SAND-98-0164C
CONF-980907--

SAND98-0164C

Quantification Results from an Application of a New Technique for Human Event Analysis (ATHEANA) at a Pressurized Water Reactor*

Donnie W. Whitehead, Sandia National Laboratories,
Alan M. Kolaczkowski, Science Applications International Corporation, and
Catherine M. Thompson, US Nuclear Regulatory Commission

1 Introduction

This paper presents results from the quantification of the three human failure events (HFEs) identified using the ATHEANA methodology as discussed in an earlier companion paper presented at this conference [1]. The following sections describe the quantification task, important basic events, and the results obtained from quantifying the three HFEs that were identified—the first two of which were simulated at the Seabrook Station Simulator.

2 Establishing the Expressions to be Quantified

The first step in the quantification process was to derive expressions that represented the likelihoods for the HFEs of interest. This was done in a successively detailed fashion, following the ATHEANA HRA multidisciplinary framework. Quantification started with a general expression at the PRA event tree-level of resolution of what had to be quantified, and finally led to an expression that contained the specific elements of the error-forcing context, unsafe actions, and non-recoveries to be quantified. The expressions for each of the three HFEs of interest are presented in the following subsections.

2.1 HFE #1 – Inappropriate termination of makeup

The expression at the PRA event tree-level for this HFE of interest is given as follows:

MLOCA * Failure of all injection

(i.e., a medium size loss-of-coolant (LOCA) and failure of all injection)

---

*This work was supported by the U.S. Nuclear Regulatory Commission and was performed at Sandia National Laboratories. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the U.S. Department of Energy under Contract DE-AC04-94AL85000.

DISCLAIMER

At this level, and in its most simple form, the above expression captured the intent of what was to be quantified. However, there are many ways to fail all injection, many of which are already included in a typical PRA. The ATHEANA project was interested in quantifying a particular failure as described by the following expression at the HFE-level:

MLOCA * Operators shut off injection and injection is not recovered .

While the above expression appropriately describes the particular HFE to be quantified, it had to be broken down further into the specific elements that make up the error-forcing context, unsafe action(s), and non-recovery events that together, define the HFE. The ATHEANA quantification approach can be represented by the following equation:

$$P(HFE_{ijr}) = P(EFC_i) * P(UA_j|EFC_i) * P(\overline{R}|EFC_i|UA_j|E_{ij}) \quad (1)$$

where:

$P(HFE_{ijr})$ is the probability of human failure event, HFE_{ijr}, resulting from unsafe action (UA_j) occurring in context (EFC_i) and not being recovered given the error-forcing context, the occurrence of the unsafe action, and the existence of additional evidence (E_{ij}) following the unsafe action.

Using this general equation format, the HFE-level expression above was replaced with a more detailed expression in order to quantify the HFE for the context believed to be error-forcing:

$$P(\text{HFE \#1}) \text{ per year} = MLOCA_{freq} * P(\text{failure of 2 wide-range reactor coolant system (RCS) pressure indications}) * P(\text{crew shuts off injection (at least 3 of 4 pumps per the PRA)}) * P(\text{injection is not restored before core damage}) \quad (2)$$

where:

$MLOCA_{freq}$ = frequency of the initiator, MLOCA (per year), and
P(--) = probability of the event described within each parenthesis .

Note that in this case, the occurrence of a particular LOCA size (MLOCA) and the failure of specific indicators together make up the most significant aspects of the error-forcing context. Only one unsafe action was quantified (crew shuts off injection) along with a single event used to describe the non-recovery aspect of this HFE.

2.2 HFE #2 - Inappropriate depletion of resources

In a similar way as for HFE #1, a successively detailed set of expressions was developed to address this HFE. The PRA event tree-level expression was:

MLOCA * Failure of high-head core cooling recirculation .

At the HFE-level, this was further described by the expression:

MLOCA * Operators fail to shut off high head pumps when the raw water storage tank (RWST) is empty and the pumps are not yet configured for recirculation .

At the error-forcing context, unsafe action, non-recovery level, the following expression was derived to define the specific probabilities to be quantified:

$$P(\text{HFE \#2}) \text{ per year} = MLOCA_{freq} * P(\text{high head pumps are not yet configured for recirculation}) * P(\text{RWST "empty" alarm fails}) * P(\text{crew does not stop the pumps in time}) \quad (3)$$

where:

$MLOCA_{freq}$ = frequency of the initiator, MLOCA (per year), and
P(--) = probability of the event described within each parenthesis .

Note that the three actions in this case (the occurrence of a particular LOCA size (MLOCA), the fact that the high-head pumps are not yet configured for recirculation, and the RWST "empty" alarm has failed) all make up the most significant aspects of the error-forcing context. Only one unsafe action was quantified (crew does not stop the pumps in time). At Seabrook Station, the low-head pumps automatically reconfigure upon low RWST but the high-head pump reconfiguration, taking suction on the low-head pumps, requires manual actions. These actions largely rely upon low level RWST indication and the fact that if reconfiguration is not complete by the time the RWST "empty" audible alarm sounds, operators should stop the high-head pumps to avoid damaging them. The operators then can complete the reconfiguration process and restart the pumps using the containment sump as the suction supply. It was believed that failing the audible RWST "empty" alarm might induce the error of leaving the high-head pumps running while the RWST depleted. In such a circumstance, no recovery for the HFE was credited since it was assumed that if the pumps continue to operate with a depleted suction source, they would fail in an irreparable manner. With no high-head recirculation, core damage would eventually result. It was recognized that it may be possible to further depressurize the plant and use low-head recirculation to cool the core. However, it was decided that such a recovery action would be examined only if the probability of this HFE, as calculated using the expression above, came out "high."

2.3 HFE #3 – Failure to shut down (temporarily) a diesel generator

In a similar way as for HFE #1 and HFE #2, a successively detailed set of expressions was developed to address this HFE. The PRA event tree-level expression was:

LOSP * Stuck-open PORV * SBO * Non-recovery of power

where:

LOSP = loss-of-offsite power initiator,
Stuck-open PORV = a demand for and the subsequent sticking-open of a PORV which causes a valid safety injection and decreases the timing of the scenario for preventing core damage,
SBO = a resulting station blackout condition (i.e., loss of all AC power), and
Non-recovery of power = AC power is not restored in time sufficient to restore injection, resulting in core damage .

At the HFE-level, this was further described by the expression:

LOSP * Stuck-open PORV * DGA-OOS * DGB cooling fails * Operator does not "protect" DGB by shutting it down * power is not restored .

At this level, DGA is described as out-of-service (DGA-OOS), and the mode of "imminent" failure for DGB is described as a cooling failure. Together, these events provide further context as to the specifics of the situation.

Finally, at the error-forcing context, unsafe action, non-recovery level, the following expression was derived to define the specific probabilities to be quantified:

$$P(\text{HFE \#3}) \text{ per year} = LOSP_{freq} * P(\text{PORV is demanded}) * P(\text{PORV sticks open}) * P(\text{DGA-OOS}) * P(\text{DGB cooling fails}) * P(\text{operator does not shut down DGB}) * P(\text{non-recovery of power}) \quad (4)$$

where:

$LOSP_{freq}$ = frequency of the initiator, LOSP (per year), and
P(--) = probability of the event described within each parenthesis .

Again note that if DGB is not shut down, it is assumed to suffer irreparable damage and so its restoration to service is not credited as part of possibly recovering power.

3 Important Events in the Quantification of the HFEs

Using the expressions developed in the previous section, the SAPHIRE code was used to develop event trees and fault trees to quantify each HFE. The basic events used to construct the fault trees, along with brief definitions are provided in Table 1.

Table 1 Basic Events Used in Model

Basic Event	Description	Point Estimate	Uncertainty Distribution
WR-PI-TR-A(B)-FAILS	Hardware failure of train A(B) wide-range pressure indication (WRPI)	1.7E-2	LN, EF = 3
WR-PI-TR-A(B)-OOS	Unavailability of train A(B) WRPI	1E-2	ME, LE = 3E-3 & UE = 2
TR-A(B)-WR-PI-MISCAL	Miscalibration of train A(B) WRPI	3E-3	LN, EF = 10
WR-PI-MISCAL-APP	The portion of miscalibrations that produce the desired WRPI response	1E-1	ME, LE = 1E-2 & UE = 5E-1
WR-PI-MISCAL-CCF	Common cause miscalibration of trains A and B WRPI indication	4.2E-4	LN, EF = 10
OPS-SHUT-OFF-SI	Operators shut off enough pumps (i.e., three of four) so that core damage is assumed to occur due to inadequate coolant inventory	7.7E-1 10/13	ME, LE = 5E-1 & UE = 1.0
OPS-FAIL-RESTORE-SI	Operators fail to turn on at least two pumps	1E-1	CND
OPS-F-R-PUMPS-RECIRC	Operators fail to complete the reconfiguration of the high-head pumps for recirculation before the RWST "empty" alarm occurs	5E-1	ME, LE = 1E-1 & UE = 1.0
LT-1(2, 3, or 4)	Failure of an individual level transmitter (LT) that feeds the RWST "empty" alarm	3.4E-2	LN, EF = 3
LT-X-CCF	The "first failure" portion of the common cause failure of the LTs	3.4E-2	LN, EF = 3
BETA-4LT	The beta factor for failure of 4 level transmitters	1E-2	CND
MPC-SURROGATE-IRTU	Unavailability of the two IRTUs whose failure would prevent the RWST "empty" alarm from occurring	7.2E-4	LN, EF = 5
OPS-F-STOP-PUMPS	Operators fail to stop the high-head pumps before damage by low suction pressure given failure of the RWST "empty" alarm	8.33E-1 5/6	CND
LOSP-SW	Severe weather LOSP initiating event	1E-2	LN, EF = 5
LOSP-NSW	Non-severe weather LOSP initiating event	4.9E-2	LN, EF = 3
PORV-DEMAND	Probability that a PORV will be demanded given that a LOSP event has occurred	1.6E-1	ME, LE = 1.6E-2 & UE = 2E-1
PORV-FAIL-TO RECLOSE	PORV fails to reclose given that it has been demand open	5E-2	LN, EF = 3
DG-A-OOS-S	Short-term OOS unavailability of one DG	2.3E-4	LN, EF = 10
DG-A-OOS-L	Long-term OOS unavailability of one DG	1E-2	LN, EF = 3
DG-B-COOLING -F	Cooling failure of the other DG.	2.54E-3	LN, EF = 5
OPS-FTSTOP-DGB-S	Operators fail to stop the DG with a cooling problem given that the other DG's OOS unavailability is for the short term	5E-1	ME, LE = 4E-1 & UE = 6E-1
OPS-FTSTOP-DGB-L	Operators fail to stop the DG with a cooling problem given that the other DG's OOS unavailability is for the long term	1.25E-1	ME, LE = 0.0 & UE = 2.5E-1
OPS-FTRES-OSP-SW	Non-recovery of power given that power was lost because of severe weather	7E-1	ME, LE = 6E-1 & UE = 8E-1
OPS-FTRES-OSP-NSW	Non-recovery of power given that power was lost because of non-severe weather	3E-1	ME, LE = 2E-1 & UE = 4E-1

LN - Log Normal EF - Error Factor
ME - Maximum Entropy LE - Lower End UE - Upper End
CND - Constrained Noninformative Distribution

4 Results from Quantification of HFEs

Results from the quantification of each HFE are presented in Table 2. From this table it can be seen that the mean core damage frequency associated with HFE #1 is approximately 1.8E-9, for HFE #2 it is about 2.0E-7, and for HFE #3 it is about 5.6E-10.

5 Observations

The quantification of these three HFEs demonstrated the successful application of the ATHEANA quantification process. The resulting core damage sequence

frequencies involving the HFEs of interest range in value from 2E-7 to 5E-10. Without a complete comparison to the existing Seabrook Station PRA results, it can not be equivocally stated that these frequencies are or are not important from a risk contribution perspective. Nevertheless, as with PRA, the value of the results is often determined by the insights gained doing the process, and not just by the quantification results. While none of the quantified results are particularly "distressing," the Seabrook Station staff acknowledged that performing the ATHEANA process provided valuable insights into how they might improve training and how the training and PRA staffs at Seabrook Station may be able to work more closely together in the future.

Table 2 HFE Quantification Results

HFE	Mincut Upper Bound	Uncertainty		Cut Sets	
1	2.284E-9	5th Perc.	7.425E-14	1.6E-9	OPS-FAIL-RESTORE-SI, OPS-SHUT-OFF-SI, WR-PI-MISCAL-APP, WR-PI-MISCAL-CCF
		Median	9.298E-11	2.0E-10	OPS-FAIL-RESTORE-SI, OPS-SHUT-OFF-SI, TR-A-WR-PI-MISCAL, WR-PI-MISCAL-APP, WR-PI-TR-B-FAILS
		Mean	1.794E-9	2.0E-10	OPS-FAIL-RESTORE-SI, OPS-SHUT-OFF-SI, TR-B-WR-PI-MISCAL, WR-PI-MISCAL-APP, WR-PI-TR-A-FAILS
		95th Perc.	6.087E-9	1.2E-10	OPS-FAIL-RESTORE-SI, OPS-SHUT-OFF-SI, TR-A-WR-PI-MISCAL, WR-PI-MISCAL-APP, WR-PI-TR-B-OOS
		Stand. Dev.	8.893E-9	1.2E-10	OPS-FAIL-RESTORE-SI, OPS-SHUT-OFF-SI, TR-B-WR-PI-MISCAL, WR-PI-MISCAL-APP, WR-PI-TR-A-OOS
				3.5E-11	OPS-FAIL-RESTORE-SI, OPS-SHUT-OFF-SI, TR-A-WR-PI-MISCAL, TR-B-WR-PI-MISCAL, WR-PI-MISCAL-APP
2	2.209E-7	5th Perc.	2.221E-9	1.5E-7	MPC-SURROGATE-IRTU, OPS-F-R-PUMPS-RECIRC, OPS-F-STOP-PUMPS
		Median	4.588E-8	7.1E-8	BETA-4-LT, LT-X-CCF, OPS-F-R-PUMPS-RECIRC, OPS-F-STOP-PUMPS
		Mean	2.037E-7	2.8E-10	LT-1, LT-2, LT-3, LT-4, OPS-F-R-PUMPS-RECIRC, OPS-F-STOP-PUMPS
		95th Perc.	8.808E-7		
		Stand. Dev.	5.825E-7		
3	6.019E-10	5th Perc.	9.822E-12	3.7E-10	LOSP-NSW, DG-A-OOS-L, DG-B-COOLING-F, OPS-FTRES-OSP-NSW, OPS-FTSTOP-DGB-L, PORV-DEMAND, PORV-FAIL-TO-RECLOSE
		Median	1.717E-10	1.8E-10	LOSP-SW, DG-A-OOS-L, DG-B-COOLING-F, OPS-FTRES-OSP-SW, OPS-FTSTOP-DGB-L, PORV-DEMAND, PORV-FAIL-TO-RECLOSE
		Mean	5.597E-10	3.4E-11	LOSP-NSW, DG-A-OOS-S, DG-B-COOLING-F, OPS-FTRES-OSP-NSW, OPS-FTSTOP-DGB-S, PORV-DEMAND, PORV-FAIL-TO-RECLOSE
		95th Perc.	2.191E-9	1.6E-11	LOSP-SW, DG-A-OOS-S, DG-B-COOLING-F, OPS-FTRES-OSP-SW, OPS-FTSTOP-DGB-S, PORV-DEMAND, PORV-FAIL-TO-RECLOSE
		Stand. Dev.	1.555E-9		

References

1. Forester, J.A., Kiper, K., and Ramey-Smith, A. Application of a New Technique for Human Event Analysis (ATHEANA) at a Pressurized Water Reactor, In proceedings: *PSAM 4, International Conference on Probabilistic Safety Assessment and Management*, New York City, September 13-18, 1998.

Report Number (14) SAND--98-0164C
CONF-980907--

Publ. Date (11) 199805
Sponsor Code (18) DOE/ER, XF
UC Category (19) UC-900, DOE/ER