A Study on A Dynamic Reliability Analysis Model

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

동적신뢰도 평가모델의 연구

제무성
한성대학교
산업시스템공학부

Abstract

This paper presents a new dynamic approach for assessing feasibility associated with the implementation of accident management strategies by the operators. This approach includes the combined use of both the concept of reliability physics and a dynamic event tree generation scheme. The reliability physics is based on the concept of a comparison between two competing variables, i.e., the requirement and the achievement parameter, while the dynamic event tree generation scheme on the continuous generation of the possible event sequences at every branch point up to the desired solution. This approach is applied to a cavity flooding strategy in a reference plant, which is to supply water into the reactor cavity using emergency fire systems in the station blackout sequence. The MAAP code and Latin Hypercube sampling technique are used to determine the uncertainty of the requirement parameter. It has been demonstrated that this combined methodology may contribute to assessing the success likelihood of the operator actions required during accidents and therefore to developing the accident management procedures.

요 약

이 논문은 중대사고가 발생하였을때 운전원에 의하여 사고관리방안을 수행하는 경우 그 실현성(Feasibility)을 평가하는데 사용할 수 있는 새로운 시간의존적 신뢰도 분석방법을 제시하였다. 이 방법은 성능요구 (Performance Requirement)와 성능성취 (Performance Achievement)의 상관관계의 개념을 이용하는 신뢰도물리(Reliability Physics)와 모든 시간의존적 사고경위를 도출하는 동적사건수목 생성방법에 기초하고있다. 신뢰도물리는 성능요구변수와 성능성취변수의 비교를 이용한 신뢰도분석방법인 반면 동적사건수목 생성방법은 바람직한 해를 얻을때까지 모든 가능한 사고경위를 도출해 내는 방법이다. 이 방법론을 정전사고시 참조원전의 공동에 비상화재시스템을 이용하여 물을 공급하는 공동범람사고관리 방안에 적용시켰다. Latin Hypercube Sampling 방법은 성능요구변수의 불확실성을 평가하는데 사용되었다. 제시된 방법론은 사고시 필요한 운전원의 방안수행 성공가능성을 평가하는데 사용될 수 있을 뿐만아니라 궁극적으로 사고관리 절차서 개발에 도움이 될 수 있음을 보여주었다.

1. Introduction

Since the conventional risk and reliability methodologies, such as event trees and fault trees, have some limitations for the risk and reliability analysis of dynamic systems, a new methodology is required for assessing the feasibility of accident management strategies, which involves dynamic reliability assessment. This paper presents a new dynamic approach for assessing feasibility associated with the implementation of accident management strategies by the operators during an accident. This approach includes the combined use of both the concept of reliability physics and a dynamic event tree generation scheme. The proposed approach is applied to assessing the feasibility in implementing a cavity flooding strategy in a reference plant (CE type, 1050 MWe PWR) [1]. The strategy considered in this study is to supply water into the reactor cavity using emergency fire systems in the station blackout sequence. Through the IPE (Individual Plant Examination) study of the reference plant, the cavity flooding strategy was identified as one of the promising strategies [2]. The MAAP code [3] and Latin Hypercube sampling technique are used to determine the requirement parameter uncertainty, i.e., the distribution of the phenomenological event timing. The dynamic event tree method is used to produce all of the possible sequences and calculate the event frequencies with the operational timing of the each sequence [4]. Finally, the non-success probability associated with the implementation of accident management strategy has been evaluated using the proposed methodology.

2. Methodology

The assessment of feasibility in implementing an accident management strategy depends on the determination of both the required performance distribution and the achieved performance distribution. The concepts of requirement and achievement are presented in References [5, 6]. The quantified correlation between requirement and achievement represents a comparison between two competing variables. The successful implementation of the accident management strategy is governed by the time available for actions (requirement) and the time required by the operators (achievement). Since both times are uncertain, the non-success probability in implementing the strategy is simply the fraction of times that the required time (operational time) exceeds the available time (phenomenological time).

The successful implementation of the strategy is to fill the reactor cavity before the core slumps using the emergency fire pump system. The time to core slumping is used because if the water reaches the vessel lower head after a significant amount of debris has relocated there, a film boiling situation will exist and the heat transfer will not be sufficient to cool the vessel enough to prevent melting and failure [7]. Since the current EOPs (Emergency Operating Procedures) do not contain specific instructions for initiating the flooding of the reactor cavity in the station blackout sequence, 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 must reach the top of the vessel lower head before the core slumps, the core slumping time is 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 uncertainty of the core slumping time is associated with the critical time determined by the various phenomena occurring during the melt progression. If we define the critical time T_C as the time from core uncovery (T_{CU}) to core slump (T_{CS}), and t as the time required by the operators to fill the cavity up to the required level, then the non-success probability in implementing strategy is the probability that t exceeds T_C, i.e.,

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

,where i: each accident sequence, $f_{TC}(t)$: the probability density function of the critical time, T_C, $F_t(t)$: the cumulative density function of the time required to fill the reactor cavity using emergency fire pumps, where the term in the Eqn (1), $(1 - F_t(t))$, involves the factors associated with the achievement time, $Pr_{ti}(i)$: the frequency of the i-th accident sequence at the required time, t_i, and $F_{tc}(t_i)$: the cumulative probability that the time t_i exceeds the critical time, T_C.

The Latin Hypercube sampling and MAAP code are used to determine the phenomenological uncertainty. After obtaining the cumulative distribution of the core slumping time, the non-success probability in implementing accident management strategy is calculated through following steps:

1. Generate all of 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 Eq. (1) for each time, t_i.
5. Sum up all of the results obtained in the 4-th step to get the overall non-success probability.

3. The Time to Core Slumping

3.1. Variable screening for MAAP parameters

Sensitivity analysis investigates the effect of changes in input variables on output predictions. MAAP sensitivity analysis has been performed by changing model parameters associated with the event timing of core slumping for the reference plant [1]. The core support plate failure time in the MAAP output corresponds to the core slumping time. The MAAP parameters that may highly affect the time to core slumping are primarily selected according to the suggestions from the report [3]. Each variable is changed by an estimated amount and the MAAP code is run to

determine the change in the time to core slumping due to the change in that variable. The core slumping times calculated by the MAAP code are used as criteria to eliminate unimportant variables. Only 8 variables which cause changes that are larger than three minutes are screened out as shown in Table 1.

Table 1. Eight variables selected via screening analysis.

Variables	Base Case 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. Latin Hypercube Sampling

There are several methods developed for the propagation of uncertainty; the method employed here is the Latin Hypercube technique [8]. A sample size of 100 was used to propagate the uncertainty for the key variables through the MAAP code. How each variable is sampled is determined by what kind of uncertainty is associated with it. Deterministic variables are sampled zero-one. This means that every sample observation contains either the value of 0.0 or 1.0 for the discrete variables (X1, X8). For variables with stochastic characteristics (X2 - X7), the continuous distributions are sampled. The MAAP code is run for every member of Latin Hypercube samples and results in a point value for the time to core slumping for each member. The distribution of the time to core slumping is found through the MAAP calculation using a set of input data produced by Latin Hypercube sampling. The cumulative distribution function (CDF) of the time-to-core-slumping is fitted by the third polynomial regression method, as shown in Figure 1.

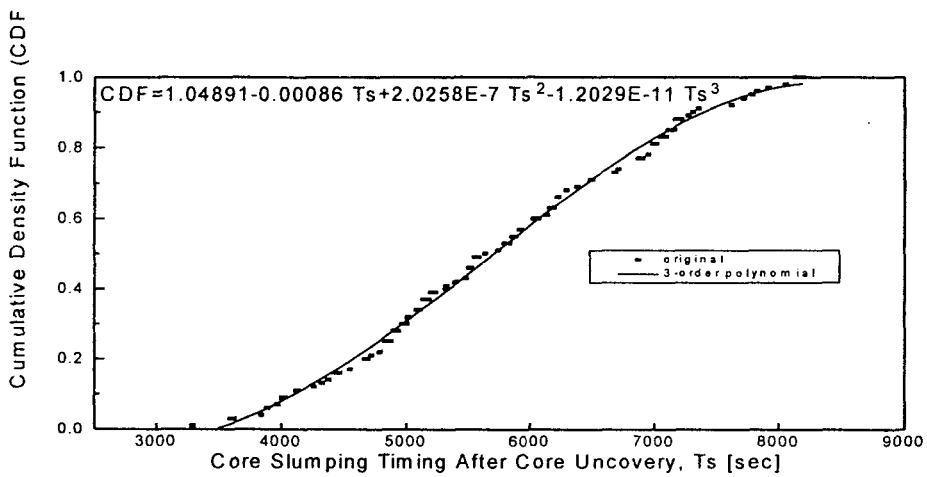

Figure 1. Core slumping timing produced from MAAP 3.0B calculations with 100 LHS sample sets of inputs.

4. The Time Required to Fill the Reactor Cavity

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 are available. They are all the same capacities of 2140 gpm. Their demand failure rates, Φ_p, and the random failure rates, λ_p, are 2×10^{-3}, 2×10^{-5}/h=6.944×10^{-9}/s, respectively [9]. The emergency fire pumps are not repairable when they fail and the distributions of their failure times are assumed to be exponential. Then, the pump reliability is represented as follows:

$$R_p = e^{-\lambda_p t} \tag{2}$$

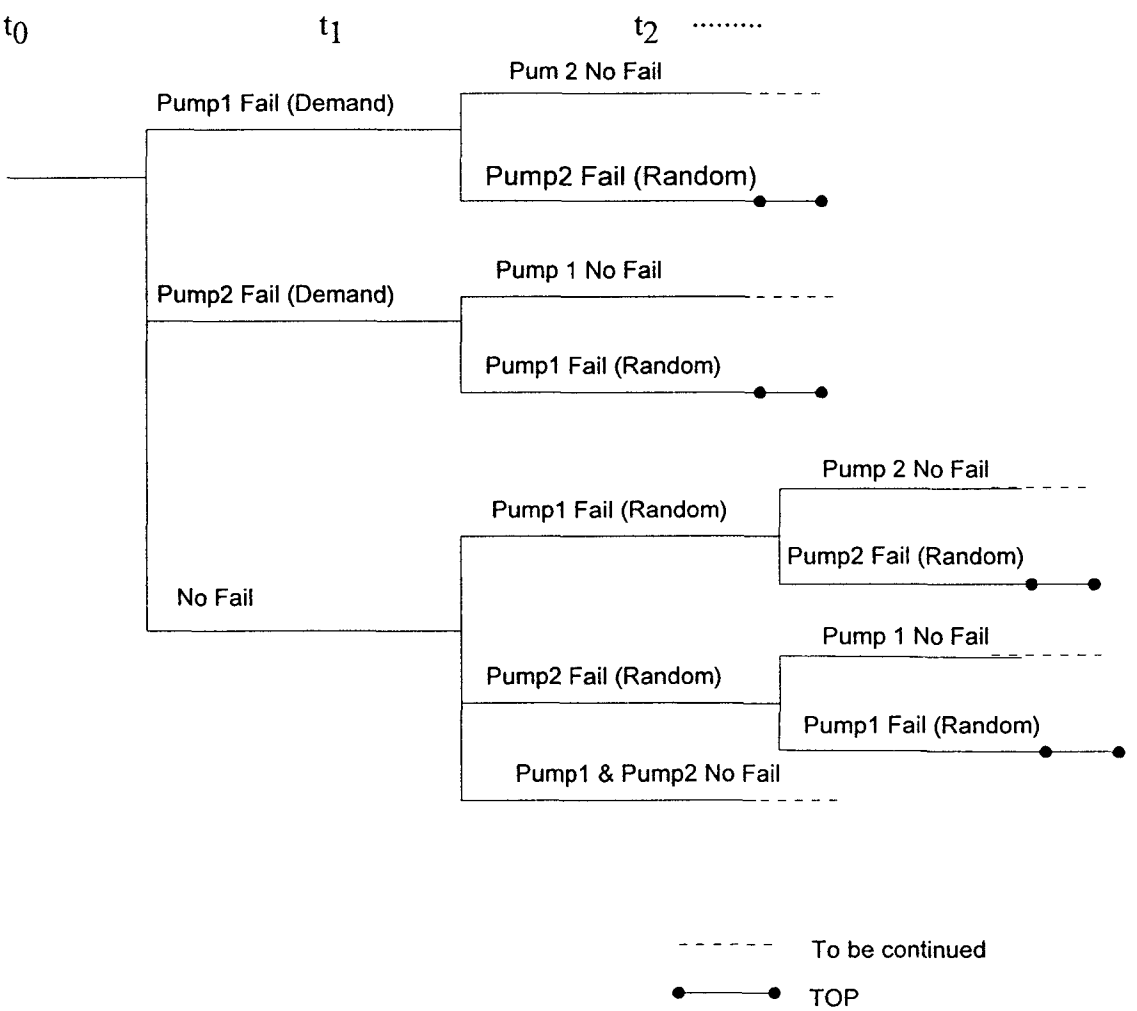

Figure 2. Dynamic accident sequences produced for the emergency fire pumps

The time required to fill the reactor cavity up to the required 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) [1]. When the operator starts the emergency fire pump, the time changes according to the 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.

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, called random failure. Multiple failures that both pumps fail at the same time, are neglected in generating new branches. This event sequence generating scheme is based on the dynamic method which 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 by the developed computer program.

5. Results

As shown in Figure 2, the first branch point is generated at point t_1 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 $R(t_2)=R_2=R_1 w$ 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 $t>=t_1$, and the associated probability: P(2)
3. Pump is safe at $t<t_2$, fails at $t>=t_2$, and the associated probability: P(3).

The first probability, P(1), is 1, R1, and R2 for each time step, [0, t1], [t1, t2], and [t2, t3], respectively. In the same manner, the second probability, P(2), is 0, 1-R1, and 1-R1, while the last probability, P(3), is 0, 0, and R1-R2 for each time step, [0, t1], [t1, t2], and [t2, t3], respectively.

Using the method explained in the previous section, all the possible accident sequences are generated at every time step. 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. We obtained 1521 accident sequences by this procedures. 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 3885.6 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. The time required to fill the reactor cavity, each event frequency, the non-success probability, and the results of the sensitivity analysis.

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
.	.	.	.	.
		1.0190E-12	1.0	1.0190E-12
$Pnon\left(\sum_i [Pr_{ti}(i) * F_{Tc}(t_i)]\right)$				6.3736E-2

	λp	$0.1\lambda p$	$10\lambda p$
Φp	6.3736E-2	6.3714E-2	6.3964E-2
$0.1\Phi p$	6.0525E-2	6.0502E-2	6.0753E-2
$10\Phi p$	9.5197E-2	9.5175E-2	9.5417E-2

Table 2 also shows the non-success probability of 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. 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,

6. Conclusions

A new dynamic methodology for assessing feasibility in implementing accident management strategies is introduced. This approach includes the combined use of both the concept of reliability physics and a dynamic event tree generation method. The proposed approach has been applied to assessing feasibility in implementing the cavity flooding strategy in the reference plant. This paper shows that this approach is useful and flexible in that it can be applied to assessing feasibility of any kind of accident management strategy. This methodology may also contribute to developing the plant-specific accident management procedures as well as assessing the cognitive human error probability.

References

1. KEPCO, "Final Safety Analysis Report for Yonggwang Units 3&4," 1993.
2. C. K. Park, *et al*, "The Study of IPEs of Nuclear Power Plants," KEPCO, Feb., 1994.
3. EPRI, "MAAP 3.0B Users Manual-Modular Accident Analysis Program for LWR Power Plants," NP-7071-CCML, November, 1990.
4. A. Amendola, "Accident Sequence Dynamic Simulation versus Event Trees," Reliability Engineering and System Safety, Vol. 22, 1988.
5. A. E. GREEN and A. J. BOURNE, Reliability Technology, Wiely-Interscience, London (1972).
6. M. Jae and C. K. Park, "Quantification of Human Error Probabilities in Implementing Accident Management Strategies," Proceedings of International Conference, "New Trends in Nuclear System Thermohydraulics," Pisa, Italy, May 30 - June 2, 1994.
7. H. Park and V. Dhir, "Steady-State Thermal Analysis of External Cooling of a PWR Vessel Lower Head," AiCHE Symposium Series, No. 283, Vol. 97, P.1, 1991.
8. R. L. IMAN and M. J. SHORTENCARIER, "*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, 1984.
9. D. I. Gertman, etc., "Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)," INEL, NUREG/CR-4639, Vol. 1, May, 1990.