September 13, 1999

To: Gareth Parry

From: Dennis C. Bley, Buttonwood Consulting

Subject: Review of HRA for spent fuel pools

I have reviewed your "Spent Fuel Pool HRA" and have arranged my comments under the questions that you proposed.

1. Is the general approach sound and consistent with current HRA practices?

The general approach is sound and consistent with current PRA and HRA practice. Whatever problems exist, they are more a matter of defining appropriate conditions and context than in structuring the problem and selecting methods and data bases. The event trees appear to be a good set for covering the spent fuel pool situation. However, the attached PRA package is not complete enough to follow all the connections between the event trees and the selected fault trees. Also, the basis for the three case approach is not always clear. It appears that you have attached parts of the original analysis and commented on appropriate changes. I get the impression that the three case approach was set up to cover uncertainties, but that it often ignores the high likelihood that no human failure event occurs, i.e., it is almost always (except in a few cases I raise below) a pessimistic evaluation. Now to specific comments.

The second paragraph of the introduction indicates that the "objective...is to...identify...under what conditions...the non-response probabilities can be argued to be low." The report does a good job of addressing this objective and most of the following ideas are covered, but turning the question around seems a better approach. From my point of view, the chance of failing to detect and recover from a loss of cooling is very, very small on its face. The better question seems to me to be: Under what conditions might the non-response probabilities *not* be low? Then, for such conditions, the question would be: What training, procedures, instruments and alarms would ensure successful detection and recovery? The danger of the approach, of focusing first on conditions that make success likely, is that we miss some unusual and unlikely conditions that foil our best laid plans.

A Begged Question. In many places the report talks of long, even protracted times for response, but nowhere I looked was this made specific, except in Appendix A of the original PRA and, even there, these times were not justified. From previous work, I seem to recall that the time can vary between about 6 hours immediately after completely filling the pool with the hottest possible final core load to several days as the time after that load extends, to weeks or more for partially filled pools.

Those old analyses calculated, I believe, that makeup requirements for boil-off are very low. If this is the case, much simpler alternatives such as a garden hose connected to city water or

occasional deliveries by tank truck would suffice. Then, with a little pre-planning of the sort described in IV.2, detection becomes the only problem. To cross the Potomac, we don't need the Queen Mary. We really may not need the volume flow rate of the fire water system or the capabilities of a fire engine.

Initiating Events. Your focus on loss of cooling events seems appropriate, with two caveats:

- Seismic events. These are in the event tree. However, a generic analysis may be misleading. Most fuel pools I have seen are part of the structure of the containment and, according seismic fragility experts, will never fail from any plausible earthquake. Note that they acknowledge that, under some conditions, the water can be thrown out of the pool (rather like the swimming pools in California). I have heard that there are some spent fuel pools with much less capable design. For such plants, a thorough analysis may show this to be a significant contributor, with little or no chance for recovery.

- Siphons and pump-down events. Loss of inventory events are modeled with what seems to me an unreasonable high frequency (0.01/year). Again, most pools have no low suction connection that would enable pumping down the pool. Pumping from the high suction with no makeup should be modeled, as it would substantially decrease the initial inventory, when cooling is lost. If there is a low suction or if there is a vacuum cleaner that can discharge outside the pool, all possible hardware and human failure events must be considered. All filling systems or temporary hoses should be examined to ensure no siphon possibilities exist. Special attention is required for any "recovery devices" such as fill hoses, to ensure that hardware and procedural systems prevent the development of a siphon. Errors of commission that enable low suction draining of the pool can defeat all perceived time advantage.

III.1 Detection.

a) Alarms and instruments. I would add two criteria.

- Instruments and alarms should measure, as directly as possible, the parameters that they purport to monitor. While I agree that measurement of diverse parameters is essential backup, far too many incidents in nuclear and other applications are associated with indirect and highly processed measurements; e.g., monitoring pump current as a substitute for flow. Under unusual conditions (and many of these will exist during decommissioning) and in the face of partial failures, operators and control systems have often been led astray.

- Additional parameters. Monitoring humidity and airborne radiation, may be especially important additions to your list. They have been responsible for identifying a number of shutdown loss of cooling events, when the reactor vessel was open.

b) Factors used in assessing effectiveness. I would add trending as well as logging. Again there are many examples of trends going unnoticed as individual readings are logged as if they were

independent events. Trends may be the earliest indicators of problems.
III.2 Procedures. It seems to me that, as in the case of LP&SD, the use of abnormal and maintenance procedures to handle operational concerns during decommissioning is not likely to be effective. Developing one, or a few, formal Decommissioning EOPs for the plant would have great payoff in confidence and assurance that shift operators will be prepared for unusual or common interruptions of cooling. As you indicate in later sections we need to have higher confidence that:

i) Operators will detect losses of cooling and of inventory, and

ii) Operators will know where needed equipment (valves, connectors, hoses, trucks) is or can be obtained, and how best to use it

IV. Introduction. You provide an argument about why you must take a "what do I need to succeed" approach rather than the "what conditions must exist to fail" point of view that I recommend early on. It is a reasonable argument. I still think that focusing on the kinds of things that must go wrong would make a stronger case. The current approach may be open to more questioning and "what-if'ing."

IV.1.1 HEP-RES-ALARM, from "Because there is a significant amount of time..." through three paragraphs to "...annunciator panel light.)" This analysis is suspect and is the first decidedly non-conservative part of the HRA. The 95% probability of a second crew observing the alarm depends on the salience of the alarm. Several things about this analysis makes me believe that it is very optimistic:

- Fuel pool alarms are not generally prominent

- During normal operations there are few lighted alarm tiles and a new one is fairly obvious, especially when an operator scans the panels to assess status before relieving the watch. During "normal" LP&SD conditions, there are many alarm tiles lit, but the patterns are well recognized from years of experience. During decommissioning, nothing is normal or part of our experience. In a plant with hundreds, or even thousands, of alarm tiles, there will be a shifting pattern of lit tiles day to day. Therefore, unless special highlighting of the spent fuel pool alarms is implemented by hardware or training and procedures, Swain's analysis is probably not applicable. Something much more pessimistic akin to the walkdown discussion in Section IV.1.2 may be much more appropriate.

Your subsequent analysis of several related alarms would seem to offer a more sound basis foe the analysis, especially if additional parameters such as humidity and radiation are highlighted.

Event names. Given the arguments presented in the text, it would be nice if detection and recovery events had codes that make that distinction obvious

IV.2.1 I was initially confused to read that "Given that the time scales are so long, it is not clear

that this is an important factor" and then turn to Appendix A and find values from 10^{-4} to 0.1. Similarly at IV.2.3

2. 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? Can the criteria be objectively measured?]

The proposed practices are reasonable. In my response to question (1), I indicated a few additional recommendations: a dedicated plant-specific EOP, alarms on high radiation and high humidity, instruments that directly measure parameters of concern, and monitoring trends.

I think that the criteria are adequately defined for now. It would appear to be up to the licensees to prepare procedures and training. NRC would still have an approval role. The criteria are reasonably objective. It's back to your awareness, situation assessment, response planning and response implementation. These are fairly simple for the condition of concern. The primary emphasis is and should be on detection.

3. Can you identify possible mechanisms for inter-crew common cause failures that would defeat the defenses? For example, is it feasible that plant conditions could be such that both alarms and walkdown indications could be rationally argued away?

This is, of course, the key. Some strong context is required to interfere with detection (unless some rapid drain-down or pump-down condition is permitted to exist and someone enables it). You suggested some alternatives and, without careful analysis, another comes to mind: some high-profile, potentially hazardous evolution could distract multiple crews from their normal surveillance practice. Examples could include lifting the reactor vessel or dismantling and moving the turbine-generator–some evolution where the utility wants to keep a close watch on contractor operations to protect investment or worker safety.

In addition, the revised ATHEANA process is specifically developed to address such issues. What we would seek are plant conditions that could mislead operators so that they develop an incorrect situation assessment. Then, rational inferences, from an incorrect starting point, are likely to be flawed. ATHEANA may be a useful tool to identify such mechanisms. The latest version of the ATHEANA process is based on two observations: (1) most serious accidents involve human unsafe acts performed when the plant (or facility, vehicle or platform) enters a regime of operation not understood by its crew[1]; and (2) the original ATHEANA process was relatively unhelpful in identifying such scenarios that deviate from standard, well-analyzed scenarios. ATHEANA is now structured around four related search schema:

i. A HAZOP-like search for physical deviations

---

[1]The other common condition occurs when the machine is degrading too quickly for effective operator recovery, an unlikely case for the normally slow nuclear power plant response.

ii. A search of formal procedures that apply normally or that might apply under the deviation scenario identified in the first search

iii. A search for support system dependencies and dependent effects of pre-initiating event human actions, and

iv. A "reverse" search for operator tendencies and error types. The first three searches identify plant conditions and rules that involve deviations from some base case. In this search, a catalog of error types and operator tendencies is examined to identify those that could cause HFEs or UAs of interest. Then plant conditions and rules associated with such inappropriate response are identified. It is rather a catch-all to see if any reasonable cases were missed in the earlier searches.

Along with the restructuring, ATHEANA is presented as a tool for investigating specific issues, so it might be appropriate for us or for you to give it a try for this question.

4. Can you suggest suitable representative values, including extreme values, for each of the HEPs, particularly taking into account the long times available?

If we identify the time available, *and if* it spans three shift turn-overs as indicated, *and if* all the sound practices you recommend are in place, then something near zero (well below 1×10^{-4}) would be appropriate. While direct data may be hard to find, some arguments based on every day observations could be developed. For example, every day __k__ million people start their cars an average of __n__ times and only __s__ of them destroy the starter motor by failing to release the key from the start position. That sort of thing. Or count the number of crash free airplane landings. Or something more relevant dealing with observing their fuel gages, etc.

However, if we make a real effort to be realistic for the conditions when error is unlikely, we are obligated to work very hard at identifying error-forcing context. Right now, the conservatism can be thought of as some sloppy average that includes the severe context situations.

5. Are there other factors [than those identified in the draft report] 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?

If the human action issues were reframed to match the context and control tasks described by Erik Holnagel, then there is a reasonable method and quantification technique presented in Chapter 9 of his book, *Cognitve Reliability and Error Analysis Method: CREAM*, Elsevier, Oxford, 1998. Also, for a coarse estimate of cognitively demanding tasks, HEART may be useful. I assume that you have Williams papers. If not, I would be happy to send copies. We are using HEART as something of a sanity check.

6. Language. Although my purpose was not to mark up the draft as a technical editor, here are a few minor edits:

I Intro, para 2, l 3: "...it can be argued that...can be argued..."

IV.1.1 HEP-RES-ALARM seems to come out of nowhere. Please prepare your reader for the shift to specifics from the PRA/HRA.

IV.2.1. The introductory paragraph is very difficult to parse. While I finally figured it out, I initially thought you were talking about all three events, with early and late being two cases of " as a result of alarm" and the third being no alarm. It took iteration between Appendix A and the paragraph to decipher it.

Hi Gareth- I will be sending this as a formal response in the form of a letter. We can discuss next week, as you would like.

General Approach

I believe that the analysis approach as outlined will result in a thorough consideration of the ability of operating staff to respond to a spent fuel pool incident. Because of the changes that may be present due to the decommissioning phase it is important that the best possible information be gathered. In particular are changes that may occur in the conduct of operations, and in the general rigor generally associated with nuclear power plant operation. These changes could have a possible impact in terms of reducing the complexity of operations and producing a more singular focus, but also could substantially change the way the facility is operated.

I have a few specific additions to the method as identified. In section III.1 b, I would add the check and review of logs as a part of the requirement to log results of monitoring. These checks and reviews are important contributors in reducing the error rates associated with monitoring. Also noted in this section are the requirements for a formal shift turnover meeting. This is particularly important I believe in this case and should be expanded to include the quality of that turnover, the formality and procedures associated with the turnover. This also needs to reflect any potential changes that might occur as the plant goes into a decommissioning stage as previously mentioned. In section III2 I would add the general clarity and accuracy of the procedures focussing on examples that are present from plants that have experienced spent fuel pool events in the recent past. In section IV.1.1 where it is stated that.... For some initiating events, there are several related alarms, the probability may be argued to be even lower.... I would simply caution that it is important to understand the independence of the alarms in relation to a spent fuel pool event as opposed to other unrelated events.

Operational Practices

Key to the operational practices will be the relative quality of the procedures available, how well they tie to alarms and indications, and how well the particular facility does conduct of operations. Looking to past operating events will provide useful indicators of the state of practice in these areas, but as also pointed out above some of these practices may changes during decommissioning. It is important to gather some indication of the types of changes that may occur. If the facility becomes more singular in focus it can be argued that they will be better able to detect problems associated with the spent fuel pool. It would be useful to develop what the work processes may look like for such a facility as a best case.

Time Available

The large time window available for detection, response formation and action in these scenarios is indeed a critical factor. I searched the NUCLARR database for simulator data that would help to calibrate the values suggested in the methodology. The data in the table below comes from the LaSalle Unit 1 and are for recovery actions taken from the control room. Of interest is the fact that values are very similar for equipment operators as well. Essentially these data suggest that

an improvement is seen with an increase in the time window availability, approximately by a factor of 10. These improvements are not inconsistent with the data you suggest. It is of interest that the number in an absolute sense is not small however.

Data from NUCLARR

Scenario: La Salle Country Unit 1 control room operators performing a variety of recovery actions. The data for equipment operators are similar. The HEPS were based on simulator data. Data taken from NUCLARR records			
Time available	Number of records	Median HEP	Error Factor
Very short (<10 min)	23	.651	1.4
Long (>60 min)	11	0.023	7.8

In addition, I also examined the AEOD database for operating events for any specifics that might support the method as outlined. Some 56 loss of spent fuel pool cooling events are included in the AEOD database. Examples of the effect of various performance shaping factors can be found in these events. An event that occurred at Wolf Creek Station 1 on September 23 1991 (documented in an AIT report) gives an example. On the positive side, the operator's training and familiarity with the plant were determined to be assets in coping with the event. On the negative side it took approximately 3 days for the operators to begin to take action once a low-level alarm was activated in the control room. The important piece from this event is that the operators were aware of the alarm but because of the context of the situation it was not perceived to be important. This low-level alarm was within normal variation and no specific procedure existed for a loss of SFP inventory to alert the operators. In short, given a slow leak even in the presence of an alarm days can pass before action is taken. This indicates the importance of the connection between alarms, their independence and direct connection to specific events and procedure that guide the operator to take action early. There may other good examples to help support the basis for selection for failure rates from the AEOD database. I believe it would be important to review each of the events for such collaborative evidence. Also important are the considerations of the changes facilities have made in response to these events.

Suggestions for error rates and other factors

As a part of the SPAR program we recently compared several HRA methods in terms of their base human error rates and multipliers for performance shaping factors. The tables given are meant to provide a calibration of the rates suggested in your method. In sum your values appear to be right in range with these other methods. From a high level it is important to note that most methods do give credit for increasing amounts of time. I chose to only present the multipliers for diagnosis, but values are available for actions as well. This data is the most germane to the proposed method as it is the diagnosis portion which may be most effected by the long time window. Note that HEART does indicate that expansive time can be a problem, but this is indicative of a situation where complacency might come into effect. Also of note is the fact that HEART is the one method that really rolls PSF factors into the base rates so that the multipliers have a more subtle effect. Unlike the simulator data, these HRA methods give approximately a

two order of magnitude improvement from adequate time to expansive time. This could be indicative of the lack of a complete set of simulator data. Most important is the fact that these values are consistent with the values reported in the method outline.

Comparison of Multipliers for Diagnosis

PSF	Levels	HEART multipliers	CREAM multipliers	ASEP multipliers	THERP multipliers
Available Time	Inadequate Time			P(failure)= 1.0	P(failure)= 1.0
	Barely Adequate time (<20 min)	11	5	10	10
	Nominal Time (=30 min)		1	1	1
	Extra Time (>60 min)		.5	.1	.1
	Expansive Time (>24hrs)	1.1 for 1st half hour 1.05/hour after		.01	.01

A factor not overtly included in the outline method that I believe should be covered is that of work process. Work process refers to aspects of doing work including crew dynamics, safety culture, work planning, and communication. This is especially important given the changes that potentially could occur in terms of the decommissioning plant, and the status of alarms and the quality of procedures present to aid the operators. There is a potential for change in the rigor of operation when moving from a facility at power to one that is being decommissioned. Two methods specifically address work processes in terms of quantification, HEART and CREAM. The table below compares those methods. Keep in mind that HEART tends to include more in the base rate representing both possible and negative aspects of human performance whereas CREAM is more constructive.

Multipliers for Work Process

PSF	PSF Levels	HEART Multipliers	CREAM Multipliers

	Poor	2 (dangerous procedures) 1.6 (unclear allocation of function & responsibility) 1.2 (low morale) 1.06 (task pacing) 1.03(more team members than normal/necessary)	2 (adequacy of organization, collaboration) 1.2 (adequacy of organization) 1 (adequacy of organization)
	Nominal		1 (adequacy of organization, collaboration)
	Good		.8 (adequacy of organization) .5 (collaboration)

The values presented in this table have the ability to effect the error rates in both directions and would be sensitive to the kinds of concerns contained in the methods outline including surveillance, maintenance, procedures, teams, and shift turn over. In addition, work process is often a factor cited in various analyses of events.

Summary

I would suggest that the following steps be taken:

1. Review the AEOD events for examples of PSF impact.
2. Obtain and evaluate a set of procedures for a facility that has had a recent spent fuel pool event.
3. Identify plans for utilities to change the current work processes.
4. Using the quantification techniques develop a list of HEPs that can be supported by the events.