International Journal of Reliability and Application
Vol. 2, No. 1, pp. 27-35, 2001

Use of Dynamic Reliability Method in Assessing Accident Management Strategy

Moosung Jae
Department of Industrial and Systems Engineering
Hansung University, Seoul, Korea

Abstract. This paper proposes a new methodology for assessing the reliability of an accident management, which is based on the reliability physics and the sheme to generate dynamic event tree. The methodology consists of 3 main steps: screening; uncertainty propagation; and probability estimation. Sensitivity analysis is used for screening the variables of significance. Latin Hypercube sampling technique and MAAP code are used for uncertainty propagation, and the dynamic event tree generation method is used for the estimation of non-success probability of implementing an accident management strategy. This approach is applied in assessing the non-success probability of implementing a cavity flooding strategy, which is to supply water into the reactor cavity using emergency fire systems during the sequence of station blackout at the reference plant.

Key Words : *dynamic systems, dynamic envent trees, uncertainty propagations, Latin Hypercube sampling, non-success probability.*

1. INTRODUCTION

Since the conventional risk and reliability methodologies such as event tree and fault trees have some limitations in assessing dynamic systems due to their inherent static charateristics, a new methodology with capability to consider dynamic characteristics of the systems is required. The assessment of an accident management is the case since the reliability of an accident management strategy depends on the distributions of the required and the achieved performances (Green and Bourne, 1972, Jae and Park, 1994). The quantified correlation between required and achieved performances could be obtained through a comparison between two variables that are involved with time. It can be simply thought that a successful implementation of the accident management strategy is governed by the time available for actions (requirement) and the time required by the operators (achievement).

This paper proposes a new methodology for assessing dynamic systems, in particular, assessing the reliability of an accident management, which is based on the reliability physics and the sheme to generate dynamic event tree. Then, the methodology is applied in assessing the reliability of a cavity flooding strategy that was identified as one of the promising strategies during the sequence of station blackout thorugh its individual plant examination (Park, et al., 1994) of the reference plant (Korea Electric Power Corporation, 1993), which is typical CE-type PWR of 1050 Mwe.

This methodology consists of 3 main steps: screening; uncertainty propagation; and probability estimation. Sensitivity analysis is for screening the variables of significance. Latin Hypercube sampling technique (Iman and Shortencarier, 1984) and the computer code of MAAP (Electric Power Research Institute, 1990) are used for uncertainty propagation. And the dynamic event tree (Amendola, 1988) generation method is used for the estimation of the probability of not implementing an accident management strategy.

2. OVERVIEW OF THE METHODOLOCY

In the step of screening, the M variables of significance are screened from all the input variables through the sensitivity analysis where the input variables are changed one-by-one, respectively and the impacts on the outputs due to the change of the inputs are investigated. In the step of uncertainty propagation, N samples of the M variables screened in the previous step are generated from the pre-defiened distributions with Latin Hypercube sampling technique and $N \times M$ input matrix is constructed. Then, the cumulative distribution function of the output of interest is generated using the N outputs calculated for N input vectors. After obtaining the cumulative distribution of the output variable, the non-success probability is estimated in the step of probability estimation.

The cavity flooding strategy considered in this paper is to supply water into the reactor cavity using emergency fire systems during the sequence of station blackout. The crierion to determine if the strategy is successfully implemented is whether or not to fill the reactor cavity before the core slumps using the emergency fire pumps. If the water reaches the vessel lower head after a significant amount of debris has relocated there, a film boiling will occur and the heat transfer will not be sufficient to cool the vessel enough to prevent melting and failure (Park and Dhir, 1991). Hence, the core slumping time is selected as the variable for which the non-success probability is estimated in this paper.

The procedure to estimate the non-success probability of implementing the strategy is as follows. Since both times are uncertain, the non-success probability is simply the fraction of times that the required time (operational time) exceeds the available time (phenomenological time). Let the critical time, T_C, be the time from core uncovery (T_{CU}) to core slump (T_{CS}), and t the time required by the operators to fill the cavity up to the required level. Then the non-success probability is the probability that t exceeds T_C, i.e.,

$$\begin{aligned} P_{non} &= \Pr(t > Tcs - Tcu) \\ &= \int_0^{\infty}[1 - F_t(t)]f_{Tc}(t)dt \\ &= \sum_i [\Pr_{ti}(i) * F_{Tc}(ti)] \end{aligned} \qquad (2.1)$$

where i denotes each accident sequence, $f_{Tc}(t)$ the probability density function of the critical time, T_C, and $F_t(t)$ the cumulative density function of the time required to fill the reactor cavity using emergency fire pumps, respectively. The term of $1 - F_t(t)$ in Equation (2.1) is associated with the achievement time. $Pr_{ti}(i)$ is related to the frequency of the i-th accident sequence at the required time. t_i and $F_{tc}(t_i)$ are related to the cumulative probability that the time t_i exceeds the critical time, T_C. Then, non-success probability can be estimated as follows:

1. Generate all the possible accident sequences associated with the availabilities of accident management systems and calculate each corresponding time, t_i, which is the time required to complete the strategy with respect to each accident sequence;
2. Estimate the event frequency, $Pr_{ti}(i)$;
3. Calculate the probability, $F_{tc}(t_i)$, for each time, t_i;
4. Multiply $Pr_{ti}(i)$ by $F_{tc}(t_i)$ in the equation (2.1) for each time, t_i;
5. Sum up all the results obtained in the previous step to get the overall non-success probability.

3. APPLICATION OF THE METHODOLOGY

3.1 Screening

Since the current emergency operating procedures of the reference plant do not contain specific instructions for initiating the flooding of the reactor cavity during station blackout, it is assumed that the current procedures to allow this strategy would be provided, and that the actions would be initiated at the time of core uncovery. Since the water should reach the top of the vessel lower head before the core slumps, the core slumping time is considered as the performance requirement parameter, and the time to required to fill the reactor cavity up to the required level is the performance achievement parameter.

The impact on output predictions due to change of input variables are investigated through sensitivity analysis where the parameters to model the timing of core slumping event for the reference plant are changed. According to the recommendations for screeing the important variables (Electric Power Research Institute, 1990), the parameters that may highly impact on the core slumping time are screened. MAAP code is used to determine the amount of change of the core slumping time due to the changes of the parameters is. The core slumping time generated at each calculation is the criterion for the elimintation of the insignificant variables. Finally, 8 variables are screened out, which cause changes larger than 3 minutes in the core slumping time and are summarized in Table 1.

Table 1. Eight variables selected through screening analysis.

Variables	Default Value	Typical Range	Distribution Type
X1: FCRBLK	1	0/1	Discrete
X2: TEU	2500	2100. - 2800. [K]	Uniform
X3: LHEU	2.5E5	1.E5 -4.E5 [J/Kg]	Uniform
X4: FAOX	1.0	1.0 - 2.0	Uniform
X5: VFSEP	0.35	0.25 - 0.6	Uniform
X6: HTSTAG	850.0	100.-5000. [J/sec/m^2/K]	Uniform
X7: FAOUT	0.5	0.1 - 0.5	Uniform
X8: IEVENT	0	0/1	Discrete

3.2 Uncertainty Propagation

Considering characteristics of the uncertainties of them, 100 samples for the 8 variables screened in the previsous step are generated using Latin Hypercube sampling technique. For discrete variables, X1 and X8, one of two values, that is, 0 or 1, is generated in each sampling. For variables with stochastic characteristics, X2 to X7, 100 samples are taken

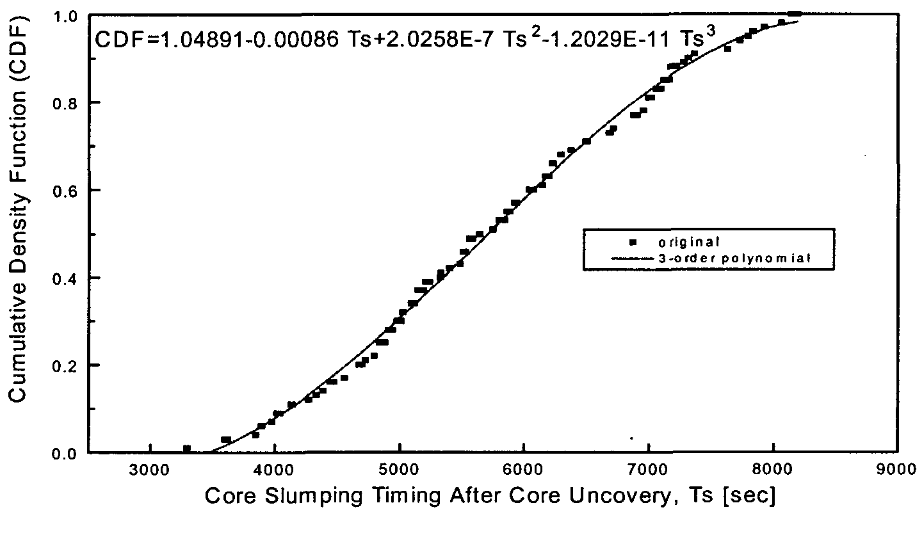

Figure 1. The distribution of core slumping time with 100 LHS sample input sets.

from the continuous uniform distributions over the ranges defined in Table 1. Through the above sampling processes, 100×8 input matrix is constructed. For each set of inputs, the core slumping time is calculated using MAAP code, and the distrinbuton of the core sluming time is generated. The cumulative distribution function of the time-to-core-slumping is fitted by the third polynomial regression method, as shown in Figure 1.

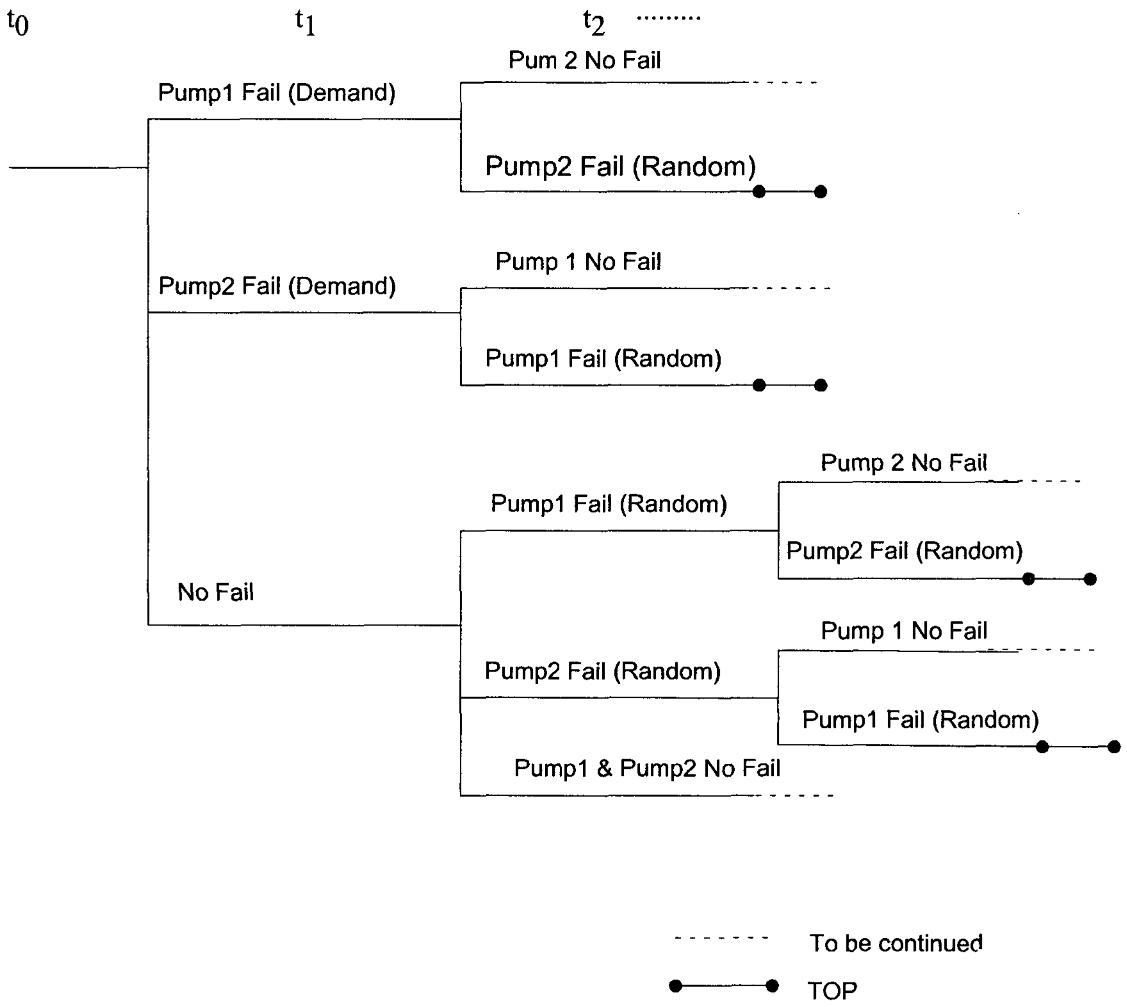

Figure 2. Dynamic accident sequences produced for the emergency fire pumps.

3.3 Probability Estimation

Prior to probability estimation, first, it is assumed that the operators may recognize the accident states of core uncovery during the station blackout sequence, and start the emergency fire pump according to the accident management procedures. In the reference plant, two emergency fire pumps with the capacitiy of 2140 gpm are available. Their demand failure rates, Φ_p , and the random failure rates, λ_p , are $2\text{x}10^{-3}$, and $2\text{x}10^{-}$

^{5}/h=6.944x10^{-9}/s, respectively (Gertman et al. 1990). Asumming that the pumps cannot be repairable if they fail and the distribution their failure times is a exponential function, then, the pump reliability can be represented as follows:

$$R_P = e^{-\lambda_P t} \quad (3.1)$$

The time required to fill the reactor cavity up to the perscibed level is the function of the reactor cavity volume (523.85 m^3) of the reference plant and the pump capacity (2140 gpm = 0.1348 m^3/s). When the operator starts the emergency fire pump, the time to fill the cavity is dependent on operating states of the two pumps. For example, if the two pumps operate successfully to the time when the cavity is filled up, it takes the optimal time, but if one of pumps or both of them fail on demand or during operation, then the required time is different from each other, depending on failure mode and failure timing.

To estimate the time, the dynamic event tree is generated as shown in Figure 2. Figure 2 shows the possible accident sequences as time goes on. The initial branch splits into three states, where one of two pumps fail on demand or both of them operate successfully. The next failure may occur due to the failure during operation, so called, random failure. Multiple failures that both pumps fail at the same time are neglected in generating new branches. This scheme is based on the dynamic method that generates new accident sequences at every time interval. Either when the both pumps fail or when it succeeds in filling the cavity up to the required level, the sequence generation stops, and then the event frequency as well as the required time for each sequence is calculated.

As shown in Figure 2, the first branch point is generated at point t_l after Δt since the initiating event takes place, and the pump reliability at that point is $R(t_1)=R_1=w$. The second branch point is generated after another Δt , and the pump reliability at t_2 is $R(t_2)=R_2=R_1w$ in the same manner. Three event cases, for example, are possible up to the time step t_3 as follows:

1. Pump is safe at any time, and the associated probability, *P(1)*
2. Pump is safe at $t < t_1$, fails at $t \geq t_1$, and the associated probability, *P(2)*
3. Pump is safe at $t < t_2$, fails at $t \geq t_2$, and the associated probability, *P(3)*.

Let *P(1)*, be *1*, R_1, and R_2; *P(2)* be 0, *1*- R_1, and *1*- R_1; and P(3) be *0*, *0*, and R_1- R_2 for each time period [*0*, t_1], [t_1, t_2], and [t_2, t_3], respectively.

When both of the pumps fail or at least one of them succeeds in filling the cavity up to the required level, the sequence generations stops. 1,521 accident sequences are obtained through this procedure. Table 2 shows the time required to fill the cavity up to the required level and the corresponding frequency of each event. The time required to fill the cavity up ranges from 3,885.6 sec (the minimum time) to ∞ sec (the infinite time), that is, from the time when it takes in case all pumps operate successfully without any failure to the time when it takes if both pumps fail before filling the cavity up to the required level.

Table 2 also shows the non-success probability for the implementation of accident management strategy. When the operators detect core uncovery and start the emergency fire pump, the success probability that fills the reactor cavity up is 0.9363 (=1 – 0.0637). It is shown that the results of sensitivity analysis of the non-success probability are obtained by changing the demand failure rate, Φ_p , and the random failure rate, λp, by the factor 10, respectively. The relative ratio of the maximum and the minimum probability, $(P\lambda_{,10}$ - $P\ \lambda_{,0.1})/\ P\ \lambda_{,0.1}$, results in a value of 0.58. It means that the non-success probability is not so sensitive to the variation of Φ_p and λp ,

Table 2. The time to required to fill the cavity up with the non-success robabilities

i	t_i [sec]	$\Pr_{ti}(i)$	$F_{Tc}(t_i)$	$\Pr_{ti}(i)*F_{Tc}(t_i)$
1	3885.6	0.99595	6.0142E-2	5.9899E-2
2	3888.3	1.4247E-6	6.0606E-2	8.6346E-8
3	3990.5	1.4247E-6	7.8592E-2	1.1197E-7
4	4092.6	1.4247E-6	9.7801E-2	1.3934E-7
5	4194.8	1.4247E-6	1.1816E-1	1.6834E-7
6	4297.0	1.4247E-6	1.3958E-1	1.9886E-7
7	4399.2	1.4247E-6	1.6200E-1	2.3080E-7
8	4501.4	1.4247E-6	1.8533E-1	2.6404E-7
9	4603.5	1.4247E-6	2.0950E-1	2.9947E-7
·	·	·	·	·
	$\propto$	1.0190E-12	1.0	1.0190E-12
Pnon $(\sum_i [\Pr_{t_i}(i) * F_{Tc}(t_i)])$				6.3736E-2

	λp	0.1λp	10λp
Φp	6.3736E-2	6.3714E-2	6.3964E-2
0.1Φp	6.0525E-2	6.0502E-2	6.0753E-2
10Φp	9.5197E-2	9.5175E-2	9.5417E-2

4. CONCLUSIONS

This paper proposes a new methodology for assessing the reliability of an accident management, which is based on the reliability physics and the sheme to generate dynamic event tree. The methodology consists of 3 main steps: screening; uncertainty propagation; and probability estimation.

Sensitivity analysis is for screening the variables of significance. Latin Hypercube sampling technique and MAAP code are used for uncertainty propagation, and the dynamic event tree generation method is used for the estimation of non-success probability of implementing an accident management strategy. Latin Hypercube sampling technique is used for uncertainty propagation, and the dynamic event tree generation method is for non-success probability estimation.

The methodology is applied in assessing feasibility in implementing the cavity flooding strategy in the reference plant. Through the application of the methodology, it is shown that this approach is useful and flexible in that it can be applied to assessing a plant-specific accident management that is required to consider the time-dependent factors such as accident progression and states of an equipment.

ACKNOWLEDGEMENT

This work was supported by the Korea Science and Engineering Foundation (KOSEF) through the Innovative Technology Center for Radiation Safety (iTRS), Seoul, Korea.

REFERENCES

GREEN, A. E. and BOURNE, A. J. (1972), Reliability Technology, Wiely-Interscience, London.

Jae, M. and Park, C. K. (1994), Quantification of Human Error Probabilities in Implementing Accident Management Strategies, *Proceedings of International Conference, New Trends in Nuclear System Thermohydraulics*, Pisa, Italy.

Park, C. K., *et al.* (1994), *The Study of IPEs of Nuclear Power Plants*, Korea Electric Power Corporation.

Korea Electric Power Corporation. (1993), *Final Safety Analysis Report for Yonggwang Units 3&4.*.

IMAN, R. L. and SHORTENCARIER, M. J. (1984), *A FORTRAN 77 Program and Users Guide for the Generation of Latin Hypercube and Random Samples for Use with Computer Models*, SNL, NUREG/CR-3624, USA.

Electric Power Research Institute. (1990), MAAP 3.0B Users Manual-Modular Accident Analysis Program for LWR Power Plants, NP-7071-CCML.

Amendola, A. (1988), Accident Sequence Dynamic Simulation versus Event Trees, *Reliability Engineering and System Safety*, **22**.

Park, H. and Dhir, V. (1991), Steady-State Thermal Analysis of External Cooling of a PWR Vessel Lower Head, *AiCHE Symposium Series*, **97(283),** 1.

Gertman, D. I., et al., (1990), *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)*, INEL, NUREG/CR-4639, **1.**