered for this event tree. It is assumed that the loss of power is obvious to the operator, and that he is aware of the need to take actions if the outage extends beyond several hours.

Figure 4 shows the Severe Weather Loss of Offsite Power event tree sequence progression.

1.5.1. Initiating Event LP2 – Severe Weather Loss of Offsite Power

1.5.1.1. Event Description and Timing

Initiating event IE-LOOP-LP2 represents losses of offsite power due to severe weather. 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 event tree in that the probability of offsite power recovery is reduced.

1.5.1.2. Relevant Assumptions

None.

1.5.1.3. Quantification

The LOSP frequency from severe weather events is 7.0E-3/yr, taken from NUREG/CR-5496 (Ref 8).

1.5.2. Top Event OPR – Offsite Power Recovery

1.5.2.1. Event Description and Timing

This top event is modeled by fault tree GFFT172, and includes a single basic event, which represents the non-recovery probability of offsite power. The NRC draft report estimated non-recovery probability based on 128 hours. However, if power is recovered after 33 hours (the onset of pool bulk boiling), the operator may not be able to use the SFP cooling system because the pool water level may drop below its suction level by the time cooling is established. Therefore, the operator must start a firewater pump to makeup inventory. It is assumed that if power is recovered before boil-off starts (33 hours), the operator has a chance to reestablish cooling using SFP cooling system.

1.5.2.2. Relevant Assumptions

If power is not recovered within the first 33 hours, it is assumed that problem is significant and the probability of recovering power within 128 hours is very small.

1.5.2.3. Quantification

Non-HEP Probabilities

The NRC draft report estimated a non-recovery probability for this event (REC-OSP-SW) of 0.02 based on 128 hours, derived from NUREG/CR-5496 (Ref 8).

1.5.3. Top Event OCS – Cooling System Restart and Run

1.5.3.1. 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 GCSR112 has several basic events: one operator error to establish SFP cooling, and several hardware failures of the system. This top event is dominated by the operator error to restart/realign the SFP cooling 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.

1.5.3.2. Relevant Assumptions

- Operator has 9 hours to start the SFP cooling system (this is equivalent to the conservative assumption that offsite power is recovered at exactly 24 hours).
- Task completion time 1 hour
- Well-written procedures exist
- It takes two shifts (16 hours) to contact maintenance personnel, make a diagnosis, and get new parts
- Operator has received the necessary training
- Potential harsh environment (hot and humid)

1.5.3.3. Quantification

Human Error Probability

One operator error is modeled under this top event (HEP-COOL-LOP-E). In the NRC draft report, a probability of 3.5E-3 was assigned to the operator error to restart/realign the SFP cooling system, based on event SFP-XHE-XE-LP from INEL-96/0334 (Ref 3). This event represents operator failure to restart/realign the SFP cooling system in 9 hours given that power is recovered. The operator can restart the previously running pump and may not have to make any valve alignment. If he decides to restart standby pump he may have to make some valve alignment. The ASP methodology provides a failure probability of 5.0E-4 for this event.

Non-HEP Probabilities

In the NRC draft report, a probability of 9.4E-4 was estimated for the hardware failures of the system. If the system fails to start and run for a few hours then the operator 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 to repair the SFP cooling system.

1.5.3.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-COOL-LOP-E	5.0E-4	3.5E-3

1.5.4. Top Event OMK – Operator Recovery Using Onsite Sources

1.5.4.1. Event Description and Timing

This top event represents the unavailability of the firewater pumps. If offsite power is recovered then the fault tree GLPR112 represents this top event. In this case, the operator has both electric and diesel

firewater pumps available. The top event has two basic events: an operator error to start any firewater pump, and failure of electric and diesel firewater pumps to start and run.

If offsite power is not recovered then fault tree GLPR142 represents this top event. In this case, operator has only diesel firewater pump available. The top event has two basic events: an operator error to start the diesel firewater pump and failure of the diesel firewater pump to start and run. (Note that if power is recovered later in the event, operator has an option of starting the electrical firewater pump.)

It is assumed that the operator will first try to reestablish the SFP cooling system, and will wait some time for offsite power to be restored before resorting to the firewater system as a source of makeup. Failure to restore power or failure to restart/realign the SFP cooling system would eventually result in pool boiling and loss of inventory. Once the pool level drops below the SFP cooling system suction level (assumed to occur at about 43 hours – see Section 1.2.5.1), the operator would have to provide makeup using the firewater system. Therefore, the operator would have about 85 hours to provide firewater makeup (128 hours less 43 hours). Because of the severe weather, if one or both pumps fail to start or run, we assume that it takes another four to five shifts (48 hours) to contact maintenance personnel, to perform the diagnosis, and to get new parts. Therefore, the operator would have 37 hours (85 hours less 48 hours) to perform repairs.

1.5.4.2. Relevant Assumptions

- Maintenance is performed per schedule on diesel and electric firewater pumps to maintain operable status
- Operator has 85 hours to start a firewater pump
- On average, it takes 10 hours to repair a pump if it fails to start and run
- Because of the severe weather, it takes four to five shifts (48 hours) to contact maintenance personnel, make a diagnosis, and get new parts
- The hose in the SFP area can be secured in less than 1 hour
- Both firewater pumps are located in a separate structure or protected from the potential harsh environment in case of pool bulk boiling

1.5.4.3. Quantification

Human Error Probabilities

If offsite power is recovered, the operator will have two pumps available to perform this action. If offsite power is still unavailable, then he has only the diesel firewater pump. For this quantification, the number of pumps available has no effect on the probability of failure. Therefore, this event represents the operator's failure to establish makeup with one or two firewater pumps, and is identical to basic event HEP-FW-START described in Section 1.3.3.3. Success is defined as the operator starting a firewater pump and securing a firewater hose in the spent fuel pool area. There are multiple shifts available to start the pump. It is assumed the task requires 1 hour. The ASP methodology produced a value of 1.0E-5 for this event.

Non-HEP Probabilities

In the NRC draft report, the failure probabilities (including both failure to start and failure to run) for electric and diesel firewater pumps are 6.0E-2 and 0.18, respectively. Either pump may be required to run at the most 8 hours, given that the water inventory drops by 20 feet (i.e., 3 feet from the top of the fuel). For the electric firewater pump, we recommend 3.7E-3 failure probability for the pump to start and run for 10 hours, based on INEL-96/0334 (Ref 3).

The operator would first try to start all available pumps. If he fails to do so, he would try to fix one pump. Therefore, credit for repairing a pump is given to only one pump. Given that the operator will not initiate firewater until the water level in the pool drops below the SFP cooling system suction level, he would have about 85 hours to provide makeup (128 hours less 43 hours). Assuming that it takes another four to five shifts (48 hours) to contact maintenance personnel, make a diagnosis, and get new parts, then the

operator has 37 hours (85 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 2.5E-2 (Exp [-(1/10) × 37]). Therefore, the probability of the diesel and electric firewater pumps failing to start and run (basic event FP-MKUP-FTF) would be 0.18 × 3.7E-3 × 2.5E-2 = 1.7E-5.

Similarly, given that offsite power is not recovered, the probability of the diesel firewater pump failing to start and run (basic event FP-DGPUMP-FTF) would be 0.18 × 2.5E-2 = 4.5E-3.

1.5.4.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-FW-START	1.0E-5	1.0E-2 (HEP-ALTCL-LP-E)
FP-MKUP-FTF	1.7E-5	1.0E-2
FP-DGPUMP-FTF	4.5E-3	0.18

1.5.5. Top Event OFD – Operator Recovery Using Offsite Sources

1.5.5.1. 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 GFFT111 represents this top event, and it is quantified twice to account for whether or not power has been recovered

1.5.5.2. Relevant Assumptions

- The operator has 128 hours from the onset of the initiator to provide makeup and inventory cooling
- He has sufficient time to recognize the need for external sources of makeup

1.5.5.3. Quantification

Human Error Probabilities

The operator must recognize that extreme measures must be taken to provide makeup to the SFP. He has had ample time up to this point to attempt recovery of both the SFP cooling system and both firewater pumps. This event (REC-INV-OFFSITE1) represents the failure of the operator to recognize that he must bring in offsite resources to mitigate the event. Success implies that offsite resources are brought to bear on the situation, but no effort is made to quantify hardware failures or human errors related to execution of any actions. It is assumed that once the operator is no longer acting alone, once regional authorities are aware of the situation, the sequence will be successfully terminated.

The ASP methodology generated a failure probability for this action of 1.0E-4 (with no difference between the cases where offsite power is recovered within 24 hours or not).

1.5.5.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
REC-INV-OFFSITE1	1.0E-4	1.0E-2

1.5.6. Summary

Table 4 presents a summary of basic event changes relative to the NRC draft report.

Table 4 Basic Event Changes from the NRC Draft Report for the Severe Weather LOSP Event Tree

Basic Event Name	Description	INEEL	NRC	Remarks and Assumptions in INEEL analysis
REC-OSP-SW	Failure to recover offsite power	2.0E-2	2.0E-2	Minarick, J. W., 'Revised LOOP Recovery and PWR Seal LOCA Models', ORNL/NRC/LTR-89/11
HEP-COOL-LOP-E	Operator fails to restart SFPC system	5.0E-4	3.5E-3	Procedures and training provided
HEP-FW-START	Operator fails to start FW pump and provide alignment	1.0E-5	1.0E-2	Procedures, training, and equipment provided. Extra staff available. (NRC draft report basic event name HEP-ALTCL-LP-E)
FP-MKUP-FTF (Power Recovered)	Failure of diesel FW pump system Failure of electric FW pump system Operator fails to repair FW system	1.8E-1 3.7E-3 2.5E-2	1.8E-1 6.0E-2 —	Based on INEL-96/0334 Based on 10 hrs MTTR and 37 hrs to repair
FP-DGPUMP-FTF (Power not recovered)	Failure of diesel FW pump system Operator fails to repair FW system	1.8E-1 2.5E-2	1.8E-1 —	Based on INEL-96/0334 Based on 10 hrs MTTR and 37 hrs to repair
REC-INV-OFFSITE1	Operator fails to provide alternate sources of cooling from offsite	1.0E-4	5.0E-2	Procedures, training, and equipment provided. Extra staff available.

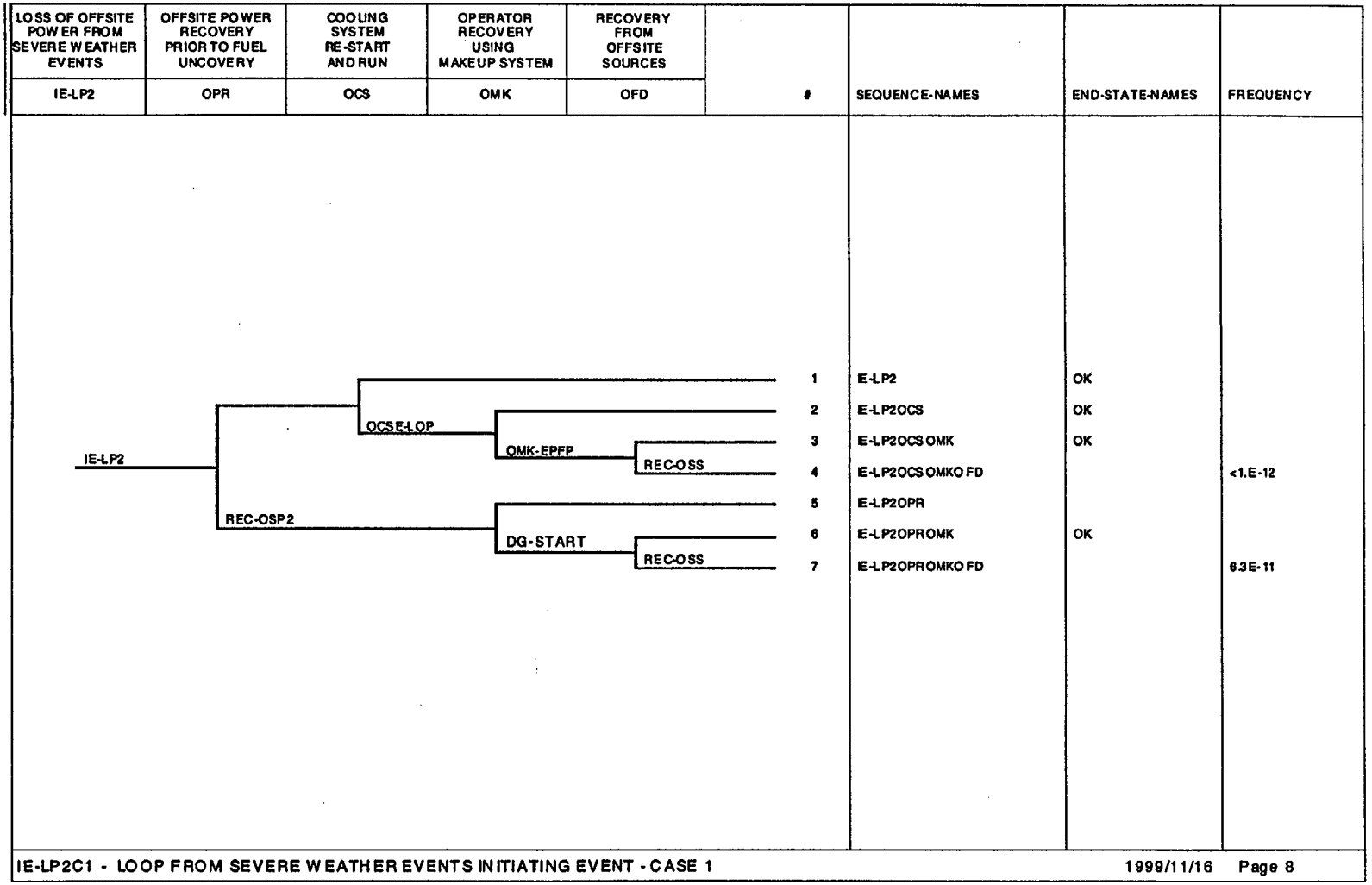

Figure 4 Severe Weather-related Loss of Offsite Power Event Tree

1.6. Loss of Inventory Event Tree

This event tree models general loss of inventory events, which challenge the safety envelope within much shorter timeframes relative to other types of events. For the loss of inventory event, it is assumed that the SFP cooling system suction pipe extends into the pool 15 ft below the normal level (in earlier loss of cooling scenarios, it was assumed that suction was lost below 2 ft). It is assumed that once the water level drops below the suction level, the leak would be isolated automatically by the fact that the siphon would be lost; thereafter, loss of inventory would occur as a result of boil-off.

Figure 5 shows the Loss of Inventory event tree.

1.6.1. Initiating Event LOI – Loss of Inventory

1.6.1.1. Event Description and Timing

This initiator (IE-LO-POOL-INV) 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 1), 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.

1.6.1.2. Relevant Assumptions

- Only those events in which level decreased over one foot have been included in the calculation of initiator frequency
- The SFP cooling system suction pipe extends down 15 ft below the normal pool water level

1.6.1.3. Quantification

Less than one event per 100 reactor years is equivalent to a frequency of 0.01/yr.

1.6.2. Top Event NLL – Loss Exceeds Makeup Capacity

1.6.2.1. Event Description and Timing

This phenomenological event divides the losses of inventory into two categories: those for which isolation is required before the SFP makeup system can replenish the pool, and those for which the SFP makeup system's capacity is sufficient to prevent fuel uncovery without isolation of the leak.

1.6.2.2. Relevant Assumptions

- In the case of a large leak, the water level would drop below 15 ft between 24 and 36 hours after the initiation of the event (based on a leak rate twice the capacity of the SFP makeup system)
- In the case of small leak, the water level would drop below 15 ft in more than 48 hours after the initiation of event (based on a leak rate less than the capacity of the SFP makeup system)

1.6.2.3. Quantification

Non-HEP Probabilities

This top event is quantified by a single basic event, LOI-SMALL. Using the information from NUREG-1275 (Ref 1), it can be assumed that 6% of the loss of inventory events will be large enough or will have durations long enough so that isolation of the loss is required if the only system available for makeup is the SFP makeup system. For the other 94% of the cases, operation of the makeup pump is sufficient to prevent fuel uncovery.

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, it is assumed that 2/37 ≈ 0.06 of events result in large losses of inventory.

1.6.3. Top Event CRA – Control Room Alarms

1.6.3.1. Event description and Timing

This top event represents the failure of remote level indicator alarms in the control room or the operator's failure to respond to those alarms. This top event is represented by fault tree GCRA112.

Given a large leak (i.e., the upper branch of event NLL), it is assumed that the water level would drop 15 ft in about 24 hours of the initiation of the event (we're using 24 hours, though it could be up to about 36 hours). Thus, the water level would drop below the low-level alarm set point within a couple of hours after the initiation of the event, and that the low-level alarm would be annunciated or displayed in the control room. Because it is assumed that the suction pipe extends no more than 15 ft below the normal level, a loss of SFP cooling alarm is not expected until the water level drops below the suction level of the SFP cooling system. Once the water level drops below the suction level, it is expected that the operator would receive a loss/trouble of SFP cooling alarm in the control room.

For a small leak (i.e., the lower branch of event NLL), the leak rate is such that the makeup pump is of sufficient capacity to overcome the loss. It is assumed that it would take more than 48 hours from the initiating event for the water level to drop below 15 ft. Once the water level drops below the suction level of the SFP cooling system, it is expected that the operator would receive a loss/trouble of SFP cooling alarm in the control room.

1.6.3.2. Relevant Assumptions

- 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
- The loss of inventory will eventually produce a failure of SFP cooling, resulting in high temperature and SFP cooling system trouble alarms in the control room
- Operators are trained and receive training on the regular basis
- Training plans are revised as needed to reflect current plant configuration

1.6.3.3. Quantification

Human Error Probabilities

One operator error, HEP-RES-ALARM; is modeled under this top event. In the Draft report, a probability of 3.0E-3 was assigned to the operator fails to respond given alarm for both large and small leak events. This event represents operator failure to respond after receiving a low-level alarm. Success is defined as the operator investigating the alarm and taking appropriate actions. THERP analysis provides a probability of 3.0E-3 for this event.

Non-HEP Probabilities

In the NRC draft report, a probability of 2.0E-3 was estimated for the hardware failures of the level monitoring and alarm system.

1.6.3.4. Changes from the NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-RES-ALARM	3.0E-3	3.0E-3

1.6.4. Top Event IND – Other Indications of Loss of Inventory

1.6.4.1. Event Description and Timing

This top event represents the operator's failure to observe the inventory loss during walkdowns. Given a loss of inventory, an operator may not have received the low-level alarm due to hardware failure or perhaps he failed to take appropriate action. This event represents the operator's failure to notice low-level or localized alarms in the SFP area during his walkdown.

Two fault trees are used to represent large and small inventory losses, each comprising a single basic event. Once the water level drops below the SFP cooling system suction level (i.e., 15 ft below normal pool level), the time needed to boil-off to 3 ft above the top fuel is estimated to be 36 hours. Therefore, the total time available for operator action in the large leak case is 60 hours (24 hours + 36 hours). Similarly, the total time available for operator action in the small leak case is 84 hours (48 hours + 36 hours).

Following an alarm in the large break case, the operator has about 60 hours before the water level reaches 3 ft above the top of the fuel. Assuming the leak occurs immediately after the first walkdown, the operator would have a minimum of 5 to 6 chances to observe the decreasing level. Also, after a couple of shifts the water would have started boiling, degrading the pool environment. This event is modeled by fault tree GFFT132.

In the case of small break event, it is estimated that it would be more than 84 hours before the water level would drop below the 3 ft above the top fuel. However, the operator may not receive any alarm indicating loss of inventory and may not be able to observe significant decrease of level within the first couple of shifts. Depending on the leak location, he may notice water on the floor or in a sump and may investigate. In this case, operator would have more than 7 or 8 opportunities to observe the decreasing level. Also, after 3 or 4 shifts, water would have started boiling, degrading the pool environment. This event is modeled by fault tree GFFT134.

1.6.4.2. Relevant assumptions

- Operators are trained and receive training on the regular basis
- Training plans are revised as needed to reflect the modes as they occur
- 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
- Water level measurement stick with clear marking is installed in the pool at a location that is easy to observe
- Operator is required to make a round per shift and record the level reading per shift
- Procedure/guidance exit for operator what to do in the case of leakage events

1.6.4.3. Quantification

Human Error Probabilities

One operator error is modeled under this top event for large leak and small leak events. For large case, the basic event REC-WLKDWN-LOI-L represents operator error of failure to observe the decreasing level in the pool. In the NRC draft report, a probability of 0.1 was assigned to this event. After the initiation of the event, an operator may have received the alarm and failed to take actions or the low-level alarm failed due to hardware failures. However, operator fails to observe the level decreasing during 5 to 6 walkdowns. The probability of failure was determined using THERP, assuming only two independent shift walkdowns (1.0E-5).

For small case, the basic event REC-WLKDWN-LOI-S represents operator error of failure to observe the decreasing level in the pool. In the Draft report, a probability of 0.01 was assigned to this event. After the initiation of the event, an operator may have received the alarm and failed to take actions or the low-level alarm failed due to hardware failures. However, operator fails to observe the level decreasing

during 7 to 8 walkdowns. The probability of failure was determined using THERP, assuming only two independent shift walkdowns (1.0E-5).

1.6.4.4. Changes from NRC Draft report

Basic Event	INEEL	NRC Draft Report
REC-WLKDWN-LOI-L	1.0E-5	0.1
REC-WLKDWN-LOI-S	1.0E-5	0.01

1.6.5. Top Event OIS – Operator Isolates Leak and Initiates SFP Makeup

1.6.5.1. Event Description and Timing

This top event represents the operator's failure to isolate a large leak and initiate the SFP makeup system, and is represented by fault trees GLIR121 and GLIR151. Included in this probability is the proportion of leaks that are not isolable.

A large leak is assumed to drain the pool down 15 ft in about 24 hours. It is assumed that the SFP cooling system is not functional during that time, because of the possibility that the leak is in a location that disables the cooling function. Therefore, given the loss of inventory and concomitant loss of cooling, it is assumed that bulk boiling begins several hours before the time that the pool level reaches 15 ft below nominal and the leak self-isolates. For simplicity, we've assumed that boiling begins when the pool level reaches 15 ft below nominal. At that time, the SFP makeup system becomes ineffectual, because its capacity is not sufficient to overcome boil-off. Therefore, the operator must isolate a large leak before the level reaches the 15-ft level (i.e., within 24 hours).

If the operator responds to the initiator early (i.e., CRA is successful), he would have the full 24 hours to isolate the leak. If he successfully isolates the leak, he can restart the SFP makeup system or the firewater pumps to replenish inventory, then restart the SFP cooling system. This event is represented by fault tree GLIR121.

If the loss of inventory is discovered through walkdowns, it is assumed that several shifts have passed since the initiator (i.e., up to 24 hours). Therefore, it is assumed that there is not enough time available to isolate the leak in time to provide for SFP makeup system success, and has been assigned a value of 1.0. This event is represented by fault tree GLIR151.

1.6.5.2. Relevant Assumptions

- Operators are trained and receive training on the regular basis
- Training plans are revised as needed to reflect the current plant configuration
- In the case of a large leak, the water level would drop below 15 ft in about 24 hours after the initiation of the event
- It is assumed that a fraction of the large leaks are not isolable, but that this fraction is dominated by the SFP makeup system failure rate
- The leak location is such that the SFP cooling system is failed
- The capacity of the SFP makeup system is not sufficient to overcome the rate of boil-off

1.6.5.3. Quantification

Human Error Probabilities

Four HEPs were developed to cover both early and late detection cases, including diagnosis, performing isolation, and starting a makeup pump.

The HEP for diagnosis was the same for both early and late cases (HEP-LGLK-DIAG-E), and was given a value of 4.0E-5 using the ASP method.

Two HEPs for isolation were developed for early and late detection, HEP-LEAK-ISO-E and HEP-LEAK-ISO-L, respectively. For the early case, a value of 5.0E-5 was derived. For the late case, a value of 5.0E-3 was derived.

Finally, two HEPs for starting an SFP makeup pump were developed for early and late detection. HEP-MKUP-START (early) was given a value of 2.5E-4 using the ASP method. HEP-MKUP-START (late) was assumed to be 1.0, because there is not enough time available to establish makeup, or the pool may have begun boiling.

Non-HEP Probabilities

The NRC draft report assigned a value of 0.1 for failure of the SFP makeup system (SFP-REGMKUP-F), based on a two-unit site with a shared spent fuel pool, and one unit in a refueling outage (from INEL-96/0334 – Ref 3). Unavailability of a single SFP makeup system at a critical plant was assumed to be 5.0E-2. Because the leak has been isolated in this case, and the operator has several hours and no other tasks demanding his attention, we recommend the latter. This basic event also includes the second set of operator actions described above.

1.6.5.4. Changes from NRC Draft report

Basic Event	INEEL	NRC Draft Report
HEP-LGLK-DIAG-E	4.0E-5	1.0E-2 (HEP-INV-MKUP-E)
HEP-LEAK-ISO-E	5.0E-5	
HEP-LEAK-ISO-L	5.0E-3	
HEP-MKUP-START (early)	2.5E-4	
HEP-MKUP-START (late)	1.0	
SFP-REGMKUP-F	5.0E-2	0.1

1.6.6. Top Event OIL – Operator Initiates SFP Makeup System

1.6.6.1. Event Description and Timing

This top event represents the unavailability of the SFP makeup system as a result of operator error or hardware failure, and is represented by fault tree GLIR181. The leak is small enough that isolation is not required for success. However, the operator may fail to recognize the need to provide makeup or may fail to initiate the system successfully, or the SFP makeup system itself could fail.

If the operator responds to the initiator early (i.e., CRA is successful), he would have somewhat less than 33 hours to terminate the event using the SFP makeup system. This is because the leak is assumed to disable the SFP cooling system. Under normal conditions, bulk pool boiling would begin at about 33 hours. With the loss of inventory, boiling would begin somewhat earlier.

If operator responds late (i.e., IND success), it is assumed that he would have about 17 hours to terminate the event using the SFP makeup system (33 hours less 16 hours).

1.6.6.2. Relevant Assumptions

- Operators are trained and receive training on the regular basis
- Training plans are revised as needed to reflect the current plant configuration
- In the case of small leak, the water level would drop below 15 ft in more than 48 hours after the initiation of the event
- The leak location is such that the SFP cooling system is failed
- The capacity of the SFP makeup system is not sufficient to overcome the rate of boil-off

1.6.6.3. Quantification

Human Error Probabilities

To establish SFP makeup, the operator would have 33 hours available in the case of an early response and 17 hours available in the case of late response. Success is defined as the operator starting the makeup pump and performing valve manipulation as needed. Because the time available to establish SFP makeup (minimum 17 hours) is expansive compared to the time required to perform the task (about 1 hour), only one operator error was quantified, although it includes both a diagnosis and an action component.

Operator failure to diagnose the need to start the SFP makeup system (event HEP-SMLK-DIAG-E) was assigned a value of 5.0E-6, using the ASP method. Similarly, the operator's failure to start the SFP makeup system (HEP-MKUP-START) was assigned a value of 2.5E-6.

Non-HEP Probabilities

The NRC draft report assigned a value of 0.1 for failure of the SFP makeup system (basic event SFP-REGMKUP-F), based on a two-unit site with a shared spent fuel pool, and one unit in a refueling outage (from INEL-96/0334 – Ref 3). Unavailability of a single SFP makeup system at a critical plant was assumed to be 5.0E-2. Because the leak is within the capacity of SFP makeup system, and the operator has several hours and no other tasks demanding his attention, we recommend the latter. This basic event also includes the second set of operator actions described above.

1.6.6.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-SMLK-DIAG-E	5.0E-6	2.0E-3 (HEP-INV-MKUP-SML)
HEP-MKUP-START	2.5E-6	
SFP-REGMKUP-F	5.0E-2	0.1

1.6.7. Top Event OMK - Operator Recovery Using Onsite Sources

1.6.7.1. Description and Timing

This top event represents the failure of the operator to initiate makeup using the firewater system, and is represented by three different fault trees: GLIR123, GLIR153, and GLIR183. There are two basic events in each fault tree: an operator failure to establish makeup, and unavailability of both pumps due to hardware failure. At this point, the SFP makeup system is not available (either it failed, or the operator failed to start it, or the leak is large and not isolated so that the SFP makeup system is insufficient). So the operator must use the firewater system to reestablish inventory because the capacity of the SFP makeup system is assumed to be inadequate (due to losses from boil-off and through leak).

For a large leak with early indication and response, the time available to establish makeup using the firewater system would be about 60 hours (24 hours to drain down 15 ft and begin bulk boiling, then 36 hours for boil-off to reach 3 ft above the top of fuel). This situation is modeled by fault tree GLIR123.

If the large leak were discovered late (i.e., IND successful), the time available to establish makeup using FW system would be less than 36 hours (60 hours less 3 shifts or about 24 hours). This situation is modeled by fault tree GLIR153.

In the case of a small leak, the time required to decrease water level below the SFP suction level (15 ft) is assumed to be 48 hours. It is assumed that bulk boiling would begin sometime during this draining period. The time required to boil off the water level to 3 ft above the top of fuel is estimated to be an additional 36 hours. Therefore, the time available to establish makeup is between 60 and 84 hours, depending on whether the event is discovered early or late. Because the minimum time is expansive

compared to the time required to execute the action, 60 hours is assumed to be available to establish makeup using the firewater system. This situation is modeled by fault tree GLIR183.

1.6.7.2. Relevant Assumptions

- Operators are trained and receive training on a regular basis
- Training plans are revised as needed to reflect the current plant configuration
- It takes two shifts (16 hours) to contact maintenance personnel, make a diagnosis, and get new parts
- It is assumed that 1/10 of the large leaks have leak rates greater than the firewater system capacity

1.6.7.3. Quantification

Human Error Probabilities

Human errors are involved in both of the cases used to model this top event.

For large leaks, basic event HEP-LGLK-DIAG-L represents a second opportunity for the operator to diagnose the leak. This event is dependent on HEP-LGLK-DIAG-E (see top event OIS), and it has a conditional probability of 0.05.

For small leaks, basic event HEP-SMLK-DIAG-L represents a second opportunity for the operator to diagnose the need to provide makeup using the firewater system. This event is dependent on HEP-SMLK-DIAG-E (see top event OIL), and it has a conditional probability of 0.05.

The final HEP represents the operator's failure to makeup inventory using the firewater system (HEP-FW-START). The operator has 60 hours to establish the makeup using either firewater pump. Success is defined as operator's ability to start the diesel or electric firewater pump and secure a hose in the spent fuel pool area. There are multiple shifts available to start the pump, and it is assumed that the task requires about 1 hour. The ASP method generated a value of 1.0E-5 for this event.

Non-HEP Probabilities

In the NRC draft report, failure probabilities for electric and diesel firewater pumps to start and run are 6.0E-2 and 0.18, respectively. The pump may be required to run at most 8 hours, given that the water inventory drops by 20 ft (i.e., 3 ft from the top of the fuel). For the electric firewater pump, we recommend 3.7E-3 failure probability for the pump to start and run (Ref 3).

Basic event FP-MKUP-FTF represents failure of the firewater system as a result of both diesel and electric pumps failing to start and run. As discussed earlier, the time available to start the firewater system in the case of a loss of coolant inventory event is 36 hours (because the operator will delay the use of firewater until inventory drops below the SFP cooling system suction). If both firewater pumps fail to start and run, the operator will attempt to repair one pump. Assuming that it takes another two shifts (16 hours) to contact maintenance personnel, to perform the diagnosis, and to get new parts, then the operator has 20 hours (36 hours less 16 hours) to perform repairs and start the system. Assuming a 10-hr mean time to repair, the probability of failure to repair the pump would be Exp [-(1/10) × 16] = 0.20. Therefore, a probability of the diesel and electric firewater pumps failing to start and run would be 0.18 × 3.7E-3 × 0.20 = 1.3E-4.

Additionally, a basic event (SFP-250GPM-F) has been added to the fault tree to represent the fraction of large leaks that are greater than the makeup capacity of the firewater system (i.e., about 250 gpm). In this case the operator has failed to isolate the leak, so the only recourse left to the operator is to bring in offsite sources of makeup. It is assumed that 1/10 of the large leaks will be larger than the firewater system capacity.

Note that this approach neglects the possibility of a sort of feed-and-bleed approach whereby cooling and inventory are maintained by adding firewater, while inventory continues to flow out the leak. This feed and bleed technique could be effective for any size leak, given that we've assumed that the leak is no

more than 15 feet below the nominal pool level. However, the fact that we do not credit this technique allows for the fact that a leak may occur below the 15-ft level.

This new event is ANDed with the failure to isolate event (HEP-INV-MKUP-E) from OIS (Section 1.6.5.3). These two events combined represent the inadequacy of the firewater system in the case for which the leak rate is greater than 250 gpm and the operator fails to isolate.

1.6.7.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-LGLK-DIAG-L	5.0E-2	N/A
HEP-SMLK-DIAG-L	5.0E-2	
HEP-FW-START	1.0E-5	1.0E-2 (HEP-ALTCL-LP-E)
FP-MKUP-FTF	1.3E-4	1.0E-2
SFP-250GPM-F	0.1	N/A

1.6.8. Top Event OFD – Operator Recovery Using Offsite Sources

1.6.8.1. 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. Although loss of inventory sequences allow less time for recovery than do other types of initiators, 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. This top event is quantified using fault tree GFFT111.

1.6.8.2. Relevant Assumptions

- The operator has at least 60 hours from the onset of the initiator to provide makeup and inventory cooling
- The operator has failed to restore the SFP cooling system, and has attempted to start both firewater pumps
- There is sufficient time to recognize the need for and provide external sources of makeup

1.6.8.3. Quantification

Human Error Probabilities

Event HEP-OFFSITE-DIAG represents the operator's failure to diagnose the need for offsite resources, given that he has failed to diagnose the need for makeup in top events OIS or OIL, and OMK. It has been given a value of 1.0, based on the dependency on the previous events. The operator will not have any additional cues at this point.

If the operator has successfully diagnosed the need for makeup in early top events (OIS, OIL, or OMK), then he must recognize that extreme measures must be taken to provide makeup to the SFP given that makeup and firewater systems have failed. He has had ample time up to this point to attempt recovery of the diesel firewater pump. This event (REC-INV-OFFSITE) represents the failure of the operator to bring in offsite resources to mitigate the event. Success implies that offsite resources are brought to bear on the situation, but no effort is made to quantify hardware failures or human errors related to execution of any actions. It is assumed that once the operator is no longer acting alone, once regional authorities are aware of the situation, the sequence will be successfully terminated.

The ASP methodology generated a failure probability for this action of 1.0E-4. In the NRC draft report, this event was represented by three different basic events: REC-INV-OFFSITE1, REC-INV-OFFSITE2, and REC-INV-OFFSITE3.

1.6.8.4. Changes from NRC Draft Report

Basic Event	INEEL	NRC Draft Report
HEP-OFFSITE-DIAG	1.0	N/A
REC-INV-OFFSITE	1.0E-4	1.0E-1 (REC-INV-OFFSITE1) 2.0E-1 (REC-INV-OFFSITE2) 5.0E-2 (REC-INV-OFFSITE3)

1.6.9. Summary

Table 5 presents a summary of basic event changes relative to the NRC draft report.

Table 5 Basic Event Changes from the NRC Draft Report for the Loss of Inventory Event Tree

Basic Event Name	Description	INEEL	NRC	Remarks-Assumptions in INEEL analysis
HEP-RES-ALARM	Operator fails to respond to a signal indication in the control room	3.0E-3	3.0E-3	Single alarm, procedures and training
REC-WLKDWN-LOI-L	Failure to observe fast level decrease during walkdowns (large leak)	1.0E-5	0.1	Active monitoring, procedures, training, shift change over discussion
REC-WLKDWN-LOI-S	Failure to observe slow level decrease during walkdowns (small leak)	1.0E-5	1.0E-2	Active monitoring, procedures, training, shift change over discussion
HEP-LGLK-DIAG-E	Operator fails to diagnose large leak and need to isolate – early	4.0E-5	—	procedures, training, shift change over discussion (Time available ~ 24 hrs)
HEP-LGLK-DIAG-L	Operator fails to diagnose large leak and need to isolate-late (dependency on HEP-LGLK-DIAG-E)	5.0E-2	—	procedures, training, shift change over discussion (Time available ~ 8 to 12 hrs)
HEP-LEAK-ISO-E†	Operator fails to isolate large leak –early (dependency on HEP-RES-ALARM)	5.0E-5	—	procedures, training, shift change over discussion (Time available ~ 24 hrs)
HEP-LEAK-ISO-L†	Operator fails to isolate large leak –late (dependency on REC-WLKDWN-LOI-L)	5.0E-3	—	procedures, training, shift change over discussion (Time available ~ 8 to 12 hrs)
HEP-SMLK-DIAG-E	Operator fails to diagnose need to start SFPC makeup (dependency on HEP-LGLK-DIAG-E)	5.0E-6	—	procedures, training, shift change over discussion (Time available ~ 60 hrs)
HEP-SMLK-DIAG-L	Operator fails to diagnose need to start FW (dependency on HEP-SMLK-DIAG-E)	5.0E-2	—	procedures, training, shift change over discussion (Time available ~ 60 hrs)
HEP-MKUP-START†	Operator fails to start SFPC makeup system Large leak- Early Large leak - Late Small leak	 2.5E-4 1.0 5.0E-6	 0.1 0.1 1.0E-2	procedures, training, shift change over discussion -
HEP-FW-START†	Operator fails to start FW pump and provide alignment	1.0E-5	1.0E-2	Procedures, training, and equipment provided. Extra staff available. (NRC draft report basic event name HEP-ALTCL-LP-E)
FP-MKUP-FTF	Failure of diesel FW pump system Failure of electric FW pump system Operator fails to repair FW system	1.8E-1 3.7E-3 2.5E-2	1.8E-1 6.0E-2 —	Based on INEL-96/0334 Based on 10 hrs MTTR and 37 hrs to repair

† In the NRC draft report isolation and establishment of makeup events are modeled as one event: HEP-INV-MKUP-E for large leak and early recognition, HEP-INV-MKUP-L for large leak and late recognition, and HEP-INV-MKUP-SML for small leak.

Basic Event Name	Description	INEEL	NRC	Remarks-Assumptions in INEEL analysis
HEP-OFFSITE-DIAG	Operator fails to diagnoses need for offsite resources (dependency on early diagnoses failures)	1.0	—	Procedures and training provided.
REC-INV-OFFSITE1 REC-INV-OFFSITE2 REC-INV-OFFSITE3	Operator fails to provide alternate sources of cooling from offsite	1.0E-4	0.1 0.2 5.E-2	Procedures, training, and equipment provided. Extra staff available.

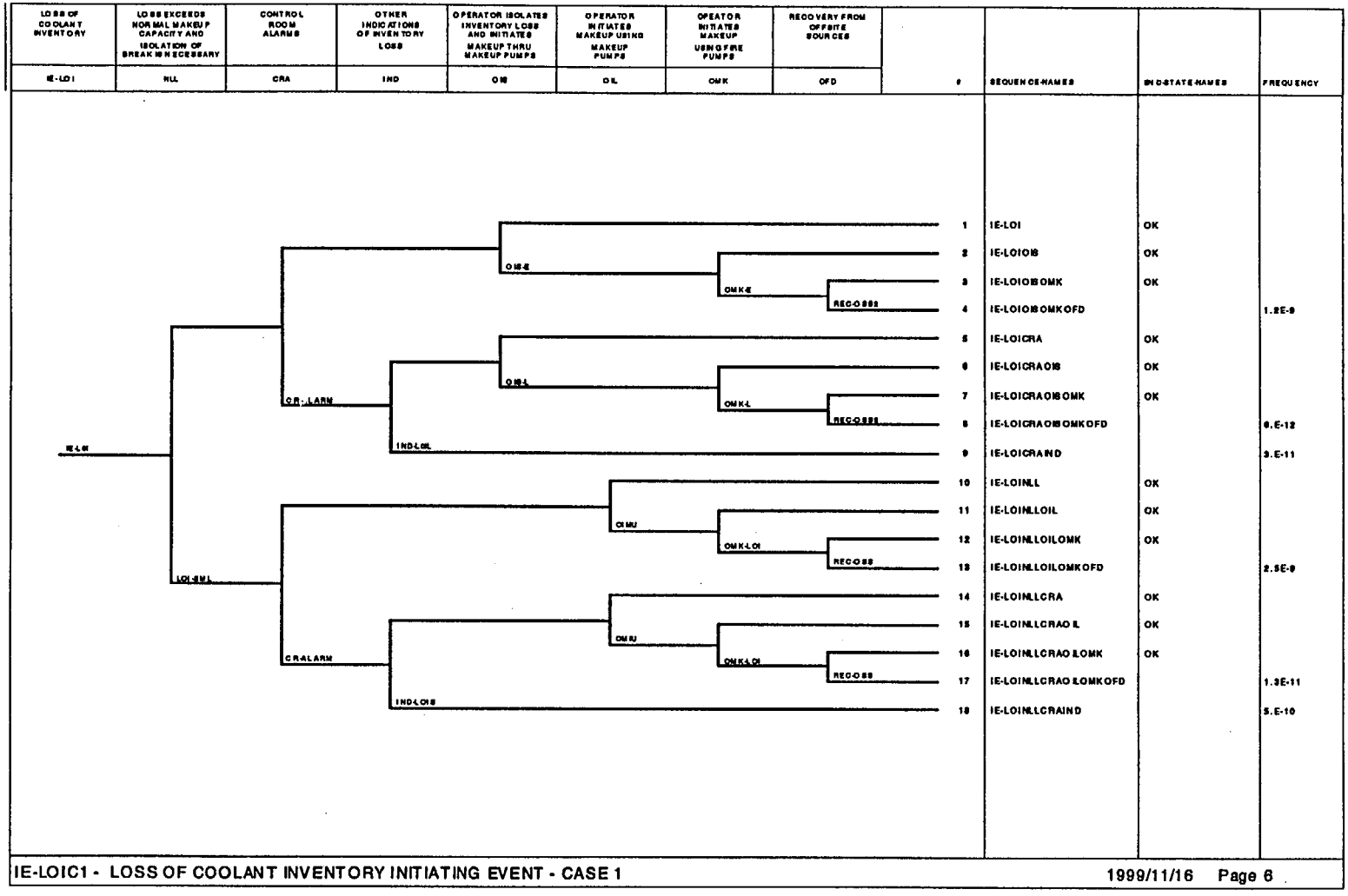

Figure 5 Loss of Inventory Event Tree

2. RESULTS

See Table 6.

Table 6 Sequence Results

Sequence ID		Sequence Description	End State Frequency (1/yr)*		Remarks
NRC	INEEL		NRC	INEEL	
FIR-4	FIR-4	IE-FIRE * Failure to suppress fire * Failure to provide FW using Diesel-driven pump * failure to recover using offsite resources	8.6E-7	3.0E-11	Failure to suppress fire leads to loss of SFPC and electric FW pumps.
LOC-4	LOC-4	IE-LOC * Failure to restart SFPC * Failure to provide FW using diesel or electrical pump * Failure to recover using offsite resources	6.0E-11	1.5E-9	Loss of SFPC system
LOC-8	LOC-8	IE-LOC * Failure of control room alarms or fail to respond * Failure to restart SFPC * Failure to provide FW using diesel or electrical pump * Failure to recover using offsite resources	<1.0E-12	8.0E-12	Loss of SFPC system
LOC-9	LOC-9	IE-LOC * Failure of control room alarms or operator respond * Failure to discover LOC or respond during walkdown	1.5E-7	1.5E-10	Loss of SFPC system
LP1-11	LP1-4	IE-LP1 * Power recovered * Failure to restart SFPC * Failure to provide FW using diesel or electrical pump * Failure to recover using offsite resources	3.7E-7	<1.0E-12	Loss of offsite power from plant centered and grid related events
LP1-13	LP1-7	IE-LP1* Failure to recover power * Failure to provide FW using diesel pump * Failure to recover using offsite resources	7.6E-7	<1.0E-12	Loss of offsite power from plant centered and grid related events
LP2-11	LP2-4	IE-LP2 * Power recovered * Failure to restart SFPC * Failure to provide FW using diesel or electrical pump * Failure to recover using offsite resources	3.2E-8	<1.0E-12	Loss of offsite power from severe weather
LP2-13	LP2-7	IE-LP2* Failure to recover power * Failure to provide FW using diesel pump * Failure to recover using offsite resources	1.3E-6	6.3E-11	Loss of offsite power from severe weather
LOI-4	LOI-4	IE-LOI * Large leak * Failure to provide makeup using makeup system * Failure to provide FW using diesel or electrical pump * Failure to recover using offsite resources	6.6E-7	1.2E-9	Operator responds to control room alarm

* End state is defined as the water level dropping to 3 ft above the top of the fuel.

Sequence ID		Sequence Description	End State Frequency (1/yr)*		Remarks
NRC	INEEL		NRC	INEEL	
LOI-8	LOI-8	IE-LOI* Large leak * Failure of control room alarm or fail to respond * Failure to provide makeup using makeup system * Failure to provide FW using diesel or electrical pump * Failure to recover using offsite resources	2.8E-8	6.0E-12	Operator fails to respond alarm, leak is discovered during walkdown
LOI-9	LOI-9	IE-LOI* Large leak * Failure of control room alarm or fail to respond * Failure to discover leak during walkdowns	3.0E-7	3.0E-11	
LOI-13	LOI-13	IE-LOI* Small leak * Failure to provide makeup using makeup system * Failure to provide FW using diesel or electrical pump * Failure to recover using offsite resources	1.4E-6	2.5E-9	Operator responds to control room alarm
LOI-17	LOI-17	IE-LOI* Small leak * Failure of control room alarm or fail to respond * Failure to provide makeup using makeup system * Failure to provide FW using diesel or electrical pump * Failure to recover using offsite resources	7.1E-9	1.3E-11	Operator fails to respond alarm or control room alarm fails, leak is discovered during walkdown
LOI-18	LOI-18	IE-LOI* Small leak * Failure of control room alarm or fail to respond * Failure to discover leak during walkdowns	4.7E-7	3.0E-10	

3. REFERENCES

1 NUREG-1275, "Operating Experience Feedback Report – Assessment of Spent Fuel Cooling," Volume 12, U.S. Nuclear Regulatory Commission, February 1997

2 NUREG/CR-1740, "Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at U.S. Commercial Nuclear Power Plants from January 1, 1976 to December 31, 1978," U.S. Nuclear Regulatory Commission, May 1981

3 INEL-96/0334, "Loss of Spent Fuel Pool Cooling PRA: Model and Results," Idaho National Engineering and Environmental Laboratory, September 1996

4 EPRI TR-100370,"Fire-Induced Vulnerability Evaluation (FIVE)," EPRI, April 1992

5 NSAC-181, "Fire Requantification Studies," EPRI, March 1993

6 Draft Regulatory Guide DG-1069, "Fire Protection Program for Nuclear Power Plants During Decommissioning and Permanent Shutdown," U.S. Nuclear Regulatory Commission, July 1998

7 IEEE ANSI Std

8 NUREG/CR-5496

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

10 Technical Letter ORNL/NRC/LTR-89/11, "Revised LOOP Recovery and PWR Seal LOCA Models," U.S. Nuclear Regulatory Commission, August 1989

11 NUREG/CR-5032