From: Diane Jackson NRR
To: Gareth Parry, Richard Barrett, William Huffman NRR
Date: Thu, Sep 16, 1999 3:59 PM
Subject: Re: HRA

Gareth -

As requested, attached are the final files I gave to Projects - the cover letter did get changed before issuance.

Bill - Could you send the final cover letter "to the public" to Gareth please.

I am out tomorrow and in training next week. If you would like a hard copy, look in the file folders at the back of my desk - the row on the right is all TWG - towards the back is one labeled "human reliability."

ALSO - please check in with **Rich Barrett** before Tuesday 21st to give him an update/ status of HRA. NEI is coming in to speak to Brian Sheron at 9:00 on the 21st and HRA is a topic they designated.

Rich - FYI just in case NEI complains about the due date - The "short" time (4 weeks) for HRA comments is to fit into the whole ITQR process to be able to make the current schedule. Also, the public received the same comment period as the experts. It was released about a week later due to internal processing - we had to give it to projects, who had to issue it. As a result, our experts were due a week before public comments were due. Public comments are due this a Friday - Sept. 17. If they are substantially later than this date, we can not guarantee they will get full consideration.

Thanks,
Diane

>>> Gareth Parry 09/16 8:22 AM >>>
Diane:

Could you please send me the final version of the HRA document by e-mail, or is it, God forbid, on ADAMS yet? Why don't you send it me even if it is?

Thanks

Gareth

CC: GTH

9/99

August 11, 1999

TO: Harold Blackman
Dennis Bley

FROM: Gareth Parry

SUBJECT: HUMAN RELIABILITY ANALYSIS (HRA) FOR SPENT FUEL POOLS

As we discussed, I would appreciate your input on the assessment of human error probabilities for spent fuel pool risk assessment for decommissioned plants. Attached is a strawman document discussing the assessment of the contribution of operating staff failure to respond to an incident leading to a loss of the cooling function. Also attached is the probabilistic risk assessment (PRA) model in the form of event trees, fault trees and functional assignments that identify the correspondence between the fault tree gates and the event tree branch points.

The focus of the discussion is on the identification of plant operational practices that serve to enhance performance in responding, or equivalently as defences against failures to respond, to losses of the spent fuel pool cooling function, and to use simple models to calibrate the failure probabilities for example plant practices. This will be used to form the basis for making judgements as to whether existing or planned plant practices are adequate to justify that the likelihood of failing to respond when required to prevent fuel uncovery and possible zirconium fires is a small contributor to risk.

Please review and provide your comments. Specifically could you please address the following:

- Is the general approach sound and consistent with current HRA practices? Suggest modifications or improvements you think are necessary.

- Are the operational practices that are proposed as aids to good performance reasonable? Are additional conditions required to define what constitutes a "good" implementation of the practice. For example, is it necessary to be clearer about the frequency and content of training? I don't believe it is necessary to be overly prescriptive, but it is useful to have some objective criteria against which to assess the "quality" of the practices. Many of the practices are already written so they can be objectively judged.

- One of the keys to arguing for low failure probabilities is that there is so much time for recovery of errors made by a particular crew. Based on your experience in analyzing significant event histories can you identify possible mechanisms for inter-crew common cause failures that would defeat the defences? For example, is it feasible that plant conditions could be such that both alarms and walkdown indications could be rationally argued away?

- Can you suggest suitable representative values, including extreme values, for each of the human error probabilities (HEPs), particularly taking into account the long times

available? Please indicate the assumed conditions for the values you suggest.

- The analysis of the repair and leak isolation events is outside the scope of typical HRA models. In the draft document there are some factors identified that impact the likelihood of success. Are there other factors you could point to that should be identified, perhaps during a walkdown? Do you know of any sources of data that could be used to provide some generic ranges for failure probabilities?

In order to meet our overall schedule, your response is requested by September 10, 1999.

TO: Distribution

SUBJECT: HUMAN RELIABILITY ANALYSIS FOR THE STUDY OF SPENT FUEL POOL ACCIDENTS AT DECOMMISSIONING PLANTS

The Office of Nuclear Reactor Regulation (NRR) is in the process of developing a risk-informed technical basis that will support the establishment of a predictable approach for requesting and granting exemptions to licenses and to increase the efficiency and effectiveness of decommissioning regulations. We developed a draft technical study using deterministic and probabilistic assessments to evaluate spent fuel pool accidents at decommissioning plants. We made this draft report, "Draft Technical Study of Spent Fuel Pool Accidents at Decommissioning Plants," available to the industry and the public and held several public meetings to solicit public comment and provide information to the industry and the public as to how we are proceeding in the process of developing a risk informed approach. We conducted a public workshop on July 15-16, 1999. The purpose of the workshop was to provide the public an opportunity to identify risk perspectives, design characteristics, procedures, capabilities, or other aspects of decommissioning plants that may refine the scenarios and analyses in the draft technical study. At the workshop, we agreed to look further at the human reliability aspects of the risk assessment and involve the public in the process as much as possible.

Attached, for your information, is a draft document on human reliability assessment that is being sent to Dr. Harold Blackman of Idaho National Engineering and Environmental Laboratory, and Dr. Dennis Bley of Buttonwood Consulting, Inc., for their review and comment. They were chosen because they have experience in the following areas:

- Human reliability analysis (HRA), specifically with defining and incorporating human failure events (HFEs) into logic models and the quantification with a variety of models (understanding what are typical probabilities for these HFEs and the conditions they represent);

- Behavioral Science/Cognitive Science, particularly in identifying and characterizing those factors that can influence human performance, in responding to alarms and changing plant conditions, in the performance of routine surveillance, and in the performance of tasks;

- Understanding failures of organizations in preventing major accidents; and

- Probabilistic risk assessments of spent fuel pools

Once their comments are received, the document will be finalized and will represent the staff approach to HRA for this particular application. Comments, particularly from experts with experience matching the criteria above, received by September 10, 1999 will also be considered. Comments should be addressed to U.S. Nuclear Regulatory Commission, Attn: Richard Dudley, Mail Stop O-11 D19, Washington D.C., 20555. Along with your comments, please include a description of your background in this area.

Attachment: As stated

Concurrence: RDudley DTJackson GHubbard JHannon

internal distribution include: GParry GHolahan RBarrett JHannon GHubbard
DTJackson
TEaton

Spent Fuel Pool Human Reliability Analysis (HRA)

I. Introduction

One of the issues that has been raised with respect to the probabilistic risk assessment (PRA) performed for the spent fuel pool during the decommissioning phase of plant life is how much credit can be given to the operating staff to respond to an incident at a spent fuel pool that would, if not attended to, lead to a loss of cooling 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 and the relative simplicity of the required actions, the non-response probabilities should be very low, and, in particular, much lower than those assumed in the staff analysis.

The objective of this task is to explore this issue and identify, in a systematic way, under what conditions, taking into account the full range of possible challenges to the pool functionality, it can be argued that the non-response probabilities can be argued to be low. This exercise will provide input to a technical study that will assist the exemption process and rulemaking development for decommissioning nuclear power plants. The conditions include the physical plant characteristics (e.g., nature and number of alarms, available mitigation equipment) and identifiable and measurable characteristics of operational and management practices, procedures, and training.

II. Analysis Approach

For spent fuel pool operation during the decommissioning phase, there are unique conditions not typical of those found during full-power operation. For most scenarios, the time-scale for changes to plant condition to become significant are protracted so that there are many opportunities for 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. In addition, there is only one function to be maintained, namely decay heat removal, and the systems available to perform this function are relatively simple. However, because the back-up systems are not automatically initiated, operator action is essential to successful response to failures of the cooling function. In the staff's initial evaluation, because there is little in the way of redundant onsite equipment, the failure to bring on offsite equipment is one of the most important contributors.

In developing this approach, the following characteristics were identified as being desirable.

- 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 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.

- Those factors that the industry has suggested that will help ensure adequate response

(monitoring strategies, procedures, contingency plans) should be addressed.

- Where possible, any evaluations of human error probabilities (HEPs) should be calibrated against currently acceptable ranges of HEPs.

- The current PRA model is accepted as being an appropriate framework for analyzing the risk from a spent fuel pool, and is maintained as a framework within which to discuss the human performance issues.

- The reasoning behind the assumptions made should be transparent.

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 represented in some way 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).

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. 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
- 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 existence of independent alarms that measure different primary parameters (e.g., level, temperature), 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)
- active measurement of (multiple, e.g., temperature, level) parameters rather than simply observing the condition of the pool
- requirement to log 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 repair of systems, 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:

- procedures that provide for early action on contingencies (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.

In addition:

- training for plant staff to give an awareness of the time available for response 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. Analysis of the Specific Human Failure Events (HFEs) of the PRA model

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 an indication of the factors that would help assure that human performance in responding to an incident is as effective as possible.

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".

A more accurate description of this event is, 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 is an event in the functional fault tree for event CRA.

The THERP (Techniques for Human Error Rate Prediction) handbook 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. 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. (These values are converted from the median values quoted to rounded off mean values, using the error factors given.) In the context of the model, the HFE can be regarded as failure to recognize that there is a problem rather than a failure to diagnose the cause. Therefore, as long as it is a plant rule that the cause of the alarm be investigated, a base HEP of 3E-04 for a single crew is appropriate.

Because 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. 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 would be canceled but the annunciator light would remain lit until the problem had been fixed. Swain gives very little credit for the operator who canceled the alarm responding to the legend light once one minute has elapsed form the initial cancellation of the annunciator. However, if it is normal practice that on a crew change, the status of all equipment is checked, a probability of 0.95 that the deviant indication would be detected (Table 11-8) is suggested.

One PSF that could influence the likelihood of not responding immediately to the alarm is that the alarm set-point is such that there is a history of false alarms. It is not unreasonable to suppose that the annunciator be canceled and, because of other activities, the corrective action is put off. Using Table 11-12 gives a value of 1E-03 for such a response.

Taking these issues into consideration, a range of values can be estimated for this HEP. The most conservative is:

1E-03 x .05 = 5E-05 (oversensitive alarm and no formal shift change, requiring the second shift to notice the annunciator panel light)

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. 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-LOI-S/REC-WLKDWN-LOC/REC-WLKDWN-LOI-L Operator fails to notice ... . Again, these events should really be described as operating staff fail to detect, over several shifts, that .... .

In Chapter 19 of the handbook, Swain and Guttmann present 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 include (numbers in parenthesis refer to numbers taken from the referenced table in THERP):

- 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 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.

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 have to be a wilful decision, motivated by some plant conditions that were misleading.

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.

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.

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 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.

IV.2.2 Events HEP-INV-MKUP-E, and HEP-INV-MKUP-L are events that represent the failure to isolate leaks <u>and</u> 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, 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.

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.

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.

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.