November 30, 1999

To: Glenn Kelly

From: Gareth Parry

cc: Diane Jackson
Mark Rubin

Subject: INEEL rework of the SFP risk study

The following is based on a review of the loss of spent fuel pool cooling event tree. The same problems are almost certain to exist for the other event trees.

There are some logic problems with the INEEL analysis that substantiates the concern Mike Cheok expressed about dependencies between HEPs. If you look at the Loss of Cooling event tree, you will see, in the fault tree for event OCS, a basic event HEP-COOL-LOC-E/L, which for the E version, is calculated as failure to repair within 17 hours. Now in the fault tree for event OFD, the basic event FP-MKUP-FTF is really a composite, or logically it is an AND gate of a) failure of a diesel pump, b) failure of an electric pump, and c) failure to repair in 37 hours. It is true that the success criteria of the human failure events are different, and that they take place in different time phases of the accident. For OCS the time window begins with the loss of cooling, and it is the time at which bulk boiling begins that determines the time available for repair. For OFD, it is the time to fuel uncovery, with the clock starting after the bulk boiling has started or spent fuel pool cooling cannot be reestablished because of low level. However, these human failure events may still be dependent. For example, something that prevents the operating crew contacting outside sources would be a failure mode of both human failure (to repair) events. In any case, without worrying too much about the potential common cause failure mechanisms at this stage, it is good PRA practice not to include composite basic events that contain human error terms, that have a potential for dependency with other explicit HEPs.

It seems that the basic event REC-INV-OFFSITE1 is also essentially a human failure, which means that the model is generating conditional cutsets (i.e., with the initiating event removed) consisting of multiple human failure events that, when combined, have a probability of as low as 1E-09. This is optically not very good, since even though we can argue that there are additional cues for each of the recoveries, there comes a point when we cannot argue that there might not be an underlying problem that cuts across them all, which is at the level of the management structure or physical conditions or something we haven't thought about. Furthermore, it is not necessary to argue such low probabilities. What we should do is to use the PRA model to demonstrate that there is value in imposing the requirements.

It's not clear why we need the extra diagnosis failure probabilities associated with HEP-DIAG-SFPC. Failure of diagnosis of the need for action is included in the CRA and IND top events. The events HEP-DIAG-FW-LOC and HEP-DIAG-OFF-LOC are useful in that they separate out the diagnosis/awareness issues from the execution issues, and relate to different requirements.

489

For example, the issue of procedural guidance on when to initiate these contingency measures would be relevant PSFs for the evaluation of these HEPs. Procedural guidance on how to align the system would affect the HEP-FW-START and REC-INV-OFFSITE1 events. So, if the response procedures contained specific instructions to begin using the fire pumps when bulk boiling begins, this could be used as a cue in the assessment of the likelihood of the recognition of the conditions for starting the pumps. The HEPs calculated for these events should be conditioned on the operators attempting to restore cooling.

I believe setting the model up this way, (deleting the unnecessary diagnosis term for the HEP-DIAG-SFPC event) would highlight the significance of having the contingency procedures for using the fire pumps and offsite sources.

As an additional explanatory tool, it would help to draw an assumed timeline, to help understand the time dependence, and even the functional dependency, between the human error basic events.