A Numerical Simulation Approach for Reliability Analysis of Fault-tolerant Repairable System

Xiaofeng Liang, Hong Yi, Yufang Zhang
School of Naval Architecture, Ocean and Civil Engineering, Shanghai Jiaotong University, Shanghai 200030, P.R. China

Abstract—This paper proposes a numerical simulation approach for reliability analysis of fault-tolerant system with repairable components. In the traditional method for the reliability analysis of fault-tolerant system, the system structure is described by means of binary decision diagram (BDD) and Markov Process, and then the reliability indexes are calculated. However, as the size of system augments, the size of state space will increase exponentially. In addition, Markov approach requires that the failure and repair time of the components obey exponential distribution. In this paper, by combining dynamic fault tree (DFT) and numerical simulation based on the Minimal Sequence Cut Sets (MSCS), we propose a new method to evaluate reliability of fault-tolerant system with repairable components. The approach presented does not depend on Markov model, so that it can effectively solve the problem of the state-space combination explosion. Moreover, our method does not require the system to have Markov property, and it is suitable for systems whose failure and repair time obey arbitrary distributions. Therefore, our method is more flexible than traditional method. At last, one example is given to verify the method.

Keywords— Reliability Analysis; Fault-tolerant Repairable System; Numerical Simulation; Dynamic Fault Tree; Minimal Sequence Cut Sets

I. INTRODUCTION

In the field of reliability analysis, static fault tree (SFT) model is well accepted by reliability engineers and researchers for its advantages of compact structure and integrated analyzing methods. Many methods have been developed for the evaluation of static fault trees, such as Binary Decision Diagram (BDD)[1, 2], Prime Implication (PI)[3], Monte carlo [4, 5], Bayesian networks[6, 7].

However, for some dynamic systems, e.g. fault-tolerant systems, and redundancy repairable systems, the occurrence of top event relies on not only the combination of basic events, but also on the occurrence order of basic events. Former SFT analysis methods are not applicable to some new situations, because SFT can not handle the systems that are characterized by dynamic behaviors. To overcome this lack, Dugan et al. presented some new dynamic gates[8], such as FDEP, HSP, CSP, PAND and SEQ gates, and put forward dynamic fault trees (DFT) to analyze dynamic systems[9].

Dynamic fault trees use Markov models as analytical representations. In [10], Amari et al. proposed an method to evaluate DFT considering sequence failures. However, in the processes to evaluate spare gates, the method has to employ Markov model which will confront the problem of state-space combination explosion.

For the sake of simplicity, Dugan et al. introduced the concept of modular decomposition into the DFT analysis [11-14]. In [13], Dugan presented a modular solution to non repairable dynamic systems, which provides a combination of static modules, and Markov chain solution techniques for dynamic modules. When the dynamic sub-tree is small, modular solution is efficient to analyze the dynamic system. However, if the sub-tree under top event is a large dynamic tree, one also has to confront the problem of state-space combination explosion with Markov chain based approaches.

In [15], Tang et al. provided the concept of minimal cut sequence set (MCSS) and introduced it to the DFT analysis. To some extent, the method Tang et al. introduced can simplify the system, and can resolve the problem of the state-space combination explosion. However, because of the application of the Markov method, it requires the system to have Markov property. It is not applicable to the system whose failure and repair time obey arbitrary distribution.

In this paper, by combining DFT and Monte Carlo Simulation, we propose a new approach to the reliability analysis of fault-tolerant system with repairable components. In this method, the reliability model of the fault-tolerant system is described by means of DFT. Then, reliability indexes of fault-tolerant system are calculated by numerical simulation method based on the MCSS of the DFT.

The approach has following advantages:

- Due to independence on Markov model, it can effectively solve the problem of the state-space combination explosion caused by Markov method.

- As the numerical simulation being adopted, our method does not require the system to have Markov property. Therefore, it is applicable to systems whose failure and repair time obey arbitrary distribution.

- It is an efficient exploration of the reliability analysis of the standby system on the condition of that the
component failed is repairable during system operating.

The remaining of the paper is organized as follows. Section 2 introduces the way to model the dynamic system. Section 3 presents an integrated method. In section 4, an example is given to illustrate the processes and the validity of our method. Finally, concluding remarks are made in Section 5.

II. RELIABILITY MODEL OF THE FAULT-TOLERANT REPAIRABLE SYSTEM

A Dynamic Fault Tree Model

The model of traditional SFT is based on static logic and static fault mechanism. The top event of the SFT is described only by logical combination of the basic events. But in the real word, the system is characterized by dynamic behaviors, i.e. fault tolerant system, redundancy repairable system. SFT is not suitable to model the system with dynamic characters.

To model the dynamic system, not only the combination of the basic event, but also their occurrence must be taken into account, and many scholars have made great efforts. Dugan et al. introduced some new dynamic gates, such as FDEP, HSP, CSP, PAND and SEQ gates [8], and put forward dynamic fault trees to analyze dynamic systems [9]. In [16-19], further researches about DFT have been conducted. Using dynamic gates, DFT obtains the ability to describe dynamic systems in a more feasible and flexible way.

B Modularization Idea of the DFT

In the quantitative analysis of the SFT, computational complexity performs exponential growth as the increasing of the basic events and gate events. In order to solve this problem, Rosenthal proposed a modularization idea [20], which divides the complicated system into many simple modules, and solves them independently, and then combines the results for the solution of the entire system using the module joint probability method.

Rosenthal’s modularization idea also can be extended to the dynamic fault tree analysis. Many researches on finding ways to modularize the fault tree have been employed [11-14]. In [13], Qu and Dugan presented a modular solution to non-repairable dynamic systems, which provides a combination of BDD solution techniques for static modules, and Markov chain solution techniques for dynamic modules.

C Equivalent Minimal Cut Sets of the DFT

The cut sets of the SFT are the combination of the basic events whose failure will cause the failure of the top event. Over the past four decades, various techniques to search cut set of the static fault tree have developed, for example, Upward Method, Downward Method, and BDD Method.

For a dynamic fault tree, due to being added dynamic logic gates, e.g. Spare gate, SEQ gate, the occurrence of top event relies on not only the combination of basic events, but also on the occurrence order of basic events.

In [15], Tang et al. expanded the concept of minimal cut set for static fault trees, and provided the concept of minimal cut sequence for DFT. Compared to minimal cut set, which does not consider the sequences among basic events, minimal cut sequence is a basic event sequence that can result in the occurrence of top event in DFT. To obtain the minimal cut sequence set of the DFT, Liu et al. divided the constraints of the dynamic gate into the logic constraint and time constraint, and proposed a method to search the minimal cut sequence set [21]. Minimal cut sequence sets can be applied to not only the qualitative analysis of the DFT, but also the quantitative analysis [22].

In this study, DFT was adopted to describe the reliability model of the fault tolerant system and the redundancy repairable system. By integrating the minimal cut sets of the static sub-tree and the minimal cut sequence sets of the dynamic sub-tree, we can obtain the minimal cut sequence sets of the entire dynamic fault tree, which are defined as equivalent minimal cut sets (EMCS). In next chapter, we introduce a numerical simulation approach based on equivalent minimal cut sets for quantitative analysis of dynamic fault tree.

III. GENERAL FRAMEWORK FOR ESTIMATING RELIABILITY OF THE DYNAMIC SYSTEM

A Numerical Simulation Logic Based on EMCS

The logic relation of the dynamic fault tree can be expressed by the logic product of all equivalent cut sets. If the top event occurs, at least one equivalent cut set will occur. Therefore, we can draw a conclusion that the equivalent cut set which occurs first is the one that causing the failure of the system.

Suppose that $F_i(t)$ is the failure distribution of the basic event $e_i$, $G_i(t)$ is the repair distribution. Then, the failure time denoted by $T_i$ and repair time denoted by $U_i$ can be given by

$$
\begin{align*}
T_i &= F_i^{-1}(\xi) \\
U_i &= G_i^{-1}(\xi)
\end{align*}
$$

Where $\xi$ is the uniformly distributed random numbers in the interval $[0, 1]$.

Denoting $T_k(n)$ as the failure time of the $k$ th equivalent cut set in the $n$ th stochastic sampling, the failure time of the system denoted by $Ts(n)$ can be given by

$$
Ts(n) = \min(T_1(n), T_2(n), T_3(n), ..., T_k(n))
$$

Suppose that T is the mission time of the system, and N is the times of simulation. The time that simulation mission succeed is denoted by $Ns$, whose initial value is 0. If $Ts(n) \geq T$, we consider this simulation mission is successful, then $Ns = Ns + 1$. If $Ts(n) < T$, simulation mission fails and next simulation mission begin. Figure 2 shows the procedure of estimating reliability of the dynamic system.
According to figure 2, the reliability of the system can be expressed by

\[ R(t) = \frac{N_c}{N} \]  \hspace{1cm} (3)

After having modularized the DFT into static sub-tree dynamic sub-tree and dynamic sub-tree, both the occurring time of the static minimal cut sets and that of the minimal cut sequence sets can be obtained by using stochastic sampling method.

### B Simulation Method for Occurring Time of the Static Minimal Cut Sets

In static sub-tree, the static minimal cut sets do not happen until all its basic events have failed. Let \( t_i \) \((i = 1, 2, 3, 4, \ldots, n)\) denote the failure time of the basic events in the static cut set. Let \( T_s \) denote the occurring time of the static minimal cut set, and it can be given by

\[ T_s = \max(t_1, t_2, t_3, \ldots, t_n) \] \hspace{1cm} (4)

### C Simulation Method for Occurring Time of the Minimal Cut Sets

The minimal cut sequence set of the dynamic sub-tree consists of two parts. One is the combination of the static events, defined as static subset. Another is the combination of the dynamic events, defined as dynamic subset. The relationship between the static subset and the dynamic subset is logic AND.

Let \( T_m \) denote the time that static subset occurs, and \( T_d \) denote the time that dynamic subset occurs, then the time that minimal cut sequence set happens denoted by \( T_p \) can be given by

\[ T_p = \max(T_m, T_d) \] \hspace{1cm} (5)

It is corresponding relation between the dynamic subset and the dynamic gates. Accordingly, HSP dynamic subset, CSP dynamic subset SEQ dynamic subset, PAND dynamic subset, FDEP dynamic subset are defined.

In the next section, the approach of sampling the occurring time of the dynamic subset will be introduced.

#### (1) HSP Dynamic Subset

In the HSP system, all components operate simultaneously. Moreover, the components failed can put into operation again after being repaired. In another word, if only one or more events fail, not all fail simultaneously, the system is at normal state.

For HSP dynamic subset, only when all basic events are in repairing state, would the HSP dynamic subset occur. State transition diagram of HSP system is depicted in Figure 3.
intervals, which are denoted by
\[ \pi_{1,1}, \pi_{1,2}, \pi_{1,3}, \ldots, \pi_{1,m} \]
\[ \pi_{2,1}, \pi_{2,2}, \pi_{2,3}, \ldots, \pi_{2,m} \]
\[ \ldots \]
\[ \pi_{n,1}, \pi_{n,2}, \pi_{n,3}, \ldots, \pi_{n,m} \]

Set up a state diagram for every basic event, as shown in Figure 4.

![State diagram of the basic event from HSP system](image)

From Figure 4, we can see that the basic event is at “1” state in the odd number intervals, and at “0” state in the even number intervals. Then, the state function of the can be expressed by
\[ \Phi(\pi_{i,j}) = \begin{cases} 1 & j = 2n - 1 \quad n = 1, 2, 3, \ldots \\ 0 & j = 2n \quad n = 1, 2, 3, \ldots \end{cases} \quad (6) \]

It should be noted that the intervals are semi-open and semi-closed. The critical point from odd-number interval to even number intervals is at state “0”. Conversely, it is at state “1”.

Then, by assembling and realigning that of the all events, we can construct a new time series represented by
\[ T_1, T_2, \ldots, T_n, T_{n+1}, \ldots, T_m \]

Taking a value from \( T_1 \) to \( T_m \) successively, and judging which interval it is within, we can determine the state of the event in this interval. If all events are in state “0”, the value taken from above time series is the occurring time of HSP dynamic subset.

(2) CSP Dynamic Sub Set

CSP system has a primary unit and one or more alternate units. The primary unit is initially powered on, and the alternate units are used as the cold spare unit to substitute the primary unit when it fails. The CSP system fails when all units are in repairing state.

Simulating the occurring time of the CSP dynamic subset is different from that of the HSP dynamic subset. All events in CSP dynamic subset can be classified into many groups, namely first operating events, second operating events, third operating events, and so on. When first operating events are at work, other events do not work. If the first operating events fail, the second operating events put into service. Then, the failed events are regarded as the last operating events after being repaired.

As an example, we take a CSP system with three basic events to show how to simulate the occurring time of the CSP dynamic subset. Figure 5 depicts the state transition diagram for CSP system.

![State transition diagram for CSP system](image)

For every basic event of the CSP system, there are three alternate states, which are operating state, repairing state and standby state. According to their failure rate and repair rate, the failure time and repair time can be obtained by simulation. The standby time is related to the work time and repair time of the other units.

The time series of the CSP system with three basic events can be represented by
\[ l_{1,1} + u_{1,1} + l_{2,1} + u_{2,1} + s_{2,1} + l_{1,2} + u_{1,2} + s_{2,1} + l_{2,2} + u_{2,2} + \ldots (i = 1, 2, 3) \]

Denoted by
\[ 0, A_{i,1}, A_{i,2}, A_{i,3}, \ldots, A_{i,m} (i = 1, 2, 3) \]

Mark the adjacent time segments of the time series above as an interval, which are denoted by
\[ \pi_{i,1}, \pi_{i,2}, \pi_{i,3}, \ldots, \pi_{i,m} (i = 1, 2, 3) \]

Set up a state diagram for every basic event, as shown in Figure 6.

![State diagram of the basic event from CSP system](image)

From Figure 6, we can see that the basic event is at “1” state
in the $3n+1$ intervals, at “0” state in the $3n+2$ intervals and at “1” state in the $3n+3$ intervals. Then, the state function of the can be expressed by

$$
\Phi(\sigma_i) = \begin{cases} 
0 & j = 3n+1 \\
1 & j = 3n+2 \\
\Phi & j = 3n+3 
\end{cases} \quad n = 0, 1, 2, 3, \ldots \quad (7)
$$

It should also be noted that the intervals are semi-open and semi-closed. The critical points from 3 intervals to intervals are at state “0”, and it is at state “1” from $3n+2$ intervals to $3n+3$ intervals.

(3) SEQ Dynamic Sub Set

SEQ dynamic subset forces events to occur in a particular order. SEQ dynamic subset does not occur until all its events have occurred in the left-to-right order.

As discussed earlier, $t_i(i = 1, 2, 3, 4, \ldots, n)$ denotes the failure time of the basic events in the static cut set, which can be obtained by random sampling.

If $t_1 \leq t_2 \leq \ldots \leq t_n$, the output of the SEQ dynamic subset occurs. Then one sampling is completed, and $t_n$ is the occurring time of the dynamic subset.

In the situation of $n = 2$, SEQ dynamic subset is converted to PAND dynamic subset.

(4) Transformation of the FDEP Gate

FDEP gate reflects the occurrence relation among inner events in a fault tree. In practice, FDEP gate is equivalent to a combination of other logic gates, just like k/n gate, AND gate, OR gate. In the process of analyzing a fault tree with FDEP gate, the first step is to transform the FDEP gate to its equivalent static gates, then get the CSS of the new generated fault tree.

IV. A CASE STUDY

In this section, a case study is presented to illustrate the validity of our method. The system in question is named Damage Detecting System for Underwater Pipeline (DDSUP). The DDSUP consists of three modules, which are detecting module, power module and control module. The reliability model of the DDSUP is depicted as Figure 7.

![Fault Tree of DDSUP](image)

Figure 7. The fault tree of Damage Detecting System for Underwater Pipeline.

Via modularization, we can obtain the static sub-tree and dynamic sub-tree. The minimal cut sets of the static sub-tree are \{A\}, \{B\}, \{C, D\}, \{E\}, \{F\}, \{G\}, \{H\}, and the minimal cut sequence sets of the dynamic sub-tree are \{1\}, \{J\}, \{L, M\}.

The next step is collecting the basic data for evaluating the reliability of the UDMC. In this study, main portion of the basic data is obtained from reliability test for a period of 2 years, and partial data comes from handbooks. The failure rates/repair rates and distributions of the each basic event in fault tree of the DDSUP are listed in Table 1.

<table>
<thead>
<tr>
<th>code</th>
<th>basic events</th>
<th>failure rate</th>
<th>repair rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>data transmission system</td>
<td>0.000667</td>
<td>0.56</td>
</tr>
<tr>
<td>B</td>
<td>data analyzing system</td>
<td>0.000909</td>
<td>0.56</td>
</tr>
<tr>
<td>C</td>
<td>mechanical detector</td>
<td>0.000286</td>
<td>0.19</td>
</tr>
<tr>
<td>D</td>
<td>infrared detector</td>
<td>0.00037</td>
<td>0.4</td>
</tr>
<tr>
<td>E</td>
<td>propulsion system</td>
<td>0.000125</td>
<td>0.08</td>
</tr>
<tr>
<td>F</td>
<td>power supply</td>
<td>0.00025</td>
<td>0.41</td>
</tr>
<tr>
<td>G</td>
<td>location system</td>
<td>0.0004</td>
<td>0.79</td>
</tr>
<tr>
<td>H</td>
<td>pipeline tractor system</td>
<td>0.00087</td>
<td>0.18</td>
</tr>
<tr>
<td>I</td>
<td>switch</td>
<td>0.00033</td>
<td>0.67</td>
</tr>
<tr>
<td>J</td>
<td>system monitor</td>
<td>0.0002</td>
<td>0.69</td>
</tr>
<tr>
<td>L</td>
<td>main control system</td>
<td>0.000461</td>
<td>0.39</td>
</tr>
<tr>
<td>M</td>
<td>standby control system</td>
<td>0.000461</td>
<td>0.39</td>
</tr>
</tbody>
</table>

At last, the unreliability of the DDSUP was calculated by means of the simulation method we suggested. As a comparison, we also evaluated DDSUP using “Relex” software that uses Markov model to solve dynamic gates. The unreliability of DDSUP for different time is listed in Table 2.

<table>
<thead>
<tr>
<th>No.</th>
<th>Time (h)</th>
<th>Markov method</th>
<th>Simulation method</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>0.0368</td>
<td>0.0325</td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td>0.0723</td>
<td>0.0767</td>
</tr>
<tr>
<td>3</td>
<td>30</td>
<td>0.1066</td>
<td>0.1103</td>
</tr>
<tr>
<td>4</td>
<td>40</td>
<td>0.1396</td>
<td>0.1317</td>
</tr>
<tr>
<td>5</td>
<td>50</td>
<td>0.1714</td>
<td>0.1698</td>
</tr>
<tr>
<td>6</td>
<td>60</td>
<td>0.2021</td>
<td>0.2006</td>
</tr>
<tr>
<td>7</td>
<td>70</td>
<td>0.2317</td>
<td>0.2406</td>
</tr>
<tr>
<td>8</td>
<td>80</td>
<td>0.2602</td>
<td>0.2697</td>
</tr>
<tr>
<td>9</td>
<td>90</td>
<td>0.2877</td>
<td>0.2976</td>
</tr>
<tr>
<td>10</td>
<td>100</td>
<td>0.3142</td>
<td>0.3383</td>
</tr>
<tr>
<td>11</td>
<td>110</td>
<td>0.3397</td>
<td>0.3252</td>
</tr>
<tr>
<td>12</td>
<td>120</td>
<td>0.3643</td>
<td>0.3701</td>
</tr>
<tr>
<td>13</td>
<td>140</td>
<td>0.4108</td>
<td>0.4016</td>
</tr>
<tr>
<td>14</td>
<td>160</td>
<td>0.4541</td>
<td>0.4695</td>
</tr>
<tr>
<td>15</td>
<td>180</td>
<td>0.4942</td>
<td>0.5012</td>
</tr>
<tr>
<td>16</td>
<td>200</td>
<td>0.5314</td>
<td>0.5472</td>
</tr>
</tbody>
</table>
From Table 2, it can be seen that evaluation result based on simulation method is close to that based on Markov model. And the maximum error is less than 2.97%.

V. CONCLUSION AND FUTURE WORK

In this paper, a numerical simulation approach is developed to evaluate the reliability analysis of fault-tolerant system with repairable components. Because of the shortcomings of the SFT, DFT is used to describe the reliability model of the fault-tolerant system with repairable components. Then, reliability indexes of fault-tolerant system can be calculated by numerical simulation methodology based on the Minimal Cut Sequence Sets (MCSS) of the DFT.

Due to independence on Markov model, the approach presented can effectively solve the combination explosion problem of calculation caused by traditional method based on BDD and Markov model. Moreover, our method does not require the system to have Markov property, and it is applicable to the system whose failure and repair time obey an arbitrary distribution. Therefore, our method is more flexible.

Finally, a case study is given to show the performance of our approach. It is shown that evaluation result based on our method is close to that based on Markov model. It indicates that our solution is feasible in reliability analysis of fault-tolerant repairable system.

Further work will focus on calculation of the important degree by using simulation method and solving the time redundancy of the mission reliability evaluation.

REFERENCES