Article citation info:
GE D, LI D, LIN M, YANG Y-H. SFRs-Based Numerical Simulation for the Reliability of Highly-coupled DFTs. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2015; 17 (2): 199–206, http://dx.doi.org/10.17531/ein.2015.2.5.

Daochuan GE
Dong LI
Meng LIN
Yan-Hua YANG

SFRS-BASED NUMERICAL SIMULATION FOR THE RELIABILITY OF HIGHLY-COUPLED DFTS

METODA SYMULACJI NUMERYCZNEJ OPARTA NA POJĘCIU ZAKRESÓW USZKODZEŃ SEKWENCYJNYCH SŁUŻĄCA DO OBLICZANIA NIEZAWODNOŚCI UKŁADÓW MODELOWANYCH METODĄ SILNIE SPRZĘŻONYCH DYNAMICZNYCH DRZEW BŁĘDÓW

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.*

Zachowania uszkodzeniowe wielu działających w rzeczywistości układów są bardzo złożone i zależą od sekwencji w jakiej występują uszkodzenia. Zachowania takie można modelować za pomocą silnie sprzężonych dynamicznych drzew błędów (DFT). Istniejące podejścia do rozwiązywania DFT, takie jak metody markowowskie oparte na pojęciu przestrzeni stanów i metody oparte na zasadzie włączeń i wyłączeń mają swoje ograniczenia:albo borykają się z problemem eksplozji przestrzeni stanów albo są narażone na eksplozję kombinatoryczną. Dodatkowo, podejścia markowowskie stają się niedostępne, gdy elementy składowe mają niewykładnicze rozkłady czasu do uszkodzenia, co ma miejsce w przeważającej części układów spotykanych w rzeczywistości. Aby przezwyciężyć mankamenty powyższych metod, zaproponowano metodę symulacji numerycznej opartą na pojęciu zakresów uszkodzeń sekwencyjnych (sequence failure regions, SFR). Proponowana metoda znajduje zastosowanie w modelowaniu systemów nienaprawialnych o elementach, które charakteryzuje arbitralnie przyjęty rozkład czasu do uszkodzenia. Metodę można stosować w modelowaniu opartym zarówno na uogólnionej sekwencji niezdatności (generalizedcut sequence), jak również silnie sprzężonych DFT. Wyniki uzyskane w przedstawionym przykładzie potwierdzają zasadność proponowanego przez nas podejścia.

Słowa kluczowe: *silnie sprzężone dynamiczne drzewo błędów, zakres uszkodzeń sekwencyjnych, arbitralnie przyjęty rozkład, symulacja numeryczna.*

1. Introduction

Dynamic fault trees have been presented [6, 7, 8] as an extension of traditional static fault trees with the aim to model complex systems having sequence- and function-dependent failure behaviors. Such modeling techniques are widely used in Nuclear Power Plant (NPP) industry, space mission systems and chemical process plant where systems safety is emphatically focused. The problem is how to quantify the reliability index of complex systems modeled by highly-coupled DFTs. Markov-based methods [1, 15, 19] have been proved to be efficient and versatile. But these approaches are subjected to the problem of "state space explosion". To mitigate the scale of the system state space to be considered, some hierarchical methods [11, 23, 24] (i.e., modularization techniques) are developed. Such hierarchical approaches can greatly reduce the Markov state space using a "divide and conquer" strategy under some circumstances. Yet these techniques become unfeasible when the independent sub-modules are placed under a dynamic gate. The IE-based approach [14, 18] is a combinatorial method based on enumerating the complete minimal cut sequences/sets (MCSs) of a considered DFT. In contrast to Markov-based methods, the IE-based approach is efficient since it does not require highly-coupled DFTs converted to state space forms. To calculate the reliability of a considered DFT, the complete minimal cut sequences/sets would be rewritten using the inclusion-exclusion principle. Given that a DFT has *n* MCSs, the IE formula would generate 2^n-1 logic products. Hence the IE-based approach is vulnerable to the problem of combinatorial explosion.

To overcome the shortcomings of existing methods mentioned above, sequence failure regions (SFR)-based 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.

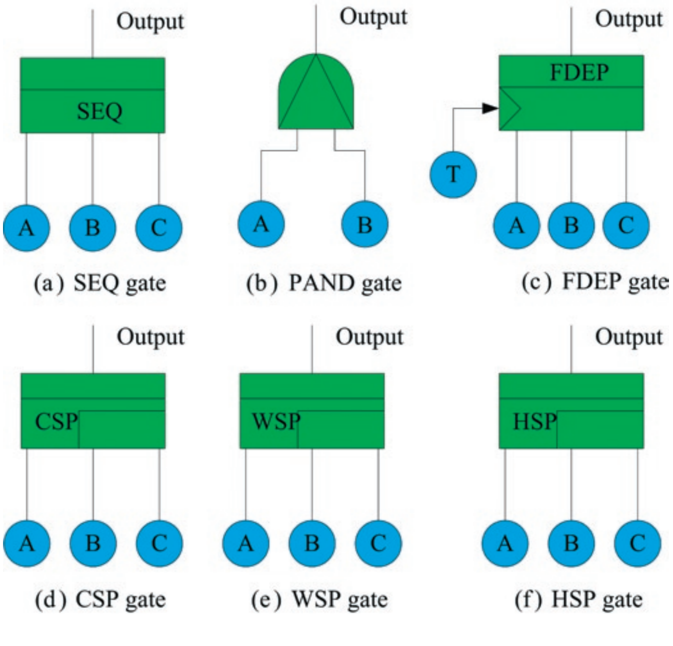

Fig. 1 Dynamic gates used in DFT

(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, the 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), 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 "→" 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: ${}^{0}_{A_i}A_j$, ${}^{\alpha}_{A_i}A_j$ and ${}^{1}_{A_i}A_j$. The symbol ${}^{0}_{A_i}A_j$ represents A_j fails as a cold spare of A_i and means A_j fails after A_i, ${}^{\alpha}_{A_i}A_j$ denotes A_j fails as a warm spare of A_i in standby state and implies A_j fails before A_i fails, and ${}^{1}_{A_i}A_j$ 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:

$$\begin{aligned} \mathrm{SFL}_{\mathrm{MCSS}} &= \mathrm{MCS}_1 \cup \mathrm{MCS}_2 \cup \cdots \cup \mathrm{MCS}_n \\ &= \bigcup_{i=1}^{n} \mathrm{MCS}_i \end{aligned} \tag{1}$$

where, MCS_i represents the i_{th} MCS. Hence, for the WSP gate in Fig.1 (e), the SFL can be written as:

$$\begin{aligned} \mathrm{SFL}_{\mathrm{MCSS}} = &\left(\mathrm{A} \rightarrow {}^{1}_{\mathrm{A}}\mathrm{B} \rightarrow {}^{1}_{\mathrm{B}}\mathrm{C}\right) \cup \left(\mathrm{A} \rightarrow {}^{\alpha}_{\mathrm{B}}\mathrm{C} \rightarrow {}^{1}_{\mathrm{A}}\mathrm{B}\right) \cup \left({}^{\alpha}_{\mathrm{A}}\mathrm{B} \rightarrow \mathrm{A} \rightarrow {}^{1}_{\mathrm{A}}\mathrm{C}\right) \\ &\cup \left({}^{\alpha}_{\mathrm{A}}\mathrm{B} \rightarrow {}^{\alpha}_{\mathrm{A}}\mathrm{C} \rightarrow \mathrm{A}\right) \cup \left({}^{\alpha}_{\mathrm{B}}\mathrm{C} \rightarrow \mathrm{A} \rightarrow {}^{1}_{\mathrm{A}}\mathrm{B}\right) \cup \left({}^{\alpha}_{\mathrm{B}}\mathrm{C} \rightarrow {}^{\alpha}_{\mathrm{A}}\mathrm{B} \rightarrow \mathrm{A}\right) \end{aligned} \tag{2}$$

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.

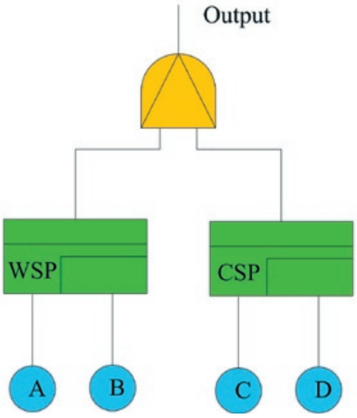

Fig. 2. An illustrative example

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

$$\begin{aligned}\mathrm{SFL_{MCSS}} = &\left(\mathrm{A} \to {}_{\mathrm{A}}^{1}\mathrm{B} \to \mathrm{C} \to {}_{C}^{0}\mathrm{D}\right) \cup \left(\mathrm{A} \to \mathrm{C} \to {}_{\mathrm{A}}^{1}\mathrm{B} \to {}_{C}^{0}\mathrm{D}\right)\\ &\cup \left(\mathrm{C} \to \mathrm{A} \to {}_{\mathrm{A}}^{1}\mathrm{B} \to {}_{C}^{0}\mathrm{D}\right) \cup \left({}_{\mathrm{A}}^{\alpha}\mathrm{B} \to \mathrm{A} \to \mathrm{C} \to {}_{C}^{0}\mathrm{D}\right)\\ &\cup \left({}_{\mathrm{A}}^{\alpha}\mathrm{B} \to \mathrm{C} \to \mathrm{A} \to {}_{C}^{0}\mathrm{D}\right) \cup \left(\mathrm{C} \to {}_{\mathrm{A}}^{\alpha}\mathrm{B} \to \mathrm{A} \to {}_{C}^{0}\mathrm{D}\right)\end{aligned} \quad (3)$$

In this article, we use τ_{X} to represent the time-to-failure of X in a working state at full power, and use $\overline{\tau_{\mathrm{X}}}$ 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→${}_{A}^{1}$B→C→${}_{C}^{0}$D for example: A starts at t=0, and then fails in the region (0, t_m); B also 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.

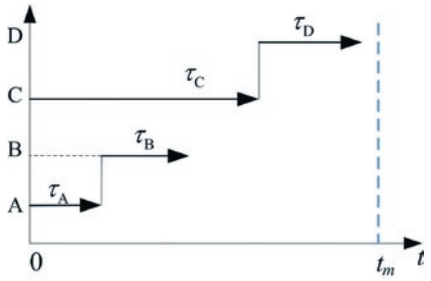

Fig. 3. SFLD for A→${}_{A}^{1}$B→C→${}_{C}^{0}$D

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→A_2→···→A_n, the SFLD with a SFR is shown in Fig. 4.

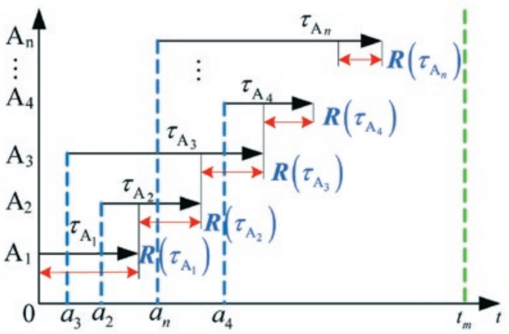

Fig. 4. SFLD for a GMCS with a SFR

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

$$\begin{aligned}&R\left(\tau_{\mathrm{A}_1}\right)=\left\{\tau_{\mathrm{A}_1} \mid\ 0<\tau_{\mathrm{A}_1}<t_m\right\}\\ &R\left(\tau_{\mathrm{A}_2}\right)=\left\{\tau_{\mathrm{A}_2} \mid\ \phi_2\left(\tau_{\mathrm{A}_1},a_2,t_m\right)<\tau_{\mathrm{A}_2}<\varphi_2\left(\tau_{\mathrm{A}_1},a_2,t_m\right)\right\}\\ &\qquad\vdots\\ &R\left(\tau_{\mathrm{A}_i}\right)=\left\{\tau_{\mathrm{A}_i} \mid\ \phi_i\left(\tau_{\mathrm{A}_1},\tau_{\mathrm{A}_2},\cdots,\tau_{\mathrm{A}_{i-1}},a_2,a_3,\cdots,a_{i1},t_m\right)<\tau_{\mathrm{A}_i}\right.\\ &\qquad\left.<\varphi_i\left(\tau_{\mathrm{A}_1},\tau_{\mathrm{A}_2},\cdots,\tau_{\mathrm{A}_{i-1}},a_2,a_3,\cdots,a_{i1},t_m\right)\right\} \qquad 1<i\le n,\end{aligned} \quad (4)$$

where ϕ_i/φ_i is a linear expression representing the lower/upper boundary of $R(\tau_{\mathrm{A_i}})$, and the explicit expressions of ϕ_i and φ_i 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:

$$\begin{aligned}&R\left(\tau_{\mathrm{A}_1}\right)=\left\{\ \tau_{\mathrm{A}_1} \mid\ 0<\tau_{\mathrm{A}_1}<t_m\right\}\\ &R\left(\overline{\tau_{\mathrm{A}_2}}\right)=\left\{\ \overline{\tau_{\mathrm{A}}} \mid\ \tau_{\mathrm{A}_1}<\overline{\tau_{\mathrm{A}}}<\infty\right\}\\ &R\left(\tau_{\mathrm{A}_2}\right)=\left\{\ \tau_{\mathrm{A}_2} \mid\ \phi_2\left(\tau_{\mathrm{A}_1},a_2,t_m\right)<\tau_{\mathrm{A}_2}<\varphi_2\left(\tau_{\mathrm{A}_1},a_2,t_m\right)\right\}\\ &\qquad\vdots\\ &R\left(\tau_{\mathrm{A}_i}\right)=\left\{\ \tau_{\mathrm{A}_i} \mid\ \phi_i\left(\tau_{\mathrm{A}_1},\tau_{\mathrm{A}_2},\cdots,\tau_{\mathrm{A}_{i-1}},a_2,a_3,\cdots,a_{i1},t_m\right)\right.\\ &\qquad\left.<\tau_{\mathrm{A}_i}<\varphi_i\left(\tau_{\mathrm{A}_1},\tau_{\mathrm{A}_2},\cdots,\tau_{\mathrm{A}_{i-1}},a_2,a_3,\cdots,a_{i1},t_m\right)\right\} \qquad 1<i\le n\end{aligned} \quad (5)$$

As to the MCS expressed by Eq. (4), the corresponding SFR can be expressed as:

$$\mathrm{SFR}_{\mathrm{A}_1\to\mathrm{A}_2\cdots\to\mathrm{A}_n}=\left\{\mathbf{\Omega}_f \mid \ \bigcap_{i=1}^{n} R\left(\tau_{\mathrm{A}_i}\right)\right\}, \tag{6}$$

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

$$\mathrm{SFR}_{\mathrm{A}_1\to{}_{\mathrm{A}_1}^{\,1}\mathrm{A}_2\cdots\to\mathrm{A}_n}=\left\{\mathbf{\Omega}_f \mid \ R\left(\overline{\tau_{\mathrm{A}_2}}\right)\bigcap_{i=1}^{n} R\left(\tau_{\mathrm{A}_i}\right)\right\}. \tag{7}$$

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 $\mathbf{\Omega}_{f-j}$. According to the Eq. (1), the system sequence failure regions (SFRs) can be expressed as:

$$\mathrm{SFRs}_{system}=\left\{\mathbf{\Omega}_{sys} \mid \ \bigcup_{j=1}^{m}\mathbf{\Omega}_{f-j}\right\}, \tag{8}$$

where the $\mathbf{\Omega}_{sys}$ 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 $\mathbf{X}=\{x_1, x_2, \ldots, x_n\}$, and $\mathbf{X}\subseteq \mathrm{R}^{(n)}$ where $\mathrm{R}^{(n)}$ represents a n-dimensional real space, the failure probability of which the $\mathbf{X}$ occur in the failure region $\mathbf{\Omega}_f=\{\mathbf{X}|\ g(\mathbf{X})<0\}$ can be calculated by:

$$P_f=\int_{-\infty}^{+\infty} I\left[g(\mathbf{X})\right] f(\mathbf{X}) d(\mathbf{X}), \tag{9}$$

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

$$I\left[g(\mathbf{X})\right]=\begin{cases}1 & g(\mathbf{X})<0\\ 0 & others\end{cases} \tag{10}$$

However, the Eq. (9) cannot be solved analytically when the explicit inverse function of $f(\mathbf{X})$ 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:

$$\widehat{P_f}=\frac{1}{N}\sum_{i=1}^{N} I\left[g(\mathbf{X})\right] \tag{11}$$

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

$$\lim_{N\to\infty} P\left(\frac{\left|P_f-\widehat{P_f}\right|}{\sigma_{\widehat{P_f}}^{2}}<x\right)=\frac{1}{\sqrt{2\pi}}\int_{-x}^{x} e^{-\frac{t^2}{2}}\,dt, \tag{12}$$

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

$$\lim_{N\to\infty} P\left(\left|P_f-\widehat{P_f}\right|<x\sqrt{\widehat{P_f}\cdot\left(1-\widehat{P_f}\right)\cdot {}^{1}\!/_{N}}\right)=1-\alpha, \tag{13}$$

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

$$\varepsilon_a=\left|P_f-\widehat{P_f}\right|\le z_{\alpha/2}\cdot\sqrt{\widehat{P_f}\cdot\left(1-\widehat{P_f}\right)\cdot {}^{1}\!/_{N}}, \tag{14}$$

where the $\mathrm{z}_{\alpha/2}$ is the quantile of the $\alpha/2$. And the relative error for the $\widehat{P_f}$ can be also expressed by:

$$\varepsilon_r=\frac{\left|P_f-\widehat{P_f}\right|}{P_f}\le z_{\alpha/2}\cdot\sqrt{\frac{1-\widehat{P_f}}{N\widehat{P_f}}} \tag{15}$$

Considering $\widehat{P_f}$ is a small amount, the simulation number N is approximately expressed as:

$$N\approx\frac{z_{\alpha/2}^{2}}{\widehat{P_f}\cdot\varepsilon_r^{2}} \tag{16}$$

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

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:

$$\begin{aligned}P_{GMCS\_f}&=\int_{R^{+(\mathrm{n})}} I\left[h(\tau)\right] f(\tau)d\tau\\&=\int_{R\left(\tau_{A_1}\right)} d\tau_{A_1}\int_{R\left(\tau_{A_2}\right)} d\tau_{A_2}\cdots\int_{R\left(\tau_{A_2}\right)}\prod_{i=1}^{n} f_i(\tau_{\mathrm{A}_i})d\tau_{A_n}\end{aligned} \tag{17}$$

Where $R^{+(n)}$ represents a n-dimensional positive real space; $f(\boldsymbol{\tau})$ is the joint PDF; $f_i(\tau_{\mathrm{A}_i})$ is the PDF of τ_{A_i}; $I[h(\boldsymbol{\tau})]$ is the indicator function, and $I[h(\boldsymbol{\tau})]=1$ given $\boldsymbol{\tau}\subseteq\mathbf{\Omega}_f$ (SFR), otherwise, $I[h(\boldsymbol{\tau})]=0$. Yet the primitive function $f_i(\tau_{\mathrm{A}_i})$ 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 $R_i(\tau_{\mathrm{A}_i})$. 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 $\tau=\left\{\tau_{A_1},\tau_{A_2},\cdots,\tau_{A_n}\right\}$ is denoted as: $\hat{\tau}=\left\{\widehat{\tau_{A_1}},\widehat{\tau_{A_2}},\cdots,\widehat{\tau_{A_n}}\right\}$. Then, the P_{GMCS_f} can be evaluated using the CMC method as:

$$\widehat{P}_{GMCS\_f}=\frac{1}{N}\sum_{i=1}^{N}I\left[h\left(\hat{\tau}\right)\right] \tag{18}$$

where the statistical indicator function (SIF) $I[h(\hat{\tau})]$ is defined as:

$$I\left[h\left(\hat{\tau}\right)\right]=\begin{cases}1 & \left(\widehat{\tau_{A_1}}\in R\left(\tau_{A_1}\right),\widehat{\tau_{A_2}}\in R\left(\tau_{A_2}\right),\cdots,\widehat{\tau_{A_n}}\in R\left(\tau_{A_n}\right)\right)\\ 0 & others\end{cases} \tag{19}$$

The simulated sample point $\hat{\tau}$ can be obtained using a random sampling approach. Given that the cumulative distribution function (CDF) of τ_{A_i} is $F\left(\tau_{A_i}\right)$, then the τ_{A_i} can be always expressed as:

$$\tau_{A_i}=G\left(F\left(\tau_{A_i}\right)\right) \tag{20}$$

And the sample point can be sampled by

$$\widehat{\tau_{A_i}}=G\left(\varepsilon\right) \tag{21}$$

where ε is a uniform random number used to replace $F(\tau_{A_i})$ in Eq. (20), and ε can be obtained in [0,1] by any standard random number generator.

Suppose that τ_{A_i} follows the exponential distribution with a failure rate parameter λ, and the $f(\tau_{A_i})$, $F(\tau_{A_i})$ of τ_{A_i} provided by the following expressions:

$$f\left(\tau_{A_i}\right)=\lambda e^{-\lambda\cdot\tau_{A_i}},$$

$$F\left(\tau_{A_i}\right)=1-e^{-\lambda\cdot\tau_{A_i}}.$$

Then the τ_{A_i} is expressed as a function of $F(\tau_{A_i})$, i.e., $G(F(\tau_{A_i}))$.

$$\tau_{A_1}=G\left(F\left(\tau_{A_i}\right)\right)=\frac{1}{\lambda}\ln\left(\frac{1}{1-F\left(\tau_{A_1}\right)}\right). \tag{22}$$

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 $\hat{\tau}=\left\{\widehat{\tau_{A_1}},\widehat{\tau_{A_2}},\cdots,\widehat{\tau_{A_n}}\right\}$.

Step 3. Calculate $I\left[h\left(\hat{\tau}\right)\right]$.

Step 4. If the $I\left[h\left(\hat{\tau}\right)\right]=1$, 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:

$$P_{GMCS\_f}=\frac{N_{GMCS\_f}}{N}.$$

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: $SFRs_{system}=\left\{\Omega_{sys}\mid\bigcap_{j=1}^{m}\Omega_j\right\}$. 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_{syst_f} is the simulated unreliability of a considered system.

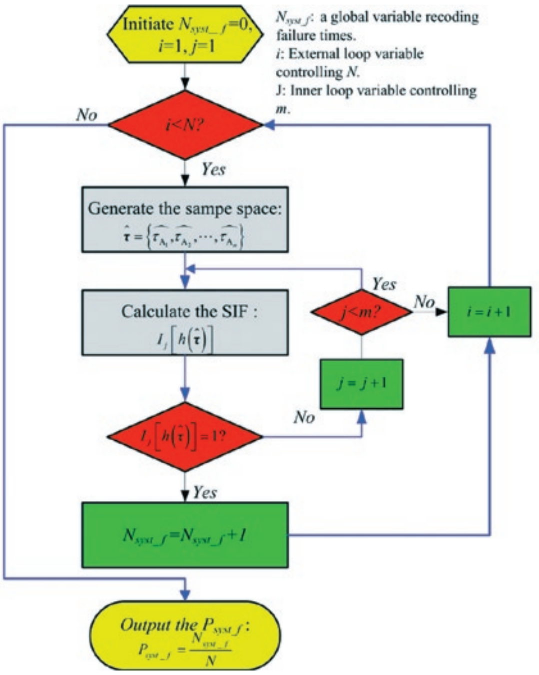
Initiate $N_{syst\_f}=0$, $i=1$, $j=1$
N_{syst_f}: a global variable recoding failure times.
i: External loop variable controlling N.
J: Inner loop variable controlling m.
No
$i<N$?
Yes
Generate the sampe space: $\hat{\tau}=\left\{\widehat{\tau_{A_1}},\widehat{\tau_{A_2}},\cdots,\widehat{\tau_{A_n}}\right\}$
Calculate the SIF : $I_j\left[h\left(\hat{\tau}\right)\right]$
Yes
$j<m$?
No
$i=i+1$
$j=j+1$
No
$I_j\left[h\left(\hat{\tau}\right)\right]=1$?
Yes
$N_{syst\_f}=N_{syst\_f}+1$
Output the P_{syst_f}: $P_{syst\_f}=\frac{N_{syst\_f}}{N}$

Fig. 5. Flow chart of SFRs-based CMC method for a highly coupled DFT

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

Component	A	B	C	D

Failure rate (/h)	5.5e-3	1.0e-3(s*)
		7.0e-3(a*)
			3.5e-3	5.0e-3

s*: the failure rate in a standby state.

a*: the failure rate in a working state.

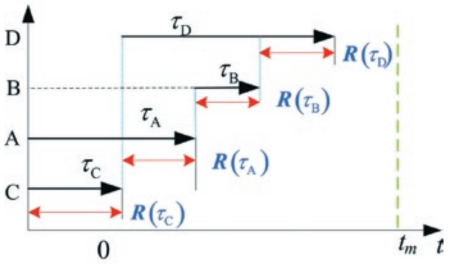

Fig. 6. SFLD of C→A→${}_{A}^{1}B$→${}_{C}^{0}D$

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 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 $\overline{\tau_B} > \tau_A$. Hence, the SFR of the MCS can be expressed as $\Omega_f = R(\tau_C) \cap R(\tau_A) \cap R(\overline{\tau_B}) \cap R(\tau_B) \cap R(\tau_D)$, where,

$$R(\tau_C) = (0,\ t_m),$$
$$R(\tau_A) = (\tau_C,\ t_m),\ R(\overline{\tau_B}) = (\tau_A, +\infty),$$
$$R(\tau_B) = (0, t_m - \tau_A),\ R(\tau_D) = (\tau_A + \tau_B - \tau_C, t_m - \tau_C).$$

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.

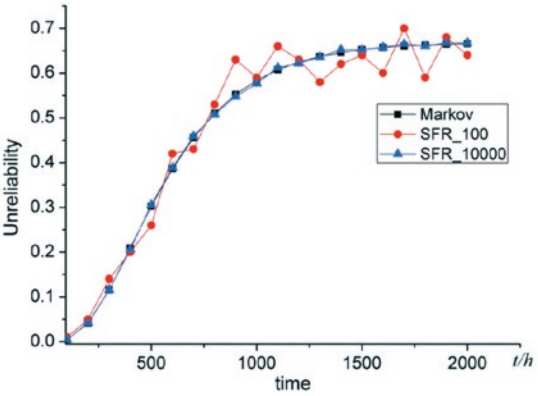

Fig. 7. Comparisons of the results under exponential distributions

With the simulation sample size *N*=100, the ε_r (relative error) of the results obtained by SFRs-based simulation and Markov-based approaches is notable. Yet with the increasing of *N*, ε_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 (shape: *m*=2, scale: *η*=80), B is the exponential distribution (s*=4.0e-3/h, a*=2.0e-2/h), C follows the lognormal distributions with parameters (*μ*=15, *δ*=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

Mission time (h)	SFRs-based simulation method	IE- based method
100	0.014566	0.014932
200	0.046863	0.047943
300	0.064775	0.065541
400	0.075933	0.076180
500	0.083211	0.083529

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 (M=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 P_1 and P_2 among which P_1 is the primary supplier and P_2 is a cold spare as P_1. The simplified DFT model of the system is shown in Fig. 8.

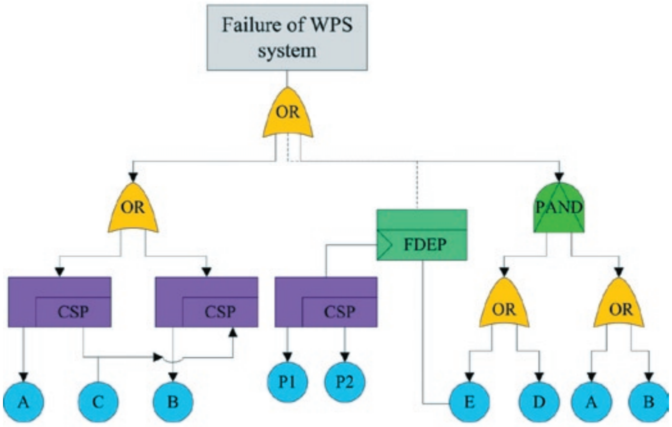

Fig. 8. Simplified DFT model of WPS system

Given that the time to failure of pumps follows the lognormal distributions, the failure parameters are: mean: $\mu_{A,B,C}$=15, variances: σ_A=25, σ_B=30, σ_C=35. The switch D follows the uniform distribution in the lifespan [0, 10^4 *h*]. Power suppliers P_1 and P_2 are the Weibull distributions with the arguments: m_{P_1}=2 (shape), η_{P_1}=80 (scale); m_{P_2}=2 (shape), η_{P_2}=100 (scale), and the sensor system E is exponentially distributed with failure rate λ_E=1.0e-4. The system failure logic can be expressed using its MCSS by:

$$\begin{aligned}\mathrm{SFL_{MCSS}} = {} & \mathrm{P_1} \rightarrow {}_{\mathrm{P_1}}^{0}\mathrm{P_2} \rightarrow \mathrm{A+P_1} \rightarrow {}_{\mathrm{P_1}}^{0}\mathrm{P_2} \rightarrow \mathrm{B+D} \rightarrow \mathrm{A+D} \rightarrow \mathrm{B} \\ & +\mathrm{A} \rightarrow {}_{\mathrm{A}}^{0}\mathrm{C+B} \rightarrow {}_{\mathrm{B}}^{0}\mathrm{C+E} \rightarrow \mathrm{A+E} \rightarrow \mathrm{B+A} \rightarrow \mathrm{B+B} \rightarrow \mathrm{A}\end{aligned} \tag{23}$$

Considering that there exist non-exponential distributions in the considered system, Markov-based approaches are not longer applicable. The IE-based method is suitable for such case, yet the IE (inclusion-exclusion) formula would generates 2^{10}-1 (1023) logic terms, *Table 3. the results obtained by SFR simulation*

Mission time	N_1=1.0e+4		N_2=1.0e+5		N_3=1.0e+6	
	Unreliability	Comp. time	Unreliability	Comp. time	Unreliability	Comp. time
500 (h)	0.3843	2.4s	0.3846	26.3s	0.3851	277.4s
1000 (h)	0.3938	2.2s	0.3935	20.5s	0.3932	274.5s
1500 (h)	0.3991	2.4s	0.3979	27.4s	0.3982	291.8s

and the logic terms should be further expanded into disjoint cut sequences as the repeated events appearing in different MCSs. Hence, to calculate the unreliability of the WPS system, the IE-based approach would produce tens of thousands cut sequences. It is a very tedious and error-prone process, and furthermore, as mentioned in section 4.2, the computational complexity to solve a cut sequence would reach up O (M^n). Hence, it is very time-consuming by applying the IE-based method. To make an efficient analysis of the system reliability, the SFRs-based simulation approach is applied. The results at different sampling sizes are listed in Table 3. Obviously, the SFRs-based simulation method can offer reasonable solutions efficiently.

6. Conclusion

In this paper, the SFRs-based numerical simulation approach is proposed to analyze a highly coupled DFT on its MCSS. This method is not only applicable for a DFT, but also applicable for a GMCS which is a significant contribution of this paper. The complete simulation procedures are provided. The results of the case study indicate the proposed method can offer reasonable solutions with an affordable computing time.

As to low probability events, the proposed method is time-consuming, which can be viewed as a disadvantage of this approach. In the feature work, we are focused on advanced sampling techniques to 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

1. Alam M, Al-Sagaf UM. Quantitative reliability evaluation of repairable phased-mission systems using Markov approach. IEEE Transactions on Reliability 1986; R-35(5):498-503, http://dx.doi.org/10.1109/TR.1986.4335529.
2. Alireza Ejlali, Seyed Ghassem Miremadi. FPGA-based Monte Carlo simulation for fault tree analysis. Microelectronic Reliability 2004; 44(6): 1017-1028, http://dx.doi.org/10.1016/j.microrel.2004.01.016.
3. Au SK, Beck JL. A new adaptive importance sampling scheme for reliability calculations. Structural Safety 1999; 21(2): 135-158, http://dx.doi.org/10.1016/S0167-4730(99)00014-.
4. Au SK, Beck JL. Important sampling in high Dimensions. Structural Safety, 2003; 25(2): 139-163, http://dx.doi.org/10.1016/S0167-4730(02)00047-4
5. Coppit D, Sullivan KJ, Dugan JB. Formal semantics of models for computational engineering: a case study on dynamic fault tree. Proceeding of the 11th International Symposium on Software Reliability Engineering 2000; 270-282.
6. Dugan JB, Bavuso SJ, Boyd MA. Dynamic fault-tree models for fault-tolerant computer systems. IEEE Transactions on Reliability 1992; 41(3): 363-377, http://dx.doi.org/10.1109/24.159800.
7. Dugan JB, Bavuso SJ, Boyd MA. Fault Trees and Sequence Dependencies. Proceedings of Annual Reliability and Maintenance Symposium 1990; 286-293, http://dx.doi.org/10.1109/ARMS.1990.67971.
8. Dugan JB, Sullivan KJ, Coppit D. Developing a low-cost high-quality software tool for dynamic fault-tree analysis. IEEE Transactions on Reliability 2000; 49(1): 49-59, http://dx.doi.org/10.1109/24.855536.
9. Dugra Rao K, Gopika V, Sanyasi Rao VVS, Kushwaha HS, Verma AK, Srividya A. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. Reliability Engineering and System Safety 2009; 94(4): 872–883, http://dx.doi.org/10.1016/j.ress.2008.09.007.
10. Ge D, Zhang R, Chou Q, Yang Y. Probabilistic model-based multi-integration formulas for quantifying a generalized minimal cut sequence. Proceedings of the institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 2014 (in press); DOI: 10.1177/1748006X14552004.
11. Gulati R, Dugan JB. A Modular Approach for Analyzing Static and Dynamic Fault Trees. Proceedings of Annual Reliability & Maintenance Symposium 1997; 57-63.
12. Liang X, Yi H, Zhang Y, Feng Z. Numerical simulation to reliability analysis of fault-tolerant repairable system. Journal of Shanghai Jiaotong University (Science) 2010; 15(5): 526-534, http://dx.doi.org/10.1007/s12204-010-1044-9.
13. Liu D, Xing W, Zhang C, et al. Cut sequence generation for fault tree analysis. Proceeding of the 4th International Conference on Embedded Software and Systems, 2007; 592–603, http://dx.doi.org/10.1007/978-3-540-72685-2_55.
14. Long W, Sato Y, Horigome M. Quantification of sequential failure logic for fault tree analysis. Reliability Engineering and System Safety 2000; 67(3): 269-274, http://dx.doi.org/10.1016/S0951-8320(99)00075-7.
15. Manian R, Dugan JB, Coppit D, Sullivan KJ. Combining various solution techniques for dynamic fault tree analysis of computer systems. Proceeding of the Third IEEE International High-Assurance System Engineering Symposium 1998; 21-28.
16. Oh M-S, Berger JO. Adaptive importance sampling in Monte Carlo integration. Journal of Statistical Computation and Simulation 1992; 4: 143-168, http://dx.doi.org/10.1080/00949659208810398.
17. Merle G, Roussel J-M, Lesage J-J. Algebraic determination of the structure functions of Dynamic Fault Trees. Reliability Engineering and

System Safety 2011; 96(2): 267–277, http://dx.doi.org/10.1016/j.ress.2010.10.001.
18. Merle G, Roussel J-M, Lesage J-J. Quantitative Analysis of Dynamic Fault Trees Based on the Structure Function, Quality and Reliability Engineering International 2014; 30(1): 143-156, http://dx.doi.org/10.1002/qre.1487.
19. Misra KB (Editor). Handbook of performability engineering. London: Springer-Verlag, 2008, http://dx.doi.org/10.1007/978-1-84800-131-2.
20. Shrestha M, Xing L, Xu H. Complete sequence set generation algorithm for reliability analysis of dynamic systems with sequence-dependent failures. Proceeding of the 16th ISSAT International Conference on Reliability and Quality in Design 2010; 382–386.
21. Tang Z, Dugan JB. Minimal cut set/sequence generation for dynamic fault trees. Proceedings of Annual Reliability and Maintenance Symposium 2004; 1-5.
22. Tokdar ST, Kass RE. Importance sampling: a review. Computational statistics 2010; 2(1): 54-60, http://dx.doi.org/10.1002/wics.56.
23. Xing L, Shrestha A, Meshkat L, Wang W. Incorporating Common-Cause Failures into the Modular Hierarchical Systems Analysis. Reliability, IEEE Transactions on 2009; 58(1):10-19, http://dx.doi.org/10.1109/TR.2008.2011855.
24. Yevkin O. An improved modular approach for dynamic fault tree analysis. Proceedings of Annual Reliability and Maintenance Symposium 2011; 1-5.
25. Yevkin O. An improved Monte Carlo method in fault tree analysis. Proceedings of Annual Reliability and Maintenance Symposium 2010; 1-5.

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