Quick Quantitative Calculation of DFT for NPP's Repairable Systems Based on Minimal Cut Sequence Set

Daochuan Ge[a,b,*], Qiang Chou[b], Ruoxing Zhang[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 calculations of Nuclear Power Plant (NPP)'s repairable system are mainly based on Markov model. However, with the increase of the system's size, the system's state space increases exponentially, which makes the problem hard or even not to be solved. This paper proposes a method about quick calculation of Dynamic Fault Tree (DFT) for NPP's repairable system based on Minimal Cut Sequence Set (MCSS), which divides a complex DFT into individual failure chain defined by MCSS. For each failure chain, the Markov model is applied. Then the unavailability of system is obtained synthesizing the result of each failure chain. This approach decreases the system's size increasing from exponentially to linearly and reduces the computation complexity. As to the NPP's dynamic systems with low failure rate and high repair rate, this approach can give a solution with a high-precision and conservative result and has practical value.

Keywords: Failure Chain, Quick Quantitative Calculation, Unavailability, Repairable Systems, NPP.

1. INTRODUCTION

To ensure the operating safety and design balance of NPP, it is essential to make reliability assessment of critical safety-critical systems. The real-life safety- critical systems of NPP often exhibit dynamic failure mechanisms, i.e., sequence- and functional- dependent failure behaviours, which make it hard to model and analyze the systems' reliability. For the powerful modelling ability and intuitiveness of DFT, NPPs often adopt DFT to describe the failure behaviours of the systems. The commonly-used methods for quantifying a DFT are mainly Markov-based [1,2], multi-integration-based [3,4,5] and Monte Carlo simulation-based methods [6,7]. However, each of these approaches has its own shortcomings: For Markov-based method, it is only applicable for exponential components time-to-failure distribution systems. Moreover, this method often confronts the problem of "state space explosion"; as to the multi-integration-based method, this method is only applied to non-repairable systems; as to the Monte Carlo simulation-based method, it may be very time-consuming, especially when the solutions with high degree of accuracy are desired. In addition, a new simulation procedure must be implemented whenever a component's failure parameters value changes. Considering some components existing in NPP are repairable, it is necessary to develop a practical approach for evaluating the reliability of repairable systems of NPP which should be easily to be implemented and computed. In this paper, an approach used to evaluate the reliability of repairable system of NPP based on MCSS is proposed.

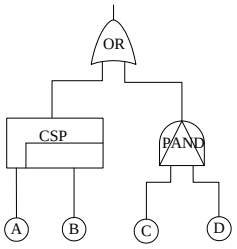
The reminder of this paper is organized as follows: Section 2 gives some related models and concept, including the MCSS model, the proposed model, and the uniqueness property of DFT's MCSS. Section 3 implements numerical experiments of the proposed model. Section 4 presents two cases study. Section 5 gives the final conclusions.

2. RELATED MODELS AND CONCEPTS

2.1. The MCSS Model

It is well known the occurrences of a DFT's top event not only depend on the combination of basic events but also depend on their failure orders. To characterize this failure behaviour, the researchers [8] propose a new concept of Minimal Cut Sequence (MCS) which is used to express what minimal basic events combination and in what failure orders that can lead to the occurrence of a DFT's top event. A MCS comprises several capital letters characterizing the failure behaviour of basic events and some temporal connecting symbols ($\prec$) expressing specific failure sequence. For an illustrative purpose, an example is shown in Fig.1.

Fig.1: An Illustrative Example



The OR gate, i.e., top event, fires if any input event occurs. As to the CSP gate, it fires only if all input events fail. Considering the cold standby component B never fails before primary B fails, the MCS of the CSP gate is written as: $A \prec B$. As to the PAND gate, it fires only if all input events fail in a left to right failure order, thus the MCS of the PAND gate is expressed as: $C \prec D$. Since the failure behaviour of the example is expressed by the logic OR of the two dynamic gates, the Minimal Cut Sequence aggregate of the system is $\{A \prec B, C \prec D\}$. How to obtain the complete MCS of a general DFT is beyond the scope of this paper, the interested readers can refer to Refs. [9,10,11] for more information.

A DFT generally have more than one MCS and all these MCS compose a set, i.e., Minimal Cut Sequence Set (MCSS). So the MCSS captures the complete failure information of a DFT. Suppose a DFT has *n* MCSs, and then the MCSS of the DFT can be written as:

$$MCSS = MCS_1 \cup MCS_2 \cup \cdots \cup MCS_n \tag{1}$$

The occurrence probability of the top event can be expressed by

$$\begin{aligned} P_r\left(system\ failure\right) &= P_r\left(MCSS\right) \\ &= P_r\left(MCS_1 \cup MCS_2 \cup \cdots \cup MCS_n\right) \end{aligned} \tag{2}$$

To solve the Eq. (2), an Inclusion-Exclusion Principle [12] is applied as follows:

$$\begin{aligned} P_r\left(system\ failure\right) &= P_r\left(MCS_1 \cup MCS_2 \cup \cdots \cup MCS_n\right) \\ &= \sum_{i=1}^{n} P_r\left(MCS_i\right) - \sum_{1 \le i < j \le n} P_r\left(MCS_i \cap MCS_j\right) + \cdots \\ &\quad + \left(-1\right)^{n-1} P_r\left(MCS_1 \cap MCS_2 \cap \cdots \cap MCS_n\right) \end{aligned} \tag{3}$$

Apparently, the MCSS model is an algebraic approach. it avoids the notorious problem of "state space explosion". Yet this approach is becoming unavailable when the system is repairable.

2.2. The Uniqueness of A DFT's MCSS

The uniqueness of a DFT's MCSS means that the MCSS is unique once the system's DFT is modelled determinately. That to say the MCSS is independent on whether the system is repairable or not. It is well know the occurrences of a DFT's top event are determined jointly by the combinatorial and sequential constraints. For a DFT, the combinatorial and sequential restrictions are uniquely decided. As a result, whether a system is repairable or not, the MCSS of the system's DFT is unique. Suppose a system has *n* components and its corresponding DFT has *m* MCSs, then the Eq. (4) must hold.

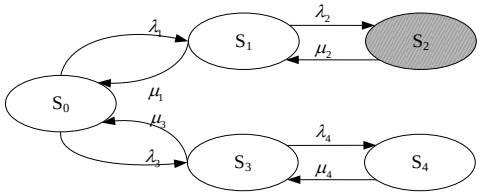
$$\begin{cases} MCS_i\left(b_1(\lambda_1,\mu_1),\cdots,b_n(\lambda_n,\mu_n)\right) = MCS_j\left(b_1(\lambda_1),\cdots,b_n(\lambda_n)\right) \quad 1\le(i,j)\le m \\ MCSS_R = MCSS_{NR} = \sum_{j=1}^{m} MCS_j \end{cases} \tag{4}$$

Where $b(\lambda)$ denotes a non-repairable component, $b(\lambda,\mu)$ expresses a repairable component, λ, μ is the failure rate and repair rate of a component, $MCSS_R$ is the MCSS of the repairable system and $MCSS_{NR}$ is the MCSS of the non-repairable system. Therefore, the MCSS of a repairable system can be obtained using the approaches mentioned in [9,10,11].

3. THE PROPOSED MODEL

As to a repairable system's DFT, the top event fails if any MCS occurs, and vice versa. Therefore, the reliability of a repairable system is closely related to the MCSS of its corresponding DFT. Assume a system components has low failure rate and high repair rate, then the time deviating from the normal state, especially the time in failure state is much less than in normal state. For an illustrative purpose, we suppose a system state set {S0, S1, S2, S3, S4}. S0 is the initial state, S1, S3, S4 are the degraded states, S2 is the failure state. The system states transition schematic is shown in Fig. 2.

Fig.2: The Schematic of System States Transition



Assume the system runs for T hours and the time staying at every state are T_{S0}, T_{S1}, T_{S2}, T_{S3}, T_{S4}. Then the unavailability Q of the system can be calculated by

$$Q = \frac{T_{S2}}{\sum_{i=0}^{4} T_{Si}} = \frac{T_{S2}}{T} \tag{5}$$

To reduce the model scale, we directly adopt the failure chain ($S0 \rightleftarrows S1 \rightleftarrows S2$), i.e., approximate model, to express the system states. Meanwhile we suppose the time at each state are T'_{S0}, T'_{S1} T'_{S2}, and then the approximate unavailability Q_{app} of the system can be computed by

$$Q_{app} = \frac{T'_{S2}}{\sum_{i=0}^{i=2} T'_{Si}} = \frac{T'_{S2}}{T} \tag{6}$$

Considering the approximate model gives up two degraded states, i.e., S3 and S4, it increase the duration that the system staying at failure state, i.e., $T'_{S2} > T_{S2}$. Combining the Eq. (5) and (6), we have

$$Q = \frac{T_{S2}}{T} < \frac{T'_{S2}}{T} = Q_{app} \tag{7}$$

The Eq. (7) indicates the solution obtained by the approximate model is comparatively conservative. Let $\lambda = \max\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}$, $\mu = \min\{\mu_1,\mu_2,\mu_3,\mu_4\}$, and then the following Equation holds.

$$\lim_{\substack{\lambda\to 0 \\ or \\ \mu\to\infty}} \left(Q_{app} - Q\right) = 0 \tag{8}$$

Apparently, as λ is small or μ is large, we can adopt an approximate model to evaluate the reliability of a repairable system, i.e., $Q \approx Q_{app}$. As to the repairable system with small failure and high repair rate, the failure chains capture the most failure information which can be understood as the failure chains contribute significantly to the system failure. In this point of view, we propose a generalized approximate model for evaluating the reliability of a repairable system. Suppose a repairable system has n failure chains, i.e., $\overline{L_1}, \overline{L_2}, \cdots, \overline{L_n}$ determined by the MCSS, and then the approximate model is expressed by

$$Q(\textit{repairable system}) = Q\left(\overline{L_1}, \overline{L_2}, \cdots, \overline{L_n}\right) \approx Q_{app}\left(\overline{L_1}\right) + Q_{app}\left(\overline{L_2}\right) + \cdots + Q_{app}\left(\overline{L_n}\right) \quad (9)$$

4. NUMERICAL EXPERIMENT

4.1. Experiment Design

To validate the proposed model, a numerical experiment is implemented. First, we define the ratio of a DFT's failure chains as $N_{\overline{L}} / N$. Where, $N_{\overline{L}}$ is the number of the failure chains, N is the total number of the chains. For $1 \le N_{\overline{L}} \le N$, and then we can get $1/N \le \varphi \le 1$. Without loss of generality, we choose PAND gate ($\varphi = 1/N$) and WSP gate ($\varphi = 1$) as our experimental subjects. The corresponding approximate models are shown in Fig.3 and Fig.4 separately.

Fig.3: Approximate Model for PAND gate (n=2)

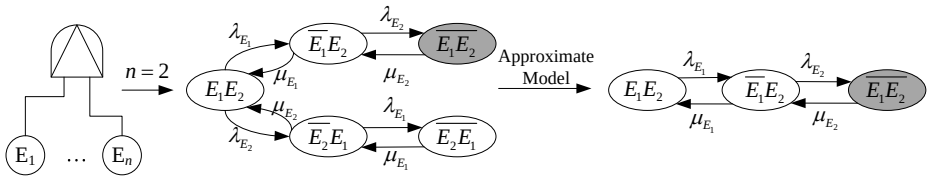
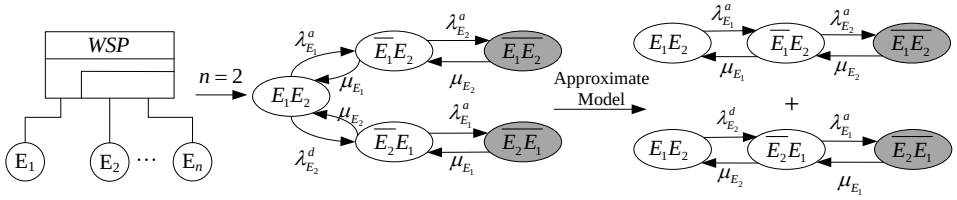


Fig.4: Approximate Model for WSP gate (n=2)



The experiment designs are described in Table 1.

Table 1: The Experiment Designs

The Gate Type	The Schemes	Design Parameters	Design Points	Mission Time(h)
PAND	Scheme 1: n=2	$\lambda_1 = \lambda_2 = \cdots = \lambda_n$ $\mu_1 = \mu_2 = \cdots = \mu_n$	$(\lambda_i^{(1)}, \mu_i^{(1)})$	T=10^6
	Scheme 2: n=3		$(\lambda_i^{(2)}, \mu_i^{(2)})$	
	Scheme 3: n=4		$(\lambda_i^{(3)}, \mu_i^{(3)})$	
WSP	Scheme 1: n=2	$\lambda_2^d = \lambda_3^d = \cdots = \lambda_n^d = \alpha\lambda_1$ $\mu_1 = \mu_2 = \cdots = \mu_n$	$(\lambda_i^{(1)}, \mu_i^{(1)})$	
	Scheme 2: n=3		$(\lambda_i^{(2)}, \mu_i^{(2)})$	
	Scheme 3: n=4		$(\lambda_i^{(3)}, \mu_i^{(3)})$	

Note：the right superscript "*d*" of design parameters presents component in standby state; α is a dormant factor, and α =0.1; n is the total number of the input events; $\mu_i^{(1)} = 0.5\mu_i^{(2)} = 0.25\mu_i^{(2)} = 0.5$, $\{\lambda_1^{(1)}, \lambda_2^{(1)}, \ldots, \lambda_n^{(1)}\}$ ={1.0E-2, 5.0E-3, 2.5E-3, 1.0E-3, 5.0E-4, 2.5E-4, 1.0E-4, 5.0E-5, 2.5E-5, 1.0E-5, 5.0E-6, 1.0E-6, 5.0E-7, 1.0E-7}, $\lambda_i^{(1)} = \lambda_i^{(2)} = \lambda_i^{(3)}$.

4.2. Experiment Results and Analysis

The experiment results are shown in Fig.5-Fig.10, and the relative error between approximate model and exact model are shown in Fig.11-Fig.14. The relative error is defined as: $\varepsilon_{er} = \left(Q_{app} - Q_{exc}\right) / Q_{exc}$, where the Q_{exc} is the exact solution.

Fig.5: Scheme 1 of PAND Gate

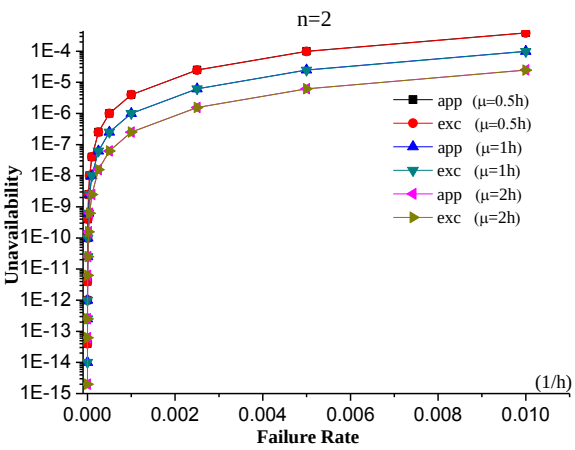


Fig.6: Scheme 2 of PAND Gate

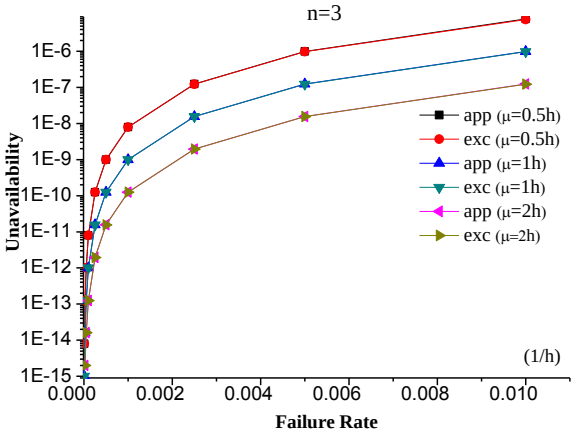


Fig.7: Scheme 3 of PAND Gate

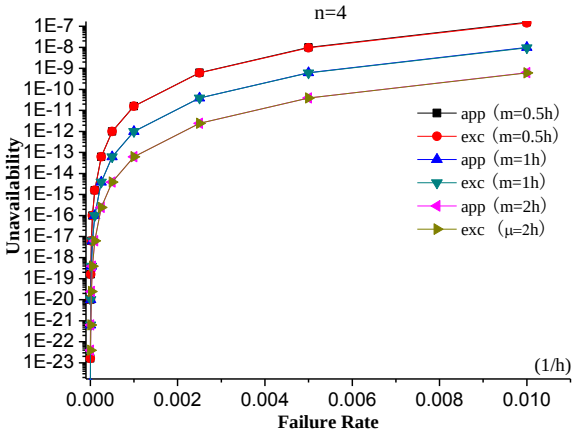


Fig.8: Scheme 1 of WSP Gate

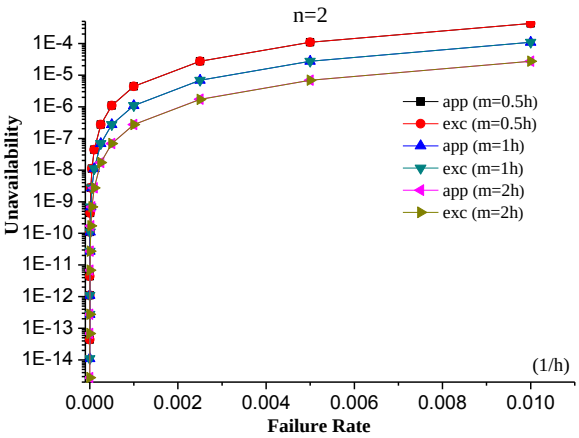


Fig.9: Scheme 2 of WSP Gate

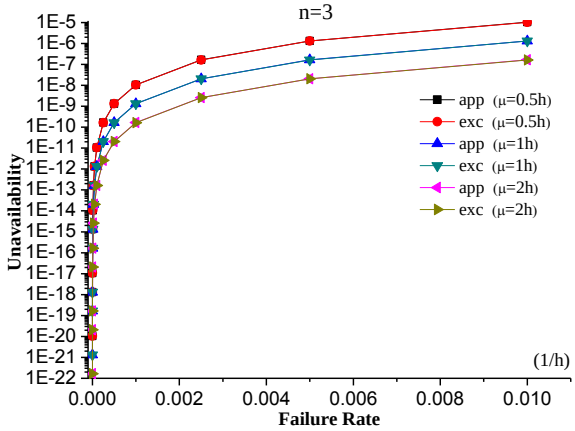


Fig.10: Scheme 3 of WSP Gate

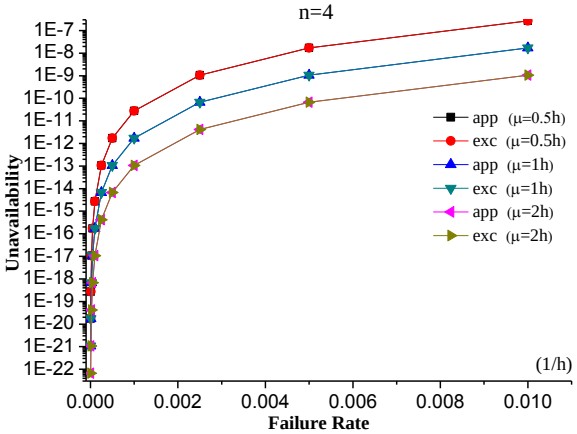


Fig.11: the ε_{er} for Scheme 1 of PAND Gate

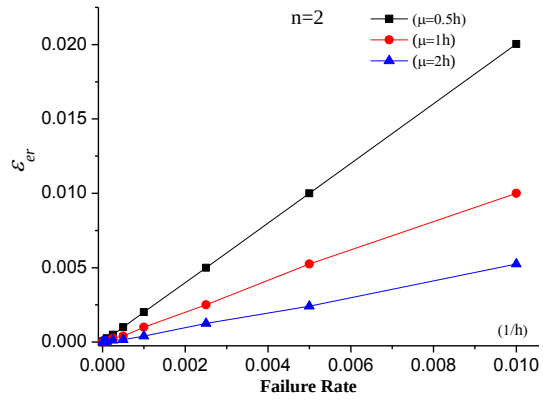


Fig.12: the ε_{er} for Scheme 1 of WSP Gate

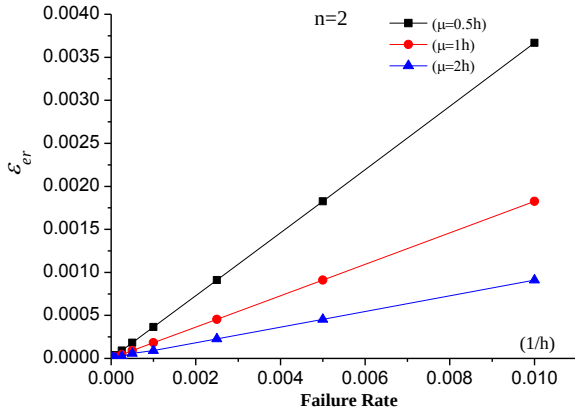


Fig.13: the ε_{er} for Scheme 3 of PAND Gate

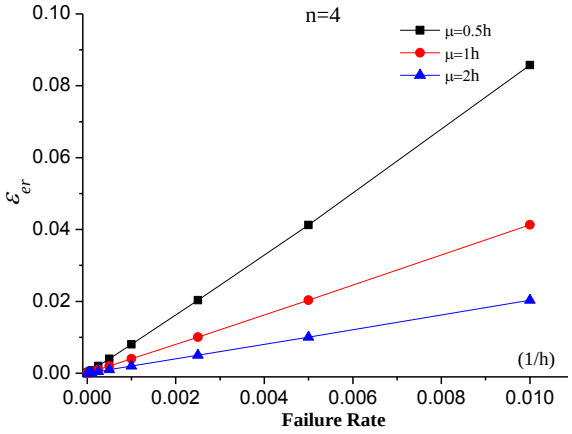


Fig.14: the ε_{er} for Scheme 3 of WSP Gate

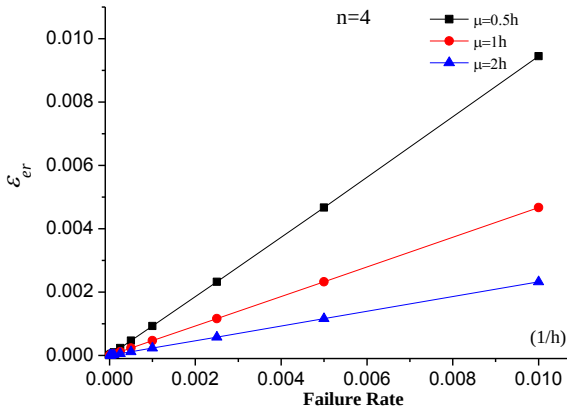


Fig.5-Fig.10 shows at each design point, the result obtained from the approximate model is in good agreement with that from the exact model (Markov-based). In addition, Fig.11-Fig.14 demonstrates the results calculated by the approximate model are conservative compared with the exact solutions. Moreover, with the decrement of the failure rate or the increment of the repair rate, the value ε_{er} is becoming smaller and smaller, and even can be neglected. It is found the value ε_{er} from WSP gate is smaller than that from PAND gate at the same design point, which can be interpreted as that with the augment of the failure chain ration (φ), the accuracy of the approximate model is becoming higher and higher. Considering $\varphi \in$ [1/N, 1] and most components in NPP with high repair rate and low failure rate, it is reasonable that the proposed model is valid and conservative for NPP's dynamic repairable systems.

5. CASE STUDY

5.1 Case Study 1

For model validation purpose, a case study is analyzed which is from a partial safety system of one Chinese NPP. The system's DFT model is shown in Fig.15 and its corresponding approximate model is shown in Fig.16.

Fig.15: The Simplified DFT Model

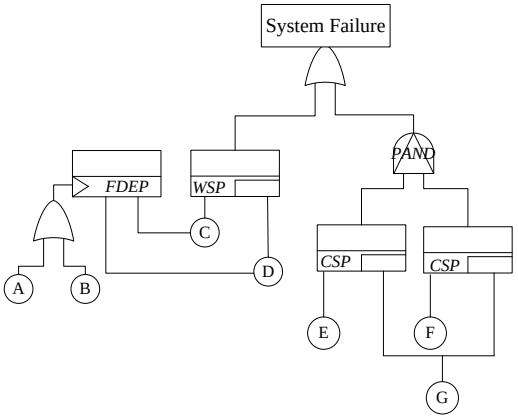
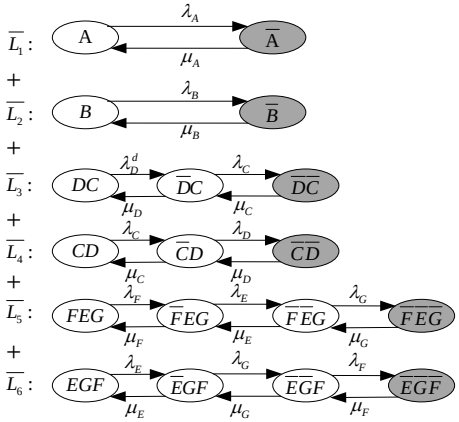


Fig.16: The Approximate Model



The reliability parameters of the components contained in the case 1 are listed in table 2.

Table 2: Reliability Parameters for Case 1

Component	Failure Rate	Repair Rate	Component	Failure Rate	Repair Rate
A	1.0e-7	0.25	D_d	2.0e-4	1.00
B	5.0e-7	1.20	E	1.4e-3	2.00
C	1.0e-7	1.50	F	2.5e-3	3.00
D_a	5.0e-7	1.00	G	2.0e-3	0.50

Note: the symbol D_a denotes the component D in working state; D_d denotes the component D in standby state; the time-to failure and time-to-repair of all components are following exponential distributions.

We suppose that the mission time of the system is 5000h. For comparison purpose, we apply the approximate model and exact model, i.e. Markov-based model, respectively to analyze the system's unavailability. The steady and average unavailability of the system calculated by the approximate model and exact model are listed in Table 3.

Table 3: Results of Case 1

	Approximate solution	Exact Solution	Relative Error (ε_{er})
Average Unavailability	1.93036E-6	1.93031E-6	2.5903e-5
Steady Unavailability	1.95397E-6	1.95367E-6	1.5356e-4

Analysis: As to the Markov-based model, i.e., converting the whole DFT into Markov Chain, the number of the system states would grow up to 2^7. It is a hard and error-prone job. By contrast, the max number of the states defined by the longest failure chain involved in our proposed model is only 4. Therefore, the proposed method is more efficient than the Markov-based approach. In addition, the results calculated by the proposed method are highly matched with those obtained by the Markov-based method.

5.2. Case Study 2

For further model validation purpose, a more complex case is analyzed, which is from a partial I&C safety system of one Chinese NPP. The system's simplified DFT model is shown in Fig.17.

Fig.17: The Simplified DFT Model

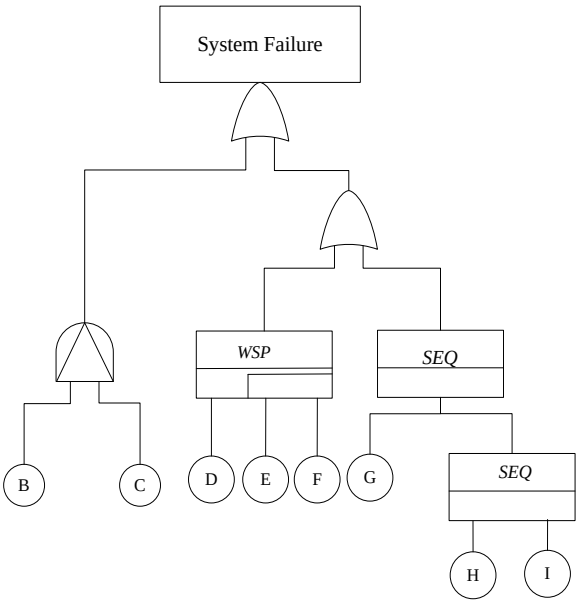
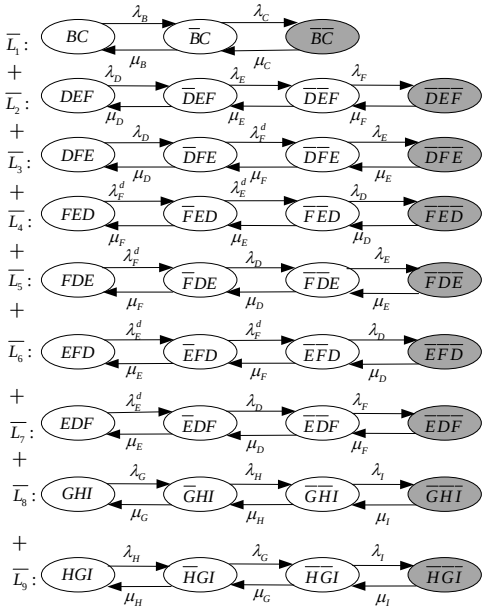


Fig.18: The Approximate Model



The reliability arguments of the system's components are shown in Table 4.

Table 4: The Reliability Parameters for Case 2

Component	Failure Rate	Repair Rate	Component	Failure Rate	Repair Rate
B	8.5e-4	0	F_a	1.0e-2	3
C	1.0e-4	12	F_d	2.0e-3	3
D	1.0e-2	3	G	1.0e-2	2.5
E_a	1.0e-2	3	H	6.0e-3	3.5
E_d	2.0e-3	3	I	5.0e-3	2

Similarly, we adopt the proposed method and Markov-based method to analyze this system's unavailability separately. Assume the failure time and repair time of system's components follow exponential distribution and the mission time of the system is 5000h, and then the solutions of the system's unavailability obtained by the two methods are listed in Table 5.

Table 5: Results of Case 2

	Approximate solution	Exact Solution	Relative Error (ε_{er})
Average Unavailability	8.42951E-6	8.42191E-6	9.024E-4
Steady Unavailability	6.49651E-6	6.48887E-6	1.200E-3

Obviously, the results obtained by our proposed method are very close to those derived by the Markov-based method.

6. Conclusions

As to the repairable systems modelled by DFTs, the quantitative analyses of these systems are mainly based on Markov approach. Although this approach can offer an exact solution, it may confront the notorious problem of "state space explosion". For a large-scale DFT, the conventional Markov-based method would become hard to be implemented. To solve this problem, this paper proposes an approximate method to analyze DFT with repairable components. This method divides the whole Markov Chain into separate failure chain and neglects the successful chains. Each failure chain is quantified by Markov-based method, and then the results of the separate failure chains are integrated to obtain the system's unavailability. Therefore, in contrast to the conventional state space-based method, this method gets over the problem of "state space explosion". The results of experimental design and cases analysis demonstrate, as to a system with high repair rate and low failure rate, this method can offer a solution with a high accuracy.

For the NPP's repairable systems, most components involved have low failure rate and high repair rate. It is reasonable the proposed method has a high engineering application value in NPP, which can be used to estimate the reliability of safety-critical system quickly. However, as to the repairable systems with high failure rate and low repair rate, it still needs further research.

References

[1] M. Alam, and U.M. Al-Saggaf, "Quantitative reliability evaluation of repairable phased-mission systems using Markov approach." *IEEE Trans. Rel.*, vol.R-35, n.5, pp. 498-503. Dec. 1986.

[2] L. Xing, K.N. Fleming, and W.T. Loh, "Comparison of Markov model and fault tree approach in determining initiating event frequency for systems with two train configurations." *Reliab. Eng. Syst. Saf.*, Vol. 53, n. 1, pp. 17-29. Jul. 1996.

[3] W. Long, Y. Sao, and M. Horigome, "Quantification of sequential failure logic for fault tree analysis." *Reliab. Eng. Syst. Saf.*, vol. 67, no. 3, pp. 269-274.Mar. 2009.

[4] S.V. Amari, G. Dill, and E. Howald, "A new approach to solve dynamic fault tree." In *Proc. Annu. Reliab. Maintainability Symp.*, PP. 1-7. 2003.

[5] D. Liu, , C. Zhang, , W. Xing, R. Li, and H. Li, "Quantification of Cut Sequence set for Fault Tree Analysis." in Proc. *HPCC*, vol. 4782, *Lecture Notes in Computer Science*, 2007, pp. 755-765.

[6] K.D. Rao, V. Gopika, V.V.S.S. Rao, H.S. Kushwaha, A.K. Verma, and A. Srividya, "Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment." *Reliab. Eng. Syst. Saf.*, vol. 94, no. 4, pp. 872-883. Apr. 2009.

[7] P. Zhang, and K.W. Chan, "Reliability Evaluation of Phasor Measurement Unit Using Monte Carlo Dynamic Fault Tree Method." IEEE Trans. Smart Grid., vol. 3, n. 3, pp. 1235-1243. Sep. 2012.

[8] Z. Tang, and J.B. Dugan, "Minimal Cut Set /Sequence Generation for Dynamic Fault Trees." In *Proc. Annu. Reliab. Maintainability Symp.*, pp.207-213. Jan. 2004.

[9] D. Liu, W. Xing, C. Zhang, R. Li, and H. Li, "Cut Sequence Set Generation for Fault Tree Analysis." in Proc. *ICESS*, vol. 4523, *Lecture Notes in Computer Science*, 2007, pp. 592-603.

[10] G. Merle, J.-M.Roussel, J.-J. Lesage, Algebraic determination of the structure of Dynamic Fault Trees. *Reliab. Eng. Syst. Saf.*, vol. 96, no. 2, pp. 267-277. Feb.2011.

[11] J. Liu, w. Tang, and Y. Xing, "A Simple Algebra for Fault Tree Analysis of Static and Dynamic Syatems" *IEEE Trans. Rel.*,vol. 62, n. 4, pp. 846-861. Dec. 2013.

[12] J.B. Dugan, and S.A. Doyle, "New results in fault-tree analysis." In *Proc. Annu. Reliab. Maintainability Symp., Tutorial Notes*, pp.1-23. 1997.