Eksploatacja i Niezawodnosc – Maintenance and Reliability
Volume 23 (2021), Issue 1
journal homepage: http://www.ein.org.pl
Article citation info:
Xu Z, Guo D, Wang J, Li X, Ge D. A numerical simulation method for a repairable dynamic fault tree. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2021; 23 (1): 34–41, http://dx.doi.org/10.17531/ein.2021.1.4.

# A numerical simulation method for a repairable dynamic fault tree

Indexed by: Web of Science Group

Zhixin Xu[a], Dingqing Guo[b,a], Jinkai Wang[a], Xueli Li[c,d], Daochuan Ge[c]*

[a]State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, China
[b]School of Mechanical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[c]Key Laboratory of Neutronics and Radiation Safety, Institute of Nuclear Energy Safety Technology, HFIPS, Chinese Academy of Sciences, Hefei, Anhui 230031, China
[d]University of Science and Technology of China, Hefei, Anhui 230026, China

## Highlights

- The adapted sequential failure region is developed to characterize the failure mechanism of a minimal cut sequence.
- The proposed approach is applicable for nonexponential distribution situations.
- The proposed approach is more efficient than the Markov chain state space methods.

## Abstract

Dynamic fault trees are important tools for modeling systems with sequence failure behaviors. The Markov chain state space method is the only analytical approach for a repairable dynamic fault tree (DFT). However, this method suffers from state space explosion, and is not suitable for analyzing a large scale repairable DFT. Furthermore, the Markov chain state space method requires the components' time-to-failure to follow exponential distributions, which limits its application. In this study, motivated to efficiently analyze a repairable DFT, a Monte Carlo simulation method based on the coupling of minimal cut sequence set (MCSS) and its sequential failure region (SFR) is proposed. To validate the proposed method, a numerical case was studied. The results demonstrated that our proposed approach was more efficient than other methods and applicable for repairable DFTs with arbitrary time-to-failure distributed components. In contrast to the Markov chain state space method, the proposed method is straightforward, simple and efficient.

## Keywords

repairable dynamic fault tree, numerical simulation, Monte Carlo, sequential failure region, minimal cut sequence set.



## 1. Introduction

Dynamic fault trees are extended from the traditional static fault trees (SFTs) by integrating several dynamic logic gates, such as Warm Spare (WSP) gate, Priority AND (PAND) gate, and Function Dependent (PDEP) gate. With the help of integrating these dynamic gates, DFTs can model industrial systems with sequential failure behaviors that are not permitted in SFTs. Currently, dynamic fault trees are successfully applied to system safety design, reliability evaluation, and risk management [14, 26, 32]. During the past few years, researchers have done much work in this field, making fruitful achievements [6, 16, 18]. However, it is not easy to quantify a repairable DFT when applying the Markov chain state space method, because the executive process is time consuming and error prone, especially for a large-scale repairable DFT.

The primary analyzing techniques for quantifying a DFT are divided into three main categories: Markov chain state space methods [1, 7, 24, 29], combinatorial methods [21, 23, 31, 34], and numerical simulation methods [8, 25, 35]. Markov chain-based and combinatorial approaches are analytical methods that can provide exact solutions. Markov chain-based methods are not only applicable for a nonrepairable DFT but are also applicable for a repairable DFT. However, Markov chain state space methods are vulnerable to state space explosion when analyzing large-scale DFTs, In addition, Markov chain-based methods require the components' time-to-failure to follow exponent distributions. By contrast, combinatorial approaches (such as inclusion exclusion principle (IEP) methods [19], sequential binary decision diagram (SBDD) methods [30, 31], improved SBDD methods [11], dynamic binary decision tree (DBDT) methods [13], and adapted K.D.Heidtmann methods [12]) are seldom trapped into state space explosion and often more efficient than the Markov chain methods. Nevertheless, most existing combinatorial approaches are limited in solving nonrepairable DFTs. It is worth noting that some researchers have tried to develop a kind of combinatorial method to solve a repairable DFT with PAND gates under a steady state [33]. Hence, for a repairable DFT, combinatorial approaches need to be further studied and improved.

Numerical simulation analyzing techniques are also commonly used to deal with DFTs, such as Monte Carlo (MC) numerical simulation [4, 5, 27]. Compared with the analytical approaches, numerical simulation methods can either provide great generalities on a DFT structure and failure distribution of their input events or reduce the

(*) Corresponding author.
E-mail addresses: Z. Xu - xuzhixin@cgnpc.com.cn, J. Wang - wangjinkai@cgnpc.com.cn, D. Guo - guodingqing@cgnpc.com.cn, X. Li - 1328931871@qq.com, D. Ge - daochuan.ge@inest.cas.cn

scale of the problem to be handled. Generally, simulation methods are more versatile than analytical approaches, especially for probability density functions (PDFs) of input events' time-to-failure, which are quite complex and lack explicit primitive functions. Rao KD et al. ever applied the Monte Carlo simulation technique to analyze repairable DFTs based on failure logics of various dynamic logic gates [25], and calculated the reliability index (i.e., unavailability) of a given system. However, the state of a DFT's top event could not be determined until all dynamic gates' logic states were simulated, which meant more simulating time might be needed due to the redundant logic terms. Zhang P et al. then used a similar Monte Carlo simulation technique to evaluate the reliability of a Phasor Measurement Unit [35]. Ge D et al. ever proposed a Monte Carlo simulation approach based on the coupling of DFTs' minimal cut sequence set and sequence failure regions (SFR) to analyze a nonrepairable DFT, but this method was not extended to repairable DFTs [10]. Merle G et al. developed a Monte Carlo simulation method based on DFTs' structure functions, but this method is only applicable for nonrepairable DFTs [22]. DFTsim [3] and MatCarloRE [20] are two analyzing tools for DFTs, and both tools use Monte Carlo simulation for solving DFTs, but do not allow repairable basic events. Recently, Gascard E et al. proposed an event-driven Monte Carlo simulation approach for quantitative analysis of DFTs [9], but the authors also assumed that the basic events are nonrepairable.

As mentioned above, for repairable DFTs, the accessible analyzing tools are Markov chain state space-based methods and dynamic logic gates-based Monte Carlo numerical simulation methods. For a large-scale repairable DFT, the feasible methods are Monte Carlo numerical simulation approaches. However, the existing Monte Carlo numerical simulation methods for repairable DFTs are dependent on dynamic logic gates' failure logics, which means more simulation time might be needed due to redundant logic terms. In this study, an MCSS-based Monte Carlo simulation method that couples the DFTs' minimal cut sequence set (MCSS) and sequence failure regions is proposed, which can be the main research contribution. Compared with existing methods, the merits of our proposed method are: 1) in contrast to the Markov chain state space method, the proposed numerical simulation method is versatile and not limited to particular distribution types; 2) it can provide more reliability indices for a concerned system, such as uncertainty of system reliability and component importance; and 3) by comparison with dynamic logic gates-based numerical simulation methods, the proposed method can reduce the unnecessary redundant logic terms based on minimal cut sequence set and hence improve computing efficiency.

The remainder of this paper is organized as follows. The concepts of dynamic logic gates and repairable DFTs are clarified in section 2. In section 3, the proposed MCSS-based Monte Carlo numerical simulation method is provided. Numerical case study is chosen and implemented to demonstrate the reasonability of the proposed method in section 4. Section 5 is devoted to the final conclusion.

## 2. Dynamic fault trees

### 2.1. Dynamic logic gates and repairable dynamic fault trees

To capture the sequence failure behaviors in the industrial systems, researchers have developed several dynamic logic gates such as Function Dependent (FDEP) gates, Priority AND (PAND) gates, Sequence Enforcing (SEQ) gates, and spare gates including Cold Spare (CSP) gates, Warm Spare (WSP) gates, and Hot Spare (HSP) gates, as shown in Fig. 1. A FDEP gate (Fig. 1 (a)) has a single trigger event (basic event or the output of another gate) and several dependent basic events. It characterizes a situation where the failure of the trigger event would cause all dependent basic events to fail, yet failure of any dependent basic event does not have effects on the trigger event. The PAND gate in Fig. 1 (b) is a special case of the AND gate. The PAND gate fires if its input events fail in a left-to-right order. A SEQ gate (Fig.1 (c)) has only one failure order (i.e., from left to right), and only when all the input events fail can the SEQ gate occur. For a spare gate, it often has one primary event and some spare events. Only when the primary event fails can spare events start to replace the primary one. As all input events under a spare gate lose, the spare gate fires. Specifically, the CSP gate in Fig. 1 (d) allows modeling of the case where cold spares always stay at an unpowered state when the primary event functions. This means the primary event, $e_1$, must fail first; then the first cold spare $e_2$ fails; and finally the last one $e_n$ fails. The WSP in Fig. 1 (e) is unlike CSP gates, the spares stay at a reduced power when the primary event is normal. That is, the input events under a WSP can fail in any sequence. With regard to the HSP in Fig. 1 (f), the spares stay at full power when the primary event operates normally. Hence, the failure logic for an HSP is equivalent to the AND gate.

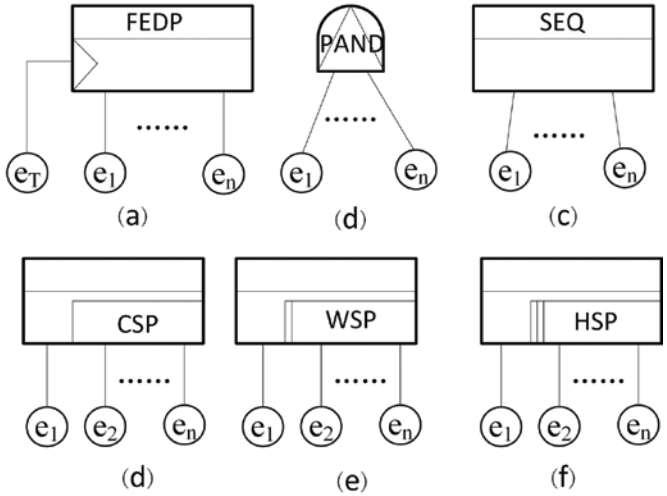


*Fig. 1. Dynamic logic gates*

To evaluate the reliability of systems with sequential failure behaviors, DFTs are proposed and developed. DFTs are defined by researchers as static fault trees integrating at least one dynamic logic gate. According to input events, regardless of whether or not they have reparability behaviors, DFTs can be classified into two categories: nonrepairable and repairable DFTs. A non-repairable DFT is defined as a DFT whose input events do not have any reparability behavior. A repairable DFT is defined as having input basic events with reparability behaviors.

### 2.2. Failure logic expressions of a repairable DFT

As mentioned above, the occurrence of a DFT's top event not only depends on combinations of its basic events but also depends on their failing orders. Therefore, the minimal cut set used to express failure behaviors in traditional static fault trees is not available. To settle this problem, Tang et al. developed the concept of minimal cut sequence for DFT analysis [28]. The minimal cut sequence (MCS) is defined as the minimal failure order that leads to occurrence of the top event of a DFT, and all the minimal cut sequences can form a universal set (i.e., minimal cut sequence set (MCSS)). The MCSS can be applied to capture the complete failure information in a DFT. In this contribution, MCSS is applied to characterize the failure logic expressions (FLE) of a DFT. Suppose a DFT has a MCSS with $m$ minimal cut sequences, then the failure logic expression $FLE_{dft}$ of this DFT can be written as:

$$FLE_{dft} = MCS_1 + MCS_2 + \cdots + MCS_m \tag{1}$$

To explicitly formulate an MCS, some special symbols are introduced. We use the symbol "→" to represent sequential failure, which means the left basic event fails before the right one. It is defined as:

$$\sigma(a \to b) = \begin{cases} 1, & 0 \le t(a) \le t(b) \le T \\ 0, & otherwise \end{cases} \quad (2)$$

where $\sigma(\cdot)$ represents the state of a considered basic event or a sequential failure event, "1" denotes the failure state, "0" denotes the normal state, $t$(a) and $t(b)$ indicates the failure time of $a$ and $b$, and $T$ is the mission time.

It should be noted that the symbol "→" just reflects the order of time-to-failure of the components represented by basic events. In fact, the start times of some components are also sequence dependent, such as cold spares, warm spares, and even the basic events under a SEQ gate. To characterize the sequence of the start time of some components, in this work, the special symbols $A$, ${}_A^0B$, ${}_A^\beta B$, and ${}_A^1B$ are also introduced, where $A$ denotes a general basic event, ${}_A^0B$ represents $B$ is a cold spare of $A$ or any one of the second and subsequent input events under a SEQ gate, ${}_A^\beta B$ indicates $B$ as a warm spare of $A$ that fails before $A$, $\beta$ is the a dormant factor ($0 < \beta < 1$), and ${}_A^1B$ expresses $B$ as a warm spare of $A$ that fails after $A$ at full power. Therefore, the minimal cut sequences of dynamic gates, each having two input events, can be written as: $FLE_{fdep} = e_T + e_1$, $FLE_{pand} = e_1 \to e_2$, $FLE_{seq} = e_1 \to {}_{e_1}^0 e_2$, $FLE_{csp} = e_1 \to {}_{e_1}^0 e_2$, $FLE_{wsp} = \left({}_{e_1}^\beta e_2 \to e_1\right) + (e_1 \to {}_{e_1}^1 e_2)$, $FLE_{hsp} = e_1 \cdot e_2 = e_1 \to e_2 + e_2 \to e_1$, where the symbol "+" means the logical operator OR and "·" means the logical operator AND. The failure logic of the FDEP gate is equal to the OR gate, and the HSP gate is equivalent to an AND gate. In addition, the SEQ and CSP gates have similar failure behaviors. The only differences lie in the fact that input events under a SEQ can be an event representing a system, and the input events under a CSP are constrained to basic events representing components. For a DFT, the MCSS is unique regardless of whether its input events have reparability.

### 2.3. Logic operation rules in a repairable DFT

To obtain the FLE of a DFT, several logic operation rules are developed and applied. Liu et al. developed a set of inference rules to obtain the FLE of a given DFT, and Merle et al. presented several logic operation rules to deduce a DFT's structure function. In contrast to Merle's methods, Liu's inference rules are straightforward and simple [17]. In our approach, Liu's inference rules were introduced to obtain the FLE of a DFT. The detailed fundamental inference rules are listed as follows:

$$(A \to B) \to C \rightleftharpoons A \to B \to C \quad (3)$$

$$A \to (B \to C) \rightleftharpoons A \to B \to C + B \to A \to C \quad (4)$$

$$A \to (B + C) \cdot A \to B + A \to C \quad (5)$$

$$(A + B) \to C \cdot A \to C + B \to C \quad (6)$$

$$(A \to A) \rightleftharpoons A \quad (7)$$

$$A \to B \to A \Rightarrow \Phi \quad (8)$$

$$A \cdot B \rightleftharpoons A \to B + B \to A \quad (9)$$

where "$\rightleftharpoons$" represents that the left are the necessary and sufficient conditions for the right, "$\Rightarrow$" means that the left are sufficient but not necessary conditions for the right, and "Φ" denotes an empty set. Based on these fundamental inference rules, ten additional deductive inference rules are also offered. Interested readers are encouraged to consult reference 17. Through applying these inference rules, we can obtain the FLE of a repairable DFT.

## 3. The proposed numerical simulation method

### 3.1. Adapted sequence failure region and its formulation for a repairable DFT

The sequence failure region concept has been proposed in our previous contributions [8] and has already been used to analyze the reliability of a nonrepairable DFT. However, in a repairable DFT, the sequence failure regions are even more complex due to reparability behaviors. When a nonrepairable component enters a failure state, it never recovers again. However, for a repairable component, successful and failed states appear alternatively due to reparability. Its running state diagram is shown in Fig. 2, where $T_i$ is the running time (i.e., time to failure), $O_i$ is the repair time (i.e., time to recovery) and $i = 1, 2, k$. Hence, the sequence failure regions of repairable DFTs are different from those of nonrepairable ones.

The time to failure $T_i$ and time to recovery $O_i$ can be obtained by the following equations:

$$\begin{cases} T_i = F^{-1}(\varepsilon) \\ O_i = G^{-1}(\eta) \end{cases} \quad (10)$$

where the $F$(x) and $G$(x) are Cumulative Distribution Functions(CDFs) of $T_i$ and $O_i$, $F^{-1}$(x) and $G^{-1}$(x) are the corresponding inverse functions. $\varepsilon$ and $\eta \in (0,1)$ are uniformly distributed random numbers generated by standard random generators. For example, suppose a component follows exponent time-to-failure distribution with parameter $\lambda$, and its probability density function $f$(x) and cumulative probability distribution function $F$(x) are obtained as follows:

$$f(x) = \lambda \cdot e^{-\lambda \cdot x} \quad (11)$$

$$F(x) = \int_0^x f(x)dx = 1 - e^{-\lambda \cdot x} \quad (12)$$

Then, the $x$ formulated as a function of $F$(x) is obtained as:

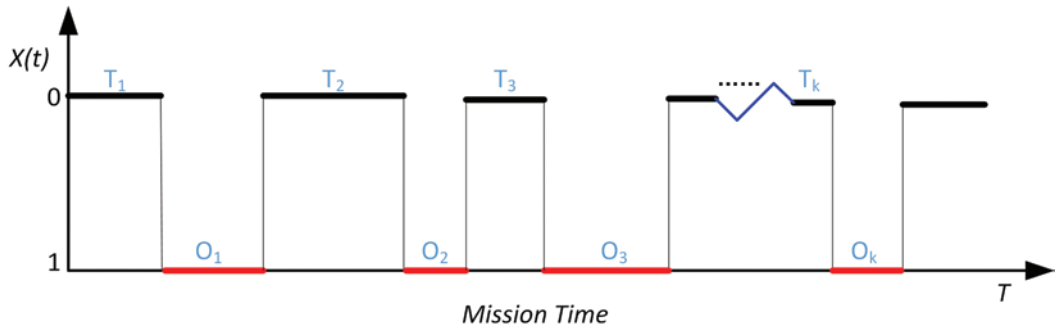


*Fig. 2. Running state diagram of a repairable component*

$$x = \frac{1}{\lambda} \cdot ln\left(\frac{1}{1-F(x)}\right) \tag{13}$$

Let $\lambda$ be $1.0\times10^{-3}$/h, and the generated random number is 0.5 which is used to replace the $F$(x). Through applying Eq. (13), the time-to-failure of the component is simulated as 693.1 h. In the same way, we can get the time-to-recovery of the component. Alternately, the component's running state diagram can be derived.

A repairable DFT's failure state is determined by its MCSS. According to the semantics of an MCS, its failure state should satisfy two requirements: 1) the time-to-failure of components must occur in a sequential order; and 2) under the conditions of 1), all the components follow in a failure state at the common failure time interval. The sequential failure region of an MCS is demonstrated by a general minimal cut sequence $e_1 \rightarrow e_2 \rightarrow \cdots \rightarrow e_n$, which is shown in Fig. 3.

The variables $t_{i,j}$, $\mu_{i,j}$ represent the $j$th time-to-failure and time-to-recovery of the $i$th component respectively. The variables $T_{i,j}$ and $U_{i,j}$ represent the $j$th failure time and recovery time located at the sequential failure region of the $i$th component, respectively. As observed in Fig. 3, $T_{1,1} = t_{1,1} + \mu_{1,1} + t_{1,2} + \mu_{1,2} + t_{1,3}$; $T_{2,1} = t_{2,1} + \mu_{2,1} + t_{2,2} + \mu_{2,2} + t_{2,3}$; $T_{3,1} = t_{3,1} + \mu_{3,1} + t_{3,2}$; $\cdots$; $T_{n,1} = t_{n,1} + \mu_{n,1} + t_{n,2} + \mu_{n,2} + t_{n,3}$, and $T_{1,1} < T_{2,1} < T_{3,1} < \cdots < T_{n,1}$ satisfying the sequence failure requirement, where the "+" is the notation of summation. Under this condition, the lower boundary of the failure time interval of this MCSS is $L_{sfr} = \text{Max}\{T_{1,1}, T_{2,1}, T_{3,1}, \cdots, T_{n,1}\} = T_{n,1}$, and the upper boundary is $U_{sfr} = \text{Min}\{U_{1,1}, U_{2,1}, U_{3,1}, \cdots, U_{n,1}\} = U_{3,1}$. Therefore, the failure time interval (FTI) of this MCSS can be expressed as: $FTI_{MCSS} = (L_{sfr}, U_{sfr}) = (T_{n,1}, U_{3,1})$. Suppose a DFT has $n$ minimal cut sequences (i.e., MCSS). Each MCSS has $m$ failure time intervals, and the adapted sequence failure region (SFR) for this repairable DFT can be expressed as:

$$SFR_{dft} = \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} FTI_{i,j} \tag{14}$$

In the simulation process, the obtained failure time intervals may have overlapping parts that may lead to a wrong reliability analysis result and should be merged and deleted. Four overlapping scenarios are identified (as shown in Fig. 4). The corresponding merging rules are provided for two overlapping failure time intervals ($FTI_1 = (T_{11}, T_{12})$, $FTI_2 = (T_{21}, T_{22})$) in Table 1. For two overlapping failure time intervals, the boundaries of the merged FTI are the lower and upper times of the two FTIs.

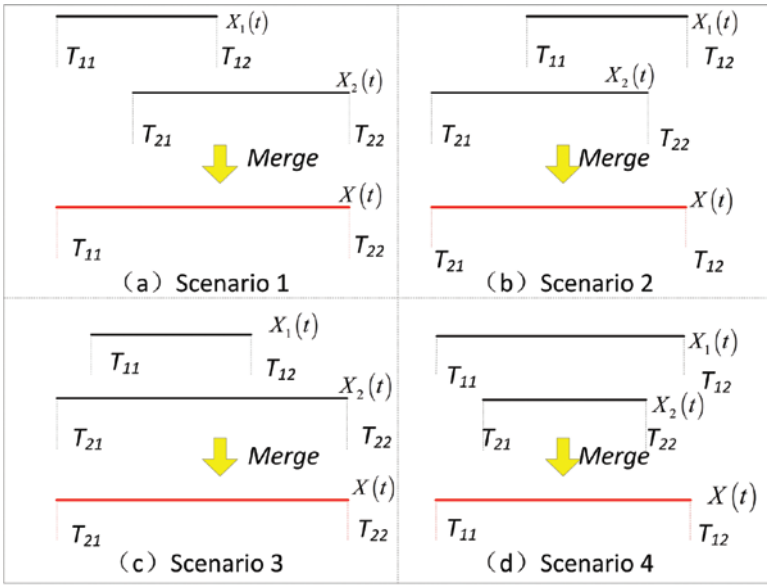


*Fig. 4. Four identified overlapping scenarios*

*Table 1. Merging rules for overlapping failure time intervals*

| No. | Overlapping Conditions | Merging Rules |
|---|---|---|
| **Scenario 1** | $0 \le T_{11} \le T_{21}$; $T_{21} \le T_{12} \le T_{22} \le T^*$ | $FTI_1 \cup FTI_2 = (T_{11}, T_{22})$ |
| **Scenario 2** | $0 \le T_{21} \le T_{11} \le T_{22}$; $T_{22} \le T_{12} \le T^*$ | $FTI_1 \cup FTI_2 = (T_{21}, T_{12})$ |
| **Scenario 3** | $0 \le T_{21} \le T_{11}$; $T_{12} \le T_{22} \le T^*$ | $FTI_1 \cup FTI_2 = (T_{21}, T_{22})$ |
| **Scenario 4** | $0 \le T_{11} \le T_{21}$; $T_{22} \le T_{12} \le T^*$ | $FTI_1 \cup FTI_2 = (T_{11}, T_{12})$ |

* *Mission time*

### 3.2. Statistical formulas for reliability indices

A system's reliability indices are the indicators that can be applied to measure the degree of reliability. In a system reliability assessment, the system indices primarily include MTBF, MTTR, availability and a component's importance.

#### (1) MTBF, MTTR, Availability and Unavailability indices

MTBF is defined as the mean working time between two failure scenarios, MTTR is defined as the mean repair time between two working periods, and $T_i$ is defined as the mission time $T$ ($T_i = T$). Based on the merged failure time intervals, we can also obtain the working time intervals as $\{[t^i_{1,2}, t^i_{2,1}], [t^i_{2,2}, t^i_{3,1}], [t^i_{3,2}, t^i_{4,1}], \cdots, [t^i_{m_i-1,1}, t^i_{m_i,1}]\}$. According to the obtained failure and working time intervals, the statistical indices of MTBF and MTTR can be expressed as:

$$MTBF_{sf} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{m_i}\left(t^i_{j,2} - t^i_{j,1}\right)}{\sum_{i=1}^{N} T_i} \tag{15}$$

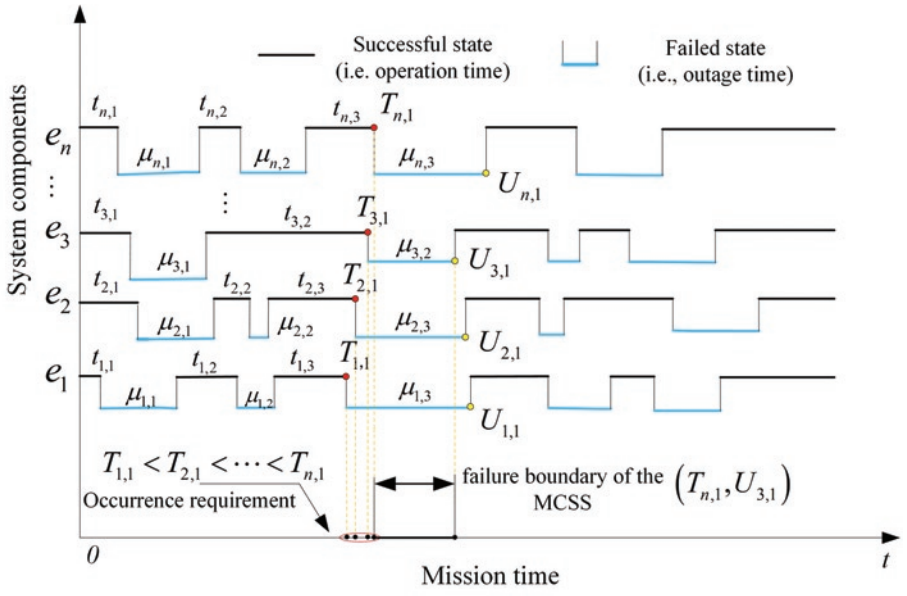


*Fig. 3. Sequence failure region of a general MCSS*

$$MTTR_{sf} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{m_i-1}\left(t_{j+1,2}^{i} - t_{j,1}^{i}\right)}{\sum_{i=1}^{N} T_i} \tag{16}$$

The availability of a system is a very important reliability index, and it not only reflects the safety of a system but also reflects its economy. Based on MTBF and MTTR, the statistical index of a system's availability ($A_{sf}$) and unavailability ($UA_{sf}$) can be described as:

$$A_{sf} = \frac{MTBF_{sf}}{MTBF_{sf} + MTTR_{sf}} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{m_i}\left(t_{j,2}^{i} - t_{j,1}^{i}\right)/\sum_{i=1}^{N} T_i}{\sum_{i=1}^{N}\sum_{j=1}^{m_i}\left(t_{j,2}^{i} - t_{j,1}^{i}\right)/\sum_{i=1}^{N} T_i + \sum_{i=1}^{N}\sum_{j=1}^{m_i-1}\left(t_{j+1,2}^{i} - t_{j,1}^{i}\right)/\sum_{i=1}^{N} T_i} \tag{17}$$

$$UA_{sf} = \frac{MTTR_{sf}}{MTBF_{sf} + MTTR_{sf}} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{m_i-1}\left(t_{j+1,2}^{i} - t_{j,1}^{i}\right)/\sum_{i=1}^{N} T_i}{\sum_{i=1}^{N}\sum_{j=1}^{m_i}\left(t_{j,2}^{i} - t_{j,1}^{i}\right)/\sum_{i=1}^{N} T_i + \sum_{i=1}^{N}\sum_{j=1}^{m_i-1}\left(t_{j+1,2}^{i} - t_{j,1}^{i}\right)/\sum_{i=1}^{N} T_i} \tag{18}$$

**(2) Importance index**

The importance index of a component can be used to arrange it according to its decreasing or increasing order of importance. In our proposed method, a simulation-based importance index for a component is introduced, namely, the failure criticality importance index ($I^{FC}$) [15]. The fundamental idea of this concept is to divide the number of system failures caused by failure of component $j$ with the failure number of the system in $(0, t)$, and the statistical formula $I_{j,sf}^{FC}$ is defined as:

$$I_{j,sf}^{FC} = \frac{n_j}{\sum_{i=1}^{N} m_i} \tag{19}$$

where $n_j$ represents the number of system failures caused by the considered component $j$, the variable $m_i$ indicates the total number of system failures in the $i$th simulation round, and "caused" here means the final event that makes the system fail.

### 3.3. MCSS-based Monte Carlo numerical simulation methodology

Based on the aforementioned statements, the proposed MCSS-based Monte Carlo numerical simulation methodology can be implemented as shown in ***Algorithm 1***.

***Algorithm 1.***
***Step 1***. Apply Liu's inference rules to obtain the MCSS of a DFT.
***Step 2***. Simulate the time-to-failure and time-to-recovery of each component contained in MCSS.
***Step 3***. Merge the overlapping parts to obtain the FTI of the MCSS.
***Step 4***. Establish statistical formulas for reliability indices.
***Step 5***. Calculate the reliability indices based on the merged FTI of the MCSS.
***Step 6.*** Output the simulated reliability results.

The detailed simulation procedure is provided as shown in Fig. 5.

## 4. Numerical validation

To illustrate the reasonability of the proposed MCSS-based Monte Carlo numerical simulation methodology, a DFT from an adapted hypothetical cardiac assist system (HCAS) was chosen as a numerical validation case since it contained many kinds of dynamic gates [2].

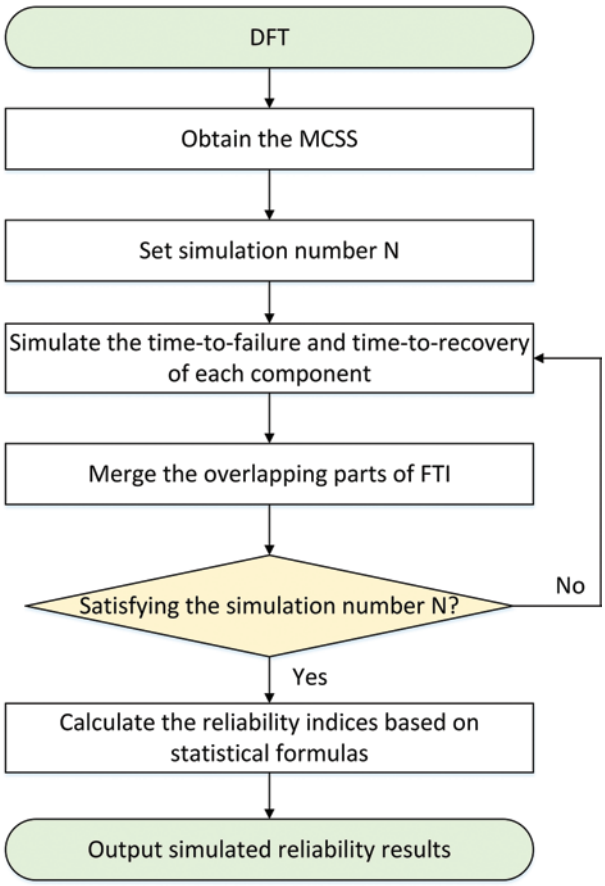


*Fig. 5. Procedure for implementing the proposed numerical simulation methodology*

### 4.1. Reliability evaluation

The original DFT model of HCAS is shown in Fig. 6. The reliability parameters $\lambda_i$, $\mu_i$ were the failure and repair rates of the $i$th component ($e_i$) and were assumed to be: $\lambda_i = 10^{-3}$, $\mu_i = 0.5$ ($i$=1, 2, 3, ⋯, 9). Based on the inference rules for temporal operations, the MCSS of this DFT could be obtained as:

$$MCSS_{dft} = e_1 + e_2 + e_3 \rightarrow e_4 + e_4 \rightarrow e_3 + e_5\, e_6 + e_7 \rightarrow {}^{0}_{e_7} e_9 \rightarrow e_8 + e_8 \rightarrow e_7 \rightarrow {}^{0}_{e_8} e_9 \tag{20}$$

where the hot spare gate (CUP) was logically equivalent to a static logic AND gate. Hence, its FLE ($e_3 \cdot e_4$) could be expanded to ($e_3 \rightarrow e_4$) $\cup$ ($e_4 \rightarrow e_3$) in the simulation process. In the same way, the AND gate (MOTOR) with input event $e_5$ and $e_6$ was expanded to ($e_5 \rightarrow e_6$) $\cup$ ($e_6 \rightarrow e_5$). The input event $e_9$ was a repeated event and was contained in two different cut sequences, $e_7 \rightarrow {}^{0}_{e_7} e_9 \rightarrow e_8$ and $e_8 \rightarrow e_7 \rightarrow {}^{0}_{e_8} e_9$.

In our study, reliability indices such as availability and the components' importance were evaluated by the proposed MCSS-based Monte Carlo numerical simulation method. To show the reasonability of the proposed methodology, the derived calculation results were compared with those obtained from the Markov chain state space-based approaches. All computations were implemented on a portable computer with an Intel (R) Core (TM) i5-4200M 2.5 GHz CPU and MATLAB programming platform.

### 4.2. Results and Discussions

We set the simulation number N as 10,000 rounds. The unavailability results at different mission times calculated by the proposed MCSS-based Monte Carlo numerical simulation methodology are shown in Table 2, which were compared with those obtained by the Markov chain state space-based methods. In addition, the compo-

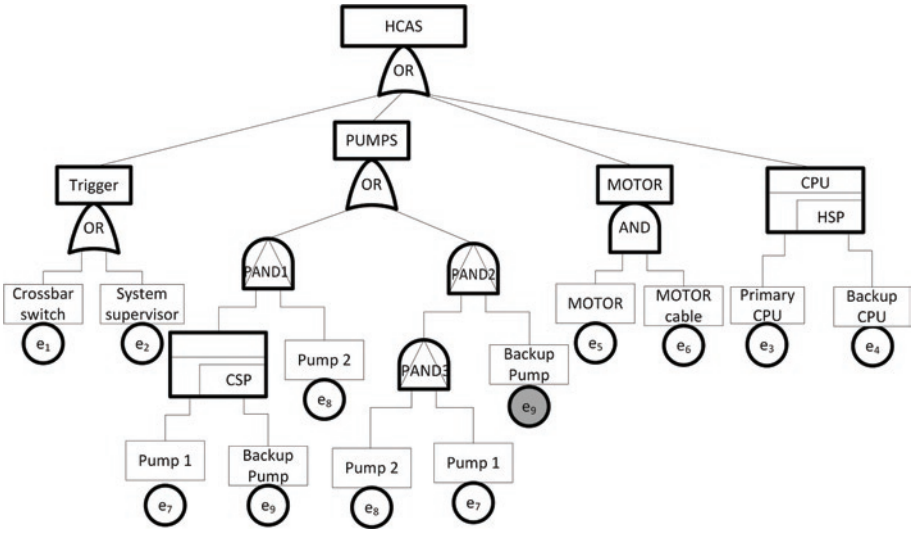


*Fig. 6. DFT model of the adapted HCAS*

*Table 2. Unavailability results (N=10,000)*

| Mission time | 100h | 200h | 400h | 600h | 800h | 1000h |
|---|---|---|---|---|---|---|
| **Proposed method** | 0.003990 | 0.004054 | 0.003998 | 0.004009 | 0.003943 | 0.004018 |
| **Markov method** | 0.003999 | 0.003999 | 0.003999 | 0.003999 | 0.003999 | 0.003999 |

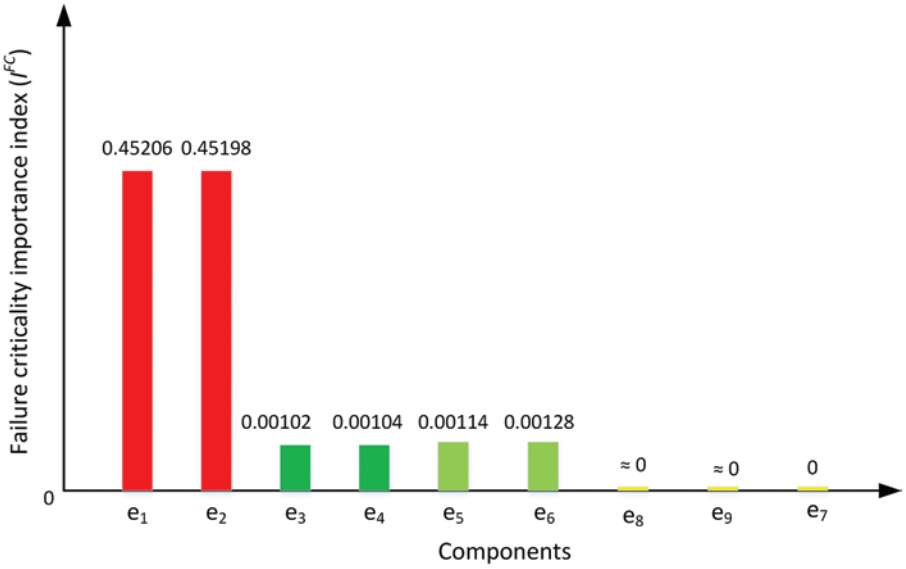


*Fig. 7. Components' failure criticality importance index ($I^{FC}$)*

*Table 3. Unavailability results with A, B, and C following lognormal distributions (N=10,000)*

| Mission time | 50h | 100h | 150h | 200h | 250h | 300h |
|---|---|---|---|---|---|---|
| **Unavailability** | 0.002534 | 0.019018 | 0.027261 | 0.029555 | 0.032073 | 0.032576 |

nents' failure criticality importance index ($I^{FC}$) was also calculated as shown in Fig. 7.

As observed in Table 2, the results calculated by our proposed methodology agreed with those obtained by the Markov chain state space-based methods, which demonstrated the effectiveness of our proposed methodology. Through applying the proposed methods, the components' failure criticality importance indices ($I^{FC}$) were also derived. As seen in the Fig. 7, $e_1$ and $e_2$ had almost the same $I^{FC}$, which was higher than those of the others and ranked as 1. The values of $e_3$, $e_4$, $e_5$ and $e_6$ had the second highest $I^{FC}$ and were ranked as 2. The remaining components ($e_7$, $e_8$ and $e_9$) were ranked as 3. In addition, when applying the pure Markov chain based methods, 272 states and 758 transitions were generated, and building the Markov Chain model manually would have cost approximately 3.5 hours. However, through applying the proposed methodology, the number of simulated minimal cut sequences was only 8, and the results could be provided in 3 ~ 4 seconds. Therefore, our proposed methodology was more effective and efficient than the Markov chain state space-based method.

To demonstrate the applicability of the proposed method for nonexponent distributions, we also assumed that the time-to-failure of components A, B, and C followed lognormal distributions, and their failure parameters were: mean $\mu_{A,B,C}$=100 and variances $\sigma_A$ =25, $\sigma_B$=30, $\sigma_C$ =35. The unavailability results at different mission times calculated by the proposed MCSS-based Monte Carlo numerical simulation methodology are shown in Table 3 (simulation number $N$=10,000). However for this case, the Markov chain state space model was unavailable because the time-to-failure of some components did not follow exponent distributions.

## 5. Conclusions and future work

In our study, an MCSS-based Monte Carlo numerical simulation methodology was proposed for analyzing a repairable DFT. The main simulation ideas, procedures and statistical formulas for reliability indices were also developed. To illustrate reasonability and applicability of the proposed methods, we used a case study. With less computing time (3 ~ 4s), the results calculated by the proposed methods and Markov chain state space methods are well matched, which can demonstrate that the proposed method was straightforward and simple for analyzing a repairable DFT. In addition, the proposed methods can give more reliability indices than those provided by Markov chain state space-based methods, such as components' importance indices. Especially for a large-scale repairable DFT where some components have nonexponent time-to-failure distributions, the proposed methodology is also applicable and promising for the future.

However, the proposed MCSS-based Monte Carlo numerical simulation methodology is only suitable for repairable DFTs with time-dependent failure events, and is not applicable for demand failure events whose occurrence probabilities are independent of time. This can be viewed as a disadvantage. In the future, we will focus on solving repairable DFTs with demand failure behaviors. Computer code development for MCSS-based Monte Carlo numerical simulation is also part of our ongoing work.

**Acknowledgments**

*This work is supported by the National Natural Science Foundation of China (71901203), the Natural Science Foundation of Anhui province (2008085MA23), and the National Key R&D Program of China (2018YFB1900301). In addition, the authors express their sincere gratitude to the State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen.*

## References

1. Alam M, Al-Saggaf UM. Quantitative reliability evaluation of repairable phased mission-time systems using Markov approach. IEEE Transactions on Reliability 1986; R-35(5): 498-503, https://ieeexplore.ieee.org/abstract/document/4335529.
2. Boudali H, Dugan JB. A discrete-time Bayesian network reliability modeling and analysis framework. IEEE Transactions on Reliability 2006; 55 (1):86-97, https://ieeexplore.ieee.org/document/1603897.
3. Boudali H, Nijmeijer A, Stoelinga M. DFTSim: A simulation tool for extended dynamic fault trees. Proceedings of the 42nd Annual Simulation Symposium, Society for Modeling and Simulation International (2009), pp. 31-38, https://dl.acm.org/doi/10.5555/1639809.1639842.
4. Budde CE, Biagi M, Monti RE, D'Argenio PR, Stoelinga M. Rare Event Simulation for Non-Markovian Repairable Fault Trees. In: Biere A., Parker D. (Eds) Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2020. Lecture Notes in Computer Science, Vol. 12078. Springer, Cham, https://link.springer.com/chapter/10.1007/978-3-030-45190-5_26.
5. Budde CE, Stoelinga M. Automated Rare Event Simulation for Fault Tree Analysis via Minimal Cut Sets[M]// Measurement, Modelling and Evaluation of Computing Systems, 20th International GI/ITG Conference, MMB 2020, Saarbrücken, Germany, March 16–18, 2020, Proceedings. 2020, https://link.springer.com/chapter/10.1007/978-3-030-43024-5_16.
6. DUAN R, LIN Y, ZENG Y. Fault diagnosis for complex systems based on reliability analysis and sensors data considering epistemic uncertainty. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2018; 20 (4): 558–566, http://dx.doi.org/10.17531/ein.2018.4.7.
7. Dugan JB, Bavuso SJ, Boyd MA. Fault trees and Markov models for reliability analysis of fault- tolerant digital systems. Reliability Engineering and System Safety 1993; 39(3):291–307, https://www.sciencedirect.com/science/article/abs/pii/095183209390005J.
8. Ejlali A, Miremadi SG. FPGA-based Monte Carlo simulation for fault tree analysis. Microelectronics Reliability 2004; 44(6): 1017-1028, https://www.sciencedirect.com/science/article/abs/pii/S0026271404000769.
9. Gascard E, Simeu-Abazi Z. Quantitative Analysis of Dynamic Fault Trees by means of Monte Carlo Simulations: Event-Driven Simulation Approach. Reliability Engineering & System Safety 2018; 180: 487-504, https://doi.org/10.1016/j.ress.2018.07.011.
10. Ge DC, Li D, Lin M, Yang YH. SFRs-based numerical simulation for reliability of highly-coupled DFTs. Eksploat Niezawodn – Maintenance and Reliability 2015; 17(2):199–206, http://dx.doi.org/10.17531/ein.2015.2.5.
11. Ge DC, Lin M, Yang YH, Zhang RX, Chou Q. Quantitative analysis of dynamic fault trees using improved Sequential Binary Decision Diagrams. Reliability Engineering and System Safety 2015; 142: 289-299, https://www.sciencedirect.com/science/article/abs/pii/S0951832015001763.
12. Ge DC, Lin M, Yang YH, Zhang RX, Chou Q. Reliability analysis of complex dynamic fault trees based on an adapted K.D.Heidtmann algorithm. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 2015; 229(6): 576-586, https://journals.sagepub.com/doi/abs/10.1177/1748006X15594694.
13. Ge DC, Yang YH. Reliability analysis of non-repairable systems modeled by dynamic fault trees with priority AND gates. Applied Stochastic Models in Business and Industry 2015; 31(6): 809-822, https://onlinelibrary.wiley.com/doi/abs/10.1002/asmb.2108.
14. Guo J, Shi L, Zhang K, Gu K, and et al. Dynamic fault tree analysis based fault diagnosis system of power transformer. The 10th World Congress on Intelligent Control and Automation (WCICA), 6-8 July 2012, Beijing China, pp. 3077-3081, https://ieeexplore.ieee.org/abstract/document/6358400.
15. Hilber P, Bertling L. A method for extracting reliability importance indices from reliability simulations of electrical networks. In Proc. 15th Power Syst. Comput. Conf. (PSCC), Liege, Belgium, Aug. 2005, https://services.montefiore.uliege.be//stochastic/pscc05/papers/fp475.pdf.
16. LI J, DUAN R. Dynamic diagnostic strategy based on reliability analysis and distance-based VIKOR with heterogeneous information. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2018; 20 (4): 610–620, http://dx.doi.org/10.17531/ein.2018.4.12.
17. Li Y, Wang B, Liu D, Yang H, Yang F. Complete Temporal Rules for Cut Sequence Generation in Dynamic Fault Tree Analysis. Proceedings of the World Congress on Engineering 2013 Vol II, WCE 2013, July 3-5, 2013, London, U.K, http://www.iaeng.org/publication/WCE2013/WCE2013_pp903-908.pdf.
18. Li YF, Huang HZ, Liu Y, Xiao N, Li H. A new fault tree analysis method: fuzzy dynamic fault tree analysis. Eksploatacja i Niezawodnosc –Maintenance and Reliability 2012; 14 (3): 208-214, http://ein.org.pl/2012-03-04.
19. Liu D, Zhang C, Xing L, Li R, Li H. Quantification of cut sequence set for fault tree analysis. HPCC lecture notes in computer science. V.4728. Houston, USA: Springer-Verlag; 2007. pp. 755–65, https://link.springer.com/chapter/10.1007/978-3-540-75444-2_70.
20. Manno G, Chiacchio F, Compagno L, DUrso N, and Trapani N. MatCarloRe: An integrated FT and Monte Carlo Simulink tool for the reliability assessment of dynamic fault tree. Expert Systems with Applications 2012; 39 (12): 10334-10342, https://doi.org/10.1016/j.eswa.2011.12.020.
21. Merle G, Roussel JM, Lesage JJ, Bobbio A. Probabilistic Algebraic Analysis of Fault Trees with Priority Dynamic Gates and Repeated Events. IEEE Transactions on Reliability 2010; 59(1): 250-261, https://ieeexplore.ieee.org/document/5361394.
22. Merle G, Roussel JM, Lesage JJ, Perchet V, Vayatis N. Quantitative Analysis of Dynamic Fault Trees Based on the Coupling of Structure Functions and Monte Carlo Simulation. Quality and Reliability Engineering International 2014; 32(1): 7-18. https://onlinelibrary.wiley.com/doi/pdf/10.1002/qre.1728.
23. Merle G, Roussel JM, Lesage JJ. Quantitative analysis of dynamic fault trees based on the structure function. Proceedings of Annual Reliability and Maintenance Symposium 2011; 24-27 Jan. 2011, Lake Buena Vista, FL, USA, pp.1-6, https://ieeexplore.ieee.org/document/5754452/authors#authors.
24. Meshkat L, Dugan JB and Andrews JD. Dependability analysis of systems with on-demand and active failure modes, using dynamic fault trees. IEEE Transactions on Reliability 2002; 51(2): 240-251, https://ieeexplore.ieee.org/abstract/document/1011531.
25. Rao KD, Gopika V, Rao VVSS, and et al. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. Reliability Engineering and System Safety 2009; 94(4): 872-883, https://www.sciencedirect.com/science/article/abs/pii/S0951832008002354.

26. Ren Y, Dugan JB. Design of reliable systems using static and dynamic fault trees. IEEE Transactions on Reliability 1998; 47(3): 234-244, https://ieeexplore.ieee.org/document/740491.
27. Ruijters E, Guck D, Drolenga P, Peters M, Stoelinga M. Maintenance Analysis and Optimization via Statistical Model Checking. In: Agha G., Van Houdt B. (Eds) Quantitative Evaluation of Systems. QEST 2016. Lecture Notes in Computer Science, Vol 9826. Springer, Cham, https://link.springer.com/chapter/10.1007/978-3-319-43425-4_22.
28. Tang Z, Dugan JB. Minimal Cut Set/Sequence Generation for Dynamic Fault Trees. Proceedings of Annual Reliability and Maintenance Symposium 2004; 26-29 Jan.2004, Los Angeles, CA, USA, pp.1-5, https://ieeexplore.ieee.org/document/1285449.
29. Xing L, Fleming KN, Loh WT. Comparison of Markov model and fault tree approach in determining initiating event frequency for systems with two train configurations. Reliability Engineering and System Safety 1996; 53(1): 17-29. https://www.sciencedirect.com/science/article/abs/pii/0951832096000336.
30. Xing L, Shrestha A, Dai Y. Exact combinatorial reliability analysis of dynamic systems with sequence-dependent failures. Reliability Engineering and System Safety 2011; 96(10): 1375-1385, https://www.sciencedirect.com/science/article/abs/pii/S0951832011001050.
31. Xing L, Tannous O, Dugan JB. Reliability Analysis of Nonrepairable Cold-Standby Systems Using Sequential Binary Decision Diagrams. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans 2012; 42(3): 715-726, https://ieeexplore.ieee.org/document/6059511.
32. Yao Y, Yang X, Li P. Dynamic fault tree analysis for digital fly-by-wire flight control system. The 15th AIAA/IEEE Digital Avionics Systems Conference, 27-31 Oct. 1996, Atlanta GA, pp. 479-484, https://ieeexplore.ieee.org/abstract/document/559203.
33. Yuge T, Yanagi S. Fault tree analysis considering sequence dependence and repairable input events. Journal of Quality in Maintenance Engineering 2013; 19(2): 199-214, https://www.emerald.com/insight/content/doi/10.1108/13552511311315986/full/html.
34. Yuge T, Yanagi S. Quantitative analysis of a fault tree with priority AND gates. Reliability Engineering and System Safety 2008; 93(11): 1577-1583. https://www.sciencedirect.com/science/article/abs/pii/S0951832008000409.
35. Zhang P, Chan KW. Reliability Evaluation of Phasor Measurement Unit Using Monte Carlo Dynamic Fault Tree Method. IEEE Transactions on Smart Grid 2012; 3(3): 1235-1243, https://ieeexplore.ieee.org/document/6151874.