

Appendix 2.0 Assessment of Spent Fuel Pool Risk at Decommissioning Plants

Introduction

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shut down and the reactor is defueled, most of the accident sequences that normally dominate operating reactor risk are no longer applicable.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

The staff's assessment found that the frequency of spent fuel uncover leading to a zirconium fire at decommissioning spent fuel pools is on the order of 3×10^{-6} per year when a utility follows certain industry commitments and certain of our recommendations. This frequency is made up of contributors from a detailed risk assessment of initiators (3.4×10^{-7} per year), both internal and external, and a quasi-probabilistic contribution from seismic events ($< 3 \times 10^{-6}$ per year) that have ground motions many times larger than individual site design basis earthquake ground motions (and higher uncertainty). It was also determined that if these commitments and recommendations are ignored, the estimated frequency of a zirconium fire could be significantly higher. Section 4 of this report discusses the steps necessary to assure that a decommissioning plant operates within the bounds assumed in the risk assessment.

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

First, the staff examined whether or not it was possible from a deterministic view point for a zirconium cladding fire to occur. Zirconium fires were chosen as the key factor because radionuclides require an energetic source to transport them off-site if they are to have a significant health effect on local (first few miles outside the exclusion area) and more distant populations. Deterministic evaluations (see Appendix 1) indicate that zirconium cladding fires cannot be ruled out for loss of spent fuel pool cooling for fuel that has been shut down and removed from an operating reactor within approximately five years¹. The consequence analysis (Appendix 4) indicates that zirconium cladding fires could give off-site doses that the NRC would consider unacceptable. To assess the risk during the period of vulnerability to zirconium cladding fires, the staff initially performed a broad preliminary risk assessment, which modeled many internal and external initiating events. The preliminary risk assessment was made

¹This estimate can be significantly shorter or perhaps somewhat longer depending on fuel enrichment, fuel burnup, and configuration of the fuel in the spent fuel pool.

433

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

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

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

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

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

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

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

1.0 Introduction

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

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

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

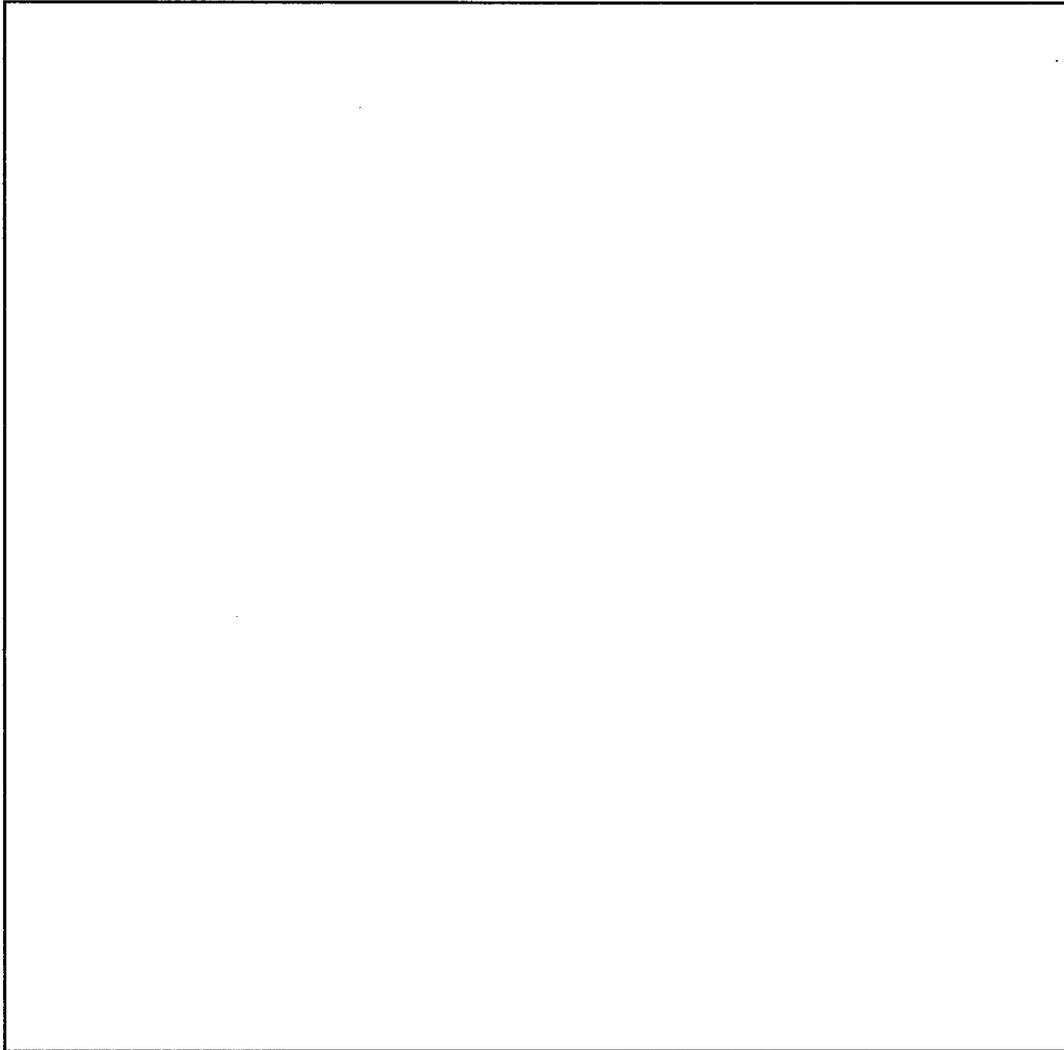
- loss of spent fuel pool cooling
- fire leading to loss of spent fuel pool cooling
- loss of off-site power due to plant centered and grid related causes
- loss of off-site power due to severe weather
- non-catastrophic loss of spent fuel pool inventory

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

2.0 System Description

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

Figure 2.1 Simplified Diagram of Spent Fuel Pool Cooling and Inventory Make-up Systems



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

3.0 Methodology

3.1 Logic Model

This section summarizes the spent fuel pool PRA model developed in this study. The description of the modeling approach and key assumptions is intended to provide a basis for interpreting the results in Sections 4 and 5. The event trees and fault trees presented in this report are meant to be generic enough to apply to many different configurations. The fault trees are documented in Attachment A to this appendix. An example of the HRA worksheet used for this analysis is presented in Attachment B.

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

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

3.2 HRA Methodology

3.2.1 Introduction

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

The objective of the HRA analysis in this PRA is to assess whether the design features and operational practices assumed can be argued to suggest that the non-response probabilities should be low. The design features include the physical plant characteristics (e.g., nature and

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

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

3.2.2 Analysis Approach

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

Examples of the positive aspects are:

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

Examples of the negative aspects are:

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

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

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

3.2.3 Human Performance Issues

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

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

- Plant personnel must be able to perform the actions required to maintain cooling of and/or add water to the spent fuel pool (Response Implementation).

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

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

3.2.3.1 Awareness/Detection of Deviant Conditions

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

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

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

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

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

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

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

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

3.2.3.2 Situation Assessment and Response Planning

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

The types of procedures that might be available are:

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

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

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

In addition:

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

3.2.3.3 Response Implementation

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

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

3.2.4 Quantification Method

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

- The Technique for Human Error Prediction (THERP, Ref. 8). This method was used to quantify the initial recognition of the problem. Specifically, the annunciator response model (Table 20-23) was used for response to alarms. The THERP approach was also used to assess the likelihood of failure to detect a deviant condition during a walk-down, and also the failure to respond to a fire. While this method was developed over twenty years ago, it is still regarded as an appropriate method for the types of HEPs for which it is being used in this analysis.
- The Exponential Repair Model (while not strictly a human reliability model) was applied to calculate the probability of failure associated with the repair of systems and components in this analysis. This method is described in the main body of the report. In cases where dependency exists with prior repair tasks, the dependency model used in THERP was used to assess the impact of that dependency.
- The Simplified Plant Analysis Risk Human Error Analysis Method (SPAR HRA, Ref. 9) was employed for all other HEPs. This model was chosen because it includes an appropriate level of detail in terms of performance shaping factors and error modes (cognition and execution) given the lack of detailed knowledge about expected plant practices and designs. The PSFs used in the model allowed the impact of the NEI commitments and additional staff assumptions to be incorporated explicitly into the evaluation.

3.3 Other Inputs to the Risk Model

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

bulk boiling to begin in the pool, or on the time it takes for the level in the pool to fall to the level of the fuel pool cooling system suction, or to a height of approximately 3 ft above the fuel, as appropriate to the definition of the corresponding human failure event.

It takes a relatively long time to uncover the fuel if the initiating event does not involve a catastrophic failure of the pool. This is due to the large amount of water in a spent fuel pool, the large specific heat of water, and the large latent heat of vaporization for water. Calculations for a typical-sized spent fuel pool yield the results in Table 3.1. These results are based on the following assumptions:

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

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

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

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

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

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

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

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

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

$$133 \text{ hrs} - \left(33 \text{ hrs} + \frac{2 \text{ ft}}{0.2 \text{ ft / hr}} \right) = 133 - 43 \text{ hrs} = 90 \text{ hrs}$$

3.4 General Assumptions

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

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

performed and administrative controls for equipment out of service will be implemented to provide added assurance that the components would be available if needed.

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

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

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

- The only significant technical specification applicable to SFPs is the requirement for radiation monitors to be operable when fuel is being moved. There are no technical specifications requirements for the cooling pumps, make-up pumps, firewater pumps, or any of the support systems.
- There are multiple sources of water for make-up via the firewater pumps or fire engine.
- Generic industry data were used for initiating event frequencies for the loss of off-site power, the loss of pool cooling, and the loss of coolant inventory.
- For the purposes of timing, the transfer of the last fuel from the reactor to the SFP is assumed to have occurred one year previously.

4.0 Model Development

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

4.1 Loss of Cooling Event Tree

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

4.1.1 Initiating Event LOC – Loss of Cooling

4.1.1.1 Event Description

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

4.1.1.2 Quantification

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

4.1.2 Top Event CRA – Control Room Alarms

4.1.2.1 Event Description and Timing

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

instrumentation to alarm given that SFP cooling has been lost, and the operators fail to respond to the alarm, respectively.

4.1.2.2 Relevant Assumptions

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

4.1.2.3 Quantification

Human Error Probabilities

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

Hardware Failure Probabilities

The value used for local faults leading to alarm channel failure (event SPC-LVL-LOP, 2.0E-3) was estimated based on information in reference 12. This event includes failure of instrumentation and local electrical faults.

4.1.2.4 Basic Event Probabilities

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

4.1.3 Top Event IND – Other Indications of Loss of Cooling

4.1.3.1 Event Description and Timing

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

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

4.1.3.2 Relevant Assumptions

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

Figure 4.1 Loss of spent fuel pool cooling system event tree

4.1.3.3 Quantification

Human Error Probabilities

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

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

4.1.3.4 Basic Event Probabilities

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

4.1.4 Top Event OCS – Operator Recovery of Cooling System

4.1.4.1 Event Description and Timing

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

The initial cause of the loss of cooling could be the failure of a running pump in either the primary or the secondary system, in which case the response required is simply to start the redundant pump. However, it could also be a more significant failure, such as a pipe break or a

heat exchanger blockage. To simplify the model, it has been assumed that a repair is necessary. While this is conservative, it does not unduly bias the conclusions of the overall study.

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

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

4.1.4.2 Relevant Assumptions

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

4.1.4.3 Quantification

Human Error Probabilities

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

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

where

λ = (inverse of mean time to repair)

t = available time

In the case where discovery was from the control room, probability of failure to repair SFPC system event, HEP-COOL-REP-E, would be 0.18 based on 17 hours available to repair.

In the case that the discovery was due to operator walk-down (HEP-COOL-REP-L), it is assumed that there is not enough time available to repair and restart the SFP make-up system in time to prevent bulk boiling, and the event has been assigned a value of 1.0.

4.1.4.4 Basic Event Probabilities

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

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

4.1.5.1 Event Description and Timing

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

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

4.1.5.2 Relevant Assumptions

- The operators have 88 hours to provide make-up.
- The operators will avoid using raw water (e.g., water not chemically controlled) if possible.
- The boil-off rate is assumed to be higher than the SFP make-up system capacity.
- The operators are aware that they must use raw water to refill the pool once the level drops to below the suction of the cooling system and the pool begins boiling, since the make-up system cannot compensate for the boiling.
- For repair of failed pumps, it is assumed that it takes 16 hours to contact maintenance personnel, identify the problem, and get new parts.

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

4.1.5.3 Quantification

Human Error Probabilities

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

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

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

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

Hardware Failure Probabilities

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

4.1.5.4 Basic Event Probabilities

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

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

4.1.6.1 Event Description and Timing

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

4.1.6.2 Relevant Assumptions

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

- Off-site resources are familiar with the facility.

4.1.6.3 Quantification

Human Error Probabilities

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

4.1.6.4 Basic Event Probability

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

4.1.7 Summary

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

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

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

Basic Event Name	Description	Basic Event Probability
IE-LOC	Loss of SFP cooling initiating event	3.0E-3
HEP-DIAG-ALARM	Operators fail to respond to a signal indication in the control room	3.0E-4

HEP-WLKDOWN-LSFPC	Operators fail to observe the loss of cooling in walk-downs (independent case)	1.0E-5
HEP-WLKDOWN-DEPEN	Operators fail to observe the loss of cooling in walk-downs (dependent case)	5.0E-2
HEP-COOL-REP-E	Repair crew fails to repair SFPC system	1.8E-1
HEP-COOL-REP-L	Repair crew fails to repair SFPC system - Late	1.0
HEP-RECG-FWSTART	Operators fail to diagnose need to start the firewater system	2.0E-5
HEP-RECG-FWSTART-L	Operators fail to diagnose need to start firewater system - dependent case	5.0E-2
HEP-FW-START	Operators fail to start firewater pump and provide alignment	1.0E-5
HEP-FW-REP-DEPEN	Repair crew fails to repair firewater system - dependent case	5.0E-2
HEP-INV-OFFSITE	Operators fail to provide alternate sources of cooling from off-site	5.0E-2
FP-2PUMPS-FTF	Failure of firewater pump system	6.7E-4
SPC-LVL-LOP	Local faults leading to alarm channel failure	2.0E-3

4.2 Internal Fire Event Tree

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

4.2.1 Initiating Event FIR – Internal Fire

4.2.1.1 Event Description and Timing

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

4.2.1.2 Relevant Assumptions

- Fire ignition frequencies from operating plants are assumed to be applicable at the SFP facility.

- Ignition sources from welding and cutting are expected to be insignificant. The facility configuration is expected to be stable, negating the need for modification and fabrication work requiring welding and cutting.

4.2.1.3 Quantification

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

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

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

Figure 4.2 Fire initiating event tree

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

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

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

4.2.1.4 Basic Event Probability

Basic Event	Basic Event Probability
IE-FIRE	3.0E-3

4.2.2 Top Event CRA – Control Room Alarms

4.2.2.1 Event Description and Timing

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

4.2.2.2 Relevant Assumptions

- The SFP area is equipped with fire detectors which are alarmed in the control room. However, the area is not equipped with an automatic fire suppression system.
- Fire alarms will be activated in the control room within a few minutes of the initiation of a fire.
- Regular maintenance and testing is performed on the fire detection system and on the control room annunciators.
- Procedures are available to guide operator response to a fire, and plant operators are trained in these procedures (NEI commitment no. 2).

4.2.2.3 Quantification

Human Error Probabilities

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

Hardware Failure Probabilities

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

4.2.2.4 Basic Event Probabilities

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

4.2.3 Top Event IND – Other Indications of Loss of Cooling

4.2.3.1 Event Description and Timing

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

4.2.3.2 Relevant Assumptions

- Operators perform walk-downs once per shift (every 8 to 12 hours) and walk-downs are required to be logged.
- If the fire is discovered during the walk-down, the SFPC system is assumed to be damaged to the extent where repair will not be feasible within a few days.
- Local instrumentation and alarms are destroyed in a fire which is not extinguished within 20 minutes.
- Procedures are available to guide plant operators for off-normal conditions, and

operators are trained in these procedures (NEI commitment no. 2).

4.2.3.3 Quantification

Human Error Probability

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

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

4.2.3.4 Basic Event Probability

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

4.2.4 Top Event OSP – Fire Suppression

4.2.4.1 Event Description and Timing

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

4.2.4.2 Relevant Assumptions

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

4.2.4.3 Quantification

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

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

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

(2) Scenarios can be postulated where the fire damage state is less severe than that described above (e.g., fire damage to the running cooling pump, with the other pump undamaged, and with off-site power available). These scenarios can be subsumed into the "Loss of Cooling" event, and SFP cooling "recovery" in these cases would be by use of the undamaged pump train.

4.2.4.4 Basic Event Probability

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

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

4.2.5.1 Event Description and Timing

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

4.2.5.2 Relevant Assumptions

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

4.2.5.3 Quantification

Human Error Probabilities

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

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

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

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

Hardware Failure Probabilities

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

4.2.5.4 Basic Event Probabilities

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

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

4.2.6.1 Event Description and Timing

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

4.2.6.2 Relevant Assumptions

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

4.2.6.3 Quantification

Human Error Probabilities

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

calculated HEP directly, a low level of dependence to account for the possible detrimental effects of the failure to complete prior tasks successfully.

4.2.6.4 Basic Event Probability

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

4.2.7 Summary

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

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

Table 4.2 Basic Event Summary for the Internal Fire Event Tree

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

SFP-FIRE-LOA	Electrical faults causing loss of alarms	2.0E-3
SFP-FIRE-DETECT	Failure of fire detectors	5.0E-3

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

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

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

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

4.3.1.1 Event Description

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

4.3.1.2 Quantification

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

4.3.2 Top Event OPR – Off-site Power Recovery

4.3.2.1 Event Description and Timing

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

NUREG-1032 (Ref. 17) classified LOSP events into plant-centered, grid-related, and severe-

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

4.3.2.2 Relevant Assumptions

- Trained electricians may not be present at the site for quick recovery from plant-centered events.

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

4.3.2.3 Quantification

The basic event that represents recovery of off-site power for plant-centered and grid-related LOSP is REC-OSP-PC. The data in NUREG/CR-5496 indicates that one event in 102 plant centered events resulted in a loss for greater than 24 hours, and all 6 of the grid centered events were recovered in a relatively short time. The majority of the plant-centered events were recovered within 7 hours, so even if there is a delay in bringing repair personnel on-site, there is a high probability of recovering off-site power within 24 hours. Therefore a non-recovery probability of 1E-02 is assumed.

4.3.2.4 Basic Event Probability

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

4.3.3 Top Event OCS – Cooling System Restart and Run

4.3.3.1 Event Description and Timing

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

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

4.3.3.2 Relevant Assumptions

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

4.3.3.3 Quantification

Human Error Probabilities

Event HEP-SFP-STR-LP1 represents operator failure to restart/realign the SFP cooling system in 9*hours. The operator can restart the previously running pump and may not have to make any valve alignment. If he decides to restart the standby pump he may have to make some valve alignment. The response part of the error was quantified using SPAR. The relevant

performance shaping factors for this event included expansive time, high stress due to previous failures, moderately complex task due to potential valve lineups, highly trained staff, good ergonomics (well laid out and labeled matching procedures), and good work process.

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

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

Non-HEP Probabilities

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

4.3.3.4 Basic Event Probabilities

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

4.3.4 Top Event OMK – Operator Recovery Using Make-up Systems

4.3.4.1 Event Description and Timing

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

4.3.4.2 Relevant Assumptions

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

4.3.4.3 Quantification

Human Error Probabilities

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

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

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

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

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

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

Hardware Failure Probabilities

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

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

4.3.4.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-RECG-DEPEN	5.0E-02
HEP-RECG-FWSTART	2.0E-5
HEP-FW-START	1.0E-5
HEP-FW-REP-DEPEN	5.0E-2
HEP-FW-REP-NODEP	1.0E-3
FP-2PUMPS-FTF	6.7E-4
FP-DGPUMP-FTF	1.8E-1

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

4.3.5.1 Event Description and Timing

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

4.3.5.2 Relevant Assumptions

- The operators have 88 hours to provide make-up and inventory cooling.
- Procedures and training are in place that ensure that off-site resources can be brought to bear (NEI commitments 2 and 4), and that preparation for this contingency is made when it is realized that it may be necessary to supplement the pool make-up.
- Procedures explicitly states that if the water level drops below a certain level (e.g., 15 ft below normal level) operator must initiate recovery using off-site sources.
- Operators have received formal training in the procedures.
- Off-site resources are familiar with the facility.

4.3.5.3 Quantification

Human Error Probabilities

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

4.3.5.4 Basic Event Probability

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

4.3.6 Summary

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

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

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

Basic Event Name	Description	Probability
IE-LP1	Loss of off-site power due to plant-centered or grid-related causes	8.0E-2
REC-OSP-PC	Recovery of off-site power within 24*hours	1.0E-2
HEP-DIAG-SFPLP1	Operators fail to diagnose loss of SFP cooling due to loss of off-site power	1.0E-6
HEP-FW-REP-DEPEN	Repair crew fails to repair firewater system - dependent case	5.0E-2
HEP-SFP-STR-LP1	Operators fail to restart and align the SFP cooling system once power is recovered	5.0E-6
HEP-RECG-FWSTART	Operators fail to diagnose need to start the firewater system	2.0E-5
HEP-RECG-DEPEN	Operators fail to recognize need to cool pool given prior failure	5.0E-02
HEP-FW-START	Operators fail to start firewater pump and provide alignment	1.0E-5
HEP-FW-REP-NODEP	Repair crew fails to repair firewater system	1.0E-3
SPC-PMP-CCF	SFP cooling pumps - common cause failure	5.9E-4
SPC-PMP-FTF-1	SFP cooling pump*1 fails to start and run	3.9E-3
SPC-PMP-FTF-2	SFP cooling pump*2 fails to start and run	3.9E-3
FP-2PUMPS-FTF	Failure of firewater pump system	6.7E-4
FP-DGPUMP-FTF	Failure of the diesel-driven firewater pump	1.8E-1
SPC-CKV-CCF-H	Heat exchanger discharge check valves-CCF	1.9E-5
SPC-CKV-CCF-M	SFP cooling pump discharge check valves-CCF	3.2E-5
SPC-HTX-CCF	SFP heat exchangers - CCF	1.9E-5
SPC-HTX-FTR	SFP heat exchanger cooling system fails	2.4E-4
SPC-HTX-PLG	Heat exchanger plugs	2.2E-5
SPC-PMP-CCF	SFP cooling pumps - CCF	5.9E-4
SPC-PMP-FTF-1	SFP cooling pump 1 fails to start and run	3.9E-3
SPC-PMP-FTF-2	SFP cooling pump 2 fails to start and run	3.9E-3

4.4 Severe Weather Loss of Off-site Power Event Tree

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

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

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

4.4.1.1 Event Description

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

4.4.1.2 Quantification

The LOSP frequency from severe weather events is $1.1E-2/\text{yr}$, taken from NUREG/CR-5496 (Ref. 16). This includes contributions from hurricanes, snow and wind, ice, wind and salt, wind, and one tornado event, all of which occurred at a relatively small number of plants. Therefore, for the majority of sites, this frequency is conservative, whereas, for a few sites it is non-conservative. Because of their potential for severe localized damage, tornados were analyzed separately in Appendix 2e.

4.4.2 Top Event OPR – Off-site Power Recovery

4.4.2.1 Event Description and Timing

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

4.4.2.2 Relevant Assumptions

- See section 4.4.2.3 below.

4.4.2.3 Quantification

Non-HEP Probability

NUREG-1032 (Ref. 17) classified LOSP events into plant-centered, grid-related, and severe-weather-related categories, because these categories involved different mechanisms and also seemed to have different recovery times. Similarly, NUREG/CE-5496 divides LOSP events into three categories and estimates different values of non-recovery as functions of time. A non-recovery probability within 24 hrs for the off-site power from the severe weather event was

estimated to be $2.0E-2$ to $<1.0E-4$ depending on the location of the plant. In the operating plant, recovery of off-site power may be very efficient due to presence of skilled electricians. In the decommissioned plant, the skilled electricians may not be present at the site. Therefore, for the purpose of this analysis, a non-recovery probability for off-site power due to severe weather event (REC-OSP-SW) of $2.0E-2$ is used.

4.4.2.4 Basic Event Probability

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

4.4.3 Top Event OCS - Cooling System Restart and Run

4.4.3.1 Event Description and Timing

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

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

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

4.4.3.2 Relevant Assumptions

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

4.4.3.3 Quantification

Human Error Probabilities

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

Event HEP-SFP-STR-LP2 represents operator failure to restart/realign the SFP cooling system in 9*hours. The operators can restart the previously running pump and may not have to make any valve alignment. If they decide to restart the standby pump they may have to make some valve alignment. This error was quantified using SPAR. The relevant performance shaping factors included expansive time, extreme stress due to severe weather, moderately complex task due to potential valve lineups and severe weather, poor ergonomics due to severe weather, and good work process.

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

Non-HEP Probabilities

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

4.4.3.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-DIAG-SFPLP2	1.0E-5
HEP-SFP-STR-LP2	5.0E-4
SPC-CKV-CCF-H	1.9E-5
SPC-CKV-CCF-M	3.2E-5

SPC-HTX-CCF	1.9E-5
SPC-HTX-FTR	2.4E-4
SPC-HTX-PLG	2.2E-5
SPC-PMP-CCF	5.9E-4
SPC-PMP-FTF-1	3.9E-3
SPC-PMP-FTF-2	3.9E-3

4.4.4 Top Event OMK – Operator Recovery Using Make-up Systems

4.4.4.1 Event Description and Timing

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

4.4.4.2 Relevant Assumptions

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

4.4.4.3 Quantification

Human Error Probabilities

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

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

HEP-FW-REP-NODSW represents the failure of the repair crew to repair a firewater pump for the scenario where power is not recovered. Note that we have assumed that since power is not recovered, the repair crew did not make any attempt to repair the SFPC system, and therefore no dependency was modeled in the failure to repair the firewater system. We assume that the operator will focus his recovery efforts on only one pump. Assuming that it takes two days (48* hours) before technical help and parts arrive, then the operator has 40*hours (88*hours less 48* hours) to repair the pump. Assuming a 10-hour mean time to repair, the probability of failure to repair the pump would be $\text{Exp}[-(1/10)*40] \approx 1.8\text{E-}2$. This event is modeled in the fault tree, LP2-OMK-L.

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

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

Non-HEP Probabilities

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

In the case of LP2-OMK-L, only the diesel-driven firewater pump is available, and its failure is

represented by basic event FP-DGPUMP-FTF.

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

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

4.4.4.4 Basic Event Probabilities

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

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

4.4.5.1 Event Description and Timing

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

4.4.5.2 Relevant Assumptions

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

- Off-site resources are familiar with the facility.

4.4.5.3 Quantification

Human Error Probability

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

4.4.5.4 Basic Event Probability

Basic Event	Basic Event Probability
HEP-INV-OFFST-SW	8.0E-2

4.4.6 Summary

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

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

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

Basic Event Name	Description	Basic Event Probability
IE-LP2	LOSP event due to severe-weather-related causes	1.1E-02
HEP-DIAG-SFPLP2	Operators fail to diagnose loss of SFP cooling due to loss of off-site power	1.0E-5

HEP-RECG-DEPEN	Failure to recognize need to cool pool given prior failure	5.0E-2
HEP-SFP-STR-LP2	Operators fail to restart and align the SFP cooling system once power is recovered	5.0E-4
HEP-RECG-FWST-SW	Operators fail to diagnose need to start the firewater system	1.0E-4
HEP-FW-START-SW	Operators fail to start firewater pump and provide alignment	1.0E-3
HEP-FW-REP-DEPSW	Repair crew fails to repair firewater system	7.0E-2
HEP-FW-REP-NODSW	Repair crew fails to repair firewater system	1.8E-2
HEP-INV-OFFST-SW	Operators fail to provide alternate sources of cooling from off-site	8.0E-2
REC-OSP-SW	Recovery of off-site power within 24*hours	2.0E-2
SPC-CKV-CCF-H	Heat exchanger discharge check valves - CCF	1.9E-5
SPC-CKV-CCF-M	SFP cooling pump discharge check valves - CCF	3.2E-5
SPC-HTX-CCF	SFP heat exchangers - CCF	1.9E-5
SPC-HTX-FTR	SFP heat exchanger cooling system fails	2.4E-4
SPC-HTX-PLG	Heat exchanger plugs	2.2E-5
SPC-PMP-CCF	SFP cooling pumps - common cause failure	5.9E-4
SPC-PMP-FTF-1	SFP cooling pump*1 fails to start and run	3.9E-3
SPC-PMP-FTF-2	SFP cooling pump*2 fails to start and run	3.9E-3
FP-2PUMPS-FTF	Failure of firewater pump system	6.7E-4
FP-DGPUMP-FTF	Failure of the diesel-driven firewater pump	1.8E-1

4.5 Loss of Inventory Event Tree

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

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

4.5.1 Initiating Event LOI – Loss of Inventory

4.5.1.1 Event Description and Timing

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

4.5.1.2 Relevant Assumption

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

4.5.1.3 Quantification

The data reviewed during the development of NUREG-1275 (Ref. 12) indicated fewer than one event per 100 years in which level decreased over one foot. This would give a frequency of 1E-02. However, it is assumed that the NEI commitments 6 and 7 when implemented will reduce this frequency by an order of magnitude or more. Thus the frequency is estimated as 1E-03 per year.

4.5.2 Top Event NLL – Loss Exceeds Normal Make-up Capacity

4.5.2.1 Event Description and Timing

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

4.5.2.2 Relevant Assumptions

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

4.5.2.3 Quantification

Non-HEP Probabilities

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

Figure 4.5 Loss of inventory event tree

4.5.3 Top Event CRA – Control Room Alarms

4.5.3.1 Event description and Timing

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

4.5.3.2 Relevant Assumptions

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

4.5.3.3 Quantification

Human Error Probabilities

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

Non-HEP Probabilities

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

4.5.3.4 Basic Event Probabilities

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

4.5.4 Top Event IND - Other Indications of Inventory Loss

4.5.4.1 Event Description and Timing

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

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

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

4.5.4.2 Relevant assumptions

- Operators have more than 40 hrs in the case of a large leak to take actions after the first alarm before the water level drops to the 3 ft above the top of fuel.
- SFP water level indicator is provided in the control room e.g., camera or digital readout.

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

4.5.4.3 Quantification

Human Error Probabilities

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

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

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

4.5.4.4 Basic Event Probabilities

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

4.5.5 Top Event OIS – Operator Isolates Leak and Initiates SFP Make-up

4.5.5.1 Event Description and Timing

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

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

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

4.5.5.2 Relevant Assumptions

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

4.5.5.3 Quantification

Human Error Probabilities

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

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

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

Hardware Failure Probabilities

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

4.5.5.4 Basic Event Probabilities

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

4.5.6 Top Event OIL - Operator Initiates SFP Make-up System

4.5.6.1 Event Description and Timing

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

4.5.6.2 Relevant Assumptions

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

4.5.6.3 Quantification

Human Error Probabilities

In the case of an early response, the operator would have more than 8 hours available to establish SFP make-up and the failure is represented by the basic event HEP-MKUP-START (see fault tree L OI-OIL-U). In the case of a late response, the operator is assumed to have 4 hours available to establish SFP make-up and is represented by the basic event HEP-MKUP-START-E (see fault tree L OI-OIL-L). Success is defined as the operator starting the make-up pump and performing valve manipulation as needed.

SPAR HRA worksheets were used to quantify each of these errors. For HEP-MKUP-START it was assumed that the 8 hour time window will allow more than 50 times the time required to complete this task, the operators are under high stress, are highly trained, have equipment that

is well labeled and matched to a procedure, and the crew has effective interactions in a quality facility. For HEP-MKUP-START-E, the time available is not as extensive, and is considered nominal, all other PSFs being equal.

Hardware Failure Probabilities

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

4.5.6.4 Basic Event Probabilities

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

4.5.7 Top Event OMK – Operator Initiates Make-up Using Fire Pumps

4.5.7.1 Event Description and Timing

This top event represents failure to provide make-up using the firewater pumps. The case of a large leak is represented by a fault tree LOI-OMK-LGLK. In this case the operators have 40 hours to start a firewater system. The case of a small leak is represented by two functional fault trees, LOI-OMK-SMLK, and LOI-OMK-SMLK-L. The difference between the two trees is that in the first, the operators are aware of the problem and are attempting to solve it, whereas in the second, the operators will need to first recognize the problem. In both small leak cases, the operator has more than 65 hrs to start a firewater system. In all cases neither of the firewater pumps would be initially unavailable.

4.5.7.2 Relevant Assumptions

- The operators have 40 to 65 hours to start a firewater pump depending on the leak size.
- There is a means to remotely align a make-up source to the spent fuel pool without entry to the refuel floor so that make-up can be provided even when the environment is uninhabitable due to steam and/or high radiation (NEI commitment no.8).
- Repair crew is different than on-site operators.
- On average, it takes 10 hours to repair a pump if it fails to start and run.
- It takes 16 hours to contact maintenance personnel, make a diagnosis, and get new parts.
- Both firewater pumps are located in a separate structure and are protected from the potential harsh environment in the case of pool bulk boiling.
- Maintenance and testing are performed on diesel and electric firewater pumps to maintain operable status (NEI commitment no. 10).

- There are procedures to guide the operators in how to deal with loss of inventory, and the operators are trained in their use. The guidance on when to begin addition of water from alternate sources is clear and related to a clearly identified condition, such as pool level or onset of boiling (NEI commitment no. 2).

4.5.7.3 Quantification

Human Error Probabilities

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

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

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

SPAR HRA worksheets were also used to quantify the HEPs.

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

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

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

For HEP-FW-START-LOI it was assumed that the operators are under high stress, are

engaged in a highly complex task due to its non-routine nature, have a high level of training, have a diagnostic procedure, and are a part of a crew that interacts well in a quality facility.

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

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

Hardware Failure Probabilities

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

4.5.7.4 Basic Event Probabilities

Basic Event	Basic Event Probability
HEP-RECG-FWSTART	2.0E-5
HEP-RECG-FWSTART-L	5.0E-02
HEP-FW-START	1.0E-5
HEP-FW-REP-NODSM	7.5E-3
HEP-FW-REP-NODLG	9.0E-2
FP-2PUMPS-FTF	6.7E-4
HEP-RECG-FW-LOI	2.0E-4
HEP-FW-START-LOI	1.3E-3

4.5.8 Top Event OFD – Recovery From Off-site Sources

4.5.8.1 Event Description and Timing

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

4.5.8.2 Relevant Assumptions

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

4.5.8.3 Quantification

Human Error Probabilities

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

4.5.8.4 Basic Event Probabilities

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

4.5.9 Summary

Table 4.5 presents a summary of basic events.

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

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

Basic Event Name	Description	Basic Event Probability

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

5.0 Summary of Results

The results of this analysis provide insight into the risks associated with storage of spent nuclear fuel in fuel pools at decommissioned nuclear power plants. The five accident initiators that were analyzed consist of: 1) internal fires, 2) loss of cooling, 3) loss of inventory, 4) plant/grid centered losses of off-site power, and 5) severe weather induced losses of off-site power. The total frequency for the endstate is estimated to be 1.8E-7/year. Table 5.1 summarizes the fuel uncover frequency for each initiator.

This frequency is to be compared with the pool performance guideline (PPG). This guideline has been established by analogy with the acceptance guidelines in RG. 1.174. In RG 1.174 it was determined that the mean value of the distribution characterizing uncertainty is the appropriate value to compare the guideline. However, it was determined that it is also necessary to investigate whether there are modeling uncertainties that could affect the decision made with respect to whether the guidelines have been met. This is the approach that has been followed here.

5.1 Characterization of Uncertainty

The frequencies are point estimates, based on the use of point estimates for the input parameters. The input parameter values were taken from a variety of sources, and in many cases were presented as point estimates with no characterization of uncertainty. In some cases, such as the initiating event frequencies derived from NUREG/CR 5496, and the HEPs derived from THERP, an uncertainty characterization was given, and the point estimates chosen corresponded to the mean values of the distributions characterizing uncertainty. For all other parameters, it was assumed that the values would be the mean values of distributions characterizing the uncertainty of the parameter value. In the case of SPAR HEPs, the authors of the SPAR HRA approach consider their estimates as mean values based on the fact that the numbers were established on the basis of considering several different sources, most of which specified mean values. Consequently, the results of this analysis are interpreted as being mean values. A propagation of parameter uncertainty through the model was not performed, nor was it considered necessary. With the exception of the spent fuel pool cooling system itself, the systems relied on are single train systems. The dominant failure contributions for the spent fuel pool cooling system are assumed to be common cause failures. Thus there are no dominant cutsets in the solutions that involved multiple repetitions of the same parameter, and under these conditions, use of mean values as input parameters produces a very close approximation to mean values of sequence frequencies. Since typical uncertainty characterization for the input parameters is a lognormal distribution with error factors of 3 or 10, the 95th percentile of the output distribution will be no more than a factor of three higher than the mean value. This is not significant to change the conclusion of the analysis.

The numerical results are a function of the assumptions made and in particular, the model used to evaluate the human error probabilities. The staff believes the models used are appropriate for the purpose of this analysis, and in particular are capable of incorporating the relevant performance shaping factors to demonstrate that low levels of risk are achievable, given an appropriate level of attention to managing the facility with a view to ensuring the health and safety of the public. Alternate HRA models could result in frequencies that are different. However, given the time scales involved, and the simplicity of the systems, we believe that the conclusions of this study, namely that, when the NEI commitments are appropriately implemented the risks are low, are robust.

Certain assumptions may be identified as having the potential for significantly influencing the results. For example, the calculated time windows associated with the loss of inventory event tree are sensitive to the assumptions about the leak size. The SPAR HRA method is, however, not highly sensitive to the time windows assumed, primarily making a distinction between time windows that represent an inadequate time, barely adequate, nominal, extra time, and expansive time. The precise definitions of these terms can be found in Reference 9. Consequently, the assumption of the large leak rate as 60 gpm is not critical. For the loss of inventory event tree, the assumption that the leak is self-limiting after a drop in level of 15 feet,

may be a more significant assumption that, on a site specific basis may be non-conservative, and requires validation. The assumption that the preparation time of several days is adequate to bring off-site sources to bear may be questioned in the case of extreme conditions. However, the very conservative assumption that this is guaranteed to fail would change the corresponding event sequences by about an order of magnitude, which would still be a very low risk contributor.

5.2 Conclusions

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

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

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

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

Table 5.1 Summary of Results

Initiating Event	Fuel Uncovery Frequency (per year)
Internal Fires	2.3E-08
Loss of Cooling	1.4E-08
Loss of Inventory	3.0E-09
Loss of Off-site Power (plant centered & grid-related events)	2.9E-8

Loss of Off-site Power (severe weather events)	1.1E-7
TOTAL =	1.8E-07

6.0 REFERENCES

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

15. OREDA-92 Offshore Reliability Data Handbook, 2nd Edition, 1992.
16. Atwood, et. al., "Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980 - 1996," NUREG/CR-5496, November 1998.
17. U.S. Nuclear Regulatory Commission, "Evaluation of Station Blackout Accidents at Nuclear Power Plants," NUREG-1032, June 1988.
18. U.S. Nuclear Regulatory Commission, "Single-Failure-Proof Cranes for Nuclear Power Plants," USNRC Report NUREG-0554, May 1979.

ATTACHMENT A

FAULT TREES USED IN THE RISK ANALYSIS

ATTACHMENT B
SPAR HRA Worksheet

agnosis

Di

ilure Probability

Fa

SPAR HRA Human Error Worksheet (Page 2 of 3)

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

Basic Event Context: _____
 Basic Event Description: _____

Part II. ACTION

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

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

B. Calculate the Action Failure Probability

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

(2) Otherwise,

	Time	Stress	Complexity	Experience/ Training	Procedures	Ergonomics	Fitness for Duty	Work Processes	
Action: 1E-3	x__	x__	x__	x__	x__	x__	x__	x__	= _____

A

ction

Fa

ilure Probability

SPAR HRA Human Error Worksheet (Page 3 of 3)

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

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

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

If all PSFs are nominal,

then

Diagnosis Failure Probability:

1E-2

Diagnosis Failure Probability:

Action Failure Probability:

+ _____

Action Failure Probability:

+1E-3

Task Failure Without

Formal Dependence ($P_{w/od}$)

= _____

$P_{w/od}$

= 1.1E-2

Part IV. DEPENDENCY

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

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

Dependency Condition Table

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

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

For Complete Dependence the probability of failure is 1.

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

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

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

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

Calculate P_{wd} using the appropriate values:

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

Appendix 2b Structural Integrity of Spent Fuel Pools Subject to Seismic Loads

1. Introduction

As a part of the Generic Issue 82, "Beyond Design Basis Accidents in Spent Fuel Pools," NRC has studied the hypothetical event of an instantaneous loss of spent fuel pool water. The recommendation from a study in support of this generic issue indicates that a key part of a plant specific evaluation for the effect of such an event, is the need to obtain a realistic seismic fragility of the spent fuel pool. The failure or the end state of concern in the context of this generic issue is a catastrophic failure of the spent fuel pool which leads to an almost instantaneous loss of all pool water and the pool having no capacity to retain any water even if it were to be reflooded.

Spent fuel pool structures at nuclear power plants are constructed with thick reinforced concrete walls and slabs lined with stainless steel liners 1/8 to 1/4 inch thick. Dresden Unit 1 and Indian Point Unit 1 are exceptions to this in that these two plants do not have any liner plates. They were decommissioned more than 20 years ago and no safety significant degradation of the concrete pool structure has been reported. The spent fuel pool walls vary from 4.5 to 5 feet in thickness and the pool floor slabs are approximately 4 feet thick. The overall pool dimensions are typically about 50 feet long by 40 feet wide and 55 to 60 feet high. In boiling water reactor (BWR) plants, the pool structures are located in the reactor building at an elevation several stories above the ground. In pressurized water reactor (PWR) plants, the spent fuel pool structures are located outside the containment structure and are supported on the ground or partially embedded in the ground. The location and supporting arrangement of the pool structures help determine their capacity to withstand seismic ground motion beyond their design basis. The dimensions of the pool structure are generally derived from radiation shielding considerations rather than structural needs. Spent fuel structures at operating nuclear power plants are inherently rugged in terms of being able to withstand loads substantially beyond those for which they were designed. Consequently, they have significant seismic capacity.

2. Seismic Checklist

In the preliminary draft report published in June 1999, the staff assumed that the spent fuel pools were robust for seismic events less than about three times the safe shutdown earthquake (SSE). It was assumed that the high confidence, low probability of failure (HCLPF)¹ value for pool integrity is 3 times SSE. For most Central and Eastern U.S. (CEUS) sites, 3 X SSE is in the peak ground acceleration (PGA) range of 0.35 to 0.5 g (where g is the acceleration of gravity). Seismic hazard estimates developed by the Lawrence Livermore National Laboratory (NUREG-1488) show that, for most CEUS plants, the mean frequency for a PGA equal to 3 X SSE is less than 2E-5 per year. For western plants, the mean frequency for PGA equal to 2 X SSE is equivalently small.

These low probabilistic frequency-of-occurrence estimates are supported by deterministic

¹A HCLPF is the peak acceleration value at which there is 95% confidence that less than 5% of the time the structure, system or component will fail.

considerations. The design basis earthquake ground motion, or the SSE ground motion, for nuclear power plant sites were based on the assumption of the largest event geophysically ascribable to a tectonic province or a capable structure at the closest proximity of the province or fault to the site. In the case of the tectonic province in which the site is located, the event is assumed to occur at the site. For the eastern seaboard, the Charleston event is the largest magnitude earthquake and current research has established that such large events are confined to the Charleston region. The New Madrid zone is another zone in the central US where very large events have occurred. Recent research has identified the source structures of these large New Madrid earthquakes. Both of these earthquake sources are fully accounted for in the assessment of the SSE for currently licensed plants. The SSE ground motions for nuclear power plants are based on conservative estimates of the ground motion from the largest earthquake estimate to be generated under the current tectonic regime. The seismic hazards at the west coast sites are generally governed by known active fault sources, consequently, the hazard curves, which are plots of ground acceleration versus frequency of occurrence, have a much steeper slope near the higher ground motion end. In other words, as the amplitude of the seismic acceleration increases, the probability of its occurrence decreases rapidly. Therefore it is reasonable to conclude that the frequency of ground motion exceeding 3 X SSE for CEUS plants and 2 X SSE for western plants is less than $2E-5$ per year.

Several public meetings were held from April to July 1999 to discuss the staff's draft report. At the July public workshop, the NRC proposed, and the industry group agreed to develop a seismic checklist, which could be used to examine the seismic vulnerability of any given plant. In a letter dated August 18, 1999, the Nuclear Energy Institute (NEI) proposed a checklist which is based on assuring a robustness for a seismic ground motion with a PGA of approximately 0.5g. A copy of this submittal is included in Appendix 5a.

The NRC contracted with Dr. Robert P. Kennedy to perform an independent review of the seismic portion of the June draft report, as well as the August 18, 1999, submittal from NEI. Dr. Kennedy's comments and recommendations were contained in an October 1999 report entitled "Comments Concerning Seismic Screening and Seismic Risk of Spent Fuel Pools for Decommissioning Plants," which is included as Appendix 5b of this report. Dr. Kennedy raised three significant concerns about the completeness of the NEI checklist.

The results of Dr. Kennedy's review, as well as staff comments on the seismic checklist, were forwarded to NEI and other stakeholders in a December 3, 1999, memorandum from Mr. William Huffman (Appendix 5c). In a letter from Mr. Alan Nelson, dated December 13, 1999 (Appendix 5d), NEI submitted a revised checklist, which addressed the comments from Dr. Kennedy and the NRC staff. Dr. Kennedy reviewed the revised checklist, and concluded in a letter dated December 28, 1999 (Appendix 5f), that the industry seismic screening criteria are adequate for the vast majority of CEUS sites.

3. Seismic Risk - Catastrophic Failure

The preliminary risk assessment report published in June 1999 used an approximate method for estimating the risk of spent pool failure. It was assumed that the HCLPF value for the pool integrity is 3 times SSE. For most CEUS sites, 3 X SSE has a ground motion with a PGA range of 0.35 to 0.5 g. Seismic hazard curves from the Lawrence Livermore National Laboratory (NUREG-1488) show that, for most CEUS sites, the mean frequency for PGA equal to 3 X SSE is less than $2E-5$. For western plants, the mean frequency of ground motion

exceeding 2 X SSE is comparably small. In the June report, the working group used the approximation that the frequency of a seismic event that will challenge the spent fuel pool integrity is 5% of 2E-5, or a value of 1E-6.

Dr. Kennedy, in his October 1999 report, pointed out that this approximation is nonconservative for CEUS hazard curves with shallow slopes; i.e., where an increase of more than a factor of two in ground motion is required to achieve a 10-fold reduction in annual frequency of exceedance. Dr. Kennedy proposed a calculation method, which had previously been shown to give risk estimates that were 5 to 20% conservative when compared to more rigorous methods, such as convolution of the hazard and fragility estimates. Using this approximation, Dr. Kennedy estimated the spent fuel pool failure frequency for a site with HCLPF of 1.2² peak spectral acceleration if sited at each of the 69 CEUS sites. A total of 35 sites had frequencies exceeding 1E-6 per year, and eight had frequencies in excess of 3E-6 per year. The remaining sites had frequencies below 1E-6³. Dr. Kennedy's report notes that spent fuel pools that pass the appropriately defined screening criteria are likely to have capacities higher than the screening level capacity. Thus, the frequencies quoted above are upper bounds.

For those CEUS plants where the ground motion of 3 X SSE is less than or equal to the NEI screening criterion of 0.5g PGA, the staff concludes that the risk is acceptably low. A similar conclusion can be drawn for western plants where the ground motion at 2 X SSE is within the screening criterion. For CEUS plants where 3 X SSE exceeds the screening criterion, a detailed assessment will be required to demonstrate that the pool HCLPF equals 3 X SSE. A similar conclusion can be drawn for western plants where the ground motion at 2 X SSE exceeds the screening criterion.

The staff has no estimate of the seismic risk for decommissioning plants at sites west of the Rockies. However, based on considerations described above, the staff estimates that western plants which can demonstrate a HCLPF greater than 2 X SSE will have an acceptably low estimate of risk.

In his letter of December 28, 1999, Dr. Kennedy concurred that this performance goal assures an adequately low seismic risk for the spent fuel pool.

4. Seismic Risk - Support System Failure

²Damage to critical SSCs does not correlate very well to PGA of the ground motion. However, damage correlates much better with the spectral acceleration of the ground motion over the natural frequency range of interest, which is generally between 10 and 25 hertz for nuclear power plants SSCs. The spectral acceleration of 1.2g corresponds to the screening level recommended in the reference document cited in the NEI checklist, and this spectral ordinate is approximately equivalent to a ground motion with 0.5g PGA.

³These estimates are based on the Lawrence Livermore National Laboratory 1993 (LLNL 93) seismic hazard curves. Recently, the Senior Seismic Hazard Analysis Committee (SSHAC) published NUREG-CR-6372, "Recommendation for Probabilistic Seismic Hazard Analysis: Guidance On Uncertainty and Use of Experts." The report gives guidance on future application of seismic hazards. However, site specific hazard estimates have not been performed for all sites with the new method.

In its preliminary draft report published in June 1999, the staff assumed that a ground motion three times the SSE was the HCLPF of the spent fuel pool. This meant that 95% of the time the pool would remain intact (i.e., would not leak significantly). The staff evaluated what would happen to spent fuel pool support systems (i.e., the pool cooling and inventory make-up systems) in the event of an earthquake three times the SSE. We modeled some recovery as possible (although there would be considerable damage to the area's infrastructure at such earthquake accelerations). The estimate in the preliminary report for the contribution from this scenario was 1×10^{-6} per year. In this report, this estimate has been refined based on looking at a broader range of seismic accelerations and further evaluation of the conditional probability of recovery under such circumstances. The staff estimates that for an average site in the northeast United States the return period of an earthquake that would damage a decommissioning plant's spent fuel pool cooling system equipment (assuming it had at least minimal anchoring) is about once in 4,000 years. The staff quantified a human error probability of 1×10^{-4} that represents the failure of the fuel handlers to obtain off-site resources. The event was quantified using the SPAR HRA technique. The probability shaping factors chosen were as follows: expansive time (> 50 times the required time), high stress, complex task because of the earthquake and its non-routine nature, quality procedures, poor ergonomics due to the earthquake, and finally a crew who had executed these tasks before, conversant with the procedures and one another. In combination we now estimate the risk from support failure due to seismic events to be on the order of 1×10^{-8} per year. The risk from support system failure due to seismic events is bounded by other more likely initiators.

5. Conclusion

Spent fuel pools that satisfy the seismic checklist, as written, would have a high confidence in a low probability of failure for seismic ground motions up to 0.5 g peak ground acceleration (1.2g peak spectral acceleration). Thus, sites in the central and eastern part of the U.S. that have three times SSE values less than or equal to 0.5 g PGA and pass the seismic check list would have an acceptably low level of seismic risk. Similarly, West Coast sites that have two times SSE values less than 0.5 g. and pass the seismic check list would have acceptably low values of seismic risk. From a practical point of view, a limited number of sites in the central and eastern part of the U.S. have three times SSE values greater than 0.5g; the two times SSE values exceed 0.5g for two West Coast plants. In order to demonstrate acceptably low seismic risk, those central and eastern sites for which the three times SSE values exceed 0.5g and the two West Coast sites would have to perform additional plant specific analyses to demonstrate HCLPF for their spent fuel pools at three times SSE and two times SSE values of ground acceleration, respectively. For these sites the frequency of failure is bounded by 3×10^{-6} per year, and other considerations indicate the frequency may be significantly lower. Plants which cannot demonstrate HCLPF values equivalent to 3 X SSE or 2 X SSE as appropriate may perform a risk assessment to demonstrate acceptably low frequency of SFP failure.

Appendix 2c Structural Integrity of Spent Fuel Pool Structures Subject to Heavy Loads Drops

1. Introduction

A heavy load drop into the spent fuel pool (SFP) or onto the spent fuel pool wall can affect the structural integrity of the spent fuel pool. A loss-of-inventory from the spent fuel pool could occur as a result of a heavy load drop. For single failure proof systems where load drop analyses have not been performed at decommissioning plants, the mean frequency of a loss-of-inventory caused by a cask drop was estimated to be 2.0×10^{-7} per year (assuming 100 lifts per year). For a non-single failure proof handling system where a load drop analysis has not been performed, the mean frequency of a loss-of-inventory event caused by a cask drop was estimated to be 2.1×10^{-5} per year. The staff believes that performance and implementation of a load drop analysis that has been reviewed and approved by the staff will substantially reduce the expected frequency of a loss-of-inventory event from a heavy load drop for either a single failure proof or non-single failure proof system.

2. Analysis

The staff revisited NUREG-0612¹ [Ref. 1] to review the evaluation and the supporting data available at that time to determine its applicability to and usefulness for evaluation of heavy load drop concerns at decommissioning plants. In addition, three additional sources of information were identified by the staff and used to reassess the heavy load drop risk:

- (1) U.S. Navy crane experiences (1990s Navy data) for the period 1996 through mid-1999,
- (20) WIPP/WID-96-2196 [Ref. 2], "Waste Isolation Pilot Plant Trudock Crane System Analysis," October 1996 (WIPP)
- (21) NEI data on actual spent fuel pool cask lifts at U.S. commercial nuclear power plants [Ref.3]

The staff's first area of evaluation was the frequency of heavy load drops. The number of occasions (incidents) where various types of faults occurred that potentially could lead to a load drop was investigated. Potential types of faults investigated included improper operation of equipment, improper rigging practices, poor procedures, and equipment failures. Navy data from the 1990s were compared to the data used in NUREG-0612. The data gave similar, but not identical, estimates of the various faults leading to heavy load drops (See Table A2c-1.) The NEI cask handling experience also supported the incident data used in this evaluation, and in NUREG-0612. Once the frequency of heavy load drops was estimated (i.e., load drops per lift), the staff investigated the conditional probability that such a drop would seriously damage the spent fuel pool (either the bottom or walls of the pool) to the extent that the pool would drain very rapidly and it would not be possible to refill it using onsite or offsite resources. To do this the staff used fault trees taken from NUREG-0612 (See Figure A2c-1.) By mathematically

¹NUREG-0612 documented the results of the staff's review of the handling of heavy loads at operating nuclear power plants and included the staff's recommendations on actions that should be taken to assure safe handling of heavy loads.

combining the frequency of load drops with the conditional probability of pool failure given a load drop, the staff was able to estimate the frequency of heavy load drops causing a zirconium fire at decommissioning facilities.

3. Frequency of Heavy Load Drop

The database used in this evaluation (primarily the 1990s Navy data) considered a range of values for the number of occasions where faults occurred, the frequency of heavy load drops and the availability of backup systems. The reason that there is a range of values is that while the number of equipment failures and load drops were reported, the denominator of the estimate, the actual total number of heavy load lifts, was only available based on engineering judgement. High and low estimates of the ranges were made, and it was assumed that the data had a log normal distribution with the high and low number of the range representing the 5th and 95th percentile of the distribution. From this the mean of the distribution was calculated. Data provided by NEI on actual lifts and setdowns of spent fuel pool casks at commercial U.S. nuclear power plants (light water and gas-cooled reactors) gave a similar estimated range for the incidents at the 95 percent confidence level.

Load drops were broken down into two categories: failure of lifting equipment and failure to secure the load.

Crane failures (failure of lifting equipment) were evaluated using the fault tree shown in Figure A2c-1, which comes from NUREG-0612. At the time that heavy loads were evaluated in NUREG-0612, low density storage racks were in use and after 30 to 70 days (a period of about 0.1 to 0.2 per year), no radionuclide releases were expected if the pool were drained. It was assumed in NUREG-0612 that after this period, the fuel gap noble gas inventory had decayed and no zirconium fire would have occurred. Today, most decommissioning facilities use high density storage racks. This analysis evaluates results at one year after reactor shutdown. Our engineering evaluations indicate that for today's fuel configurations, burnup, and enrichment, a zirconium cladding fire may occur if the pool were drained during a period as long as five years.

A literature search performed by the staff searching for data on failure to secure loads identified a study (WIPP report) that included a human error evaluation for improper rigging. This study was used by the staff to re-evaluate the contribution of rigging errors to the overall heavy load (cask) drop rate and to address both the common mode effect estimate and the 1990s Navy data. Failure to secure a load was evaluated in the WIPP report for the Trudock crane. The WIPP report determined that the most probable human error was associated with attaching the lifting legs to the lifting fixture. In the WIPP report, the failure to secure the load (based on a 2-out-of-3 lifting device) was estimated based on redundancy, procedures, and a checker. The report assumed that the load could be lowered without damage if no more than one of the three connections were not properly made. Using NUREG/CR-1278 [Ref. 4] information, the mean failure rate due to improper rigging was estimated in the WIPP report to be 8.7×10^{-7} per lift. Our requantification of the NUREG-0612 fault tree using the WIPP improper rigging failure rate is summarized in Table A2c-2. The WIPP evaluation for the human error probabilities is summarized in Table A2c-3.

These estimates provided a rate for failures per lift. Based on input from the nuclear industry at the July 1999 SFP workshop, we assumed in our analysis that there will be a maximum of 100 cask lifts per year at a decommissioning plant.

4. Evaluation of the Load Path

Just because a heavy load is dropped does not mean that it will drop on the spent fuel pool wall or on the pool floor. It may drop at other locations on its path. A load path analysis is plant-specific. In NUREG-0612 it was estimated that the heavy load was near or over the spent fuel pool for between 5% and 25% of the total path needed to lift, move, and set down the load. It was further estimated that if the load were dropped from 30 feet or higher (or in some circumstances from 36 feet and higher depending on the assumptions) when it is over the pool floor, and if a plant-specific load drop analysis had not been performed², then damage to the pool floor would result in loss-of-inventory. In addition we looked at the probability that the load drop occurred over the pool wall from eight to ten inches above the edge of the pool wall. In our analysis we evaluated the chances the load was raised sufficiently high to fail the pool and evaluated the likelihood that the drop happened over a vulnerable portion of the load path. Table A2c-2 presents the results for a heavy load drop on or near the spent fuel pool. Based on NUREG-0612, if the cask were dropped on the spent fuel pool floor, the likelihood of a loss-of-inventory given the drop is 1.0. Based on the evaluation presented in NUREG/CR-5176 [Ref. 5], if the load were dropped on the spent fuel pool wall, the likelihood of a loss-of-inventory given the drop is 0.1.

5. Conclusion

Our heavy load drop evaluation is based on the method and fault trees developed in NUREG-0612. New 1990s Navy data were used to quantify the failure rate of the lifting equipment. The WIPP human error evaluation was used to quantify the failure to secure the load. We estimated the mean frequency of a loss-of-inventory from a cask drop onto the pool floor or onto the pool wall from a single failure proof system to be 2.0×10^{-7} per year for 100 lifts per year.

However, only some of the plants that will be decommissioning plants in the future currently have single failure proof systems. Historically, many facilities have chosen to upgrade their crane systems to become single failure proof. However, this is not an NRC requirement. The guidance in NUREG-0612, phase 2 calls for systems to either be single failure proof or if they are non-single failure proof to perform a load drop analysis. The industry through NEI has indicated that it is willing to commit to follow the guidance of all phases of NUREG-0612.

For licensees that choose the non-single failure proof handling system option in NUREG-0612, we based the mean frequency of a loss-of-inventory event on the method used in NUREG-0612. In NUREG-0612, an alternate fault tree than that used for the single failure proof systems was used to estimate the frequency of exceeding the release guidelines

² If a load drop analysis were performed, it means that the utility has evaluated the plant design and construction to pick out the safest path for the movement of the heavy load. In addition, it means that the path chosen has been evaluated to assure that if the cask were to drop at any location on the path, it would not catastrophically fail the pool or its support systems. If it is determined that a portion of the load path would fail if the load were dropped, the as-built plant must be modified (e.g., by addition of an impact limiter or enhancement of the structural capacity of that part of the building) to be able to take the load drop or a different safe load path must be identified.

(loss-of-inventory) for a non-single failure proof system. We calculated the mean frequency of catastrophic pool failure (for drops into the pool, or on or near the edge of the pool) for non-single failure proof systems to be about 2.1×10^{-5} per year when corrected for the 1990s Navy data and 100 lifts per year. This estimate exceeds the proposed pool performance guideline of 1×10^{-5} per year. The staff believes that a licensee which chooses the non-single failure proof handling system option in NUREG-0612 can reduce this estimate to the same range as that for single failure proof systems by performing a comprehensive and rigorous load drop analysis. The load drop analysis is assumed to include implementation of plant modifications or load path changes to assure the spent fuel pool would not be catastrophically damaged by a heavy load drop.

References:

- (1) U.S. Nuclear Regulatory, "Control of Heavy Loads at Nuclear Power Plants, Resolution of Generic Technical Activity A-36," NUREG-0612, July 1980.
- (2) Pittsburgh, Westinghouse, P.A., and Carlsbad, WID, N.M., "Waste Isolation Pilot Plant Trudock Crane System Analysis," WIPP/WID-96-2196, October 1996.
- (3) Richard Dudley, NRC memorandum to Document Control Desk, "Transmittal of Information Received From the Nuclear Energy Institute (NEI) For Placement InThe Public Document Room," dated September 2, 1999.
- (4) Swain, A.D., and H.E. Guttman, "Handbook of Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, August 1983.
- (5) P.G. Prassinis, et al., "Seismic Failure and Cask Drop Analyses of Spent Fuel Pools at Two Representative Nuclear Power Plants," NUREG/CR-5176, LLNL, January 1989.

Attachment 2C-1

Uncertainties

1. Incident rate.

The range used in this evaluation (1.0×10^{-4} to 1.5×10^{-4} incidents per year) was based on the Navy data originally assessed by the staff in NUREG-0612. The 1999 Navy data, like the 1980 data, did not report the number of lifts made and only provided information about the number of incidents. The cask loading experience at light water reactors and Ft. St. Vrain tends to support values used for the incident range.

2. Drop rate.

The drop rate, about 1-in-10, was based on the 1999 Navy data. Previous studies used engineering judgement to estimate the drop rate to be as low as 1-in-100.

3. Load path.

The fraction of the load path over which a load drop may cause sufficient damage to the spent fuel pool to result in a loss-of-inventory was estimated to be between 0.5% and 6.25% of the total path needed to lift, move, and set down the load. This range was developed by the staff for the NUREG-0612 evaluation. No time motion study was performed to account for the fraction of time the load is over any particular location.

4. Load handling design.

The benefit of a single-failure proof load handling system to reduce the probability of a load drop was estimated to be about a factor of 10 to 100 improvement over a non-single failure proof load handling system, based on the fault tree quantifications in this evaluation. Previous studies have used engineering judgement to estimate the benefit to be as high as 1,000.

5. Load drop analysis

The benefit of a load drop analysis is believed to be significant, but is unquantified. A load drop analysis involves mitigation of the potential drop by methods such as changing the safe load path, installation of impact limiters, or enhancement of the structure, as necessary, to be able to withstand a heavy load drop at any location on a safe load path.

Table A2c-1 Summary of the 1996-1999 Navy Crane Data

		ID	Non-rigging Fraction	Rigging Fraction	Total Fraction
Summary by Incident Type (fraction of events)					
Crane collision		CC	0.17	0.00	0.17
Damaged crane		DC	0.20	0.08	0.27
Damaged load		DL	0.02	0.03	0.05
Dropped load		DD	0.03	0.06	0.09
Load collision		LC	0.11	0.03	0.14
Other		OO	0.02	0.00	0.02
Overload		OL	0.08	0.05	0.12
Personnel injury		PI	0.03	0.05	0.08
Shock		SK	0.00	0.02	0.02
Two-blocking		TB	0.05	0.00	0.05
Unidentified		UD	0.02	0.00	0.02
Totals			0.70	0.30	1.00
Summary by Incident Cause (fraction of total events)		ID	Fraction		
Improper operation		IO	0.38		
Procedures		PROC	0.20		
Equipment failure		EQ	0.05		
Improper rigging ⁽¹⁾		IR	0.30		
Others		OTHER	0.08		
Totals			1.00		
Fault Tree ID⁽²⁾	Application of new Navy data to heavy load drop evaluation	Fraction		NUREG-0612 Fraction	
F1	OL + 0.5*(DL+LC)	0.14		0.05	
F2	CC + DC + 0.5(DL+LC) + DD + OO + PI + SK + UD + 0.3*IR	0.61		0.53	
F3	TB	0.05		0.35	
F4	Assume next incident	(0.01)		(1/44)	
F5	Rigging 0.7*IR	0.21		0.07	
Totals		1.00		1.00	

Notes:

- Based on database description, 30% or "improper rigging" by incident cause were rigging failures during crane movement, and 70% of "improper rigging" by incident cause were rigging errors.
- F1 - Load hangup resulting from operator error (assume 50% of "damaged load" and "load collision" lead to hangup)
 - F2 - Failure of component with a backup component (assume 50% of "damaged load" and "load collision" lead to component failure)
 - F3 - Two-blocking event
 - F4 - Failure of component without a backup
 - F5 - Failure from improper rigging

Table A2c-2 Summary of NUREG-0612 Heavy Loads Evaluation (for cask drop) with New 1990s Navy Crane Data Values and WIPP Rigging HEP Method

Event	Description	Units	High	Low	Mean
N0	Base range of failure of handling system	/year	1.5e-04	1.0e-05	5.4e-05
	Crane Failure				
F1	Fraction of load hangup events (new 1990s Navy data)	---	0.14	0.14	0.14
CF11	Operator error leading to load hangup (N0*F1)	/year	2.0e-05	1.4e-06	7.4e-06
CF12	Failure of the overload device	/demand	1.0e-02	1.0e-03	4.0e-03
CF1	Load hangup event (CF11*CF12)	/year	2.0e-07	1.4e-09	3.0e-08
F2	Fraction of component failure events (new 1990s Navy data)	---	0.61	0.61	0.61
CF21	Failure of single component with a backup (N0*F2)	/year	9.1e-05	6.1e-06	3.3e-05
CF22	Failure of backup component given CF21	/demand	1.0e-01	1.0e-02	4.0e-02
CF2	Failure due to random component failure (CF21*CF22)	/year	9.1e-06	6.1e-08	1.3e-06
F3	Fraction of two-blocking events (new 1990s Navy data)	---	0.05	0.05	0.05
CF31	Operator error leading to Two-blocking (N0*F3)	/year	6.8e-06	4.5e-07	2.5e-06
CF32	Failure of lower limit switch	/demand	1.0e-02	1.0e-03	4.0e-03
CF33	Failure of upper limit switch	/demand	1.0e-01	1.0e-02	4.0e-02
CF3	Two-blocking event (CF31*CF32*CF33)	/year	6.8e-09	4.5e-12	4.0e-10
F4	Fraction of single component failure (new 1990s Navy data)	---	0.01	0.01	0.01
F4'	Credit for NUREG-0554	/demand	0.10	0.10	0.10
CF4	Failure of component that doesn't have backup (N0*F4*F4')	/year	2.2e-07	1.5e-08	8.1e-08
CRANE	Failure of crane (CF1+CF2+CF3+CF4)	/year	9.5e-06	7.7e-08	1.4e-06
D1	Lifts per year leading to drop (100 lifts per year, drops from non-rigging)	No.	3	3	3
CF	Failure of crane leading to load drop (CRANE*D1)	/year	2.9e-05	2.3e-07	4.4e-06
	Rigging failure - Based on WIPP method				
F5	Fraction of improper rigging events (new 1990s Navy data)	---	0.21	0.21	0.21
CR11	Failure due to improper rigging, mean from WIPP study	/year	8.7e-07	8.7e-07	8.7e-07
CR12	Failure of redundant/alternate rigging	N/A			
RIGGING	Failure due to improper rigging (CR11)	/year	8.7e-07	8.7e-07	8.7e-07
D2	Lifts per year leading to drop (100 lifts per year, drops from rigging)	No.	6	6	6
CR	Failure of rigging leading to a load drop (RIGGING*D2)	/year	5.3e-06	5.3e-06	5.3e-06
FHLS	Failure of heavy load (crane and rigging) system (CRANE+RIGGING)	/year	1.0e-05	9.5e-07	2.3e-06
CFCR	Total failures (crane and rigging) leading to a load drop (CF+CR)	/year	3.4e-05	5.5e-06	9.6e-06
	Loss-of-inventory for a single-failure proof crane				
RF	Fraction of year over which a release may occur	---	1.00	1.00	1.00
P	Fraction of path near/over pool	---	0.25	0.05	0.13
P'	Fraction of path critical for load drop	---	0.25	0.10	0.16
LOI-S	(CFCR) * P * P' * RF	/year	2.1e-06	2.8e-08	2.0e-07
	Loss-of-inventory for a non single-failure proof crane				

CFCRNO	Total failures leading to a dropped load (est. from NUREG-0612)	No.	7.5e-05	1.0e-07	2.1e-05
N					
RF	Fraction of year over which a release may occur	---	1.00	1.00	1.00
LOI-N	(CFCRNON) * P * P' * RF	/year	7.5e-05	1.0e-07	2.1e-05
	Risk reduction for a single-failure proof crane (LOI-N /LOI-S)	—	35	4	104

Table A2c-3 WIPP Evaluation for Failure to Secure Load (improper rigging estimate)

Symbol	HEP	Explanation of error	Source of HEP (NUREG/CR-1278)
A ₁	3.75x10 ⁻³	Improperly make a connection, including failure to test locking feature for engagement	Table 20-12 Item 13 Mean value (0.003, EF ⁽¹⁾ = 3)
B ₁	0.75	The operating repeating the actions is modeled to have a high dependency for making the same error again. It is not completely independent because the operator moves to the second lifting leg and must physically push the locking balls to insert the pins	Table 20-21 Item 4(a) High dependence for different pins. Two opportunities (the second and third pins) to repeat the error is modeled as 0.5+(1-0.5)*0.5 = 0.75
C ₁	1.25x10 ⁻³	Checker fails to verify proper insertion of the connector pins, and that the status affects safety when performing tasks	Table 20-22 Item 9 Mean value (0.001, EF = 3)
D ₁	0.15	Checker fails to verify proper insertion of the connector pins at a later step, given the initial failure to recognize error. Sufficient separation in time and additional cues to warrant moderate rather than total or high dependency.	Table 20-21 Item 3(a) Moderate dependency for second check
F ₁	5.2x10 ⁻⁷	Failure rate if first pin improperly connected	A ₁ * B ₁ * C ₁ * D ₁
a ₁	0.99625	Given first pin was improperly connected	
A ₂	3.75x10 ⁻³	Improperly make a connection, including failure to test locking feature for engagement	Table 20-12 Item 13 Mean value (0.003, EF = 3)
B ₂	0.5	The operating repeating the actions is modeled to have a high dependency for making the same error again. It is not completely independent because the operator moves to the second lifting leg and must physically push the locking balls to insert the pins	Table 20-21 Item 4(a) High dependence for different pins. Only one opportunity for error (third pin)
C ₂	1.25x10 ⁻³	Checker fails to verify proper insertion of the connector pins, and that the status affects safety when performing tasks	Table 20-22 Item 9 Mean value (0.001, EF = 3)
D ₂	0.15	Checker fails to verify proper insertion of the connector pins at a later step, given the initial failure to recognize error. Sufficient separation in time and additional cues to warrant moderate rather than total or high dependency.	Table 20-21 Item 3(a) Moderate dependency for second check
F ₂	3.5x10 ⁻⁷	Failure rate if first pin improperly connected	a ₁ * A ₂ * B ₂ * C ₂ * D ₂
F _T	8.7x10 ⁻⁷	Total failure due to human error	F ₁ + F ₂

(1) Note: The EF (error factor) is the 95th percentile/50th percentile (median). For an EF of 3, the mean-to-median multiplier is 0.8.

Figure A2c-1 (sheet 1 of 2) - Heavy Load Drop Fault Trees

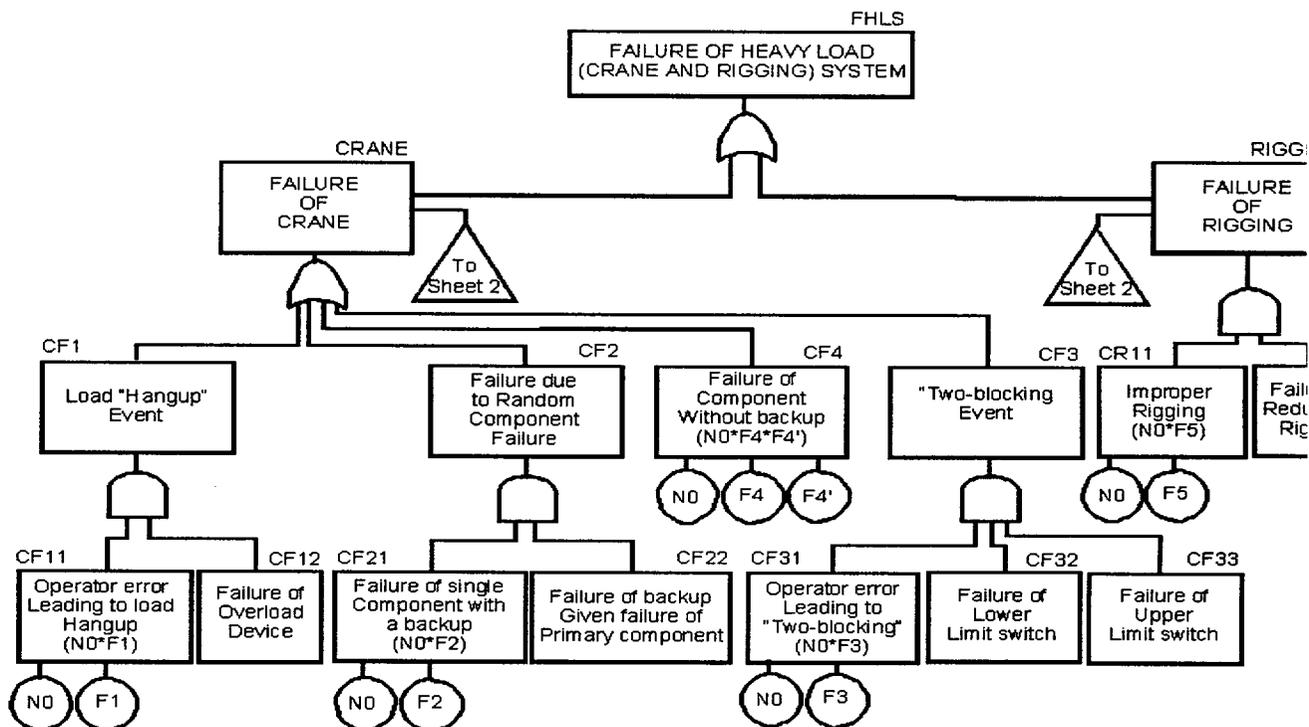
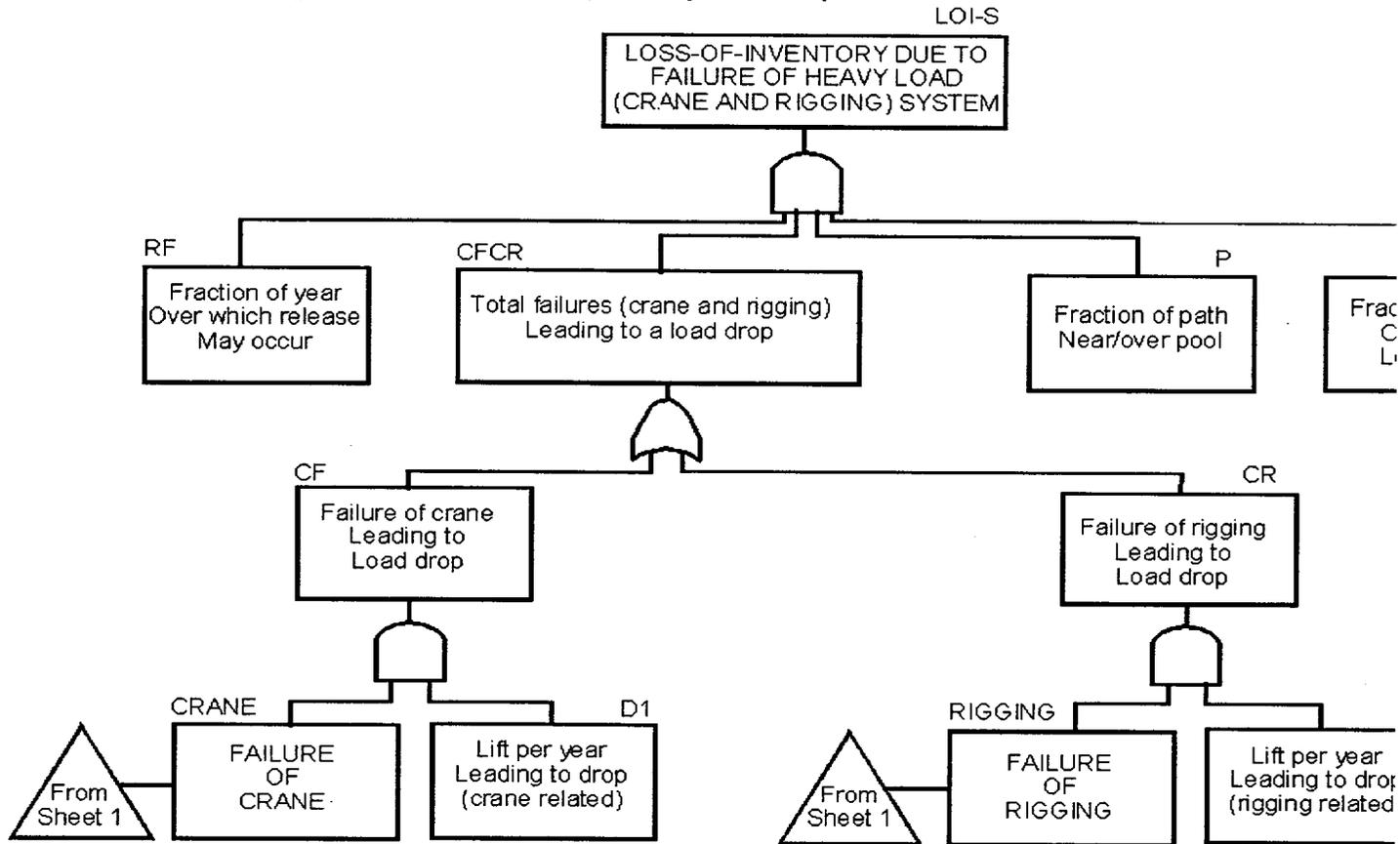


Figure A2c-1 (sheet 2 of 2) - Heavy Load Drop Fault Trees



Appendix 2d Structural Integrity of Spent Fuel Pool Structures Subject to Aircraft Crashes

1. Introduction

The mean frequency for significant PWR or BWR spent fuel pool damage resulting from a direct hit from an aircraft was estimated based on the point target model for a 100 x 50-foot pool to be 2.9×10^{-9} per year. The estimated frequency of loss of support systems leading to spent fuel pool uncover is bounded by other initiators.

2. Analysis

A detailed structural evaluation of how structures will respond to an aircraft crash is beyond the scope of this effort. The building or facility characteristics were chosen to cover a range typical of a spent fuel pool that is contained in a PWR auxiliary building or a BWR secondary containment structure. In general, PWR spent fuel pools are located on, or below grade, and BWR spent fuel pools, while generally elevated about 100 feet above grade, are located inside a secondary containment structure. The vulnerability of support systems (power supplies, heat exchangers and make-up water supplies) requires a knowledge of the size and location of these systems at decommissioning plants, information not readily available. However, we believe this analysis is adequately broad to provide a reasonable approximation of decommissioning plant vulnerability to aircraft crashes.

The staff used the generic data provided in DOE-STD-3014-96 [Ref. 1] to assess the likelihood of an aircraft crash into or near a decommissioned spent fuel pool. Aircraft damage can affect the structural integrity of the spent fuel pool or the availability of nearby support systems, such as power supplies, heat exchangers, and make-up water sources, and may also affect recovery actions.

The frequency of an aircraft crashing into a site, F , was obtained from the four-factor formula in DOE-STD-3014-96, and is referred to as the effective aircraft target area model:

where:

N_{ijk} =	estimated annual number of site-specific aircraft operations (no./yr)
P_{ijk} =	aircraft crash rate (per takeoff and landing for near-airport phases) and per flight for in-flight (nonairport) phase of operation
$f_{ijk}(x,y)$ =	aircraft crash location probability (per square mile)
A_{ij} =	site-specific effective area for the facility of interest, including skid and fly-in effective areas (square miles)
i =	(index for flight phase): $i=1,2$, and 3 (takeoff, in-flight, landing)
j =	(index for aircraft category, or subcategory)
k =	(index for flight source): there could be multiple runways and nonairport operations

The site-specific area is shown in Figure A2d-1 and is further defined as:

A_{eff} = total effective target area H= height of facility
 A_f = effective fly-in area L= length of facility
 A_s = effective skid area W= width of facility
 WS= wing span S= aircraft skid distance
 $\cot\theta$ = mean of cotangent of aircraft R= length of facility diagonal
 impact angle

and where:

Alternatively, a point target area model was defined as the area (length times width) of the facility in question, which does not take into account the size of the aircraft.

Table A2d-1 summarizes the generic aircraft data and crash frequency values for five aircraft types (from Tables B-14 through B-18 of DOE-STD-3014-96). The data given in Table A2d-1 were used to determine the frequency of aircraft hits per year for various building sizes (length, width, and height) for the minimum, average, and maximum crash rates. The resulting frequencies are given in Table A2d-2. The product $N_{ijk} * P_{ijk} * f_{ijk}(x,y)$ for Equation A2d-1 was taken from the crashes per mi^2/yr and A_{ij} was obtained from Equation A2d-2 for aircraft characteristics. Two sets of data were generated: one included the wing and skid lengths, using the effective aircraft target area model, and the other considered only the area (length times width) of the site, using the point target area model.

The results from the DOE effective aircraft target area model, using the generic data in Table A2d-1, were compared to the results of two evaluations reported in Reference 2. The first evaluation of aircraft crash hits was summarized by C.T. Kimura et al. in Reference 3. The DWTF Building 696 was assessed in the Kimura report. It was a 1-story 254-foot-long 80-foot-wide, 39-foot-high structure. The results of Kimura's study are given in Table A2d-3.

Applying the DOE generic data to the DWTF resulted in a frequency range of 6.5×10^{-9} hits per year to 6.6×10^{-5} hits per year, with an average value of 4.4×10^{-6} per year, for the effective aircraft target area model. For the point target area model, the range was 4.4×10^{-10} to 2.2×10^{-6} per year, with an average value of 1.5×10^{-7} per year.

The second evaluation was presented in a paper by K. Jamali [Ref. 4] in which additional facility evaluations were summarized. For the Seabrook Nuclear Power Station, Jamali's application of the DOE effective aircraft target area model to the final safety analysis report (FSAR) data resulted in an impact frequency 2.4×10^{-5} per year. The Millstone Unit 3 plant area was reported as 9.5×10^{-3} square miles and the FSAR aircraft crash frequency as 1.6×10^{-6} per year. Jamali applied the DOE effective aircraft target area model to information in the Millstone Unit 3 FSAR. Jamali reported an impact frequency of 2.7×10^{-6} per year, using the areas published in the FSAR and 2.3×10^{-5} per year, and using the effective area calculated the effective aircraft target area model.

When the generic DOE data in Table A2d-1 were used (for a 514 x 514 x 100-foot site), the

estimated impact frequency range was 6.3×10^{-9} to 2.9×10^{-5} per year, with an average of 1.9×10^{-6} per year, for the point target area model. The effective aircraft target area model gave an estimated range of 3.1×10^{-8} to 2.4×10^{-4} per year, with an average of 1.6×10^{-5} per year.

A site-specific evaluation for Three Mile Island Units 1 and 2 was documented in NUREG/CR-5042 [Ref. 5]. The NUREG estimated the aircraft crash frequency to be 2.3×10^{-4} accidents per year, about the same value as would be predicted with the DOE data set for the maximum crash rate for a site area of 0.01 square miles.

NUREG/CR-5042 summarized a study of a power plant response to aviation accidents. The results are given in Table A2d-4. The probability of the penetration of an aircraft through reinforced concrete was taken from that study.

Based on comparing these plant-specific aircraft crash evaluations with the staff's generic evaluation, there were no significant differences between the results from the DOE model whether generic data were used to provide a range of aircraft crash hit frequencies or whether plant-specific evaluations were performed.

3. Estimated Frequencies of Significant Spent Fuel Pool Damage

The frequency for significant PWR spent fuel pool damage resulting from a direct hit was estimated based on the point target model for a 100 x 50-foot pool with a conditional probability of 0.32 (large aircraft penetrating 6-ft of reinforced concrete) that the crash resulted in significant damage. If 1-of-2 aircraft are large and 1-of-2 crashes result in spent fuel uncovering, then the estimated range is 9.6×10^{-12} to 4.3×10^{-8} per year. The average frequency was estimated to be 2.9×10^{-9} per year.

The mean frequency for significant BWR spent fuel pool damage resulting from a direct hit was estimated to be the same as that for the PWR, 2.9×10^{-9} per year.

4. Support System Unavailability

The frequency for loss of a support system (e.g., power supply, heat exchanger, or make-up water supply) was estimated based on the DOE model, including wing and skid area, for a 400 x 200 x 30-foot area with a conditional probability of 0.01 that one of these systems is hit. The estimated value range was 1.0×10^{-6} to 1.0×10^{-10} per year. The average value was estimated to be 7.0×10^{-8} per year. This value does not credit on-site or off-site recovery actions.

As a check, we calculated the frequency for loss of a support system supply based on the DOE model, including wing and skid area, for a 10 x 10 x 10-foot structure. The estimated frequency range was 1.1×10^{-9} to 1.1×10^{-5} per year with the wing and skid area modeled, with the average estimated to be 7.3×10^{-7} per year. Using the point model, the estimated value range was 2.4×10^{-12} to 1.1×10^{-8} per year, with the average estimated to be 7.4×10^{-10} per year. This value does not credit on-site or off-site recovery actions.

5. Uncertainties

Mark-I and Mark-II secondary containments do not appear to have any significant structures that would reduce the likelihood of penetration, although on one side there may be a reduced likelihood due to other structures. Mark-III secondary containments may reduce the likelihood

of penetration, since the spent fuel pool may be considered to be protected by additional structures.

6. References

1. DOE-STD-3014-96, "Accident Analysis for Aircraft Crash Into Hazardous Facilities," U.S. Department of Energy (DOE), October 1996
2. A. Mosleh and R.A. Bari (eds), "Probabilistic Safety Assessment and Management," *Proceedings of the 4th International Conference on Probabilistic Safety Assessment and Management*, PSAM 4, Volume 3, 13-18 September 1998, New York City.
3. C.T. Kimura et al., "Aircraft Crash Hit Analysis of the Decontamination and Waste Treatment Facility (DWTF), Lawrence Livermore National Laboratory.
4. K. Jamali, et al., "Application of Aircraft Crash Hazard Assessment Methods to Various Facilities in the Nuclear Industry."
5. NUREG/CR-5042, "Evaluation of External Hazards to Nuclear Power Plants in the United States," Lawrence Livermore National Laboratory, December 1987.

Table A2d-1 Generic Aircraft Data

Aircraft	Wingspan (ft)	Skid distance (ft)	cotθ	Crashes per mi ² /yr			Notes
				Min	Ave	Max	
General aviation	50	1440	10.2	1x10 ⁻⁷	2x10 ⁻⁴	3x10 ⁻³	
Air carrier	98	60	8.2	7x10 ⁻⁸	4x10 ⁻⁷	2x10 ⁻⁶	
Air taxi	58	60	8.2	4x10 ⁻⁷	1x10 ⁻⁶	8x10 ⁻⁶	
Large military	223	780	7.4	6x10 ⁻⁸	2x10 ⁻⁷	7x10 ⁻⁷	takeoff
Small military	100	447	10.4	4x10 ⁻⁸	4x10 ⁻⁶	6x10 ⁻⁸	landing

Table A2d-2 Aircraft Hits Per Year

Building (L x W x H) (ft)	Average effective area (mi ²)	Minimum hits (per year)	Average hits (per year)	Maximum hits (per year)
With the DOE effective aircraft target area model				
100 x 50 x 30	6.9x10 ⁻³	3.2x10 ⁻⁹	2.1x10 ⁻⁶	3.1x10 ⁻⁵
200 x 100 x 30	1.1x10 ⁻²	5.3x10 ⁻⁹	3.7x10 ⁻⁶	5.5x10 ⁻⁵
400 x 200 x 30	2.1x10 ⁻²	1.0x10 ⁻⁸	7.0x10 ⁻⁶	1.0x10 ⁻⁴
200 x 100 x 100	1.8x10 ⁻²	9.6x10 ⁻⁹	5.1x10 ⁻⁶	7.6x10 ⁻⁵
400 x 200 x 100	3.3x10 ⁻²	1.8x10 ⁻⁸	9.6x10 ⁻⁶	1.4x10 ⁻⁴
80 x 40 x 30	6.1x10 ⁻³	2.8x10 ⁻⁹	1.8x10 ⁻⁶	2.7x10 ⁻⁵
10 x 10 x 10	2.9x10 ⁻³	1.1x10 ⁻⁹	7.3x10 ⁻⁷	1.1x10 ⁻⁵
With the point target area model				
100 x 50 x 0	1.8x10 ⁻⁴	1.2x10 ⁻¹⁰	3.7x10 ⁻⁸	5.4x10 ⁻⁷
200 x 100 x 0	7.2x10 ⁻⁴	4.8x10 ⁻¹⁰	1.5x10 ⁻⁷	2.2x10 ⁻⁶
400 x 200 x 0	2.9x10 ⁻³	1.9x10 ⁻⁹	5.9x10 ⁻⁷	8.6x10 ⁻⁶
80 x 40 x 0	1.1x10 ⁻⁴	1.1x10 ⁻¹¹	2.4x10 ⁻⁸	3.5x10 ⁻⁷
10 x 10	3.6x10 ⁻⁶	2.4x10 ⁻¹²	7.4x10 ⁻¹⁰	1.1x10 ⁻⁸

Table A2d-3 DWTF Aircraft Crash Hit Frequency (per year)

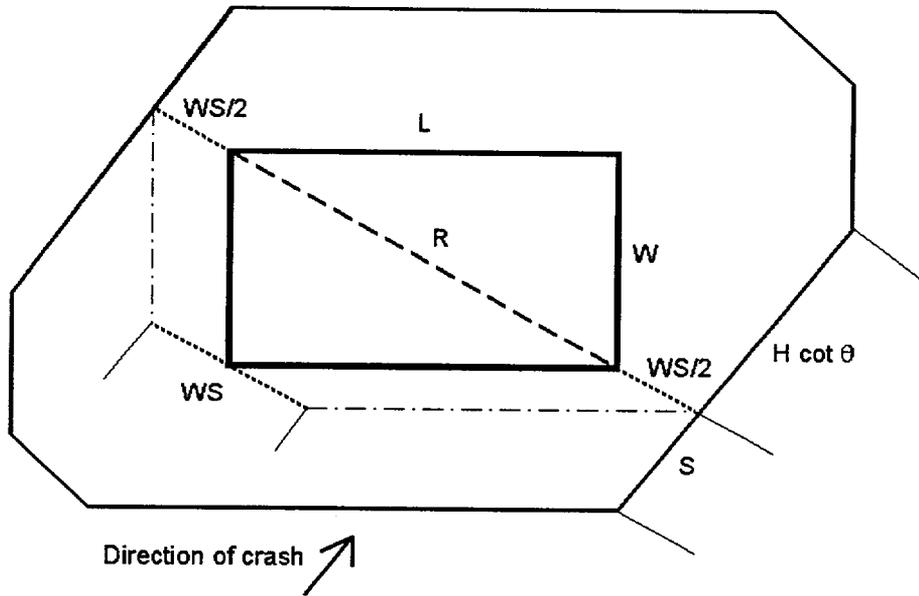
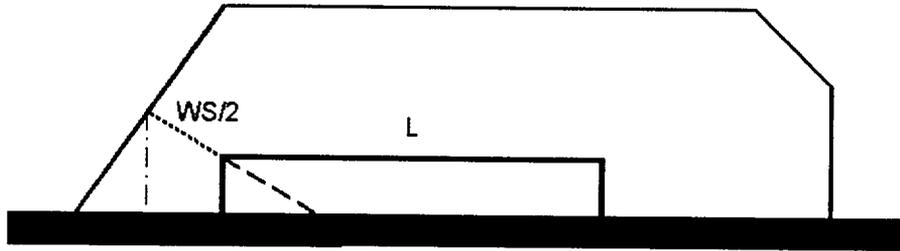
Period	Air Carriers	Air Taxes	General Aviation	Military Aviation	Total ⁽¹⁾
1995	1.72x10 ⁻⁷	2.47x10 ⁻⁶	2.45x10 ⁻⁵	5.03x10 ⁻⁷	2.76x10 ⁻⁵
1993-1995	1.60x10 ⁻⁷	2.64x10 ⁻⁶	2.82x10 ⁻⁵	6.47x10 ⁻⁷	3.16x10 ⁻⁵
1991-1995	1.57x10 ⁻⁷	2.58x10 ⁻⁶	2.89x10 ⁻⁵	7.23x10 ⁻⁷	3.23x10 ⁻⁵
1986-1995	1.52x10 ⁻⁷	2.41x10 ⁻⁶	2.89x10 ⁻⁵	8.96x10 ⁻⁷	3.23x10 ⁻⁵

Note (1): Various periods were studied to assess variations in air field operations.

Table A2d-4 Probability of Penetration as a Function of Location and Concrete Thickness

		Probability of penetration			
		Thickness of reinforced concrete			
Plant location	Aircraft type	1 foot	1.5 feet	2 feet	6 feet
≤ 5 miles from airport	Small ≤ 12,000 lbs	0.003	0	0	0
	Large > 12,000 lbs	0.96	0.52	0.28	0
> 5 miles from airport	Small ≤ 12,000 lbs	0.28	0.06	0.01	0
	Large > 12,000 lbs	1.0	1.0	0.83	0.32

Figure A2d-1 Rectangular Facility Effective Target Area Elements



Appendix 2e Structural Integrity of Spent Fuel Pool Structures Subject to Tornadoes

1. Introduction

Tornado damage from missiles have the potential to affect the structural integrity of the spent fuel pool or the availability of nearby support systems, such as power supplies, cooling pumps, heat exchangers, and make-up water sources, and may also affect recovery actions. Department of Energy (DOE) studies indicate that the thickness of the spent fuel pool walls (greater than four feet of reinforced concrete) is more than sufficient protection from missiles that could be generated by the most powerful tornadoes ever recorded in the United States. In addition, the frequency of meeting or exceeding the wind speeds of F4 to F5 tornadoes (the most powerful tornadoes on the Fujita scale) is estimated to be on the order of 6×10^{-7} per year in the areas of the U.S. that are subject to the largest and most frequent tornadoes. The likelihood of meeting or exceeding the size tornado that could damage support systems is on the order of 2×10^{-5} per year. This is not the estimated frequency of fuel uncovering on a zirconium fire since the frequency estimate does not include credit for maintaining pool inventory from either on-site or off-site sources.

The probability of failing to maintain inventory was estimated for the case of loss of off-site power from severe weather, where it was assumed that the principal impact of the severe weather was to hamper recovery of off-site power and also to increase the probability of failing to bring off-site resources to bear because of damage to the infrastructure. The situation with tornadoes is different, because the damage caused by a tornado is relatively localized. Therefore, while a direct hit on the plant could also disable the diesel fire pump, it would be unlikely to also disable off-site resources to the same degree. Therefore, the probability of failing to bring in the off-site resources can be argued to be the same as for the seismic case, i.e., $1 \text{E-}04$, under the assumption that NEI commitments 3 and 4 are implemented.

2. Analysis

The methodology assessing tornado risk developed in NUREG/CR-2944, [Ref. 1] was used for this evaluation. The National Climatic Data Center (NCDC) in Asheville, N.C., keeps weather records for the U.S. for the period 1950 to 1995 [Ref. 2]. Tornado data are reported as the annual average number of (all) tornadoes per 10,000 square miles per state and the annual average number of strong-violent (F2 to F5) tornadoes per square mile per state, as shown in Figures A2e-1 and A2e-2.

The NCDC data were reviewed and a range of frequencies per square mile per year was developed based on the site location and neighboring state (regional) data. In general, the comparison of the NUREG/CR-5042 [Ref. 3] tornado frequencies for all tornadoes to the NCDC tornado frequencies for all reported tornadoes showed good agreement between the two sets of data.

Raw data from the Storm Prediction Center (SPC), for the period 1950 to 1995 was used to develop a database for this assessment. About 121 F5, and 924 F4, tornadoes have been recorded between 1950 and 1995 (an additional 4 in the 1996 to 1998 period). It was estimated that about 30% of all reported tornadoes were in the F2 to F3 range and about 2.5% were in the F4 to F5 range.

The Department of Energy Report DOE-STD-1020-94, [Ref. 4] has some insights into wind-generated missiles:

- (1) For sites where tornadoes are not considered a viable threat, to account for objects or debris a 2x4 inch timber plank weighing 15 lbs is considered as a missile for straight winds and hurricanes. With a recommended impact speed of 50 mph at a maximum height of 30 ft above ground, this missile would break annealed glass, perforate sheet metal siding and wood siding up to to 3/4-in thick. For weak tornadoes, the timber missile horizontal speed is 100 mph effective to a height of 100 ft above ground and a vertical speed of 70 mph. A second missile is considered: a 3-in diameter steel pipe weighing 75 lbs with an impact velocity of 50 mph, effective to a height of 75 ft above ground and a vertical velocity of 35 mph. For the straight wind missile, an 8-in concrete masonry unit (CMU) wall, single wythe (single layer) brick wall with stud wall, or a 4-inch concrete (reinforced) is considered adequate to prevent penetration. For the tornado missile, an 8-to-12-in CMU wall, single wythe brick wall with stud wall and metal ties, or a 4- to 8-inch concrete (reinforced) slab is considered adequate to prevent penetration (depending on the missile). (Refer to DOE-STD-1020-94 for additional details.)
- (2) For sites where tornadoes are considered a viable threat, to account for objects or debris the same 2x4 inch timber is considered but for heights above ground to 50 ft. The tornado missiles are (1) the 15 lbs, 2x4 inch timber with a horizontal speed of 150 mph effective up to 200 ft above ground, and a vertical speed of 100 mph; (2) the 3-inch diameter, 75 lbs steel pipe with a horizontal speed of 75 mph and a vertical speed of 50 mph effective up to 100 ft above ground; and (3) a 3,000 lbs automobile with ground speed up to 25 mph. For the straight wind missile, an 8-in CMU wall, single wythe brick wall with stud wall, or a 4-inch concrete (reinforced) is considered adequate to prevent penetration. For the tornado missile, an 8 in CMU reinforced wall, or a 4-to- 10-inch concrete (reinforced) slab is considered adequate to prevent penetration (depending on the missile). (Refer to DOE-STD-1020-94 for additional details.)

3. Recommended Values for Risk-informed Assessment of Spent Fuel Pools

The tornado strike probabilities for each F-scale interval were determined from the SPC raw data on a state-averaged basis. For each F-scale, the point strike probability was obtained from the following equation:

$$P_{fs} = \left(\frac{\sum_N <a>_T}{A_{ob}} \right) \times \frac{1}{Y_{int}}$$

Equation A2e-1

where:

P_{fs} = strike probability for F-scale (fs)

$<a>_T$ = tornado area, mi²

A_{ob} = area of observation, mi² (state land area)

Y_{int} = interval over which observations were made, years

\sum_N = sum of reported tornados in the area of observation

The tornado area, $<a>_T$, was evaluated at the midpoint of the path-length and path-width intervals shown in Table A2e-1, based on the SPC path classifications. For example, an F2 tornado with a path-length scale of 2 has an average path length of 6.55 miles and with a

path-width scale of 3, an average width of 0.2 miles.

The tornado area, $\langle a \rangle_T$, was then modified using the method described in NUREG/CR-2944 (based on Table 6b and 7b) to correct the area calculation by observations of the variations in a tornado's intensity along its path length and path width (see Figure A2e-3). Table A2e-2 gives the path-length correction data. Table A2e-3 gives the path-width correction data. The corrected effective area has a calculated $\langle a \rangle_T$ of about 0.28 mi². The combined variation in intensity along the length and across the width of the tornado path is shown in Table A2e-4 (Table 15b from NUREG/CR-2944). For example, an F2 tornado with a path-length scale of 2 and a path-width scale of 3 has a calculated $\langle a \rangle_T$ of about 0.28 mi². The total area is reapportioned using Table A2e-4 to assign 0.11 mi² to the F0 classification, 0.13 mi² to the F1 classification, and 0.04 mi² to the F2 classification.

The risk regionalization scheme from NUREG/CR-2944, as shown in Figure A2e-4, was used to determine the exceedance probability for each region identified. A continental U.S. average was also determined. Figure A2e-4 shows the approximate location of commercial LWRs and independent spent fuel storage facilities.

The SPC raw data for each state was used to determine the F-scale, path-length and path-width characteristics of the reported tornadoes. The effective tornado strike area was corrected using the data from NUREG/CR-2944. Equation A2e-1 was used for each state and the summation and averaging of the states within each region (A, B, C and D, as well as a continental USA average) performed. The results for the exceedance probability per year for each F-scale are given in Table A2e-5, and graphically presented in Figure A2e-5. The SPC data analysis is summarized in Table A2e-6.

4. Significant Pool Damage

An F4 to F5 tornado would be needed to consider the possibility of damage to the spent fuel pool by a tornado missile. The likelihood of having or exceeding this size tornado is estimated to be 5.6×10^{-7} per year (for Region A), or lower. In addition, the spent fuel pool is a multiple-foot thick concrete structure. Based on the DOE-DOE-STD-1020-94 information, it is very unlikely that a tornado missile would penetrate the spent fuel pool, even if it were hit by a missile generated by an F4 or F5 tornado.

5. Support System Availability

An F2 or larger tornado would be needed to consider damage to support systems (power supplies, cooling pumps, heat exchangers, and make-up water sources). The likelihood of the exceedance of this size tornado is estimated to be 1.5×10^{-5} per year (for Region A), or lower. This frequency is bounded by other more likely initiators that can cause loss of support systems.

6. References

- 1 NUREG/CR-2944, "Tornado Damage Risk Assessment," Brookhaven National Laboratory, September 1982
- 2 <http://www.ncdc.noaa.gov/>
- 3 NUREG/CR-5042, "Evaluation of External Hazards to Nuclear Power Plants in the United States," Lawrence Livermore National Laboratory, December 1987.

- 4 DOE-STD-1020-94, "Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities," January 1996, Department of Energy

Table A2e-1 Tornado Characteristics

F-scale	Damage and wind speed	Path-length scale		Path-width scale	
		Scale	Length (mi)	Scale	Width (yds)
0	Light Damage (40-72 mph)	0	< 1.0	0	< 18
1	Moderate Damage (73-112 mph)	1	1.0 - 3.1	1	18 - 55
2	Significant Damage (113-157 mph)	2	3.2 - 9.9	2	56 - 175
3	Severe Damage (158-206 mph)	3	10.0 - 31.9	3	176 - 527
4	Devastating Damage (207-260 mph)	4	32 - 99.9	4	528 - 1759
5	Incredible Damage (261-318 mph)	5	100 >	5	1760 >

Table A2e-2 Variation of Intensity Along Length Based on Fraction of Length per Tornado^(*)

Local tornado state	Recorded tornado state					
	F0	F1	F2	F3	F4	F5
PL-F0	1	0.383	0.180	0.077	0.130	0.118
PL-F1		0.617	0.279	0.245	0.131	0.125
PL-F2			0.541	0.310	0.248	0.162
PL-F3				0.368	0.234	0.236
PL-F4					0.257	0.187
PL-F5						0.172

(*) - Table 6b from NUREG/CR-2944

Table A2e-3 Variation of Intensity Along Width Based on Fraction of Width Per Tornado^(*)

Local tornado state	Recorded tornado state					
	F0	F1	F2	F3	F4	F5
PW-F0	1	0.418	0.154	0.153	0.152	0.152
PW-F1		0.582	0.570	0.310	0.264	0.262
PW-F2			0.276	0.363	0.216	0.143
PW-F3				0.174	0.246	0.168
PW-F4					0.122	0.183
PW-F5						0.092

(*) - Table 7b from NUREG/CR-2944

Table A2e-4 Combined Variation in Intensity Along Length and Across Width of Tornado Path^(*)

Local tornado state	True maximum tornado state					
	F0	F1	F2	F3	F4	F5
CV-F0	1.0	0.641	0.380	0.283	0.298	0.286
CV-F1		0.359	0.471	0.433	0.358	0.333
CV-F2			0.149	0.220	0.209	0.195
CV-F3				0.064	0.104	0.116
CV-F4					0.031	0.054
CV-F5						0.016

(*) - Table 15b from NUREG/CR-2944

Table A2e-5 Exceedance Probability for Each F-scale

NUREG/CR-2944 Region	Exceedance probability (per year)					
	F0	F1	F2	F3	F4	F5
A	7.4E-05	4.4E-05	1.5E-05	3.5E-06	5.6E-07	3.1E-08
B	5.6E-05	3.3E-05	1.1E-05	2.5E-06	3.7E-07	2.1E-08
C	2.9E-05	1.5E-05	4.1E-06	8.9E-07	1.3E-07	4.7E-09
D	3.6E-06	1.6E-06	3.9E-07	8.7E-08	1.6E-08	---
USA	3.5E-05	2.0E-05	6.1E-06	1.4E-06	2.2E-07	1.0E-08

Table A2e-6 SPC Data Analysis Summary by State

State	NUREG/CR-2944 Region				Years	Tornado F-scale							Total	Point Strike Probability (per year)				
	A	B	C	D		F0	F1	F2	F3	F4	F5	F0		F1	F2	F3	F5	
AL	X	X			46	165	364	323	129	36	14	1031	2.9e-05	3.2e-05	1.3e-05	3.7e-06	6.9	
AZ				X	44	90	57	11	2	0	0	160	6.7e-07	2.9e-07	3.6e-08	1.8e-09		
AR	X				46	198	298	331	149	31	0	1007	3.2e-05	3.5e-05	1.3e-05	2.4e-06	1.9	
CA				X	45	142	58	21	2	0	0	223	5.1e-07	2.7e-07	6.0e-08	2.7e-09		
CO			X	X	46	616	441	99	15	1	0	1172	4.4e-06	2.0e-06	4.2e-07	3.9e-08	3.3	
CT			X		46	9	29	20	5	2	0	65	1.1e-05	1.1e-05	3.6e-06	8.5e-07	2.2	
DE			X		42	20	23	11	1	0	0	55	2.6e-05	1.5e-05	1.5e-06	6.4e-09		
DC*					1	1	0	0	0	0	0	1	1.3e-04	0	0	0		
FL		X	X		46	1156	665	293	30	4	0	2148	1.5e-05	8.6e-06	2.2e-06	2.8e-07	2.0	
GA		X			46	147	537	266	65	17	0	1032	2.9e-05	3.0e-05	1.2e-05	3.4e-06	4.3	
ID				X	42	63	53	8	0	0	0	124	4.7e-07	1.9e-07	1.4e-08	0		
IN	X				46	246	336	263	108	77	8	1038	3.3e-05	3.5e-05	1.5e-05	5.2e-06	1.2	
IA	X				46	478	506	421	119	74	9	1607	3.7e-05	3.7e-05	1.4e-05	3.1e-06	6.1	
IL	X				46	431	440	316	113	39	3	1342	3.0e-05	2.7e-05	9.8e-06	2.5e-06	3.3	
KS	X	X			46	1111	610	404	168	54	16	2363	3.5e-05	3.0e-05	1.1e-05	3.0e-06	5.8	
KY	X				46	79	168	133	65	35	3	483	1.6e-05	1.7e-05	6.9e-06	1.8e-06	3.1	
LA		X			46	225	620	268	123	16	2	1254	2.4e-05	2.2e-05	6.9e-06	1.4e-06	1.2	
ME				X	42	21	44	17	0	0	0	82	1.8e-06	1.1e-06	1.7e-07	0		
MD			X		46	49	92	26	5	0	0	172	1.5e-05	9.2e-06	9.4e-07	8.2e-09		
MA			X		45	24	72	31	8	3	0	138	1.2e-05	1.1e-05	4.3e-06	1.6e-06	3.7	
MI		X	X		45	195	308	210	57	30	7	807	1.4e-05	1.4e-05	5.2e-06	1.4e-06	2.8	
MN		X	X		46	372	336	158	53	28	6	953	1.4e-05	1.2e-05	3.5e-06	7.2e-07	1.3	
MS	X	X			46	226	468	369	136	59	10	1268	4.4e-05	4.4e-05	1.7e-05	5.0e-06	1.0	
MO	X				46	298	577	334	109	48	1	1367	1.8e-05	1.6e-05	5.3e-06	1.3e-06	2.3	
MT				X	44	174	42	33	4	0	0	253	1.0e-06	7.0e-07	2.3e-07	2.2e-08		
NE		X	X		46	827	585	255	105	42	4	1818	2.9e-05	2.9e-05	1.2e-05	3.5e-06	3.5	
NV				X	34	41	8	0	0	0	0	49	2.9e-07	4.0e-08	0	0		
NH				X	45	24	34	15	2	0	0	75	4.7e-06	2.4e-06	4.7e-07	1.1e-08		
NJ			X		45	43	58	23	4	0	0	128	1.7e-05	6.6e-06	7.9e-07	7.1e-09		
NM			X		46	261	104	31	4	0	0	400	1.5e-06	5.2e-07	8.0e-08	1.1e-09		
NY				X	44	101	106	35	21	5	0	268	7.6e-06	6.1e-06	2.3e-06	8.8e-07	2.2	
NC			X		46	153	321	143	44	26	0	687	1.5e-05	1.4e-05	4.9e-06	1.5e-06	2.5	
ND			X		46	490	211	91	28	7	3	830	4.7e-06	3.2e-06	1.1e-06	3.6e-07	9.1	
OH	X				46	157	321	166	53	27	9	733	2.1e-05	1.8e-05	5.6e-06	1.3e-06	3.0	
OK	X				46	845	808	626	209	83	9	2580	4.1e-05	3.9e-05	1.4e-05	3.6e-06	7.0	
OR				X	45	31	15	3	0	0	0	49	2.9e-07	1.5e-07	3.1e-08	0		
PA			X		46	93	220	143	26	22	2	506	9.4e-06	9.0e-06	3.3e-06	9.3e-07	2.0	
RI			X		23	3	4	1	0	0	0	8	1.9e-05	1.3e-05	1.7e-06	0		
SC		X			46	136	234	100	31	15	0	516	1.9e-05	1.9e-05	6.8e-06	1.8e-06	3.0	

SD		X	X		46	651	259	197	57	7	1	1172	9.7e-06	8.1e-06	3.0e-06	7.7e-07	1.5
TN	X				46	107	241	139	76	29	4	596	2.2e-05	2.2e-05	8.3e-06	2.1e-06	2.0
TX		X	X		46	263 2	1837	1067	317	76	5	5934	1.6e-05	1.3e-05	4.3e-06	1.1e-06	1.8
UT				X	43	53	19	6	1	0	0	79	5.1e-07	3.2e-07	1.0e-07	2.8e-08	
VT				X	41	7	14	12	0	0	0	33	3.3e-06	2.0e-06	3.4e-07	0	
VA			X		45	84	132	68	28	6	0	318	8.5e-06	7.0e-06	2.0e-06	4.4e-07	7.1
WA				X	41	24	17	12	3	0	0	56	4.9e-07	9.6e-08	2.3e-08	3.6e-09	
WV			X		45	27	36	16	8	0	0	87	2.2e-06	2.4e-06	9.7e-07	2.5e-07	
WI		X	X		46	204	378	276	62	24	5	949	2.6e-05	2.4e-05	7.9e-06	1.4e-06	2.5
WY				X	46	247	145	43	8	1	0	444	2.5e-06	1.2e-06	3.1e-07	7.1e-08	1.9
Sum						137 76	13251	7834	2553	924	121	38459					

* DC was not included in the exceedance analysis.

Figure A2e-1

Annual Average Number of Tornadoes per 10,000 Square Miles by State, 1950-1995

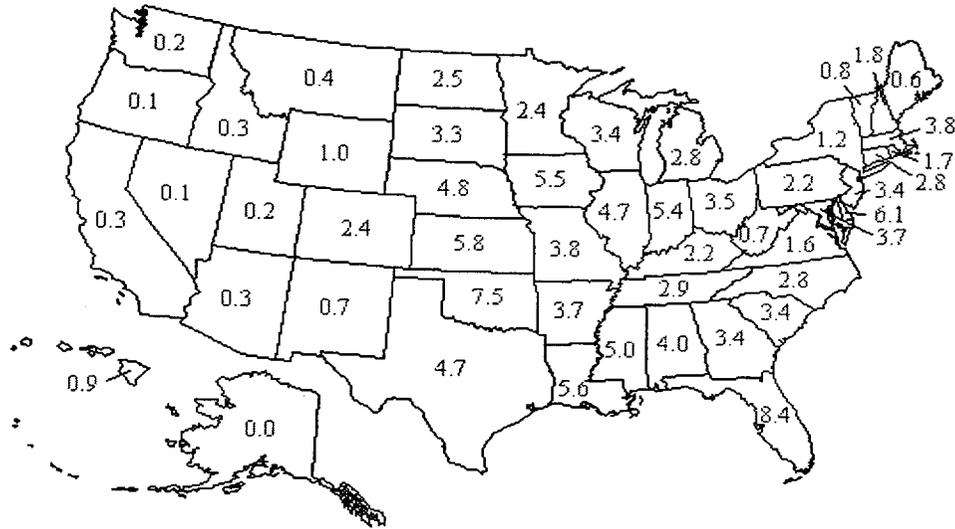


Figure A2e-2

Average Annual Number of Strong-Violent (F2-F5) Tornadoes per 10,000 Square Miles by State

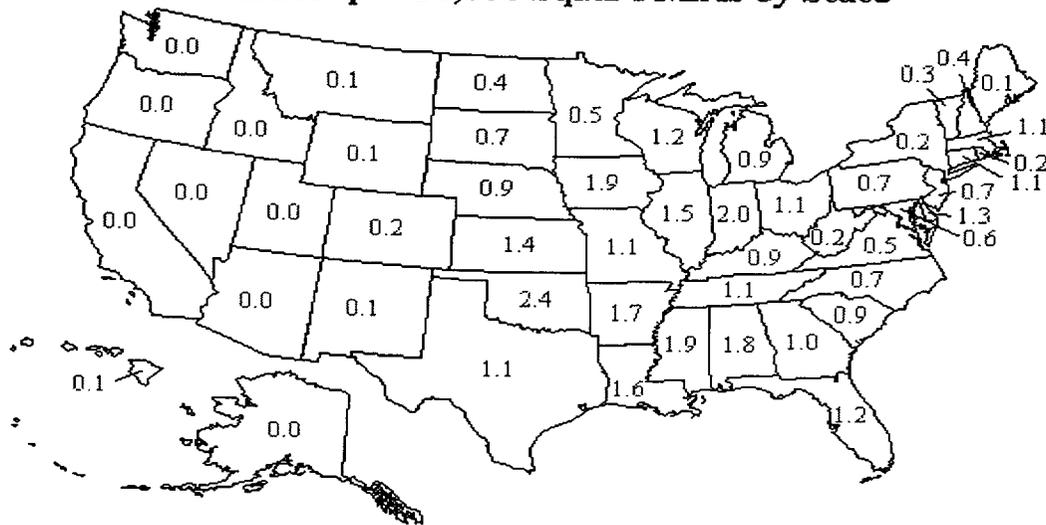


Figure A2e-3 Sketch of Hypothetical F2 Tornado Illustrating Variations

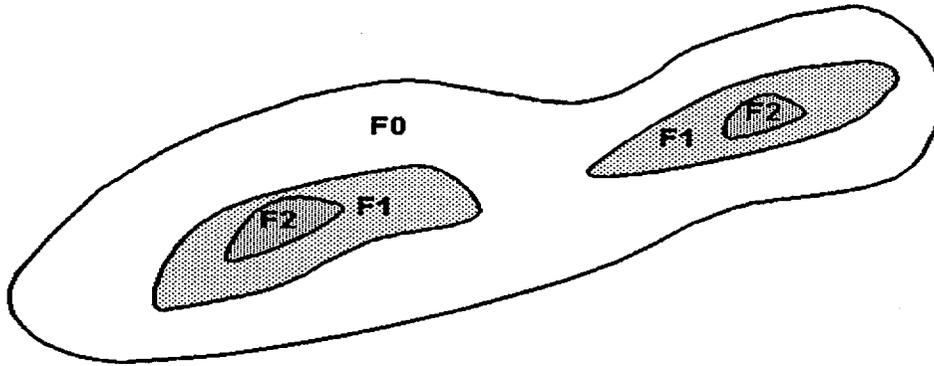


Figure A2e-4 Tornado Risk Regionalization Scheme (from NUREG/CR-2944)

Figure A2e-5 Tornado Exceedance Probability For Each F-scale

