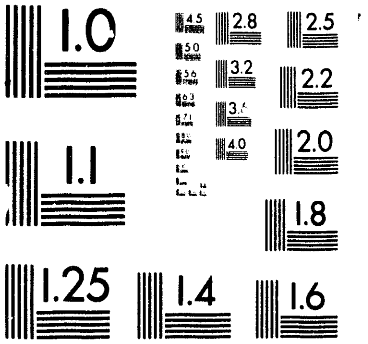

1.0
4.5
5.0
5.6
6.3
7.1
2.8
3.2
3.6
4.0
2.5
2.2
2.0
1.1
1.8
1.25
1.4
1.6

1 of 1

Conf-940912--42

2218 C
SAND93-~~2818C~~

GENERIC EVENT TREES AND THE TREATMENT OF DEPENDENCIES AND NON-PROCEDURALIZED ACTIONS IN A LOW POWER AND SHUTDOWN PROBABILISTIC RISK ASSESSMENT*

John Forester,[1] Donnie Whitehead,[2] John Darby,[3] and Jeffrey Yakle[1]

[1]Science Applications International Corporation, Albuquerque., N.M.,
[2]Sandia National Laboratories, Albuquerque., N.M.,
[3]Science & Engineering Associates, Inc., Albuquerque., N.M.

INTRODUCTION

Sandia National Laboratories was tasked by the U.S. Nuclear Regulatory Commission to perform a Probabilistic Risk Assessment (PRA) of a boiling water reactor (BWR) during low power and shutdown (LP&S) conditions. The plant chosen for the study was Grand Gulf Nuclear Station (GGNS), a BWR 6. In performing the analysis, it was found that in comparison with full-power PRAs, the low decay heat levels present during LP&S conditions result in a relatively large number of ways by which cooling can be provided to the core. In addition, because of the less stringent requirements imposed on system operability by the technical specifications for certain LP&S states, the number of system configurations possible is large and the availability of plant systems is more difficult to specify. These aspects of the LP&S environment led to the development and use of "generic" event trees in performing the analysis. The use of "generic" event trees, in turn, had a significant impact on the nature of the human reliability analysis (HRA) that was performed. This paper describes the development of the event trees for the LP&S PRA and important aspects of the resulting HRA.

GENERIC EVENT TREES

While the number of plant configurations possible during LP&S can be addressed to some extent by constraining the PRA analysis to specific plant operational states (POSs) such as cold shutdown or refueling, even within a particular POS there is still a relatively

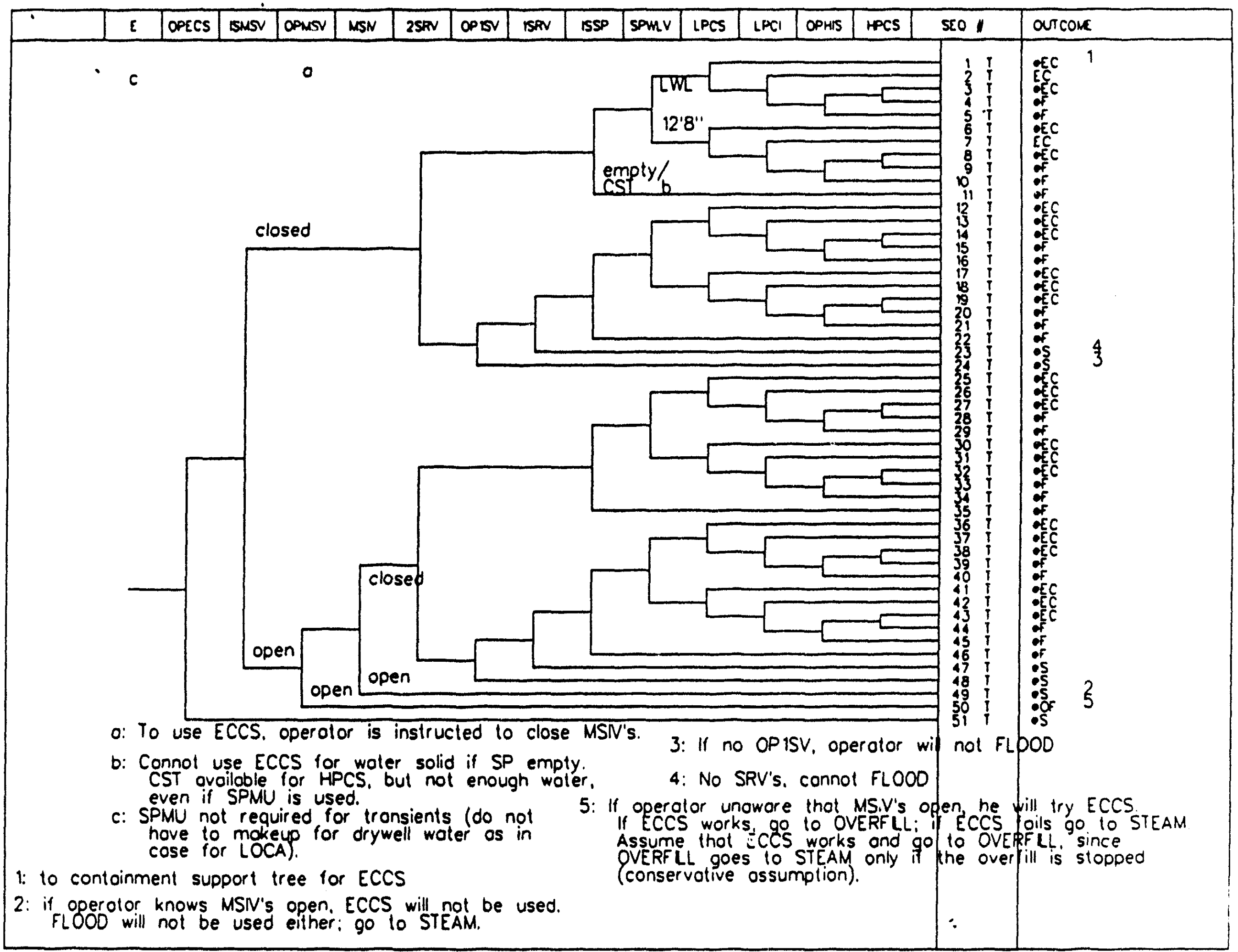
*This work was supported by the U.S. Nuclear Regulatory Commission and performed at Sandia National Laboratories, which is operated for the U.S. Department of Energy under Contract Number DE-AC04-76DP00789.

large number of system configurations that would need to be modeled. The modeling problem is further compounded by the fact (noted above) that the low decay heat levels present during LP&S allow a relatively large number of ways to provide core cooling.

In the "usual" approach to developing event trees, the different possible system configurations would be specified "up-front" in the initiator specific event trees. However, since the plant configuration at the time of a particular accident would obviously have an impact on which operations could be used to respond to an accident, and because the number of configurations and operations possible during LP&S is large, it became clear that attempting to specify all the possible configurations up-front for each specific initiator would require the development of a unacceptably large number of specific event trees for each initiator. It was determined that the event tree development task could be significantly reduced through the use of "generic" event trees that were based on the different operations that could be applied to respond to an accident occurring in a BWR 6. In most cases, the operations possible in response to any given initiator that threatened the core would be the same (some of which are specified by procedure) and would only be constrained by the existing system configurations and availabilities. Thus, it was decided that the event trees would be developed by asking questions about the configurations possible, in the context of each of the possible operations. The result was event trees related to accident response operations, which could be used for most of the initiating events analyzed. The trees were "generic" in the sense that they were designed in terms of the general operations possible in response to an accident in a BWR 6, as opposed to being drawn as a function of a specific accident.

For example, several operations, using any of several different injection systems, are possible for providing core cooling in response to a loss of the normal means of shutdown cooling. The operations include initiating a closed-loop water solid operation per procedure, steaming the vessel at low pressure, flooding the vessel/containment, or steaming the vessel at high pressure. Separate event trees were developed for each of the possible operations and relevant questions regarding operator actions, existing system configurations and system availabilities were asked in each of the operation-specific event trees. The specific impact of a given initiating event was taken into account by setting system unavailabilities accordingly.

An example of an event tree used in the LP&S study is presented in Figure 1. The tree (the "E" tree) represents one of the operations possible in response to a loss of the normal means of shutdown cooling, which could occur in the context of many different initiating events. The operation covered is that of initiating closed-loop water solid operation with an available Emergency Core Cooling System (ECCS). Water solid operation is clearly indicated in the GGNS Off-Normal Event Procedure (ONEP) for inadequate decay heat removal. The operator decision and action for initiating ECCS water solid operation is represented by the event labeled OPECS. Depending on the pattern of successes and failures in the accident scenario prior to reaching OPECS, a number of operator actions could be required in addition to those indicated by the ONEP. For example, if the operators were initially using the Alternate Decay Heat Removal System for shutdown cooling as opposed to the Residual Heat Removal shutdown cooling system, a more complex pattern of system isolations would be required to initiate ECCS water solid operation with the Low Pressure Core Injection System. Moreover, if normal vessel "letdown" had not yet been isolated, this action would also be required at this point. The OPECS event is followed by a series of events asking questions regarding the status of the main steam isolation valves (ISMSV, OPMSV, MSIV), the status of safety relief valves (2SRV, 1SRV), whether the operators would proceed with ECCS water solid operation with only one safety relief valve open (OP1SV), the water level in the suppression pool (ISSP, SPMLV), and the availability of the ECCS systems (LPCS, LPCI, OPHIS, HPCS).



a: To use ECCS, operator is instructed to close MSIV's.

b: Cannot use ECCS for water solid if SP empty. CST available for HPCS, but not enough water, even if SPMU is used.

c: SPMU not required for transients (do not have to makeup for drywell water as in case for LOCA).

1: to containment support tree for ECCS

2: if operator knows MSIV's open, ECCS will not be used. FLOOD will not be used either; go to STEAM.

3: If no OP1SV, operator will not FLOOD

4: No SRV's, cannot FLOOD

5: If operator unaware that MSIV's open, he will try ECCS. If ECCS works, go to OVERFLL; if ECCS fails go to STEAM. Assume that ECCS works and go to OVERFLL, since OVERFLL goes to STEAM only if the overfill is stopped (conservative assumption).

Figure 1. Event tree for initiating ECCS water solid operation after a loss of normal shutdown cooling.

Another important advantage of the use of generic event trees was that the approach allows the same event trees, or only slightly modified trees, to be used across analyses for different POSs. For example, the loss of shutdown cooling related trees discussed above would in general be applicable during most POSs such as cold shutdown, refueling with the water level at the main steam lines, and refueling with the water level raised and the upper pools connected. The use of more or less the same event trees across analyses for different POSs should, in principle, not only be more efficient, but should also allow a straightforward comparison of core damage frequency across the different POSs.

The resulting event trees were somewhat more complex and lengthy and they contained more frequent and more complex operator diagnosis/action events than is typically found in full-power PRAs. The increased complexity of the event trees and operator actions were in part due to the nature of the event trees. That is, since the trees were based on the multiple operations possible to respond to an event and, as determined by the initiator, a variety of systems could be available to support those operations, the trees and events were necessarily more complex. However, the nature of the operator actions were also different as a direct function of the LP&S environment. At full power, many of the operator action events in response to an accident simply involve the manual initiation of a system that has failed to auto-initiate. For such events, the indications and related operator diagnosis/actions are approximately the same regardless of the accident scenario in which they occur. In the LP&S environment, however, many of the operator actions are not strictly proceduralized and are not always explicitly covered in the Emergency Procedures. Moreover, diagnosis and performance of many of the operator actions are dependent on the initiator and on what has occurred or failed to occur previously in the accident sequence. This aspect of the analysis will be discussed in more detail below.

HUMAN RELIABILITY ANALYSIS

The general methodology used for conducting the HRA and determining the Human Error Probabilities (HEPs) for the identified human actions was the Accident Sequence Evaluation Program Human Reliability Analysis Procedure (ASEP HRAP) [1]. The ASEP HRAP was selected for several reasons, the more important being that:

(1) The HEPs obtained using the procedure are considered to be slightly conservative relative to those that would be obtained from other methodologies such as "THERP" [2]. Conservative HEP estimates were considered desirable because existing HRA methodologies have not explicitly considered the impact of potentially unique performance influencing factors (PIFs) which might be operative during LP&S conditions. For example, there is no explicit way to factor in the impact of the numerous ongoing activities and numerous non-regular personnel present during LP&S on the operators' awareness and decision making capabilities.

(2) The procedure allows for straightforward adjustments in HEPs as a function of the results from interviews with plant personnel. In situations such as LP&S, where procedures may not be all encompassing, the results of interviews with operators and other plant personnel become a critical aspect of the HRA.

In general, the HRA data collection and analysis process outlined in the ASEP HRAP was followed. One exception was that the pre-accident human actions included in the analysis used the same HEP values that were used in the full-power PRA of GGNS reported in NUREG/CR-4550, Vol. 6, Rev. 1 [3]. Thus, less emphasis was placed on collecting information relevant to pre-accident human action quantification. Nevertheless, procedures related to control of work on plant equipment and facilities, protective tagging systems, outage organization, shutdown protection plans, and surveillance on shutdown related systems were obtained from GGNS and examined.

To obtain information relevant to analyzing the post-accident human actions contained in the event and fault trees, interviews with operators and other plant personnel were conducted over a two-day period. The general level of understanding conveyed by plant personnel about the various accident scenarios addressed in the analysis was used by the HRA analyst in determining the HEPs. In most cases, information obtained from interviews was used in conjunction with the ASEP HRAP in determining whether the nominal (median) HEP or the upper or lower bound value from the ASEP HRAP diagnosis model, should be used in estimating the HEP for a particular diagnosis. In some cases, interview results indicated that operators would simply not do some of the actions included in the event trees.

Treatment of Dependencies and Non-Proceduralized Actions

As discussed above, the use of generic event trees and the nature of the LP&S environment had a significant impact on the HRA. Since system configurations and availabilities were not specified in the initial initiating event trees, they had to be considered in each of the operation related event trees. Furthermore, since the impact of failures to accomplish certain operations could have a bearing on other operations that might be attempted, it became clear that dependencies within the various accident scenarios would need to be considered. The fact that many of the possible operations were not explicitly proceduralized also indicted that a careful analysis of the sequences would be needed. Therefore, in order to accomplish a reasonably valid HRA analysis, it was necessary to do a sequence by sequence analysis of the human actions contained in the event and fault trees and to attempt to account for the dependencies among the different operator actions.

Several general guidelines were used in the treatment of non-proceduralized operator diagnoses/actions and dependencies across operator actions within an accident scenario. The guidelines included the following:

(1) In general, credit was given for operators correctly diagnosing and carrying out a non-proceduralized action if, on the basis of the site interviews, it was judged that the operators had a clear understanding of the event in question and of the requirements for responding to the event. For example, while the operation of steaming at low pressure is not explicitly described in GGNS procedures, the site interviews indicated that it would be a viable option.

(2) In most cases, credit was not given for a non-proceduralized action if a critical human action, clearly indicated by procedure, had failed earlier in the sequence being analyzed and the pattern of failures across the sequence suggested operator "confusion". For example, if the operators failed to initiate ECCS water solid operation when it was clearly indicated by procedure, credit for steaming at low pressure (a non-proceduralized action) was not taken.

(3) In determining the requirements for a particular operator diagnosis\action event in a given sequence, any human actions necessary for the success of the sequence, that had failed in earlier events, could be addressed again in an appropriate subsequent event. For example, a manual system isolation (e.g., isolation of vessel letdown) may be necessary for the success of a sequence. If a human action event which included that task had failed earlier in the sequence, but the context of a subsequent human action event in the sequence legitimately allowed that task to be addressed again, the performance of that task would be taken into account in determining the HEP for the subsequent event.

(4) Complete or zero dependence across events in a sequence was assigned as a function of the logical relationship between those events. For example, in a given human action event, it may have been possible for an operator to use any of several systems to respond to the problem. However, if limited time was available for the event being analyzed, credit for trying all the available systems may not have been taken at that point. Therefore, any subsequent events which assumed that a particular system had been initiated when it hadn't, would be set to fail. Similarly, if an event included the initiation of a system, appropriate subsequent events asking initiation of that system would be set to succeed.

The above guidelines often required subjective judgments on the part of the HRA analyst. These judgments were based on the impressions drawn from the interviews with plant personnel, on examinations of the relevant procedures, and on the basis of discussions with the other analysts on the PRA team.

Since generic event trees were used for the PRA, the operator actions asked in the analysis of the accident sequences for the different initiators were in general the same. However, because the various initiators have differing impacts on the system and therefore the nature of the accident sequences, the HEP for the same operator action could vary across initiators. Furthermore, the HEP for the same operator action could also vary within the analysis of a particular initiator as a function of the different system and operator successes and failures occurring in the different sequences. Therefore, multiple HEPs were possible for a given operator action. For example, the operator action for diagnosing and initiating ECCS water solid operation (OPECS) had 22 different values ranging from 0.003 to 1.0. A total of 115 HEPs was calculated for the approximately 40 human action events included in the analysis.

SUMMARY

The unique aspects of the LP&S environment and the resulting use of generic event trees required that each human action event be carefully examined in the context of each of the different accident sequences in which they occurred. In conducting the sequence by sequence analysis, non-proceduralized human actions had to be considered and attempts were made to address relevant dependencies across events within given scenarios. The LP&S environment appears to demand a more detailed and complex HRA than that usually performed for full-power operations.

REFERENCES

1. A.D. Swain, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, February, 1987.
2. A.D. Swain and H.E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, August, 1983.
3. M.T. Drouin et al, "Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events," NUREG/CR-4550, Vol. 6, Rev. 1, Part 1, September, 1989.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.