MCSS Based Numerical Simulation for Reliability Evaluation of Repairable System in NPP

Daochuan Ge[a,b,*], Ruoxing Zhang[b], Qiang Chou[b], Yanhua Yang[a]
[a] School of Nuclear Science and Engineering, Shanghai Jiao Tong University, Shanghai, China
[b] Software Development Center, State Nuclear Power Technology Corporation, Beijing, China

Abstract: The quantitative analyses of Nuclear Power Plant (NPP)'s repairable systems are conventionally Markov-based methods. The thing is, systems' state space grows exponentially with the increase of basic events, which makes the problem hard or even impossible to solve. In addition, the maintenance /test activities are frequently imposed on some safety-critical components, which make the Markov based approach unavailable. In this paper, a new numerical simulation approach based on MCSS (Minimal Cut Sequence Set) is proposed, which can get over the shortcomings of the conventional Markov method. Two typical cases are analyzed and results indicate that the new approach is correct as well as feasible.

Keywords: Numerical Simulation, Reliability, Minimal Cut Sequence Set, Repairable System

1. INTRODUCTION

After Fukushima nuclear accident, more and more countries focus their attention on NPP's safety, especially the reliability of safety-critical systems. The real-life safety-critical systems often have sequence- and function-dependent failure behaviours. For the description of these dynamic failure behaviors, traditional static fault tree is unfeasible. To overcome the shortcomings of the conventional static fault tree method, some researchers [1] introduced a few new dynamic gates, such as PAND, SPARE, FEDP and SEQ into static fault tree, i.e., DFT. Compared with previous static fault tree, the DFT greatly extends modeling capacities. Considering the intuitiveness and compactness of DFT, NPPs often adopt DFT to model safety-critical system's failure mechanism. The commonly-used methods for quantifying a DFT are mainly based on Markov approaches [2,3,4] or multi-integration approaches [5,6,7]. Unfortunately, each of these methods has its own shortcomings: For the Markov-based approach, it requires the time-to-failure/time-to-repair of components follows exponential distribution. In addition, the approach may confront the notorious problem of "state space explosion"; as to the multi-integration -based approach, although it avoids the problem of "state space explosion", it is only applicable for non-repairable systems. Given that the components in NPP system are usually repairable and their failure and repair time are not exponent, the methods mentioned above are unavailable. To solve these problems, some researchers proposed a Monte Carlo Simulation-based method [8,9]. This Monte Carlo Simulation method is based on the failure behaviours of DFT gates. As to simple dynamic gates, this method is easy to implement. However, when dynamic gates are highly-coupled and complex, this method usually becomes hard to carry out.

In this paper, a MCSS-based numerical simulation method is presented, which is applicable for any complex DFT and easy to implement. Results show this method is feasible and correct.

The remainder of this paper is organized as follows: Section 2 reviews some related concepts including unavailability, Minimal Cut Sequence Set, etc; Section 3 presents our proposed method. Section 4 provides two cases studies to validate our proposed method. Section 5 gives final conclusions.

2. RELATED CONCEPTS

[*] Corresponding author: Phone: +86-10-18817554483; Fax: +86-10-58197250
E-mail: gdch-2008@163.com

2.1. System's Unavailability

Suppose a repairable unit that is put into working at time t=0. As the unit fails, a repair activity is implemented to restore the function of the failed unit. The state of the unit at time t is defined by a state variable:

$$X(t)=\begin{cases}1 & if\ the\ unit\ is\ working\ at\ time\ t\\ 0 & otherwise\end{cases} \tag{1}$$

Then the reliability of a repairable unit may be measured by the availability of the unit at time t:

$$A(t)=P_r\left(X(t)=1\right) \tag{2}$$

Sometimes, $A(t)$ is referred to be as the point availability. Note if the unit is not repaired, then we can get: $A(t)=R(t)$. Where $R(t)$ is the reliability of a non-repairable unit at time t. Similarly, we can define the unavailability of a non-repairable component at time t as the probability that the unit is not in working state at time t:

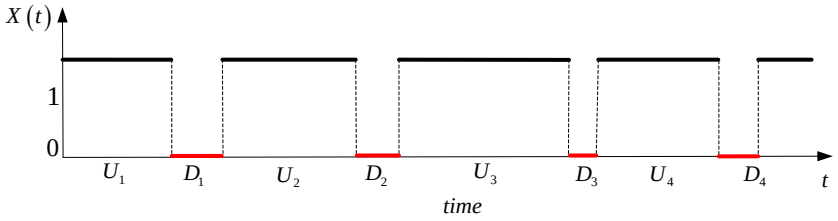
$$\overline{A(t)}=1-A(t)=1-P_r\left(X(t)=1\right) \tag{3}$$

In NPP, we are more interested in the average or mission availability $A(0, t)$ in time interval $(0, t)$, which is defined as:

$$A_{av}(0,t)=\frac{1}{t}\int_0^t A(t)dt$$

The average availability $A_{av}(0, t)$ can be interpreted as the mean proportion of the time interval $(0, t)$ where the unit is able to operate. Suppose a repairable unit that starts to work at time t=0. Whenever the unit fails, it is repaired to an "as good as new" state or substituted by a new one. Then a sequence diagram of up-times (life times) U_1, U_2 … and down-times (outage times) D_1, D_2 … appearing alternately is obtained as shown in Fig.1.

Fig.1: alternate state-time of a repairable unit



In this paper, we suppose the up-times U_1, U_2, ⋯ are independent and identical distributed and D_1, D_2, ⋯ are independent and identical distributed as well. In addition, we also suppose U_i+D_i for i=1, 2, ⋯ are independent. Assume a unit has just finished n repair, then the unit's up-times U_1, U_2, ⋯,U_n and down-times D_1, D_2, …, D_n are obtained. When the $n \to +\infty$, then the average availability of the unit can be expressed as:

$$A_{av}=\frac{\lim\limits_{n\to\infty}\sum_1^n U_i}{\lim\limits_{n\to\infty}\sum_1^n U_i+\lim\limits_{n\to\infty}\sum_1^n D_i} \tag{4}$$

Then the average unavailability of the unit can be written as:

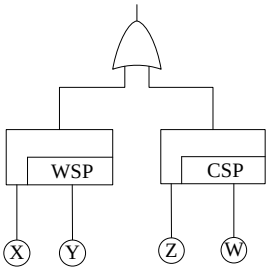
$$\overline{A_{av}}=1-A_{av}=\frac{\lim\limits_{n\to\infty}\sum_1^n U_i}{\lim\limits_{n\to\infty}\sum_1^n U_i+\lim\limits_{n\to\infty}\sum_1^n D_i} \tag{5}$$

2.2. Minimal Cut Sequence Set

As to a system modelled by DFT, the occurrence of the top event (system failure) not only depends on the combination of basic events but also depends on their failure sequences. Thus traditional minimal cut set is not able to describe this sequential failure behaviour correctly. To solve this problem, Tang et al [10] presents a concept of Minimal Cut Sequence (MCS) that expresses the minimal failure sequence that causes the occurrence of the top event of a DFT. The original expression of a minimal cut sequence comprises several capitals denoting a failure of a basic event and several temporal connecting symbols "→" which is used to express the failure sequence, i.e., the left event

fails before the right one. However in a real-life system's DFT, the failure behaviours of the basic events may be not the same: Some components are initially powered on; some components may be initially powered on just at a reduced power; and some others may be originally in a standby state without any power. In this paper, to distinguish the failure behaviours of the basic events, four special symbols are introduced: "X" denotes the component X being initially powered on at a full energy and fails randomly; " ${}_{X}^{0}Y$ " indicates the component Y as a cold spare of X is initially unpowered and fails after X; " ${}_{X}^{1}Y$ " expresses the component Y as a warm spare of X and fails after X; " ${}_{X}^{\alpha}Y$ " shows the component Y as a warm spare of X and fails before X. For an illustrative purpose, an example is given in Fig.2.

Fig.2: An Illustrative Example



For the system's top event is connected by the logic OR of the two dynamic gates, i.e., WSP gate and CSP gate, according to the failure behaviours of dynamic gates mentioned in [11], the minimal cut sequences of the system failure are obtained as $\{ X \to {}_{X}^{1}Y , {}_{X}^{\alpha}Y \to X , Z \to {}_{Z}^{0}W \}$. For a DFT, it may have more than one MCS and all these MCSs compose an aggregate, i.e., Minimal Cut Sequence Set (MCSS). Since the occurrence of each MCS leads to the failure of a system, the MCSS captures the complete information about a system's failure. Note that whether a system is repairable or not, the corresponding MCSS is unique. Therefore we can get the MCSS of a repairable system using the approaches developed for non-repairable systems [12,13].

2.3. Basic Events' Failure Behaviors

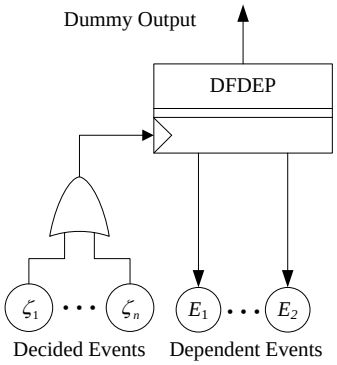
The failure behaviour of a basic event refers to the randomness of its failing. As mentioned above, basic events involved in a DFT may have different failure behaviours. According to the failure behaviours of the basic events, we classify the basic events into three categories: random basic events, semi-random basic events and decided basic events. As we know the failure time of a basic event is completely random during its mission time. Note that a component's mission time doesn't always equal the system's mission time. For example, the mission time of a cold spare is always dependent on the primary component.

In general, the occurrences (failure behaviours) of components providing the main functions during system mission period are considered to be random basic events. And the occurrences of components supplying standby function are considered semi-random basic events. In most cases, the entire spare components except hot spares are semi-random basic events, and the remains are the random basic events. In NPP, some components' function failure is caused either by a random event (random failure event) or by a decided event. The decided events here refer to the regular maintenance/test activities imposed on the safety-critical components to improve the reliability. However, when the safety-critical components are forced outage for the regular maintenance/test activities, the risk of the system will increase. In this paper, the decided basic event is supposed to be a virtual component. To reflect the influence of the decided basic events to a component' function, this paper developed a new function dependent dynamic gate. To differ from the traditional FDEP gate, this new dynamic gate is called Decided Function Dependent gate (DFDEP) where the trigger events are the decided events. When the decided events occur, the dependent events are forced outage. The DFDEP gate is shown in Fig.3. The symbols $\zeta_1 \ldots \zeta_n$ represent the decided events such as maintenance activity, test activity, etc. and the $E_1 \ldots E_n$ means the dependent events. In general, the classifications of the basic events are listed in Table 1.

Table 1: Classification of the Basic Events

Category	Basic Events	Symbols
Random basic events	The basic events under AND, PAND , OR gate; The basic events under SPARE gate representing the primary components;	X
Semi-Random basic events	The basic events under PAND gate denoting the standby components;	${}_X^0Y$, ${}_X^1Y$, ${}_X^1Y$
Decided basic event	Virtual events expressing a series of maintenance, test, etc, activities.	${}_X\zeta$

Fig.3: A Decided Function Dependent gate



3. NUMERICAL SIMULATION FOR THE MCSS

3.1. Numerical Simulation for the Failure Behavior of a Basic Event

As to a repairable component, its failure behavior can be simulated by a Monte Carlo-based approach. It is known the time-to-failure and time-to-repair of a component are only determined by their respective Cumulative Probability Distributions (CDFs). Consider the CDFs of a component's time-to-failure and time-to-repair are $F(x)$, $G(x)$, and then the time-to-failure T_f and the time-to-repair T_r are obtained by the following expressions:

$$\begin{cases} T_f = F^{-1}(\varepsilon) \\ T_r = G^{-1}(\eta) \end{cases} \tag{6}$$

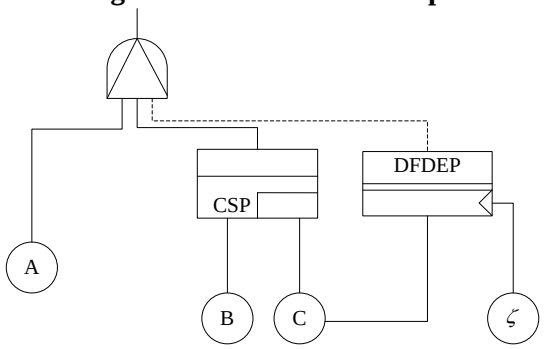
Where the ε , η are uniform random numbers generated by any standard random number generators. For the random basic events being active initially, its running state in system's mission time can be simulated directly using Eq. (6). However, for the semi-random basic event, when there is no demand, it will keep up in standby state or may be in a failed state due to on-shelf failure. Therefore the failure behaviors of the semi-random events are relatively complicated. For the cold spares, they never fail during the standby states. Considering the outage time (time-to-repair) of the primary component is the mission time of the cold spare, the failure behavior can be simulated using Eq. (6) during this mission time. As to the warm spare, the situation is even more complex. The failure rates of a warm spare in standby state and in working state are not the same. In other words, the warm spares have two CDFs of the time-to-failure in different states. Generally speaking, the failure rate of a warm spare in working state is higher than that in standby state. When the primary component is staying in a working period (time-to-failure), the failure behavior of the standby component is simulated by the Eq. (6) with one time-to-failure CDF. Similarly, when the primary component is staying in an outage period (time-to-repair), the failure behavior of the standby component is simulated by the Eq. (6) with the other time-to-failure CDF. Apparently the failure behaviors of the semi-random basic events are dependent on but not affecting the random basic events. Finally, as to the decided events, the occurrences time of these events can be obtained directly from the scheduled maintenance/test management documents.

Considering the correlation between the basic events' failure behaviors, the simulation precedence is required as: random basic events →decided events →semi-random basic events.

3.2. Numerical Simulation for the MCSS

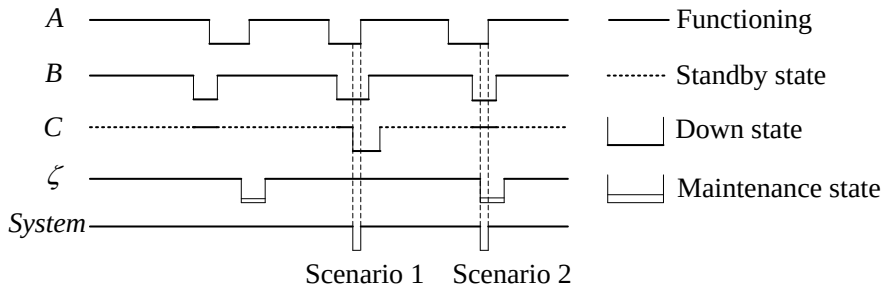
After simulating the basic events' failure behaviors, the numerical simulation of the system's MCSS is carried out. If a MCS occurs at some point, the system is considered to be failed. For demonstration purpose, an illustrative example is shown in Fig.4.

Fig.4: An Illustrative Example



Based on the temporal rules mentioned in [12,13], the MCSS of the example system is: {A→B→ ${}^{0}_{B}C$, A→B→ ${}_{C}\zeta$ }. Where the symbol ${}_{C}\zeta$ represents a series of regular maintenance activities imposed on component C. Therefore, the system has two failure scenarios: the scenario 1 is A→B→ ${}^{0}_{B}C$ and the scenario 2 is A→B→ ${}_{C}\zeta$. The state-time of the example system (MCSS) is depicted in Fig.5.

Fig.5: The State-time of The Example System's MCSS



For generating the system state time diagram, all components state time profiles, including virtual components (test/maintenance activities), involved in every MCS are compared. The system will fall in a failed state if all the components contained in a MCS failed in a pre-assigned sequence (usually from left to right), as shown in Fig.5 (first and second scenarios). In the scenario 1, the active component (A) failed followed by the second component (B), and then followed by the third component (C), the system is identified as failure since the failure sequence meets A→B→ ${}^{0}_{B}C$. As to the scenario 2, although the standby component (C) is functionally available during the repair period of the primary component (B), it is forced outage for the imposed maintenance activity, and the system is still considered to be failed since the failure order meets A→B→ ${}_{C}\zeta$.

3.3. Calculation the System Reliability Indexes

In NPP, we are interested in system average unavailability and unreliability. To obtain these reliability indexes, the total outage time (t_o^i) and time to first failure (t_f^i) of the system in a simulation are recorded. Let $\varphi(t)$ be the system state variable and the logic value of the variable is defined as:

$$\varphi(t)=\begin{cases}1, & t<T\\ 0, & t\geq T\end{cases}$$

Where, T is the mission time of the system.

Then, the system average unavailability in the mission period is evaluated as:

$$\overline{A_{av}}=\frac{\sum_{i=1}^{N}t_o^i}{NT} \tag{7}$$

Where, the N is the simulation number. And the system unreliabilityy R_s during the mission time T can be calculated using the follow equation.

$$R=\frac{\sum_{i=1}^{N}\varphi\left(t_f^i\right)}{N} \tag{8}$$

4. CASE STUDY

4.1. Case Study 1

In this section, a case study is presented to validate the proposed method. The case is excerpted from an I&C (Instrument and Controller) system in one Chinese NPP. The simplified DFT model of this system is shown in Fig.6. And every capital letter represents a component. In I&C system, every component is repairable. The components failure and repair parameters are listed in Table 2.

Fig.6: Simplified DFT of an I&C Controller System

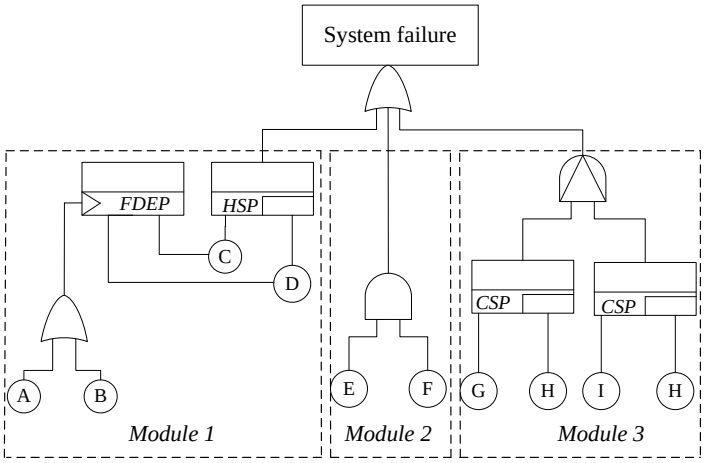


Table 2: Components failure and repair parameters

Component	Failure rate(h)	Repair rate(h)	Component	Failure rate (h)	Repair rate(h)
A	1.0E-4	0.25	F	5.0E-3	4.00
B	5.0E-4	1.20	G	1.4E-3	2.00
C	1.0E-3	1.50	H	2.0E-4	0.50
D	1.5E-3	1.00	I	2.5E-3	3.00
E	5.0E-3	5.00	-	-	-

The MCSS of the DFT is {A, B, C→D, D→C, E→F,F→E, I→G→H,G→H→I}. For the mission time 10^4h, the unavailability of I&C system calculated by our proposed method is 8.18E-4. For validation purpose, the Markov-based approach is adopted as a benchmark. To reduce the system state space, the system is divided into three independent sub-modules via modularization. Each sub-module, denoted with the dotted box, is solved by the Markov approach. Then the results of the three sub-modules are integrated to obtain the system unavailability. As applying the Markov-based approach,

the unavailability of the system is obtained 8.20E-4, which is accorded with ours. In addition, the unavailability time and first time to failure distribution for the system is shown in Fig.7-8, respectively.

Fig.7: Unavailability with Time

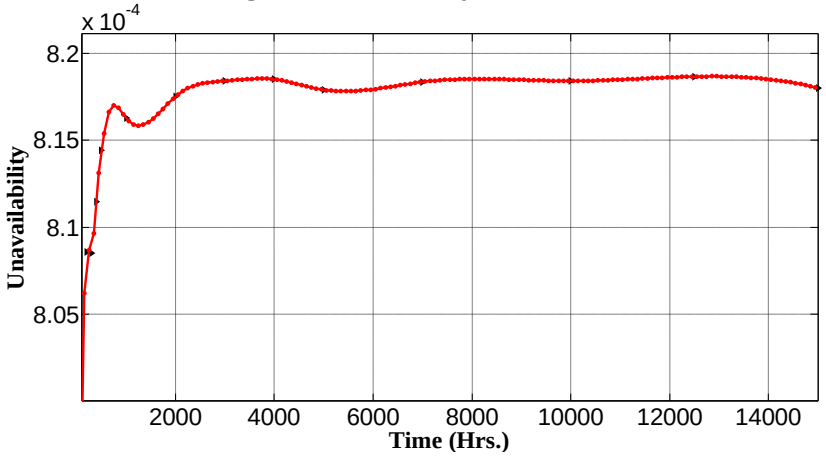
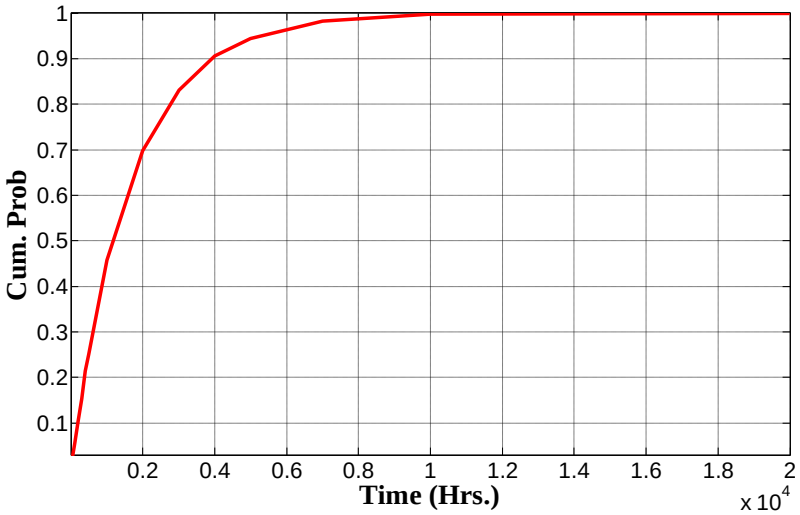


Fig.8: First Time to Failure Distribution



4.2. Case Study 2

For further validation purpose, another case with complex failure behaviors is studied. The case is the electrical power supply system of typical NPP. The system contains three subsystems: the Grid supply subsystem known as Class Ⅳ supply is the main power which feeds all the load; The diesel generator subsystem, known as Class Ⅲ supply, as the standby power of the Class Ⅳ supply is providing the emergency power in the absence of the primary power; The sensing & control subsystem is used to trigger the redundant diesel generator once detecting the failure of Grid supply system. To ensure the reliability of the electrical power supply system, the redundant diesel generator is forced outage for regular test/maintenance. Therefore the system has two failure scenarios: The Grid supply subsystem fails, and then redundant diesel generator fails or is unavailable for test or maintenance outage; the sensing & control subsystem fails before the primary diesel generator fails and it makes the standby power be not triggered. The top event (station blackout) of the system modeled by DFT is shown in Fig.9. The component failure and maintenance information is listed in Table 3.

Fig.9: Dynamic Fault Tree Model for the Station Blackout Accident

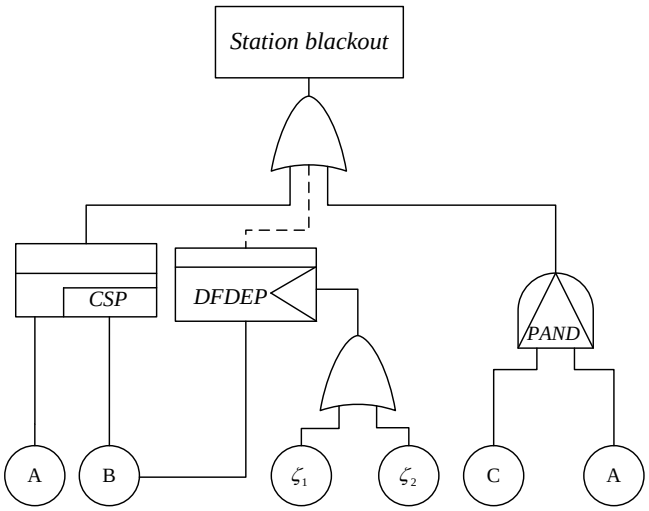


Table 3: component failure and maintenance information

component	description	Failure rate	Repair rate	Test period/time	Maint. period/time
A	Grid supply	2.34E-4	2.590	-	-
B	Standby supply	5.33E-4	8.695E-2	-	-
C	Sensor	1.00E-4	2.500E-1	-	-
ζ_1	Test activity	-	-	168/8.33E-2	-
ζ_2	Maint. activity	-	-	-	216/8

For a general dynamic repairable system, the DFT can be quantified by a Markov-based approach. However, in this case, it becomes unavailable since the test and maintenance activities are decided events. Hence an approximate solving strategy is adopted as: the unavailability of CSP gate (Q_{CSP}) is approximately obtained by the unavailability of Grid supply being multiplied the unavailability of standby supply, and the unavailability Q of the standby component is solved by the equation: Q= [1-(1-e$^{-\lambda T}$)/ λT]+[$f_m T_m$] +[λT_r]+[τ / T] suggested in IAEA P-4 [14], where λ is failure rate, T is test interval, f_m is frequency of preventive maintenance, T_m is duration of maintenance, T_r is repair time, τ is test duration; As to the unavailability of PAND gate (Q_{PAND}), it is can be solved by the conventional Markov approach. Then the approximate solution of the system unavailability (Q_{syst}) is calculated by the following equation: $Q_{syst} = Q_{CSP} + Q_{PAND} - Q_{CSP} Q_{PAND}$. For the mission time $10^4 h$, the unavailability of the system is 3.89e-7 using the approach mentioned above.

At last, the unavailability of the electrical power supply system is calculated by our proposed simulation approach. The system MCSS is {C→A, A→B, A→ζ_1,ζ_1→A, A→ζ_2,ζ_2→A}, then the system unavailability is finally simulated as 3.87e-7 with 10^7simulation numbers. Obviously, the result obtained using our method is in good agreement with that calculated by the approximate solving strategy. In addition, the unavailability-time and outage-time distribution of the system are obtained as shown in Fig.10-11.

Table.10: Unavailability with Time

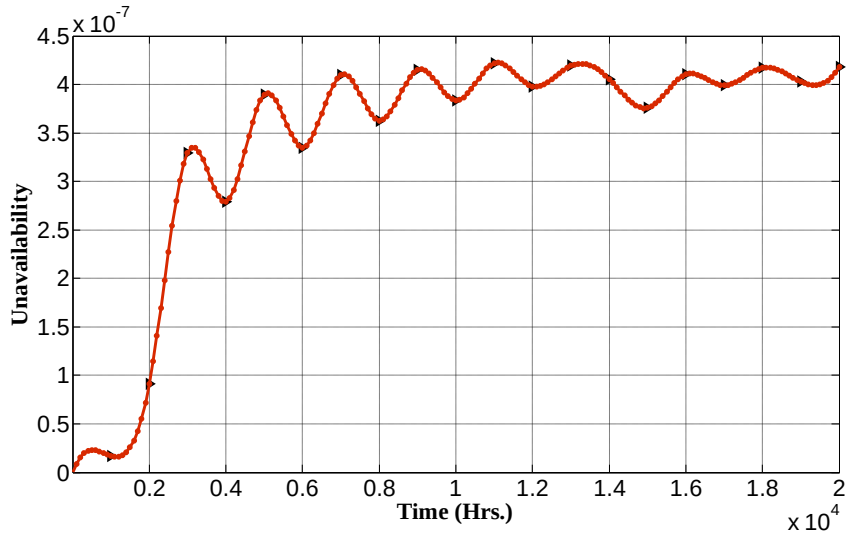
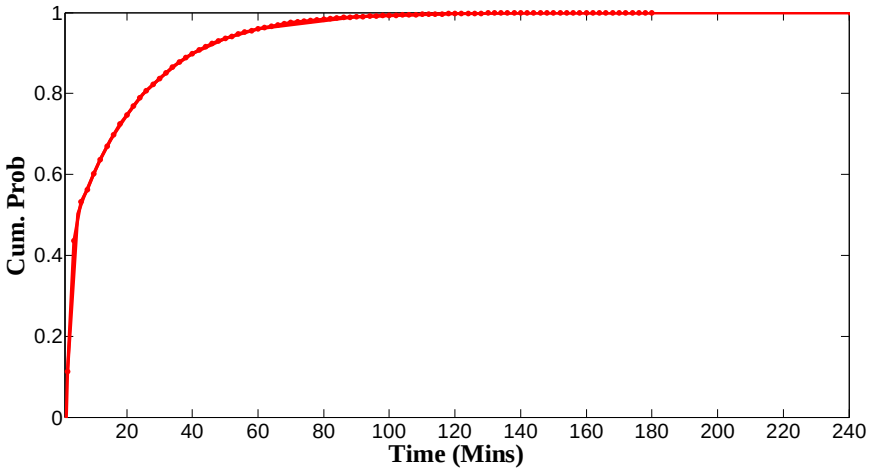


Table.11: Outage Time Distribution



5. CONCLUSION

In this paper, we propose an efficient numerical simulation approach for evaluating the reliability of repairable system in NPP. By contrast to the existing approaches, such as Markov model, multi-integration model, our proposed approach has no limitation in the size of DFT, exponential components time-to-failure and time-to-repair distributions. Moreover the proposed approach is applicable to the system components with scheduled tests and maintenance activities. The results show this simulation method is correct. Although it is intensively computational for the top event with a small occurrence probability, it is a valuable approach to be studied with the rapid development of computer technology.

References

[1] Dugan JB, Bavuso SJ, and Boyd MA. "*Dynamic fault-tree models for fault –tolerant computer systems*". IEEE Transaction on Reliability, 41(3), pp. 363-377, (1992).

[2] Alam M, Al-Saggaf UM. "Quantitative reliability evaluation of repairable phased-mission systems using Markov approach", IEEE Transaction on Reliability, R-35(5), pp. 498-503, (1986).

[3] Dugan JB, Bavuso SJ, and Boyd MA. "Fault trees and Markov models for reliability analysis for fault tolerant systems", Reliability Engineering and System Safety, 39(3), pp. 291-307, (1993).

[4] Dugan JB, Sullivan KJ, Coppit D. Developing a low-cost high-quality software tool for dynamic fault-tree analysis. IEEE Transaction on Reliability, 49(1), pp. 49-59, (2000).

[5] Long W, Sao Y, and Horigome M. "Quantification of sequential failure logic for fault tree analysis", Reliability Engineering and System Safety, 67(3), pp. 269-274, (2000).

[6] Amari SV, Dill G, and Howald E. "A new approach to solve dynamic fault tree." In Proc. Annu. Reliab. Maintainability Symp., pp. 1-7, (2003).

[7] Liu D, Zhang C, Xing W, Li R and Li H. "Quantification of Cut Sequence Set for Fault Tree Analysis", HPCC2007, Lecture Notes in Computer Science, Springer-Verlag, pp. 755-765, (2007).

[8] Durga Rao K, Gopika V, Sanyasi Rao VVS, Kushwaha HS, Verma AK, and Srividya A. "Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment" , Reliability Engineering and System Safety, 94(4), pp. 872-883, (2009).

[9] Zhang P, Chan KW. "Reliability Evaluation of Phasor Measurement Unit Using Monte Carlo Dynamic Fault Tree Method", IEEE Transaction on Smart Grid, 3(3), pp. 1235-1243, (2012).

[10] Tang Z, Dugan JB. "Minimal Cut Set/Sequence Generation for Dynamic Fault Tree", In Proc. Annu. Reliab. Maintainability Symp., pp. 207-213, (2004).

[11] Merle G, Roussel J.-M, Lesage J.-J. "Dynamic Fault Tree Analysis Based On the Structure Function", In Proc. Annu. Reliab. Maintainability Symp., pp. 1-6, (2011).

[12] Liu D, Xing W, Zhang C, Li R, and Li H, "Cut Sequence Set Generation for Fault Tree Analysis." in Proc. Lecture Notes in Computer Science, pp. 592-603 (2007).

[13] Merle G, Roussel J.-M, Lesage J.-J. "Algebraic determination of the structure function of Dynamic Fault Trees", Reliability Engineering and System Safety, 96(2), pp. 267-277, (2011).

[14] Procedure for conducting probabilistic safety assessment of nuclear power plants (level 1). Safety series no. 50-p-4. International Atomic Energy Agency, 1992.