Quantification of Cut Sequence Set for Fault Tree Analysis

Dong Liu[1], Chunyuan Zhang[1], Weiyan Xing[2], Rui Li[1], and Haiyan Li[1]

[1] School of Computer, National University of Defense Technology, Changsha, Hunan 410073, China
{LD5M,zcy89969,lirui7777,lh_lee}.163.com
[2] China Huayin Ordnance Test Center, Huayin 714200, China
weiyan.xing@tom.com

Abstract. A new evaluation method is presented that employs cut sequence set (CSS) to analyze fault trees. A cut sequence is a set of basic events that fail in a specific order that can induce top event. CSS is the aggregate of all the cut sequences in a fault tree. The paper continues its former researches on CSS and uses CSS, composed of sequential failure expressions (SFE), to represent the occurrence of top event. According to the time relationships among the events in each SFE, SFE can be evaluated by different multi-integration formulas, and then the occurrence probability of top event can be obtained by summing up all the evaluation results of SFE. Approximate approaches are also put forward to simplify computation. At last, an example is used to illustrate the applications of CSS quantification. CSS and its quantification provide a new and compact approach to evaluate fault trees.

1 Introduction

Since the first use in 1960s, fault tree analysis has been widely accepted by reliability engineers and researchers for its advantages of compact structure and integrated analyzing methods. There have been many methods developed for the evaluation of fault trees (FT) [1]. With the development of computer technology, former static fault tree (SFT) analysis is not applicable to some new situations, because SFT can not handle the systems that are characterized by dynamic behaviors, Hence, Dugan et al [2] introduced some new dynamic gates, such as FDEP, CSP, PAND and SEQ gates, and put forward dynamic fault trees (DFT) to analyze dynamic systems. In DFT, top event relies on not only the combination of basic events, but also on their occurrence order. The dynamic behaviors bring the difficulty to evaluate DFT.

Fussell et al [3] firstly analyzed the sequential logic of PAND gate, where they provided a quantitive method for PAND gate with no repair mechanism.

Tang et al [4] introduced sequential failures into the traditional minimal cut set for DFT analysis, and provided the concept of minimal cut sequence. Minimal cut sequence is the minimal failure sequence that causes the occurrence of top event, and it is the extension of minimal cut set. However, [4] did not indicate how to extend minimal cut set to minimal cut sequence and did not make quantitive analysis.

Long et al [5] compared Fussell's method [3] with Markov model, and got the same result for PAND gate with three inputs. Then, in [6], Long et al presented the

R. Perrott et al. (Eds.): HPCC 2007, LNCS 4782, pp. 755–765, 2007.

concept of sequential failure logic (SFL) and its probability model (SFLM), by which the reliability of repairable dynamic systems are evaluated by multi-integration. SFLM reveals the thought that dynamic systems can be translated into SFL, but it does not provide an integrated method to solve general DFT.

Amari et al [7] introduced an efficient 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 explosion.

Our earlier work [8] indicated that cut sequence is intuitive to express the sequential failure behavior, and that it is an applicable way to make reliability analysis using cut sequence. So, in [8], we provided an integrated algorithm, named CSSA, to generate the cut sequence set (CSS), the aggregate of all cut sequences in DFT. This paper will continue our research and focuses on the quantification of CSS based on the analysis of SFLM. The purpose of the paper is to provide a new and compact quantification approach to calculate the reliability of dynamic systems.

Section 2 of this paper provides some concepts. Section 3 introduces the generation of CSS briefly. The quantification of CSS is detailed in section 4. In section 5, an example is used to illustrate our approach. And the conclusion is made in section 6.

2 Background and Concepts

2.1 Notation

x_i	an input to SFL.
λ_{x_i}	the failure rate of x_i.
μ_{x_i}	the repair rate of x_i.
τ_i	the duration of x_i in operation state.
τ_i'	the duration of x_i in warm standby state.
$F(t)$	the probability that top event occurs at time t.
α	the dormancy factor of warm standby component, and $0<\alpha<1$.
$f_{x_i}(t)$	the failure probability density of x_i in operation state.
$\overline{f_{x_i}}(t)$	the failure probability density of x_i in warm standby state.

2.2 Dynamic Fault Trees

Using dynamic gates, DFT obtain the ability to describe dynamic systems in a more feasible and flexible way. Fig. 1 shows the symbols of dynamic gates.

PAND gate is an extension of AND gate. Its input events must occur in a specific order. For example, if a PAND gate has two inputs, *A* and *B*, the output of the gate is true if:

- Both *A* and *B* have occurred, and
- *A* occurred before *B*.

FDEP gate has tree types of events:

- A trigger event: it is either a basic event or the output of another gate in the tree.

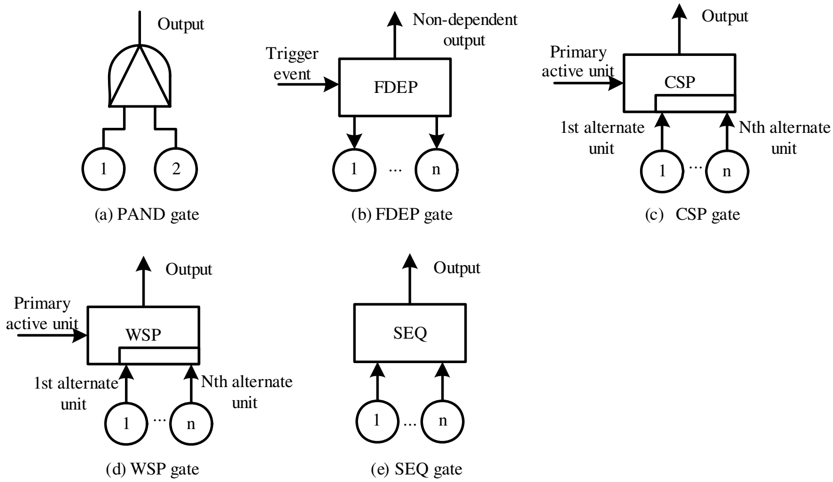

Fig. 1. Dynamic gates used in DFT

- A non-dependent output: it reflects the status of the trigger event.
- One or more dependent events: they functionally rely on the trigger event, which means that they will become inaccessible or unusable if the trigger event occurs.

CSP gate has a primary input and one or more alternate inputs. All inputs are basic events. The primary input is the one that is initially powered on, and the alternate input(s) specify the components that are used as the cold spare unit of the primary unit. The output of CSP gate becomes true if all inputs occur.

WSP gate is similar to CSP gate except that the alternate units in a WSP gate can fail independently before primary active unit.

SEQ gate forces events to occur in a particular order. The output of SEQ gate does not occur until all its inputs has occurred in the left-to-right order in which they appear under the gate. SEQ gate can be contrasted with PAND gate in that the inputs in PAND gate can occur in any order, whereas SEQ gate allows the events to occur only in a specified order. All the inputs, except the first one, of SEQ gate must be basic events, so, if the first input is a basic event, SEQ gate is the same to CSP gate.

2.3 Sequential Failure Logic Model

In SFLM [6], SFL is used to describe the failure relation among events. SFL is a qualitative expression of PAND gate. For example, if the inputs of SFL are x_1, x_2, …, x_n, respectively, the output will occur when x_1, x_2, …, x_n fail in a fixed sequence. If x_1 fails at time τ_1, and x_2 fails at time τ_2, …, x_n fails at time τ_n, where $\tau_1<\tau_2<\ldots<\tau_n$, the output of SFL will occur at τ_n. If x_i fails after x_j, where $i < j$, output will not occur.

Long et al used the following formula to provide the probability that the output of SFL occurs at time t:

$$F(t)=\int_0^t\int_{\tau_1}^t\cdots\int_{\tau_{n-1}}^t f_{x_1}(\tau_1)f_{x_2}(\tau_2)\cdots f_{x_n}(\tau_n)d\tau_n d\tau_{n-1}\cdots d\tau_1 \quad (1)$$

In formula (1), the multi-integration implies the probability that inputs remain in failed states after their failing in a particular sequence, and that the sequences by which the occurrence of the output is not generated are excluded.

In this paper, we suppose that components and system can not be repaired, and that τ_i' is independent to τ_i. Besides, we suppose that components are exponentially distributed, then, the failure probability density function of x_i in operation state is $f_{x_i}(t) = \lambda_{x_i} e^{-\lambda_{x_i} t}$, and the failure probability density function of x_i in warm standby state is $\overline{f_{x_i}}(t) = \lambda_{x_i} e^{-\alpha_{x_i} \lambda_{x_i} t}$.

3 Generation of CSS

Using dynamic gates, DFT gain the ability to describe dynamic systems in a more feasible and flexible way (refer to [2] for more information about DFT). The top event of DFT depends not only on the combination of basic events, but also on the failure sequence of basic events. Tang et al expended the concept of minimal cut set for static fault trees, and provided the concept of minimal cut sequence for DFT [4]. Compared to cut set, which does not consider the sequences among basic events, cut sequence is a basic event sequence that can result in the occurrence of top event in DFT. For example, cut sequence {*A*->*B*} means that top event will occur if event *A* fails before event *B*.

Therefore, the top event of DFT can be described in a format composed of basic events and their sequential relations. In [8], we defined a new symbol, sequential failure symbol (SFS) "→", to express the failure sequence of events.

Connecting two events, SFS indicates that the left event fails before the right event. SFS and its two events constitute sequential failure expression, SFE, such as $A \rightarrow B$, where *A* and *B* can be basic events or their combination. Several events can be chained by SFS. For example, $A \rightarrow B \rightarrow C$ indicates that *A*, *B* and *C* fail according to their positions in the expression, namely, *A* fails first, *B* fails next, and *C* fails last.

Using SFS, the top event of DFT can be expressed by SFE, which are actually cut sequences. And all the cut sequences constitute the CSS. If there are more than one cut sequences, CSS can be expressed by the logic OR of some SFE.

For the AND gate that has *n* inputs, *n*! SFE can be obtained. For example, if the structure function of a fault tree is $\Phi = ABC$, it has 3! = 6 SFE, namely

$$\begin{aligned} CSS = \{ & (A \rightarrow B \rightarrow C) \cup (A \rightarrow C \rightarrow B) \cup (B \rightarrow A \rightarrow C) \cup \\ & (B \rightarrow C \rightarrow A) \cup (C \rightarrow A \rightarrow B) \cup (C \rightarrow B \rightarrow A) \} \end{aligned} \quad (2)$$

It is relatively simpler to get the CSS of a PAND gate, since we can use SFS to connect its inputs according to their sequence. For example, if a fault tree has the structure function $\Phi = A$ PAND *B* PAND *C*, its CSS is $\{A \rightarrow B \rightarrow C\}$.

The CSS generation for FDEP gates needs to be considered carefully, since it depends on two conditions, i.e., the condition that trigger event occurs and the condition that trigger event does not occur. Let E_1 denote the trigger event of a FDEP gate. If E_1 occurs, this means that all its dependent events are forced to occur. In this condition, we can analyze the fault tree and get one or more result SFE, which are denoted by E_2. If E_1 does not occur, we can also get one or more SFE in the new condition, which is denoted by E_3. Then, the CSS of the fault tree is $(E_1 \cap E_2) \cup E_3$.

In order to get the CSS of CSP gate, a new expression is needed, i.e., ${}_A^0B$. ${}_A^0B$ means that B is a cold spare unit of A, and that B does not start to work until A fails. The failure rate of B is zero before A fails. We can use $A \rightarrow {}_A^0B$ to express the failure relation between A and B, where B is a cold spare unit of A.

WSP gate is similar to CSP gate except that the alternate units in a WSP gate can fail independently before primary active unit. In order to show this kind of relation, additional two concepts are used: ${}_A^\alpha B$ and ${}^\alpha B$.

- ${}_A^\alpha B$ means that B is a warm spare unit of A, and that B do not turn to operate until A fails. The dormancy factor of B is α, which means that the failure rate of B is α times to its normal failure rate before A fails.
- ${}^\alpha B$ means that B fails independently and its dormancy factor is α before B fails.

Using the above two symbols, we can write down the SFE that express the dynamic behavior of WSP gate.

The detailed procedures about the CSS generation can be found in [8], where an integrated study of generating CSS for DFT is discussed.

4 Quantification of CSS

In this section, we will apply the analysis method about SFL introduced in [6] to SFE, and obtain a quantitive model for CSS.

Now that CSS is expressed by SFE, we can compute the occurrence probability of top event using the following formula:

$$\begin{aligned}\Pr(CSS) &= \Pr(SFE_1 \cup SFE_2 \cdots SFE_n) \\ &= \sum_{i=1}^{n} \Pr(SFE_i) - \sum_{i<j=2}^{n} \Pr(SFE_i \cap SFE_j) + \cdots + (-1)^{n-1} \Pr(SFE_1 \cap SFE_2 \cdots SFE_n)\end{aligned} \tag{3}$$

Each term of formula (3) can be decomposed recursively into one or several SFE. And eventually, the formula comes down to compute the probability of SFE set.

4.1 Quantification of Normal SFE

For AND, SEQ and PAND gates, their SFE can be expressed using SFE= $x_1 \rightarrow x_2 \rightarrow \ldots \rightarrow x_n$, the occurrence probability of which is

$$F(t) = \int_0^t \int_{\tau_1}^t \cdots \int_{\tau_{n-1}}^t \prod_{k=1}^{n} f_{x_k}(\tau_k) d\tau_n \cdots d\tau_1 = \int_0^t \int_{\tau_1}^t \cdots \int_{\tau_{n-1}}^t Q(\tau_1, \tau_2, \cdots, \tau_n) d\tau_n \cdots d\tau_1 \tag{4}$$

where

$$Q(\tau_1, \tau_2, \cdots, \tau_n) = \prod_{k=1}^{n} f_{x_k}(\tau_k) \tag{5}$$

Proof: SFE=$x_1 \rightarrow x_2 \rightarrow \ldots \rightarrow x_n$ means that x_j fails after x_i but before x_k, where $1 \le i < j < k \le n$. If x_i fails at time τ_i ($0 < \tau_i \le t$), we have $\tau_i < \tau_{i+1} \le t$. Therefore, the occurrence probability of SFE is

$$F(t) = \Pr\{0 < \tau_1 \le t, \tau_1 < \tau_2 \le t, \cdots, \tau_{n-1} < \tau_n \le t\} \tag{6}$$

From the conditional probability function, we have

$$\begin{aligned} F(t) = &\Pr\{\tau_{n-1} < \tau_n \le t \mid \tau_{n-2} < \tau_{n-1} \le t, \cdots, 0 < \tau_1 \le t\} \cdot \\ &\Pr\{\tau_{n-2} < \tau_{n-1} \le t \mid \tau_{n-3} < \tau_{n-2} \le t, \cdots, 0 < \tau_1 \le t\} \cdot \ldots \cdot \\ &\Pr\{\tau_1 < \tau_2 \le t \mid 0 < \tau_1 \le t\} \cdot \Pr\{0 < \tau_1 \le t\} \end{aligned} \tag{7}$$

Since

$$\begin{aligned} &\Pr\{0 < \tau_1 \le t\} = \int_0^t f_{x_1}(\tau_1) d\tau_1 \\ &\Pr\{\tau_{i-1} < \tau_i < t \mid \tau_{i-2} < \tau_{i-1} < t, \ldots, 0 < \tau_1 < t\} = \Pr\{\tau_{i-1} < \tau_i < t \mid \tau_{i-2} < \tau_{i-1} < t\} \\ &\qquad = \int_{\tau_{i-1}}^t f_{x_i}(\tau_i) d\tau_i \end{aligned} \tag{8}$$

we have the final expression:

$$\begin{aligned} F(t) &= \Pr\{\tau_{n-1} < \tau_n \le t \mid \tau_{n-2} < \tau_{n-1} \le t\} \cdot \Pr\{\tau_{n-2} < \tau_{n-1} \le t \mid \tau_{n-3} < \tau_{n-2} \le t\} \cdot \\ &\quad \ldots \cdot \Pr\{\tau_1 < \tau_2 \le t \mid 0 < \tau_1 \le t\} \cdot \Pr\{0 < \tau_1 \le t\} \\ &= \int_0^t \int_{\tau_1}^t \cdots \int_{\tau_{n-1}}^t \prod_{k=1}^n f_{x_k}(\tau_k) d\tau_n d\tau_{n-1} \cdots d\tau_1 \end{aligned} \tag{9}$$

If the event number is large, the evaluation of formula (4) is difficult to perform. Then, we can turn to an approximate way that divides time t into M intervals and use $h=t/M$ as the integration step (just like Amari's approach [7]). The result is

$$F(t) \approx \sum_{i_1=1}^{M} (\sum_{i_2=i_1}^{M} (\sum_{i_3=i_2}^{M} (\cdots \sum_{i_n=i_{n-1}}^{M} Q(i_1 h, i_2 h, \cdots, i_n h) h^n))) \tag{10}$$

4.2 Quantification of SFE for CSP Gates

For CSP gates, the SFE is $x_1 \underset{x_1}{\rightarrow} {}^0 x_2 \rightarrow \cdots \underset{x_{n-1}}{\rightarrow} {}^0 x_n$, the occurrence probability of which is

$$\begin{aligned} F(t) &= \int_0^t \int_0^{t-\tau_1} \int_0^{t-\tau_1-\tau_2} \cdots \int_0^{t-\tau_1-\tau_2-\cdots-\tau_{n-1}} \prod_{k=1}^n f_{x_k}(\tau_k) d\tau_n d\tau_{n-1} \cdots d\tau_1 \\ &= \int_0^t \int_0^{t-\tau_1} \int_0^{t-\tau_1-\tau_2} \cdots \int_0^{t-\tau_1-\tau_2-\cdots-\tau_{n-1}} Q(\tau_1, \tau_2, \cdots, \tau_n) d\tau_n d\tau_{n-1} \cdots d\tau_1 \end{aligned} \tag{11}$$

Proof: $x_1 \underset{x_1}{\rightarrow} {}^0 x_2 \rightarrow \cdots \underset{x_{n-1}}{\rightarrow} {}^0 x_n$ means that x_{i+1} does not start to work until x_i fails ($1 \le i \le n$). Therefore, the occurrence probability of SFE can be represented by

$$F(t) = \Pr\{\tau_1 + \tau_2 + \cdots \tau_n \le t\} \tag{12}$$

The probability can be computed by convolution function, which is

$$F(t) = \underset{\sum_{k=1}^n \tau_i \le t}{\int \ldots \int} \prod_{k=1}^n f_{x_k}(\tau_k) \tag{13}$$

The integral region is below the n-dimension hyperplane of $\sum_{k=1}^{n} \tau_i = t$. The iterated integral form is

$$F(t) = \int_0^t \int_0^{t-\tau_1} \int_0^{t-\tau_1-\tau_2} \cdots \int_0^{t-\tau_1-\tau_2-\cdots-\tau_{n-1}} \prod_{k=1}^{n} f_{x_k}(\tau_k) d\tau_n d\tau_{n-1} \cdots d\tau_1 \tag{14}$$

Thereby, we prove the formula (11). The approximation of formula (11) is

$$\begin{aligned} F(t) &\approx \sum_{i_1=1}^{M} (\sum_{i_2=1}^{M-i_1} (\sum_{i_3=1}^{M-i_1-i_2} \cdots \sum_{i_n=1}^{M-i_1-i_2-\cdots-i_{n-1}} (\prod_{k=1}^{n} f_{x_k}(i_k h) h^n))) \\ &= \sum_{i_1=1}^{M} (\sum_{i_2=1}^{M-i_1} (\sum_{i_3=1}^{M-i_1-i_2} \cdots \sum_{i_n=1}^{M-i_1-i_2-\cdots-i_{n-1}} Q(i_1 h, i_2 h, \cdots, i_n h) h^n) \end{aligned} \tag{15}$$

4.3 Quantification of SFE for WSP Gates

For a WSP gate, its corresponding SFE has two forms, namely,

$$SFE = E \xrightarrow[E]{\alpha_{x_1}} x_1 \xrightarrow[x_1]{\alpha_{x_2}} x_2 \cdots \xrightarrow[x_{n-1}]{\alpha_{x_2}} x_n \tag{16}$$

$$SFE = E \xrightarrow{\alpha_{y_1}} y_1 \xrightarrow[E]{\alpha_{x_1}} x_1 \rightarrow \cdots \xrightarrow{\alpha_{y_{m-1}}} y_{m-1} \xrightarrow{\alpha_{y_m}} y_m \xrightarrow[x_{n-1}]{\alpha_{x_n}} x_n \tag{17}$$

E is the trigger event of WSP gate, x_i is the component that fails after going to operation, and y_i is the component that fails independently in its warm standby state.

The occurrence probability of SFE (16) is

$$\begin{aligned} F(t) = &\int_0^t \int_0^{t-\tau_E} \int_0^{t-\tau_E-\tau_1} \cdots \int_0^{t-\tau_E-\tau_1-\cdots-\tau_{n-1}} G(\tau_1', \tau_2', \cdots \tau_n') \\ &\times Q(\tau_E, \tau_1, \cdots, \tau_n) d\tau_n d\tau_{n-1} \cdots d\tau_1 d\tau_E \end{aligned} \tag{18}$$

where

$$\begin{aligned} G(\tau_1', \tau_2', \cdots, \tau_n') &= \int_{\tau_E}^{\infty} \overline{f_{x_1}}(\tau_1') d\tau_1' \int_{\tau_E+\tau_1}^{\infty} \overline{f_{x_2}}(\tau_2') d\tau_2' \cdots \int_{\tau_E+\tau_1+\cdots+\tau_{n-1}}^{\infty} \overline{f_{x_n}}(\tau_n') d\tau_n' \\ &= (1 - \int_0^{\tau_E} \overline{f_{x_1}}(\tau_1') d\tau_1')(1 - \int_0^{\tau_E+\tau_1} \overline{f_{x_2}}(\tau_2') d\tau_2') \cdots (1 - \int_0^{\tau_E+\tau_1+\cdots+\tau_{n-1}} \overline{f_{x_n}}(\tau_n') d\tau_n') \end{aligned} \tag{19}$$

Proof: The time relationships of SFE (16) can be expressed by Fig. 2. Therefore, its occurrence probability can be expressed by

$$\begin{aligned} F(t) = \Pr\{ &\tau_E + \tau_1 + \cdots + \tau_n \le t, \\ &\tau_1' > \tau_E, \tau_2' > \tau_E + \tau_1, \cdots, \tau_n' > \tau_E + \tau_1 + \cdots + \tau_{n-1} \} \end{aligned} \tag{20}$$

It easy to get the following probability

$$\Pr\{\tau_1' > \tau_E, \tau_2' > \tau_E + \tau_1, \cdots, \tau_n' > \tau_E + \tau_1 + \cdots + \tau_{n-1}\} = G(\tau_1', \tau_2', \cdots, \tau_n') \tag{21}$$

Since the duration in warm standby state for a component is independent to that in operation state, utilizing formula (11), we have the final equation:

$$\begin{aligned} F(t) = &\int_0^t \int_0^{t-\tau_E} \int_0^{t-\tau_E-\tau_1} \cdots \int_0^{t-\tau_E-\tau_1-\cdots-\tau_{n-1}} G(\tau_1', \tau_2', \cdots \tau_n') \\ &\times Q(\tau_E, \tau_1, \cdots, \tau_n) d\tau_n d\tau_{n-1} \cdots d\tau_1 d\tau_E \end{aligned} \tag{22}$$

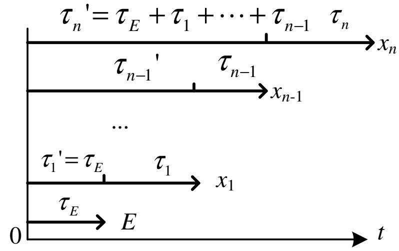

Fig. 2. Time relationships in $SFE = E \xrightarrow[E]{\alpha_{x_1}} x_1 \xrightarrow[x_1]{\alpha_{x_2}} x_2 \cdots \xrightarrow[x_{n-1}]{\alpha_{x_2}} x_n$

The approximation of formula (18) is

$$F(t) \approx \sum_{i_E=1}^{M} \Big(\sum_{i_1=1}^{M-i_E} \Big(\sum_{i_2=1}^{M-i_E-i_1} \cdots \sum_{i_n=1}^{M-i_E-i_1-\cdots-i_{n-1}} G \cdot Q(i_E h, i_1 h, \cdots, i_n h) h^{n+1} \Big)\Big) \tag{23}$$

where

$$G = (1 - \sum_{i_1'=1}^{i_E} \overline{f_{x_1}}(i_1' h)h)(1 - \sum_{i_2'=1}^{i_E+i_1} \overline{f_{x_2}}(i_2' h)h) \cdots (1 - \sum_{i_n'=1}^{i_E+i_1+\cdots+i_{n-1}} \overline{f_{x_n}}(i_n' h)h) \tag{24}$$

SFE (17) also derives from WSP gates, where y_1, y_2, …, y_n fail independently and x_1, x_2, …, x_m are warm spare units that fail in a fixed sequence. Let σ_i' denote the duration of y_i in warm standby state, then the occurrence probability of SFE (17) is

$$\begin{aligned} F(t) = & \int_0^t \int_0^{t-\tau_E} \int_0^{t-\tau_E-\tau_1} \cdots \int_0^{t-\tau_E-\tau_1-\cdots-\tau_{n-1}} G(\tau_1', \tau_2', \cdots \tau_n') \\ & \times Q(\tau_E, \tau_1, \cdots, \tau_n) K(\sigma_1', \sigma_2', \cdots, \sigma_m') d\tau_E d\tau_1 d\tau_2 \cdots d\tau_n \end{aligned} \tag{25}$$

where

$$K(\sigma_1', \sigma_2', \cdots, \sigma_m') = \int_{\tau_E}^{\tau_1+\tau_E} \overline{f_{y_1}}(\sigma_1') d\sigma_1' \cdots \int_{\sigma_{m-1}'}^{\tau_n+\tau_{n-1}+\cdots+\tau_1+\tau_E} \overline{f_{y_m}}(\sigma_m') d\sigma_m' \tag{26}$$

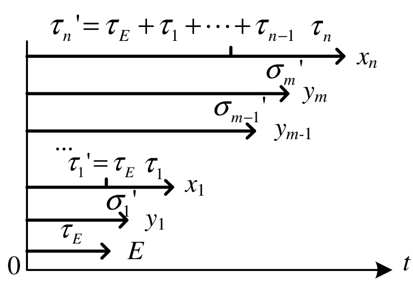

Fig. 3. Time relationships in SFE= $E \xrightarrow{\alpha_{y_1}} y_1 \xrightarrow[E]{\alpha_{x_1}} x_1 \to \cdots \xrightarrow{\alpha_{y_{m-1}}} y_{m-1} \xrightarrow{\alpha_{y_m}} y_m \xrightarrow[x_{n-1}]{\alpha_{x_n}} x_n$

Proof: The time relationship among the events in the SFE is shown in Fig. 3. Therefore, the probability of the SFE can be expressed by

$$F(t) = \Pr\{\tau_E + \tau_1 + \cdots + \tau_n \le t, \tau_1' > \tau_E, \cdots, \tau_n' > \tau_E + \tau_1 + \cdots + \tau_{n-1}, \\ \tau_E < \sigma_1' \le \tau_1 + \tau_E, \cdots, \sigma_{m-1}' < \sigma_m' \le \tau_n + \tau_{n-1} + \cdots + \tau_1 + \tau_E\} \tag{27}$$

It easy to get the following probability

$$\Pr\{\tau_E < \sigma_1' \le \tau_1 + \tau_E, \cdots, \sigma_{m-1}' < \sigma_m' \le \tau_n + \tau_{n-1} + \cdots + \tau_1 + \tau_E\} \\ = K(\sigma_1', \sigma_2', \cdots, \sigma_m') \tag{28}$$

Therefore, utilizing formula (18), we have the final equation (25).

The approximation of formula (25) is

$$F(t) \approx \sum_{i_E=1}^{M} \Big(\sum_{i_1=1}^{M-i_E} \Big(\sum_{i_2=1}^{M-i_E-i_1} \cdots \sum_{i_n=1}^{M-i_E-i_1-\cdots-i_{n-1}} G \cdot Q(i_E h, i_1 h, \cdots, i_n h) \cdot K \cdot h^{n+1} \Big)\Big) \tag{29}$$

where

$$K = \sum_{k_1=i_E}^{i_E+i_1} \cdots \sum_{k_m=k_{m-1}}^{i_E+i_1+\cdots+i_n} \overline{f_{y_1}}(k_1 h) \cdots \overline{f_{y_m}}(k_m h) h^m \tag{30}$$

For any SFE that describes event sequential failures, it has a general formation like

$$z_1 \to z_2 \xrightarrow{\alpha_{y_1}} y_1 \to E \xrightarrow{\alpha_{y_2}} y_2 \xrightarrow[E]{\alpha_{x_1}} x_1 \to \cdots z_p \xrightarrow{\alpha_{y_m}} y_m \xrightarrow[x_{n-1}]{\alpha_{x_n}} x_n \tag{31}$$

We can work out the probability of expression (31) using formula (25), and get its approximation using formula (29).

5 Case Study

In this section, we will present the quantification processes of CSS using a case system. The system is named Hypothetical Dynamic System, HDS.

HDS has four components, namely *A*, *B*, *C* and *S*. We would like to suppose that *A*, *B* and *C* are power supports of an equipment, and *S* is a switch that controls *C*. *C* is a cold spare unit that will take over *A* or *B* depending on which one fails first. If *S* fails before *A* or *B*, it will affect *C* that *C* can not switch into the system and thus can be thought failed. However, if *S* fails after it switches *C* into the system, it will no longer influence *C*. HDS requires at least two power supplies for operation. The fault tree of HDS is shown in Fig. 4, where FDEP gate indicates that its trigger event, which is the output of a PAND gate, will suspend *C*. The output of PAND gate becomes true if *S* fails before *A* or *B*.

The CSS of HDS is: [8]

$$CSS = \{(A \to B) \cup (A \xrightarrow[A]{0} C) \cup (B \xrightarrow[B]{0} C) \cup (B \to A) \cup (S \to A) \cup (S \to B)\} \\ \overset{\Delta}{=} \{SFE_1 \cup SFE_2 \cup SFE_3 \cup SFE_4 \cup SFE_5 \cup SFE_6\} \tag{32}$$

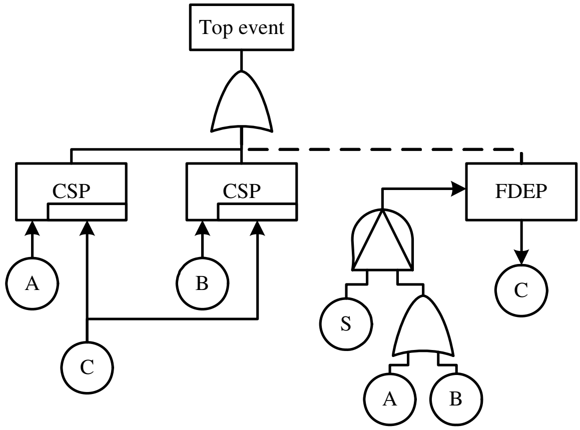

Fig. 4. The fault tree of HDS

The failure probability of HDS can be computed by the following formula:

$$\begin{aligned} F(t) &= \Pr(CSS) = \Pr(SFE_1 \cup SFE_2 \cdots SFE_6) \\ &= \sum_{i=1}^{6} \Pr(SFE_i) - \sum_{i<j=2}^{6} \Pr(SFE_i \cap SFE_j) + \sum_{i<j<k=3}^{6} \Pr(SFE_i \cap SFE_j \cap SFE_k) + \\ &\quad \cdots - \Pr(SFE_1 \cap SFE_2 \cdots SFE_6) \end{aligned} \tag{33}$$

SFE_1, SFE_4, SFE_5 and SFE_6 can be evaluated using formula (10) and SFE_2 and SFE_3 can be evaluated using formula (15).

All intersection results of $SFE_i \cap SFE_j$ are listed in Table 1. The probability of the SFE can be computed using formula (10), (15) or (29). From the conclusion in [6], we

Table 1. The results of $SFE_i \cap SFE_j$

$SFE_1 \cap SFE_2$	$(A \to B \to_A^0 C) \cup (A \to_A^0 C \to B)$	$SFE_2 \cap SFE_6$	$(S \to B \to A \to_A^0 C) \cup (A \to S \to B \to_A^0 C) \cup (A \to_A^0 C \to S \to B) \cup (S \to A \to B \to_A^0 C) \cup (S \to A \to_A^0 C \to B) \cup (A \to S \to_A^0 C \to B)$
$SFE_1 \cap SFE_3$	$(A \to B \to_B^0 C)$	$SFE_3 \cap SFE_4$	$(B \to_B^0 C \to A) \cup (B \to A \to_B^0 C)$
$SFE_1 \cap SFE_4$	Does not exist	$SFE_3 \cap SFE_5$	$(S \to A \to B \to_B^0 C) \cup (B \to S \to A \to_B^0 C) \cup (B \to_B^0 C \to S \to A) \cup (S \to B \to A \to_B^0 C) \cup (S \to B \to_B^0 C \to A) \cup (B \to S \to_B^0 C \to A)$
$SFE_1 \cap SFE_5$	$(S \to A \to B)$	$SFE_3 \cap SFE_6$	$(S \to B \to_B^0 C)$
$SFE_1 \cap SFE_6$	$(A \to S \to B) \cup (S \to A \to B)$	$SFE_4 \cap SFE_5$	$(B \to S \to A) \cup (S \to B \to A)$
$SFE_2 \cap SFE_3$	*	$SFE_4 \cap SFE_6$	$(S \to B \to A)$
$SFE_2 \cap SFE_4$	$(B \to A \to_A^0 C)$	$SFE_5 \cap SFE_6$	$(S \to A \to B) \cup (S \to B \to A)$
$SFE_2 \cap SFE_5$	$(S \to A \to_A^0 C)$		

Table 2. The unreliability of HDS

Time *t*[h]	*h*=10	*h*=1	Relex
300	0.0592	0.0496	0.0432
600	0.1548	0.1431	0.1395
1000	0.3152	0.2997	0.2947

can ignore the results of the third term and the latter terms in formula (33), because their values are very small.

Suppose that the components in HDS are exponential distributed and the failure rates are $\lambda_A=\lambda_B=0.0004$, $\lambda_C=0.0005$, $\lambda_S=0.0006$. We computed formula (33) using Matlab software given that $h=1$ and $h=10$ respectively. As a comparison, we also evaluated HDS using Relex software [9] that uses Markov model to solve dynamic gates. The unreliability of HDS for different time t is listed in Table 2. From the results, we can see that, with the decreasing of h, the evaluation result based on CSS becomes closer to that based on Markov model.

References

1. Amari, S.V., Akers, J.B.: Reliability analysis of large fault trees using the Vesely failure rate. In: Proceedings of Annual Symposium on Reliability and Maintainability, pp. 391–396 (2004)
2. Dugan, J.B., Bavuso, S., Boyd, M.: Dynamic fault tree models for fault tolerant computer systems. IEEE Transactions on Reliability 41, 363–377 (1992)
3. Fussell, J.B., Aber, E.F., Rahl, R.G.: On the quantitative analysis of priority-AND failure logic. IEEE Transactions on Reliability, 324–326 (1976)
4. Tang, Z., Dugan, J.B.: Minimal Cut Set/Sequence Generation for Dynamic Fault Trees. In: Proceedings of Annual Symposium on Reliability and Maintainability, LA (2004)
5. Long, W., Sato, Y.: A comparison between probabilistic models for quantification of priority-AND gates. In: Proc. PSAM-4, vol. 2, pp. 1215–1220 (1998)
6. Long, W., Sato, Y., Horigone, M.: Quantification of sequential failure logic for fault tree analysis. Reliability Engineering & System Safety 67, 269–274 (2000)
7. Amari, S., Dill, G., Howald, E.: A New Approach to Solve Dynamic Fault Trees. In: Proceedings of Annual Symposium on Reliability and Maintainability, pp. 374–379 (2003)
8. Liu, D., Xing, W., Zhang, C., et al.: Cut Sequence Set Generation for Fault Tree Analysis. In: Lee, Y.-H., et al. (eds.) ICESS 2007. LNCS, vol. 4523, pp. 592–603. Springer, Heidelberg (2007)
9. http://www.relex.com/