The failure behaviors of many real-life systems are very complex and sequence-dependent, and can be modeled by highly-coupled dynamic fault trees (DFTs). Existing approaches for solving DFTs, such as Markov state-space-based or inclusion-exclusion based methods all have their disadvantages. They either suffer from the problem of state space explosion or are subjected to the combination explosion. Additionally, Markov-based approaches become unavailable when components follow non-exponential time-to-failure distributions which prevail in real-life systems. To overcome shortcomings of the methods mentioned above, SFRs (Sequence Failure Regions)-Based numerical simulation approach is first proposed. The proposed method is applicable for a generalized cut sequence as well as highly-coupled DFTs modeling non-repairable systems with arbitrary time-to-failure distributed components. The results of the validation example indicate the reasonability of our proposed approach.

Keywords: highly-coupled DFTs, sequence failure region, arbitrary distributions, numerical simulation.
approach is first proposed. This method relies on the complete MCSs, i.e., minimal cut sequence set (MCSS), of a considered DFT. Some achievements for finding the MCSS have been made as: Liu et al [13] proposed a series of inference rules to generate the MCSS of a given DFT; Shrestha et al [20] put forward a sorting algorithm to enumerate the MCSS; Merle et al [17] presented several temporal operators and related operation rules to deduce the structure function of a DFT which finally can be reduced to the MCSS. Actually, as to numerical simulation for reliability of a system modeled by DFT, some researchers [2, 9, 12, 25] have made prospective studies and applications. Unfortunately, such simulation-based methods are just based on different dynamic gates. To the author’s knowledge, no articles have presented a numerical simulation approach for a generalized minimal cut sequence (GMCS) as well as a highly-coupled DFT. By contrast, the proposed method is considered to be a universal numerical simulation tool for non-repairable DFTs with arbitrary distributions, including a GMCS. Results of the validation example indicate the proposed method is reasonable.

2. Basic Concepts

2.1. Dynamic Logic Gates

To characterize sequence- and function-dependent failure behaviors existing in many real-life systems, Dugan et al [5, 6] introduced several new dynamic gates, such as Sequence Enforcing (SEQ) gate, Priority AND (PAND) gate, Function Dependent (FDEP) gate, Cold Spare (CSP) gate, Warm Spare (WSP) gate, and Hot Spare (HSP) gate. Such dynamic gates are integrated into static fault trees to form DFTs. Hence, the occurrence of a considered DFT not only depends on the combinations of basic events, but also depends on their failure orders. Figure 1 shows the commonly-used dynamic gates for a DFT.

(a) SEQ gate: SEQ gate forces the input events to fail in a left to right order. That is to say an input event never fails before all the input ones to its left hand have already failed. As to the SEQ gate in Fig.1 (a), the only failure sequence is that A fails first, then B fails, and C fails last.

(b) PAND gate: PAND gate is used to detect certain failure sequences of input events [7]. In a PAND gate, different failure orders are permitted, but only a specific failure sequence (from left to right) leads to the fire of the gate. For the PAND gate in Fig.1 (b), there exist two failure sequences: A fails first, then B fails; B fails first, then A fails. But only the former failure order can lead to the firing of the gate.

(c) FDEP gate: FDEP gate characterizes a situation where the occurrence of a trigger event may cause other dependent components unusable, but the occurrence of dependent events does not have any effect on the trigger event. As to the FDEP gate in Fig.1 (c), T is a trigger event of which the occurrence would cause dependent components A, B, and C unusable.

(d) CSP gate: CSP gate allows modeling of the case where the spares stay at an unpowered state when the primary event operates normally. That is to say cold spares never fail before the ones to its left. Hence, the failure behavior of CSP gate is similar to SEQ gate. For the CSP gate in Fig.1 (d), as A as the primary event fails first, then the first cold spare B fails, at last the second cold spare C fails.

(e) WSP gate: Unlike CSP gate, the spares in WSP gate operate at a reduced power when the primary event operates successfully. It means that warm spares can fail independently in standby state and all of the possible failure sequences may occur.

(f) HSP gate: In a HSP gate, the spares run at a full power when the primary event operates normally. Its failure behaviors are logically equivalent to static AND gate.

2.2. Minimal Cut Sequence Set

In DFTs, the occurrence of the top event not only relies on the combinations of basic events, but also relies on their failure sequences. Apparently, traditional minimal cut set is unable to express such failure behaviors. To solve this problem, the concept of a minimal cut sequence (MCS) is first proposed by Tang and Dugan [21] to express the minimal failure sequence that leads to an occurrence of a DFT’s top event. As to a general MCS, it can be written as \( A_1 \rightarrow A_2 \rightarrow \cdots \rightarrow A_n \), where the capital letter \( A_i \) represents a basic event denoting an occurrence of a failure, and the symbol “\( \rightarrow \)” indicates the order of failure precedence, i.e., the left event failing before the right one. Hence, a specific MCS expresses what events and in what ways of failing sequences that leads to an occurrence of a DFT or a module. As mentioned in section 1.1, the failure of the spares always depends on the primary event. To reflect such dependence in a MCS expression, three special symbols are introduced as: \( \alpha A_j \), \( \alpha A_j \) and \( \alpha A_j \). The symbol \( \alpha A_j \) represents \( A_j \) fails as a cold spare of \( A_i \) and means \( A_j \) fails after \( A_i \), \( \alpha A_j \) denotes \( A_j \) fails as a warm spare of \( A_i \) in standby state and implies \( A_j \) fails before \( A_i \) fails, and \( \alpha A_j \) indicates \( A_j \) fails as a warm spare of \( A_i \) after replacing the faulty primary unit and implies \( A_j \) fails after \( A_i \). Obviously, as to a non-repairable DFT, the complete MCSs, i.e., minimal cut sequence set (MCSS), can characterize its failure logic. Supposing that a DFT has \( n \) MCSs, the system failure logic (SFL) can be expressed by:

\[
\text{SFL}_{\text{MCSS}} = \text{MCS}_1 \cup \text{MCS}_2 \cup \cdots \cup \text{MCS}_n = \bigcup_{i=1}^{n} \text{MCS}_i
\]

where, MCSs, represents the \( i \)-th MCS. Hence, for the WSP gate in Fig.1 (e), the SFL can be written as:

\[
\text{SFL}_{\text{MCSS}} = \{A \rightarrow \alpha A_B \rightarrow \alpha A_C \} \cup \{A \rightarrow \alpha A_C \rightarrow \alpha A_B \} \cup \{A \rightarrow \alpha A_B \rightarrow A \rightarrow \alpha A_C \} \cup \{\alpha A_B \rightarrow \alpha A_C \rightarrow A \} \cup \{\alpha A_C \rightarrow A \} \cup \{\alpha A_B \rightarrow \alpha A_C \} \cup \{\alpha A_C \rightarrow \alpha A_B \} \cup \{\alpha A_B \rightarrow A \}
\]
3. SFLD and SFR

3.1. Sequence Failure Logic Diagram

A specific MCS is just a logic relationship and only provide qualitative information. To reflect the inner failure mechanisms of a MCS, a sequence failure logic diagram (SFLD) is introduced which is a graphical description of a MCS. In a SFLD, the failure behavior of an event is expressed by its time to failure, the vertical axis represents the failure sequence of a specific MCS where each event is placed according to its position located in the considered MCS, and the horizontal axis indicates time. To illustrate such SFLD, a complex DFT is introduced in Fig. 2, where three typical dynamic gates are highly-coupled together.

Applying the inference rules presented in Ref. [13], the SFL of the considered DFT can be expressed as:

$$ SFL_{MCS} = \left( A \to A'B \to C \to \varepsilon D \right) \cup \left( C \to A \to A'B \to \varepsilon D \right) \cup \left( A'B \to A \to C \to \varepsilon D \right) $$

In this article, we use $\tau_X$ to represent the time-to-failure of $X$ in a working state at full power, and use $\tau_X$ to express the time-to-failure of $X$ in a standby state at a reduced power. Assume the system starts at $t=0$, and mission time is $t_m$. Take the first MCS $A\to A'B\to C\to \varepsilon D$ for example: $A$ starts at $t=0$, then fails in the region $(0, t_m)$; $B$ starts at $t=0$, first it must survive the primary $A$, and then fails after $A$ in working state; $C$ starts at $t=0$ as well, and then fails after $B$; $D$ starts after $C$ fails, and then fails before $t_m$. And its SFLD is drawn in Fig. 3.

3.2. Sequence Failure Region

In our previous paper [10], we put forward probabilistic model-based multi-integration formulas to quantify a GMCS and pointed out that the occurrence probability of a GMCS can be obtained by doing integration of the random variables over the valid sequential intervals referring to time to failure of components involved in a GMCS. That is, if and only if the events occur in their valid intervals that leads to occurrence of the considered GMCS. Hence, for a GMCS, such valid sequential intervals can be considered as a sequence failure region (SFR). As to a GMCS: $A_1\to A_2\to \cdots\to A_n$, the SFLD with a SFR is shown in Fig. 4.

The $R(\tau_{A_i})$ represents the valid failure region of $\tau_{A_i} ; a_{i}(1< i\leq n)$ denotes the start point of $A_i$ considering some components do not need to start at $t=0$, such as cold spares, and $0\leq a_{i}\leq t_m$. As discussed in Ref. [10], the $R(\tau_{A_i})$ can be always expressed by:

$$ R(\tau_{A_i}) = \left\{ \tau_{A_i} \mid 0 < \tau_{A_i} < t_m \right\} $$

$$ R(\tau_{A_2}) = \left\{ \tau_{A_2} \mid \phi_2(\tau_{A_1}, a_{2}, t_m) < \tau_{A_2} < \phi_2(\tau_{A_1}, a_{2}, t_m) \right\} $$

$$ R(\tau_{A_i}) = \left\{ \tau_{A_i} \mid \phi_i(\tau_{A_1}, \tau_{A_2}, \cdots, \tau_{A_{i-1}}, a_{i}, a_{i+1}, \cdots, a_{n}, t_m) < \tau_{A_i} \right\} $$

$$ \phi_i(\tau_{A_1}, \tau_{A_2}, \cdots, \tau_{A_{i-1}}, a_{i}, a_{i+1}, \cdots, a_{n}, t_m) $$

$$ 1 < i \leq n, $$

where $\phi_i/\phi_0$ is a linear expression representing the lower/upper boundary of $R(\tau_{A_i})$, and the explicit expressions of $\phi_i$ and $\phi_0$ are defined by the specific MCS. Note that the Eq. (4) never considers the cases where some warm spares fail after replacing the faulty primary units. For such cases, the reference [10] points out that it is okay to add prerequisites that the warm spares survive the faulty ones in a standby state. Supposing that $A_2$ is a warm spare of $A_1$, then the Eq. (4) should be rewritten as:

$$ R(\tau_{A_1}) = \left\{ \tau_{A_1} \mid 0 < \tau_{A_1} < t_m \right\} $$

$$ R(\tau_{A_2}) = \left\{ \tau_{A_2} \mid \phi_2(\tau_{A_1}, a_{2}, t_m) < \tau_{A_2} < \phi_2(\tau_{A_1}, a_{2}, t_m) \right\} $$

$$ R(\tau_{A_i}) = \left\{ \tau_{A_i} \mid \phi_i(\tau_{A_1}, \tau_{A_2}, \cdots, \tau_{A_{i-1}}, a_{i}, a_{i+1}, \cdots, a_{n}, t_m) < \tau_{A_i} \right\} $$

$$ 1 < i \leq n $$

Fig. 2. An illustrative example

Fig. 3. SFLD for A→[B→C→]D

Fig. 4. SFLD for a GMCS with a SFR
As to the MCS expressed by Eq. (4), the corresponding SFR can be expressed as:

$$\text{SFR}_{\lambda_1 \rightarrow \lambda_2 \cdots \rightarrow \lambda_n} = \left\{ \Omega_f \mid \bigcap_{i=1}^m R\left(\tau_{\lambda_i}\right) \right\},$$  \hspace{1cm} (6)

where the $\Omega_s$ indicates the failure region of the considered MCS. And for the MCS expressed by Eq. (5), the failure region can be represented by:

$$\text{SFR}_{\lambda_1 \rightarrow \lambda_2 \cdots \rightarrow \lambda_n} = \left\{ \Omega_f \mid R\left(\tau_{\lambda_i}\right) \bigcap_{i=1}^m R\left(\tau_{\lambda_i}\right) \right\}. \hspace{1cm} (7)

For a general MCS with $k$ ($k<n$) warm spares failing in a working state at full power, its failure region can be also obtained inferentially from the Eq. (5). Here, we assume that a DFT has $m$ MCSs, and the sequence failure region of the $j$th MCS can be expressed as $\Omega_{j \rightarrow \lambda}$. According to the Eq. (1), the system sequence failure regions (SFRs) can be expressed as:

$$\text{SFRs}_{\text{system}} = \left\{ \Omega_{\text{sys}} \mid \bigcup_{j=1}^m \Omega_{j \rightarrow \lambda} \right\}, \hspace{1cm} (8)

where the $\Omega_{\text{sys}}$ represents the failure region of a system.

### 4. SFRs-based Numerical Simulation Approach

#### 4.1. Theoretical Foundation-CMC

The crude Monte Carlo (CMC) method is often used to study a probability problem with a statistical simulation through converting the analytical model under study into a probabilistic model. Given a set of variables sector $X=x_1, x_2, \ldots, x_n$, and $X \subseteq \mathbb{R}^n$ where $\mathbb{R}^n$ represents a $n$-dimensional real space, the failure probability of which the $X$ occur in the failure region $\Omega_s=\{x | g(x)<0\}$ can be calculated by:

$$P_f = \int_{-\infty}^{\infty} I\left[g(x)\right] f(X) dX, \hspace{1cm} (9)
$$

where $f(X)$ is the joint probability density function (PDF), and $I[g(X)]$ is an indicator function which is defined as:

$$I\left[g(X)\right] = \begin{cases} 1 & \text{if } g(X) < 0 \\ 0 & \text{others} \end{cases} \hspace{1cm} (10)
$$

However, the Eq. (9) cannot be solved analytically when the explicit inverse function of $f(X)$ does not exist. Thanks to the rule of large numbers, the $P_f$ can be evaluated approximately by a statistical simulation approach, i.e., CMC method, using the following statistical expression:

$$\widehat{P}_f = \frac{1}{N} \sum_{i=1}^N I\left[g(X)\right] \hspace{1cm} (11)
$$

Based on the Central Limit Theorem, the following equation must hold for any nonnegative number $x$:

$$\lim_{N \to \infty} P\left(\frac{\widehat{P}_f - P_f}{\sqrt{\frac{\sigma^2_{\widehat{P}_f}}{N}}} < x\right) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-\frac{t^2}{2}} dt, \hspace{1cm} (12)
$$

where $\sigma^2_{\widehat{P}_f}$ is the variance of the $\widehat{P}_f$, and $\sigma^2_{\widehat{P}_f} = \frac{1}{N} \left(\widehat{P}_f \times \left(1 - \widehat{P}_f\right)\right)$. As $N$ is chosen large enough, we can get the approximate equation as:

$$\lim_{N \to \infty} P\left(\frac{\widehat{P}_f - P_f}{\sqrt{\frac{\sigma^2_{\widehat{P}_f}}{N}}} < x\right) = 1 - \alpha, \hspace{1cm} (13)
$$

where $(1-\alpha)$ is the confidence level. Then, the absolute error for the $\widehat{P}_f$ can be evaluated by:

$$e_a = \left|P_f - \hat{P}_f\right| \leq \frac{z_{\alpha/2}}{\sqrt{N}} \frac{1}{\sqrt{P_f(1-P_f)}}, \hspace{1cm} (14)
$$

where the $z_{\alpha/2}$ is the quantile of the $\alpha/2$. And the relative error for the $\widehat{P}_f$ can be also expressed by:

$$e_r = \frac{\left|P_f - \hat{P}_f\right|}{P_f} \leq \frac{z_{\alpha/2}}{\sqrt{N}} \frac{1}{\sqrt{P_f}} \hspace{1cm} (15)
$$

Considering $\hat{P}_f$ is a small amount, the simulation number $N$ is approximately expressed as:

$$N = \frac{z_{\alpha/2}^2}{P_f e_r^2} \hspace{1cm} (16)
$$

Obviously, given a relative error $e_r$ and a confidence level $(1-\alpha)$, the simulation number $N$ is inversly proportional to $\hat{P}_f$. In general, the value of $e_r$ is set as 0.1 and the confidence level is defined as 0.95, then the simulation number $N$ should be chosen as: $N = 384/\hat{P}_f$.

#### 4.2. SFRs-based CMC for a highly coupled DFT

To explain the proposed method, the GMCS indicated by Eq. (4) is considered once again. The analytical solution to the considered GMCS can be obtained using a sequential multi-integration by:

$$P_{\text{GMCS-f}} = \int_{R^{m+n}} I\left[I(h(r)) f(r) \right] \mathcal{d}r, \hspace{1cm} (17)
$$

Where $R^{m+n}$ represents a $m+n$-dimensional positive real space; $f(r)$ is the joint PDF; $f_j(\tau_{\lambda_j})$ is the PDF of $\tau_{\lambda_j}$; $I[h(r)]$ is the indicator function, and $I[h(r)]=1$ given $r \in \Omega_s$ (SFR), otherwise, $I[h(r)]=0$. Yet the primitive function $f_j(\tau_{\lambda_j})$ cannot be found explicitly in some cases, and the Eq. (17) is calculated numerically. Note that the numerical computation complexity would reach up O ($M^n$), where the $M$ is the number of equal slices of dividing $R_{\tau_{\lambda_j}}$. Hence, solving such $n$-embedded integral by numerical integration method is very time consuming, especially a result with a high accuracy is needed. In this section, a SFRs-based CMC for simulating the occurrence probability of GMCS is proposed. Suppose that the simulated sample
point for \( \tau = \{ \tau_A, \tau_B, \cdots, \tau_n \} \) is denoted as: 
\[ \hat{\tau} = \{ \tau_{A_1}, \tau_{A_2}, \cdots, \tau_{A_m} \} \] 
Then, the \( P_{GMCS,f} \) can be evaluated using the CMC method as:
\[ \widehat{P}_{GMCS,f} = \frac{1}{N} \sum_{i=1}^{N} \left[ I[h(\hat{\tau})] \right] \tag{18} \]
where the statistical indicator function (SIF) \( I[h(\hat{\tau})] \) is defined as:
\[ I[h(\hat{\tau})] = \begin{cases} 1 & \text{if } \tau_{A_1} \in R(\tau_{A_2}), \tau_{A_2} \in R(\tau_{A_3}), \cdots, \tau_{A_m} \in R(\tau_{A_n}), \\ 0 & \text{otherwise} \end{cases} \tag{19} \]

The simulated sample point \( \hat{\tau} \) can be obtained using a random sampling approach. Given that the cumulative distribution function (CDF) of \( \tau_{A_i} \) is \( F(\tau_{A_i}) \), then the \( \tau_{A_i} \) can be always expressed as:
\[ \tau_{A_i} = G(F(\tau_{A_i})) \tag{20} \]
And the sample point \( \tau_{A_i} \) can be sampled by
\[ \tau_{A_i} = G(\epsilon) \tag{21} \]
where \( \epsilon \) is a uniform random number used to replace \( F(\tau_{A_i}) \) in Eq. (20), and \( \epsilon \) can be obtained in \([0,1]\) by any standard random number generator.

Suppose that \( \tau_{A_i} \) follows the exponential distribution with a failure rate parameter \( \lambda \), and the \( f(\tau_{A_i}), F(\tau_{A_i}) \) of \( \tau_{A_i} \) provided by the following expressions:
\[ f(\tau_{A_i}) = \lambda e^{-\lambda \tau_{A_i}}, \quad F(\tau_{A_i}) = 1 - e^{-\lambda \tau_{A_i}}. \]
Then the \( \tau_{A_i} \) is expressed as a function of \( F(\tau_{A_i}) \), i.e., \( G(F(\tau_{A_i})) \).

\[ \tau_{A_i} = G(F(\tau_{A_i})) = \frac{1}{\lambda} \ln \frac{1}{1 - F(\tau_{A_i})}. \tag{22} \]

The simulation procedures for the SFRs-based CMC for a GMCS are shown in Algorithm 1.

**Algorithm 1.**

**Step 1.** Let the failure number \( N_{GMCS,f} = 0 \).

**Step 2.** Generate the sample point \( \hat{\tau} = \{ \hat{\tau}_{A_1}, \hat{\tau}_{A_2}, \cdots, \hat{\tau}_{A_n} \} \).

**Step 3.** Calculate \( I[h(\hat{\tau})] \).

**Step 4.** If \( I[h(\hat{\tau})] = 1 \), then \( N_{GMCS,f} = N_{GMCS,f} + 1 \).

**Step 5.** Transfer to Step 2 in case that the total simulated number does not equal a given \( N \).

**Step 6.** Output the occurrence probability of a given GMCS:
\[ \widehat{P}_{GMCS,f} = \frac{N_{GMCS,f}}{N}. \]

Now we will discuss how to simulate a highly coupled DFT. As mentioned in section 3.2, an occurrence of any MCS can lead to the failure of a considered highly coupled DFT, and system failure region can be expressed as: \( SFR_{system} = \{ \Omega_{sys} \cap \bigcup_{j=1}^{m} \Omega_j \} \). Given that the DFT under study is non-repairable, the system fails only once in its lifespan. That is to say at most one MCS occurs in a simulation. Given that a DFT has \( m \) MCSs and \( n \) input events. Then referring to the Algorithm 1 for a GMCS, the complete SFRs-based numerical simulation procedures for a highly coupled DFT are shown in Fig. 5, where the \( P_{sys,f} \) is the simulated unreliability of a considered system.

### 4.3. Validation Example

In this section, the illustrative example in Fig. 2 is considered for a validation purpose. In the first case, suppose that all of the components are exponentially time-to-failure distributed, and their failure parameters are listed in Table 1.

Table 1. Failure parameters of components in Fig. 2

<table>
<thead>
<tr>
<th>Component</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure rate (/h)</td>
<td>5.5e-3</td>
<td>1.0e-3</td>
<td>3.5e-3</td>
<td>5.0e-3</td>
</tr>
<tr>
<td>s*: the failure rate in a standby state.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a*: the failure rate in a working state.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Given the MCSS expressed by Eq. (3), the SFLD of each MCS with its SFR can be drawn. As an illustration, we present the specific SFLD of the third MCS with its SFR (Fig. 6), which represents the

![Fig. 6. SFLD of C——A→B→D](image-url)
most complex failure behavior. Note that the component B failing in working state means that the B must survive the primary A. That is to say \( T_B > T_A \). Hence, the SFR of the MCS can be expressed as \( \Omega = R(T_C) \cap R(T_A) \cap R(T_B) \cap R(T_D) \), where,

\[
R(T_A) = (T_A, +\infty), \\
R(T_B) = (0, T_B), \\
R(T_C) = (0, T_C), \\
R(T_D) = (T_D + T_C - T_A, T_D - T_C).
\]

Similarly, the specific SFRs for other MCSs are also obtained. Now we use the SFRs-based simulation method to evaluate the reliability of the considered example system. For a comparison purpose, the Markov-based approach is adopted as a benchmark. The results obtained by the two methods are shown in Fig. 7.

![Fig. 7. Comparisons of the results under exponential distributions](image)

With the simulation sample size \( N=100 \), the \( \varepsilon_r \) (relative error) of the results obtained by SFRs-based simulation and Markov-based approaches is notable. Yet with the increasing of \( N \), \( \varepsilon_r \) becomes smaller and smaller. As the simulation sample size reaches up \( 1.0e+4 \), the results derived from the two methods are matched.

Without loss of generality, the case with general distributions is also considered, where A follows the Weibull distribution with arguments \( (\mu=15, \beta=10) \), B is the exponential distribution \( (\delta=80) \), C follows the lognormal distributions with parameters \( (\mu=15, \delta=10) \) and D is the exponential distribution with failure rate \( 1.5e-2/h \). Given that the Markov approach is not applicable for non-exponential distribution situations, we adopt the IE-based method as a benchmark where each cut sequence is solved numerically. The results obtained at different mission times are listed in Table 2.

![Table 2 comparisons of results for general distributions](image)

<table>
<thead>
<tr>
<th>Mission time (h)</th>
<th>SFRs-based simulation method</th>
<th>IE-based method</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>0.014566</td>
<td>0.014932</td>
</tr>
<tr>
<td>200</td>
<td>0.046863</td>
<td>0.047943</td>
</tr>
<tr>
<td>300</td>
<td>0.064775</td>
<td>0.065541</td>
</tr>
<tr>
<td>400</td>
<td>0.075933</td>
<td>0.076180</td>
</tr>
<tr>
<td>500</td>
<td>0.083211</td>
<td>0.083529</td>
</tr>
</tbody>
</table>

Obviously, the results obtained by the SFRs-based simulation method are in good agreement with those derived by the IE-based method. For the computational efficiency, the average computing time for SFRs-based approach \( (N=1.0e+6) \) is about \( 3.09 mins \), yet the average computing time for IE-based method \( (N=100) \) reaches up \( 324.7 mins \). Hence compared with the IE-based method, the SFRs-based simulation approach is more efficient.

5. A case study

The WPS (water pumping system) is a critical-safety system for PWR (Pressurized Water Reactor) and it is used to carry of the reaction heat of reactor core by pumping coolant from the water source. If the system loses its function, it will cause a severe consequence. Hence, it is quite significant to analyze the reliability of the system. The system is operational requiring at least two pumps to be successful. The system consists of three pumps among which pump A and B are operating under normal circumstances, and C as a cold spare stays at an unpowered state. Once some pump fails, the pump C will be started by a switch D to replace the faulty one. The switch is controlled by a sensor system E which is used to detect the failure signal of the active pumps. As soon as a failure signal is received, the sensor system E will activate the cold spare C through controlling the switch D. Hence, the WSP fails if pump A or B fails after D or E fails. In addition, the sensor system E is dependent on the power suppliers P1 and P2 among which P1 is the primary supplier and P2 is a cold spare as P1. The simplified DFT model of the system is shown in Fig. 8.

![Fig. 8. Simplified DFT model of WPS system](image)

Given that the time to failure of pumps follows the lognormal distributions, the failure parameters are: mean: \( \mu_{A,B,C}=15 \), variances: \( \sigma_{A,B,C}=25 \), \( \sigma_{P1}=30 \), \( \sigma_{P2}=35 \). The switch D follows the uniform distribution in the lifespan \([0, 10^4 h]\). Power suppliers P1 and P2 are the Weibull distributions with the arguments: \( m_{P1}=2 \) (shape), \( \eta_{P1}=80 \) (scale); \( m_{P2}=2 \) (shape), \( \eta_{P2}=100 \) (scale), and the sensor system E is exponentially distributed with failure rate \( \lambda_E=1.0e-4 \). The system failure logic can be expressed using its MCSS by:

\[
\text{SFL}_{\text{MCSS}} = P_1 \rightarrow \left[ P_2 \rightarrow A \wedge P_1 \rightarrow P_2 \rightarrow B \vee D \rightarrow A \wedge B \right] \\
+ A \rightarrow C \wedge B \rightarrow C \wedge E \rightarrow A \wedge E \rightarrow B \wedge A \rightarrow B \wedge B \rightarrow A
\]

(23)

Considering that there exist non-exponential distributions in the considered system, Markov-based approaches are not longer applicable. The IE (inclusion-exclusion) formula would generates \( 2^{2^{10}}-1 \) \((1023)\) logic terms,
improve its efficiency, such as importance sampling [4, 22], adaptive importance sampling [16, 3], and etc.

Acknowledgment

The Authors would like to acknowledge the financial support by the National Science and Technology Major Project (2011ZX06004-024).

References


Daochuan GE
Dong LI
Meng LIN
Yan-hua YANG
School of Nuclear Science and Engineering
Shanghai Jiao Tong University
Shanghai 200240, China

Emails: gdch-2008@163.com, lidonghzkd1@126.com, linmeng@sjtu.edu.cn, yangyh@sjtu.edu.cn