International Journal of Reliability and Applications
Vol. 3, No. 1, pp. 25-35, 2002

A New Dynamic Reliability Assessment for Mid-loop Operations in a Nuclear Power Plant

Moosung Jae*
Department of Nuclear Engineering
Hanyang University, Seoul 133-791, Korea

Abstract. This paper presents a dynamic reliability assessment methodology for use in the safety assessment of a complex system such as a nuclear power plant. The method is applied to a dynamic analysis of the potential accident sequences that may occur during mid-loop operation in a nuclear power plant. The idea behind this approach consists of both the use of the concept of the performance achievement/ requirement correlation and of a dynamic event tree generation method. The assessment of the system reliability depends on the determination of both the required performance distribution and the achieved performance distribution. The quantified correlation between requirement and achievement represents a comparison between two competing variables. It is demonstrated that this method is easily applicable and flexible in that it can be applied to any kind of dynamic reliability problem.

Key Words : *dynamic reliability, probabilistic safety assessment, shutdown, nuclear power plants, mid-loop operation.*

1. INTRODUCTION

The fundamental goal of risk assessment of industrial systems such as nuclear power plants is to identify the complete set of scenarios, to assess the consequences of those scenarios, and to calculate the probabilities that those scenarios will occur. These processes provide overall insight on the plant risk due to system or equipment failures, and the results of those processes contribute the safety regulation as well as the modification of system design and operating procedures.

Process variables and reliabilities in most systems of nuclear power plants change dynamically as time goes on. However, the conventional event tree (ET) and fault tree (FT), which is firstly used in the WASH-1400[1] that is the foundation of probabilistic risk assessment (PRA), has limitation to represent dynamic behaviors of the process variables involved.

In this study, we developed a time-dependent reliability assessment methodology that

* *E-mail address :jae@hanyang.ac.kr*

can simulate the dynamic behaviors of the associated systems and showed the applicability of the methodology to the low power and shutdown (LP/SD) PRA as a basic analysis tool. The method is based on the correlation between the performance requirement and the performance achievement and the dynamic event tree generation methodology that can generate all the possible dynamic accident sequences. As a case study, we applied the method to the calculation of core damage probability (CDP) due to the failure of residual heat removal system (RHRS) during mid-loop operation.

Mid-loop operation refers to the plant operation that drains reactor coolant and maintains the water level to the mid-point of hot leg of the reactor coolant system (RCS). During this time, core residual heat is removed by residual heat removal system (RHRS). The RHR system takes suction from the RCS coolant on the hot leg loop, and the coolant passes through the heat exchanger and comes back to the RCS loop on the cold leg side.

2. METHODOLOGY

Event tree and fault tree has been used in PRA (Probabilistic Risk Assessment) ever since the first use in WASH-1400[1] as a risk analysis tool. Fault tree is used to derive the minimal cut sets (MCS) of component failures that induce a system failure. And, event tree, when an initiating event occurs, is constructed to calculate the overall system reliability by representing the logical relations between safety systems and operator responses needed for mitigation of an initiating event.

The probability of the top event occurrence is calculated by MCS. However, the order of basic event failures and the temporal characteristic are not reflected in the MCS. The order of events is limitedly considered using the concept of mission time of a function or system without an adequate reflection of time-dependent effects. Accordingly, the conventional fault tree and event tree methodologies have a limitation to model the time-dependent characteristics of a system and the behaviors of process variables.

The dynamic reliability assessment methodology introduced in this study is to assess the reliability of a system by determining the distributions of two variables, i.e., the performance requirement variable and the performance achievement variable, and comparing the two distributions to obtain the time fraction that one variable exceeds the other. Both variables are time-dependent parameters. The concept of the performance requirement and performance achievement is described in References 2 and 3 in detail.

A simulation technique so called dynamic event tree generation methodology[4-7] is applied to obtain the distribution of the performance requirement variable. Relevant physical equations are used for the simulation of interactions between process variables, and correlation between variables is for the modeling of mechanical failure effects of a system. Once an initiating event is determined, the system model generates all the possible accident sequences by considering the changes of state variables as time goes on. However, since it is impossible to generate all the infinite number of accident sequences, accident progression is terminated when the probability of an accident sequence is below a predefined limit.

In this study, we used the suggested dynamic reliability methodology to the calculation of core damage frequency in the case of a simplified mid-loop operation problem. A successful mid-loop operation represents that the circulation loop and the

reactor coolant should be maintained at a constant level for the duration of mission time to remove the residual heat using RHR and CCW systems. The mechanical failure of the RHR and CCW pumps eventually leads to core damage as a result of the loss of residual heat removal function. At an arbitrary point into the mid-loop operation, the pumps may stop and eventually the function of residual heat removal is disabled, reactor coolant begins to boil up, and finally nuclear reactor leads to core damage. In such situation, the time duration from the initiation of mid-loop operation to the time of core damage is defined as the performance achievement variable of the system.

In order to obtain the performance achievement variable, i.e., the time to core damage, all the possible accident sequences should be generated at each time interval. In general, a component reliability decreases as time goes on, hence the pump reliability at the first branch point, t1, after Δt from an initiating event, is R(t1) = R1 = ω (weight). The second branch point occurs after another Δt, and t2 is determined from the relation, R(t2) = R2 = R1* ω. As such, the pump reliability is determined successively at each time interval, Δt. For instance, if we take the case at time t3, three states of a pump are possible and the reliability at each state is determined as one of the followings.

1) in case the pump is operating at all time, the reliability is P(1),

2) in case the pump is operating at t<t1 and fails at t>= t1, the reliability is P(2),

3) in case the pump is operating at t<t2 and fails at t>=t2, the reliability is P(3).

Then, the pump reliabilities at each time interval can be summarized as in Table 1.

New accident sequences are generated at each time interval as shown in Table 1. Accident sequence development stops when one of two pumps (RHR & CCW pumps) fails within a given time. The timings and probabilities leading to the top events (i.e., the time to pump failure) are obtained using the dynamic event tree generation methodology. Detailed description is made in Section 4. The time to functional recovery of RHRS after a failure is represented as a distribution function with uncertainty. As shown in Figure 2, if we define the time to the functional recovery of the RHRS as the performance achievement variable, core damage probability (CDP) associated with the mid-loop operation can be represented as the time fraction that the time to functional recovery of the decay heat removal system (T_r) exceeds the time to core damage (τ). Mathematical expression is as follows.

$$\begin{aligned} CDP &= \Pr\ (T_r > \tau) \\ &= \sum_t \Pr[(T_r > t)\ and\ (\tau = t)] \\ &= \int_0^\infty (1 - F_{Tr}(t)) * f_\tau(t) dt \\ &= \sum_j (P_{\tau j})(1 - F_{Tr}(t)) \end{aligned} \tag{1}$$

where, j : each accident sequence,

τ : the time to core damage,

T_r : the time to functional recovery of the decay heat removal system.

$f_\tau(t)$: the probability density function (pdf) of the performance requirement variable, τ,

$F_{Tr}(t)$: the time-dependent cumulative distribution function (cdf) of the

performance achievement variable, T_r,

P_{tj} : the probability of occurrence of the j-th accident sequence at the time of pump failure, t_j,

F_{Trj} : the cdf that the performance achievement variable (T_r) exceeds the performance requirement variable (τ) at the time of the j-th accident sequence.

P_{tj}, the probability of occurrence of the j-th accident sequence at the time of pump failure, t_j is obtained using the dynamic event tree generation methodology. And, in order to acquire F_{Trj}, two kinds of resources are used: 1) the equation on the residual heat generation and 2) the information on the time to core damage and the boiling of coolant according to thermal output from NUREG/CR-6144 (Surry LP/SD PSA)[8] is used. Detailed description is provided in Section IV.

Therefore, the CDP summed over all the possible accident sequences is calculated as follows.

1) Generate all the possible dynamic accident sequences and the time information associated with each sequence.
2) Calculate the probability of occurrence of each sequence, P_{tj}.
3) Calculate the residual thermal output (MWt) according to the occurrence of system failure.
4) Obtain the time to core damage for the corresponding residual thermal output.
5) Obtain F_{Trj} for the time to core damage.
6) Multiply P_{tj}, probability of occurrence of each accident sequence, by $(1-F_{Trj})$.
7) Calculate the CDP by summing up the results of step 6 over all the sequences.

3. MID-LOOP OPERATION

During the mid-loop operation, if the RHR function loses and operators fail to respond appropriately, core coolant boils up and, eventually, core uncovers. Being recognized the possibilities of the occurrence of such accident, U.S. NRC has asked utilities to perform Generic Letter 88-17 to prevent the loss of the RHR function[9]. According to the recent results of PSAs for the Zion and Seabrook NPPs[10], the core damage frequency (CDF) in LP/SD condition turned out to be unnegeligibly large, compared with the CDF in full-power condition7). The mid-loop operation in low power/shutdown condition requires an adequate monitoring and control of coolant water level and a successful operation of the residual heat removal system. In case the water level is too high, coolant may leak through a hole of open RCS, and in case of too low water level, a phenomenon like a vortexing may take place at the entrance of RHRS, which causes air inhalation and eventually ceases the RHRS.

Residual heat generates from the decay of nuclear fission products even during the shutdown situation. Therefore, while such activities as the maintenance of steam

generators and loading of nuclear fuel are conducted after reactor trip, the function of the RHRS is required to prevent the increase of the reactor coolant temperature. The RHRS is composed of a RHR pump, a heat exchanger, and various types of valves and components. The RHRS takes suction from the hot-leg side of the RCS and flows into the cold-leg via the heat exchanger.

The drain of reactor coolant for the mid-loop operation starts by opening drain valves of the RCS loop, aligning the nitrogen-feeding line connected on the upper part of the pressurizer, and injecting the nitrogen into the pressurizer. The draining is continued by operating the drain pump until the pressurizer water level reaches 0%. When the reactor coolant is drained to the upper head of reactor vessel, nitrogen is supplied to the side of the upper head. At this time, the pressure is maintained at 0 psig. When the reactor coolant reaches the required level, the drain valve is closed and the mid-loop operation starts. At last, plant personnel open man-ways and install nozzle dams.

If the RHR function loses during the mid-loop operation, core boiling or uncovery may take place. Therefore, it is essential to ensure the RHR function during the period of the mid-loop operation.

4. APPLICATION TO MID-LOOP OPERATION

4.1 Calculation of the mid-loop operation failure times and the probability

The loss of RHR system during the mid-loop operation may take place by various causes. The event of the RHR loss happened at the Crystal River 3 NPP in 1986 happened due to a mechanical problem. At the Diable Canyon in 1987, air intrusion into the system was the cause of the RHR loss. In 1990, the Vogtle NPP experienced loss of driving force of the RHR pump due to the loss of AC power. In the same year as the Vogtle event, at the Susquehanna NPP, there was also another event of loss of RHR function that was caused by the close of isolation valve equipped on the path from the RCS to the RHR system.

In this study, we considered a situation that operators successfully drain the reactor coolant to the required level, with injecting nitrogen into the RCS. At least one loop of the RHR systems should be operating during this time period. It is assumed that one RHR pump with the capacity of 3000 gpm and one CCW pump are available.

For demand failure rate, Φ_{RHR}, and random failure rate, λ_{RHR}, of the RHR pump, values of generic data[11], Φ_{RHR} = 2.3E-03 and λ_{RHR} = 1.0E-05 /h = 7.0E-09 /s, are used, respectively. A value of 5.0E-06 /h = 1.389E-09 /s is used for the random failure rate, λ_{RHR}.

When the RHR pump fails, the function can be recovered. The time to functional recovery is uncertain and its distribution is assumed a log function. The mean time to recovery is 10.8 h, and the error factor, which means the degree of distribution, is 10. For the case of the CCW pump, the same log function is used with the mean time of 8 hr and error factor, 10[11].

The time distribution of the pump failure is assumed to be exponential function considering the decrease of its reliability as time goes on. Then, the pump reliability is represented as follows.

$$R_{pump} = e^{-\lambda t} \tag{6}$$

The tasks mainly performed during mid-loop operation are as follows: i) opening of man-way of the SGs, ii) entering the SGs, iii) installing nozzle dam, and iv) air injection into the seal to prevent leakage. The tasks mainly performed during mid-loop operation are as follows: i) opening of man-way of the SGs, ii) entering the SGs, iii) installing nozzle, and iv) air injection into the seal to prevent leakage. The time duration for the completion of those tasks is assumed to be 48 hr.

At some time point when the mid-loop operation is demanded the RHR pump should be started. But, the RHR system can fail on demand or randomly during operation. Also, the failure of CCW pumps eventually lead to the stop of RHR system. According to the mode and timing of the system failure, the time to core damage is varied.

Figure 1 shows the time-dependent event sequences of the RHR system. At the initial point (t_0) in which the initial demand is given, the branch is splitted into two states: the RHR pump fails on demand, or the pump operates successfully on demand. The failure on demand can only take place at the initial point, and all failures afterward can fail randomly. In order to model the time-dependent system states, the Dynamic Event Tree Generation Methodology was adopted. The dynamic event sequences are generated by a computer program by which a new sequence is derived and the event frequency is calculated at every constant time interval. When either the RHR pump or the CCW pump fails, the sequence generation stops and the event frequency and time duration to the termination point are calculated.

4.2 Distribution of the time to core damage

In order to solve Equation (5), the time to core damage, t (performance requirement variable), should be calculated. In order to obtain t after the failure of RHR system, thermal-hydraulic analysis is needed. In this study, we used the fitting data from the Surry LP/SD PSA[8]. The time t has the following functional relationship under 32 °C of the atmospheric pressure,

$$t = f(P) \tag{7}$$

where, P is the decay heat [MWt] generated after reactor shutdown.

Both fitting data[8] of the time to boil-off (t_{BO}) and the time to core damage (t_{CD}) versus $P(t)$, the decay heat, are represented as following correlations using the 4-th polynomial regression:

$$t_{CD} = 47264.6 - 11183.3 * P(t) + 1183.3 * P(t)^2 - 57.2 * P(t)^3 + 1.028 * P(t)^4 \tag{8}$$

$$t_{BO} = 41969.8 - 9939.4 * P(t) + 1055.1 * P(t)^2 - 51.1 * P(t)^3 + 0.916 * P(t)^4 \tag{9}$$

For the decay heat generation, the following decay heat correlation was used.

$$P(t) = 0.1 * P_0 * \left[(t - T_o + 10)^{-0.2} - (t + 10)^{-0.2} + 0.87(t + 2Exp7)^{-0.2} - 0.87(t - T_0 + 2Exp7)^{-0.2}\right] \tag{10}$$

where, t : the time to failure of RHR pump including reactor operation time [sec]

T_0 : the operation time to reactor shutdown [sec]

P_0 : the reactor thermal power [Mwt]

Following the definition and notation in Fig.2,

$$t = T_0 + T_t + t_j \tag{11}$$

where, T_t : the transition time to mid-loop operation from reactor shutdown [sec], and

t_j : the time to failure of RHR system [sec].

T_0 and T_t are assumed 1 yr and 6 hr, respectively. P_0 at the reference plant[12] is 2825 Mwt. Accordingly, Eq. (10) is possibly solved, and using Eq. (8) and (9) the time to failure of RHR system can be obtained.

4.3 Time to Functional Recovery of the RHR Pump

The time to functional recovery of RHR pump by plant personnel after once the pump fails assume the log-normal distribution, and the mean times for RHR and CCW pumps are 10.8 hr and 8 hr, respectively. The error factors ($\sqrt{X_{.95}/X_{.05}}$) are all 10.0[11]. Therefore, the distribution function used in the study takes the following form,

$$f_{Tr}(t) = \frac{\exp\left\{-\frac{1}{2}\left(\frac{\ln t - \ln Pm}{\beta}\right)^2\right\}}{\beta\sqrt{2\pi}t} \tag{12}$$

where, the median value is

$$Pm = \exp(\mu) = \exp\left(\ln\alpha - \frac{\sigma^2}{2}\right) \tag{13}$$

and log standard deviation,

$$\beta = \frac{\ln EF}{1.645} \tag{14}$$

Accordingly, $(1 - F_{Trj})$ in Eq. (5) is obtained using the following equation,

$$1 - F_{Trj} = \int_t^\infty f_{Tr}(t)dt \tag{15}$$

The computer program was developed in order to calculate $\sum(P_{ij})(1 - F_{Trj})$ in Eq. (5) for all the accident sequences.

5. RESULTS

Using the Dynamic Event Tree Generation Methodology, time t_j is calculated for each of accident sequences and summed up over all t_j to get the CDP during mid-loop operation. The results are shown in Table 2. The total CDP is calculated to be 7.7E-04, which represents the probability leading to core damage when the RHR system fails at a certain point during mid-loop operation. Sensitivity analysis was conducted to consider the uncertainty of the time to core damage. When the time to core damage (Eq. 8) is replaced by the time to boil off (Eq. 9), the CDP due to the failure of RHR system is

calculated to be 7.4E-03. Table 3 shows the results obtained by varying the demand failure rate by factor 10. The relative ratio between the lowest CDP and the highest CDP is about 3,700, which means the CDP is highly sensitive to the value of demand failure rate.

6. CONCLUSION

In the paper, a new dynamic reliability assessment methodology, which is based on the dynamic event tree generation method and the correlation between performance achievement and performance requirement variables, was introduced and applied to the safety assessment of mid-loop operation. The method showed to some extent a possibility to resolve the limitation that the conventional event tree and fault tree had in dealing with the dynamic nature of accident scenarios. The method can be applied to the safety assessment of the low power and shutdown PSA or advanced reactor designs. Also the method can be used to represent operator's dynamic behaviors explicitly and to model dynamic operator-machine interaction.

But the proposed method can lead to unmanageable states and require large amounts of computational load for modeling entire systems, which is large and complex. Therefore, an efficient truncation technique will be needed for the method to be used in modeling large-scale systems such as nuclear power plants or chemical plants. But it is expected that the approach can be used to model detailed reliability of major systems alone.

ACKNOWLEDGEMENT

This work was supported by the KOSEF through Innovative Technology Center for Radiation Safety.

REFERENCES

1. U.S. NRC (1975). Reactor Safety Study, WASH-1400.

2. A.E. Green and A.J. Bourne (1972). Reliability Technology, Wiley-Interscience, London, 83-95.

3. M. Jae and C.K. Park (1995). A New Dynamic HRA Method and Its Application, *The Journal of Korean Nuclear Society*, **27**.

4. A. Amendola (1988). Accident Sequence Dynamic Simulation versus Event Trees, *Reliability Engineering and System Safety*, **22**, 3-25.

5. C. Acosta and N. Siu (1993). Dynamic Event Trees in Accident Sequence Analysis: Application to Steam Generator Tube Rupture, *Reliability Engineering and System Safety*, **41**, 135-154.

6. N. Siu (1994). Risk Assessment for Dynamic Systems: An Overview, *Reliability Engineering and System Safety*, **43**, 43-73.

7. G. Cojazzi (1996). The DYLAM Approach for the Dynamic Reliability Analysis of Systems, *Reliability Engineering and System Safety*, **52**(3), 279-296.

8. T.L. Chu, et al. (1994). Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1: Analysis of Core Damage Frequency from Internal Events During Mid-loop Operation, NUREG/CR-6144, BNL.

9. U.S. NRC (1988). Loss of Decay Heat Removal, 10 CFR 50.54(f).

10. U.S. NRC (1993). Shutdown and Low Power Operation at Commercial Nuclear Power Plants in the United States, NUREG-1449.

11. IAEA (1988). Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-478.

12. KEPCO (1993). Final Safety Analysis Report for Yonggwang Units 3&4.

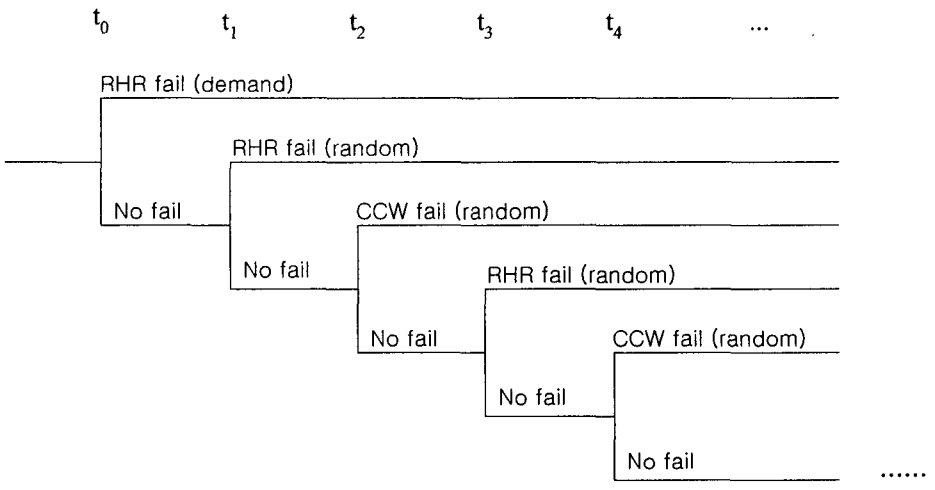
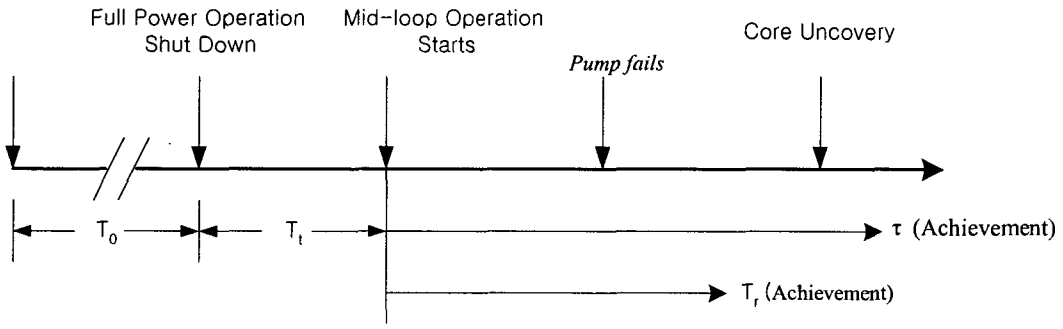


Figure 1. Dynamic possible event sequences leading to TOP event



T_0 : Operating time before the reactor shutdown [sec]
P_0 : Thermal output of the Reference Plant [MWt]
t_t : Time of the occurrence of the RHR system failure [sec]
T_t : Transition time from the reactor shutdown to mid-loop operation [sec]

Figure 2. Timings of shutdown, initiation of the mid-operation, pump failures, and core uncovery

Table 1. Pump reliabilities in each time step

	[0, t1]	[t1, t2]	[t2, t3]
$P(1)$	1	R1	R2
$P(2)$	0	1 - R1	1 - R1
$P(3)$	0	0	R1 - R2
$\sum P(i)$	1	1	1

Table 2. Calculated probabilities leading to possible accident sequences and CDP for each sequence

j	t_j [sec]	P_{ij}	$1-F_{Trj}$	$P_{ij}(1-F_{Trj})$
1	0.	2.000E-3	6.116E-5	1.223E-5
2	10.	8.372E-7	6.117E-3	5.121E-9
3	20.	1.114E-6	6.118E-3	6.818E-9
4	30	1.391E-6	6.118E-3	8.515E-9
5	40	1.668E-6	6.119E-3	1.021E-8
6	50	1.946E-6	6.120E-3	1.191E-8
7	60	2.223E-5	6.121E-3	1.361E-8
8	70	2.501E-6	6.122E-3	1.530E-7
9	80	2.777E-6	6.122E-3	1.701E-8
...	...	...	...	...
$CDP(\sum_j (P_{ij})(1-F_{Trj}))$				7.703E-4

Table 3. Sensitivity calculations of core damage probability

	λ_{RHR}	$0.1 * \lambda_{RHR}$	$10 * \lambda_{RHR}$
λ_{ccw}	7.703E-04	8.915E-05	7.592E-03
$0.1*\lambda_{ccw}$	9.191E-05	2.031E-05	8.088E-04
$10*\lambda_{ccw}$	7.554E-03	7.774E-04	7.543E-02