## Spent Fuel Pool Human Reliability Analysis (HRA)

### I. Introduction

One of the key issues that has emerged 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 initial risk assessment performed by the staff used estimates of human error probabilities that resulted in operator non-response being a significant contribution to the estimates of risk. The industry expressed its concern that, because of the very long time scales (typically, tens of hours) and the relative simplicity of the required actions compared with those needed to control nuclear power reactor transients, the non-response probabilities should be very low, and, in particular, much lower than those assumed in the staff analysis.

The objective of this report is to explore this issue and identify, in a systematic way, under what design features and operational practices, taking into account the full range of possible challenges to the pool functionality, it can be argued that the non-response probabilities can 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 identifying general design features and operational practices that can support low non-response probabilities. If the details of how the licensees intend to operate during this phase of operation were known, it would have then been possible to turn the question around, and, on a plant specific basis, identify error forcing conditions that would lead to non-response probabilities that are not low.

It should be noted that it is not the intent in this report to provide definitive values for the human error probabilities in the model, but to provide example analyses that produce a range of results that indicate the value of certain features of design or operation in achieving high reliability in operator response. This exercise will provide input to a technical study that will assist the exemption process and rulemaking development for decommissioning nuclear power plants.

Section II 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 III discusses the factors that recent studies have shown to be significant in establishing adequacy of human performance. Section IV discusses each of the human failure events of the Staff's PRA model. Conclusions are presented in Section V.

### II. Analysis Approach

The human reliability analysis (HRA) approaches that have been developed over the past few years have primarily been for use in PRAs of nuclear power plants at full power. Methods have been developed for assessing the likelihood of errors associated with routine processes such as restoration of systems to operation following maintenance, and those errors in responding to plant transients or accidents from full power. For spent fuel pool operation during the

decommissioning phase, there are unique conditions not typical of those found during full-power operation. Thus the human reliability methods developed for full power operation PRAs, and their associated error probabilities, are not directly applicable. However, some of the methods can be adapted to provide insights into the likelihood of failures in operator performance for the spent fuel pool analysis by accommodating the differences in conditions that might impact operating crew performance in the full power and decommissioning phases. There are both positive and negative aspects of the difference in conditions with respect to the reliability of human performance.

Examples of the positive aspects are:

- For most scenarios, the time-scale for changes to plant condition to become significant are protracted. This is in contrast to full power transients or accidents in which response is required in a relatively short time, ranging from a few minutes to a few hours. In the staff's analysis, times ranging from 50 to greater than 120 hours were estimated for heat up and boil off following loss of spent fuel pool cooling. Thus, there are many opportunities for different plant personnel to recognize off-normal conditions, and a long time to take corrective action, such as making repairs, hooking up alternate cooling or inventory make-up systems, or even bringing in help from off site.

- There is only one function to be maintained, namely decay heat removal, and the systems available to perform this function are relatively simple. By contrast, in the full power case there are several functions that have to be maintained, including criticality, pressure control, heat removal, containment integrity.

- With respect to the last point, it is also expected that the number of controls and indications that are required in the control room are considerably fewer than for an operating plant, and therefore, there is less cause for confusion or distraction.

Examples of the negative aspects are:

- The plant operation is not as constrained by regulatory tools such as technical specifications, and there is no requirement for emergency procedures.

- Because the back-up systems are not automatically initiated, operator action is essential to successful response to failures of the cooling function.

- There is expected to be little or no redundancy in the on-site mitigating capability as compared with the operating plant mode of operation. (In the staff's initial evaluation, because little redundant onsite equipment was assumed to be available, the failure to bring on offsite equipment was one of the most important contributors.) This implies that repair of failed functions is relatively more significant in the risk analysis for the spent fuel pool case.

In developing the arguments documented in this report, the following issues have been identified as being important:

- Because of the long time scales, it is essential to address the potential for recovery of failures on the part of one crew or individual by other plant staff, including subsequent

shifts, and to consider potential sources of dependency that could lead to a failure of the organization as a whole to respond adequately.

- Identification of the conditions under which operating staff performance can be considered as providing high reliability should be based upon current understanding of the factors that influence human performance. There are several references that provide good overviews of the factors of importance, including HEART (Williams), CREAM (Hollnagel), and ATHEANA (NRC).

- Those factors that the industry has suggested that will help ensure adequate response (instrumentation, monitoring strategies, procedures, contingency plans) should be addressed (NEI review of Staff analysis).

- 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.

The Staff's PRA logic model is adopted as being an appropriate framework for analyzing the risk from a spent fuel pool within which to discuss the human performance issues. Thus the human failure events discussed are defined in terms of the PRA model as documented in the attachments to this report.

## III. 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.

## III.1 Detection of Deviant Conditions

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

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

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

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

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

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

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

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

III.2 Situation Assessment and Response Planning

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

The types of procedures that might be available are:

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

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

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

In addition:

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

III.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

IV. <u>Analysis of the Specific Human Failure Events (HFEs) of the PRA model</u>

In order to provide a credible assessment of the effectiveness of the mitigation activities proposed, based on current models of human reliability, it is necessary to have enough detail about the way the mitigation activities are implemented that a model can be constructed. Since the details of the implementation of the mitigation strategies are not known at this time, and are likely to vary from plant to plant, the following discussion is based upon some fairly broad assumptions. The intent is to provide examples of analyses using simple models that capture the essential factors that would help assure that human performance in responding to an incident are incorporated. Each of the events in the Staff's model is discussed.

IV.1 Detection of Deviant Conditions

IV.1.1 HEP-RES-ALARM: (Original description is "Operator fails to respond to an alarm in the control room".) This event is included in the original Staff analysis as a contributor to the event tree heading CRA. The current model assumes there is only one alarm.

This basic event represents the failure of the operating staff to detect and respond to an indication of an off-normal condition, given an operable alarm (or alarms) in the control room. The failure of the alarm itself, and the failure of the electrical supply to the alarm, are represented as separate events in the functional fault tree for the event tree top event CRA.

The following discussion focuses on a single alarm.

The THERP (Techniques for Human Error Rate Prediction) handbook, NUREG/CR-1278, gives a range of probabilities for response to annunciated abnormal events. For an immediate response that is governed by plant rules, Table 20-23 suggests an HEP of 3E-04[1]. This is appropriate for a plant in which the alarm associated with the spent fuel pool is well delineated, and that all other alarms, annunciators, etc. are segregated, disconnected or otherwise made unobtrusive. Otherwise, any interference from irrelevant alarms will clearly decrease the likelihood of success. This is illustrated in Table 20-23 which shows the probability of failure increasing with the number of alarms to be attended to. If some diagnosis is involved, this HEP is considered time dependent and the screening model in Table 20-1 gives an HEP of 3E-03 at one hour, and about 1E-03 in one day. In the context of the Staff's PRA model, the HFE can be regarded as failure to recognize that there is a problem rather than a failure to diagnose the specific cause. Therefore, as long as it is an operating practice or rule that the cause of the alarm be investigated immediately, a base HEP in the range of 3E-03 to 3E-04 for a single crew is appropriate.

However, in NUREG/CR-1278, very little credit for success is given if the operator cancels the alarm and does not respond within a minute of the alarm. PSFs that could influence the likelihood of not responding immediately to the alarm include; a) the alarm set-point is such that there is a history of false alarms, b) the alarm is not perceived to be important. Furthermore, very little credit is given for detection by periodic scanning that is not dictated by procedure (Table 11-12). Thus, the alarms associated with critical process parameters associated with fuel pool cooling or level should be set at meaningful levels, and it should be understood that they are to be responded to immediately.

In those cases where there is a significant amount of time before action is required, several crews would have to fail to respond to the alarm for the failure to occur. This is likely to be the case for a loss of cooling and for a slow loss of inventory. For the large loss of inventory, the rate of loss clearly has an effect, and may determine whether a second or third crew can be credited. How much credit can be taken for successive crews depends on the nature of the alarms and crew responses. If, for example, the alarm could be permanently canceled, this would defeat the opportunities for subsequent crews to respond. However, typically, the auditory alarm and flashing light would be canceled but the annunciator tile would remain lit until the problem had been fixed. As mentioned above, NUREG/CR-1278 gives very little credit for detection of deviant conditions if not directed by a procedure. However, if there is a purposeful

---

[1]All HEPs are given as mean values, evaluated using the median values and error factors given in NUREG/CR-1278 on the assumption of a lognormal distribution.

directed checking of status, as might occur at a shift changeover for example, then a high probability of success is possible. Possible failure modes include: failing to follow an administrative procedure (Table 20-6, item (2) suggests an HEP of 1E-02); and failure to register the tile being lit (the discussion in the section "check reading indicator lamps" in Chapter 11 of NUREG/CR-1278 would suggest an HEP of 3E-03).

It could be argued that the probabilities given in Chapter 11 of NUREG/CR-1278 are somewhat pessimistic for the spent fuel pool case, as they are more applicable to the control room of an operating plant in which there is a very large number of annunciators. However, the discussion indicates the factors that can influence the likelihood of success, and taking these issues into consideration, a range of values can be estimated for this HEP.

At one extreme, if the alarm were for some reason not to be taken seriously, which could happen for example if it were set within the normally expected operating range, the probability of ignoring the alarm, even by several crews could be high. In fact there have been cases, e.g., the September 23, 1991 event at Wolf Creek, where an alarm was essentially ignored for three days. On the other hand, if the alarm, by plant practices is always something that has to be investigated, and there is a requirement to check the status of the panels at a shift changeover, then, even if the operator was distracted after canceling the alarm, a case could be made for the HEP being low, on the order of 1E-05 or less.

However, for there to be a convincing case that the function required, i.e., to provide awareness that the spent fuel pool conditions have degraded enough to warrant attention, is satisfied with high reliability, there are additional constraints that include:

- the alarm measures directly a parameter characterizing the physical state of the spent fuel pool
- the alarm is reliable

In conclusion, given an alarm with a meaningful setpoint, and a plant rule to respond by investigating the cause of the alarm, together with plant operational procedures that require checking of all equipment status at least once a shift should be adequate to assure such a low probability.

Given also, that, for some initiating events, there are several related alarms, the probability may be argued to be even lower, but only if the alarms can truly be argued to be independent and reinforcing. This could be demonstrated by constructing a more detailed logic model (fault tree) for the TOP event CRA. For example, in the case of loss of cooling, an alarm on pool temperature may be preceded by an alarm indicating trouble with the primary cooling system, or an alarm on pool level may be preceded by a drain or sump alarm. It is noted, however, that such alarms were not present at the plants visited by the staff.

IV.1.2 REC-WLKDWN-LOC/REC-WLKDWN-LOI-S/REC-WLKDWN-LOI-L "Operator fails to notice loss of cooling event/a relatively slow decreasing level in the SFP/ a relatively fast decreasing level in the SFP during walkdowns." Again, these events should really be described as "operating staff fail to detect, over several shifts, .... ." For the fast loss of inventory in particular, the credit for successive crews may be limited.

Chapter 19 of NUREG/CR-1278 presents models for detection of deviant conditions as a result of operator walkdowns. On the basis of a specific set of assumptions, including that no written

procedure is used, no special oral instructions are given, and deviations are "fairly obvious", Table 19-4 gives probabilities of failure to detect a particular deviant condition within 30 days for a variety of different inspection routines. The probability of failure for a three shift system with one inspection per shift is high, .52, driven by a low expectation on the part of the plant personnel of finding a (low probability) deviant condition, and on an assumption of reliance on memory to detect differences in plant status from one observation to the next.

The term "fairly obvious" is not defined, but by inference means noticeable without being clearly obvious, since it is assumed in the Handbook that very obvious indications such as a large pool of water on the floor, and presumably steam rising from the pool, would always be noticed. Thus, such gross indications are assumed to guarantee identification of the need to respond. The principal requirement for these obvious indications would be that the walkdowns were indeed carried out with a frequency that would result in observation of the deviant condition before fuel uncovery.

Since, for many of the initiating events, the pool conditions are expected to change slowly, and, while they may be noticeable, they need not be readily detectable. The efficacy of an early detection of a deviant condition would be greatly increased by requiring measurements to be taken, recorded, and trended. In this case, changes could be identified early.

Possible failure modes for the function, carried out using a formal walkdown procedure, include (numbers in parenthesis refer to numbers taken from the referenced table in NUREG/CR-1278):

- failure to carry out inspection (1E-03, Table 20-6)
- missing a crucial step in the written procedure (ranging from 1E-02 to 1E-03, Table 20-7)
- misreading a measuring device (on the order of 3E-03, Tables 20-10 and 20-11)

A detailed model could only be developed by making some detailed assumptions about the nature of the administrative procedure for performing the walkdown inspections. So, for example, if it were assumed that there is a procedure with a short check-off list which includes recording one parameter value, read from analog meter, then the probability of failure of one operator to measure the parameter is

1E-03, (failure to carry out inspection) +
1E-03, (omission, item (1) in Table 20-7) +
3E-03, (error of commission, item (1) in table 20-10) = 5E-03

If there are two parameters that have to be checked, then the failure probability would be dominated by the failure to carry out the inspection. If each shift can be regarded as acting independently, then the failure probability over two crews would be the square of the HEP for one crew. That over three shifts would be the cube of the HEP. The limiting factor would be something that would create a inter-crew dependency. Possible mechanisms for introducing dependency include a lack of management commitment to, or lack of enforcement of, carrying out the inspections, a poorly written procedure, or analog meters that are badly designed.

The range of possible values for the HEP is large. However, given a strict adherence to carrying out walkdowns, and a procedure that directs the checking of critical parameters, with a requirement for trending the observed values to identify slowly changing conditions, the

likelihood of not detecting a deviant condition over several crew changes can be argued to be very low. Of course, a key assumption is that the deviant condition is reported in a timely manner to the decision-maker on the operating crew.

IV.1.3 Dependency

The two events HEP-RES-ALARM and REC-WLKDWN-XXX, appear in the same sequence. Therefore it is reasonable to ask whether there is some common cause mechanism. Since the combination of failures would represent a failure of the control room operators to take charge of the situation and initiate some response, they are a single point in the process. However, given the independent nature of the separate sets of indications, failing to respond would in all likelihood have to be a wilful decision, motivated, for example, by a belief that the indications were not correct. A safety culture that allowed for non-adherence to administrative practices would also provide such a mechanism.

IV.2 Recovery Events:

There are several different recovery events in the model. It is assumed that, since the failure to recognize that there is a deviant condition is already accounted for in the events discussed in Section IV.1, these events represent the failure of the operators to identify the cause of the problem and take appropriate corrective action. These events therefore should include failures in situation assessment and response planning and in the execution of those plans. The details of the steps required to perform these recovery actions are not known at this time.

IV.2.1 The events HEP-COOL-LOC-E, HEP-COOL-LOC-L, and HEP-COOL-LOP-E, represent the failure to restore the normal cooling system, for three different conditions. The first two, early and late, refer to the cases where detection is as a result of an alarm, and when detection is a result of alternate means of detection respectively. It is assumed there will be less time to respond in the second case. Given that the time scales are so long, it is not clear that this is an important factor in determining the HEP.

The third event, HEP-COOL-LOP-E, represents the failure to restore after recovery of offsite power, and therefore represents failure to perform a straightforward system restart. Since this is assumed to be a simple, and obvious step to take, the value of 3E-03 used in the initial staff analysis is appropriate for the initial failure to restart, being a value typically used in PRAs, but given that will typically still be a significant amount of time before fuel uncovery, (restoration of offsite power from plant centered events is typically on the order of hours, and from severe weather, on the order of a day) there are ample opportunities to recover, suggesting that a case could be made for a much lower value, on the order of 1E-04 or less.

Events HEP-COOL-LOC-E, HEP-COOL-LOC-L are different in nature in that the response required is repair as opposed to a simple restoration. This is not typically addressed in PRAs by HRA techniques, but by actuarial data on repair times. In the initial staff paper, an exponential repair model with a mean time to repair of 10 hours, with a cut-off value of 1E-04. This cut-off is certainly not unreasonably high, given that what it represents is a likelihood that in 1 in 10,000 failures, the cause is sufficiently severe that it cannot be repaired, or a replacement found and installed.

IV.2.2 Events HEP-INV-MKUP-E, and HEP-INV-MKUP-L are events that represent the failure to isolate leaks and to start the make-up system. Again, these event probabilities are dependent on the location of the leaks and whether they can be isolated. The PRA model uses the same basic event in the function 'failure to use the fire system as an alternate make-up system', which essentially assumes that the dominant factor is the failure to isolate. The source of a leak large enough to exceed the capacity of both the make up pump and the fire pump and require isolation should be identifiable given accessibility to the areas adjacent to the pool or the cooling systems. Thus the factors that influence the failure probability include the location of the leak, the accessibility for both visual inspection and isolation, and the size of the leak (which in turn governs the time available to perform the isolation). A low probability could be assumed if the locations of potential leaks (structural failures of the fuel pool itself are excluded as they are non-isolable), can be demonstrated to be readily identifiable, and isolation points are accessible.

Another factor of importance is whether the leak is self-limiting. If the possible suction points within the pool are at a high enough level, or protected by anti-syphon devices, the pool cannot be drained beyond a certain level. However, for the larger leaks, it is still necessary to isolate the leak path so that the pool can be refilled and the pool cooling system restarted.

Thus again there is a range of probabilities for this human failure event, the highest being for the case that the leak is not self-limiting, and is of a sufficient size to uncover the fuel in a period of a few hours, and there is no procedure. The lowest probability would be for the case that the leak is self-limiting, there are procedures for dealing with loss of cooling due to leaks, and the leak was identified early, and is on the same order as HEP-COOL-LOP-E.

IV.2.3 HEP-MKUP-SML represents the failure to initiate the normal coolant make-up system for small leaks. This should be a commonly practiced procedure, since presumably it will be required to make up for evaporative losses from the pool. An HEP in the range of 1E-03 to 3E-03 would be typical for a failure of a single operator to start a system. However, given the extremely long time available, there are opportunities for several crews to correct an initial failure, and the likelihood of a sustained failure to correctly initiate the system should be low. The limitation would be the occurrence of an inter-crew common cause failure mechanism. It is difficult to think of such a mechanism, and issues related to a poor safety culture or lack of adherence to good practices would be covered in the failure to recognize there is a problem in the first place. However, given a procedure for loss of cooling due to the occurrence of a loss of inventory, again, the long time available can be used to argue that the probabilities of failure for this event should be low, and on the same order as HEP-COOL-LOP-E.

IV.2.4 The events HEP-ALTCL-E, HEP-ALTCL-L, HEP-ALTCL-LP-E, represent failure to establish alternate cooling, using fire pumps, given a loss of normal spent fuel pool (SFP) cooling. The different cases are: E, response to early indication from the control room; L, later indication from walkdown; and LP-E, given a loss of offsite power. The principle difference between cases E and L is in the time assumed available.

The response for which this event represents failure is contingent upon a failure to reestablish normal cooling, except in the case that there is a non-recovered loss of offsite power, in which case there is no normal cooling available. It is possible to speculate about potential failure mechanisms, e.g., a fixation on trying to repair the normal system, but it is difficult to use such reasoning to assess a probability of failure, since there may be several mechanisms, each with its own PSFs. The likelihood of the failure mechanism postulated above, for example, would be

influenced by the assessment of the operating crew on how close they are to fixing the problem, which in turn depends on the nature of the failure. Instead of building up a model from failure mechanisms, the approach proposed here is to start with an identification of those features of plant operations that could help to ensure that, if required, the action would be taken. These could include:

- clear procedural guidance that the addition of water to the SFP is an appropriate contingency,
- guidance on when to begin the alignment of the fire water systems so that action can be taken in a timely manner,
- guidance on when to start adding water to the pool,
- provision of a dedicated person to monitor conditions, and determine when water addition should begin,
- a demonstration that the alignment can be achieved within the time expected to be available and assumed in setting the guidance on when to begin addition of water to the pool,
- training in the procedures and the alignment of the systems.

Other factors that influence the possibility of success include:

- whether the there is a need to run hoses or to connect them to an existing injection path
- whether all required equipment is situated in the vicinity of where the required actions are to be taken.

With the conditions defined, the problem becomes more constrained and amenable to evaluation. Since the response is likely to involve manual action in the vicinity of the pool area, one of the constraints that needs to be addressed is that caused by environmental conditions, such as high radiation, high humidity, or flooding. These will be event specific. For example, high radiation is more of a concern for the drain-down scenario than it is for the loss of cooling. Therefore, a higher probability of failure might be considered for the drain down scenario when compared with the loss of cooling scenario. The impact is not likely to be great however, except for the large, non-self-limiting loss of inventory situation.

The probability of this event could range from relatively high if there is no procedure and the required actions are not straightforward, to values in the range of 1E-03 or lower given the response procedures clearly identify this as a possible contingency and the actions are easily performed. Distinctions between the late and early cases are probably minor given that this is a last resort type of action.

IV.2.5 Events REC-INV-OFFSITE, REC-INV-OFFSITE1, REC-INV-OFFSITE2, REC-INV-OFFSITE3, represent failure to recover inventory using offsite sources (e.g., fire trucks) for various time frames. Again, this event appears when all local means of adding water to the pool have failed. Since the actual response would be one for which a fire department could be expected to execute with a high success probability, given there are no physical obstacles that prevent access to the pool building, the key to success would be for the plant staff to plan early enough ahead to ensure that a fire truck was available when needed. As with the HEP-ALTCL-XXX events, the influence of the timing of detection of the problem is less significant if there are

procedural instructions to prepare in advance and alert the fire department in a timely manner. The defenses that would help ensure success include:

- clear procedural guidance that the addition of water to the SFP is an appropriate contingency,
- guidance on when to contact the fire brigade to ensure that action can be taken in a timely manner,
- guidance on when to start adding water to the pool,
- provision of a dedicated person to monitor conditions, and determine when water addition should begin,
- a demonstration that the alignment can be achieved within the time expected to be available and assumed in setting the guidance on when to begin addition of water to the pool,
- training in the procedures and the alignment of the systems.

HEP values should be similar to those for HEP-ALTCL-E/L/LP-E, given similar constraints.

## V Summary and Conclusions

The analysis of human performance for responses to incidents at a decommissioned plant is challenging for many reasons, not the least being that the context within which the plant operators are conducting their activities is not well defined. Furthermore, there are no readily available estimates that match the conditions expected, particularly the long times available for response. Consequently, it is not possible to provide estimates of human error probabilities except in a broad range. What has been done in this report is to provide some guidance on ranges of values that could be argued, and to identify the conditions that can help ensure that the likelihood of success is high. If these conditions can be argued to be present, then it can be argued that the human error probabilities are low enough that they do not dominate the risk profile.

## VI References


1. Swain, A. D. and Guttmann, H. E., Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, USNRC, August 1983.

2. Hollnagel, E., Cognitive Reliability and Error Analysis Method, CREAM, Elsevier, 1998.

3. Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA), NUREG-1624, draft report for comment, May 1998.

4. Williams, J. C., A Data-based Method for Assessing and Reducing Human Error to Improve Operational Performance (HEART), proceedings of IEEE 4th conference on Human Factors in Power Plants, Monterey, Ca, 6-9 June, 1988.