Liudong XING
Joanne Bechta DUGAN
Brock A. MORRISSETTE

EFEKTYWNA ANALIZA NIEZAWODNOŚCIOWA SYSTEMÓW Z PĘTLAMI ZALEŻNOŚCI FUNKCYJNYCH

EFFICIENT RELIABILITY ANALYSIS OF SYSTEMS WITH FUNCTIONAL DEPENDENCE LOOPS

Zależność funkcyjna zachodzi wtedy, gdy uszkodzenie jednego komponentu systemu prowadzi do niedostępności bądź nieużywalności innych komponentów w tym samym systemie. Zależności funkcyjne mogą tworzyć pętle. Tradycyjne podejścia do problemu pętli zależności funkcyjnych oparte są na modelach Markova, które są nieefektywne ze względu na dobrze znany problem eksplozji stanów. W niniejszym artykule przedstawiamy nowe, wydajne podejście analityczne do rozwiązywania pętli zależności funkcyjnych w analizie niezawodności systemów. Opierając się na strategii "dziel i rządź", podejście to umożliwia transformację systemu z pętlami zależności funkcyjnych w podsystemy bez zależności i bez pętli, które następnie można oceniać wykorzystując wydajne podejścia kombinatoryczne. Proponowane podejście można stosować do analizy systemów z komponentami o ogólnych rozkładach czasu do uszkodzenia. Podstawy i zalety proponowanego podejścia zilustrowano poprzez szczegółową analizę przykładu.

***Słowa kluczowe**: Zależność funkcyjna (FDEP), pętla, niezawodność, metoda transformacji, strategia dziel i rządź, dynamiczne drzewo uszkodzeń.*

Functional dependence occurs when the failure of one component causes other components within the same system to become inaccessible or unusable. And, amongst the functional dependencies there can be the existence of loops. Traditional approaches to handling functional dependence loops are based on Markov models, which are inefficient due to the well-known state space explosion problem. In this paper we propose a new and efficient analytical approach to handling functional dependence loops in the system reliability analysis. Based on the divide-and-conquer strategy, the approach transforms a system with functional dependence loops into subsystems without dependence or loops, which can then be evaluated using efficient combinatorial approaches. The proposed approach is applicable to analyzing systems with components having general time-to-failure distributions. The basics and advantages of the proposed approach are illustrated through a detailed analysis of an example.

***Keywords**: Functional dependence (FDEP), loop, reliability, transform method, divide-and-conquer, dynamic fault tree.*

1. Introduction

Functional dependence is a typical trait that occurs in many real-world systems. For example, when communication is achieved via a network interface card (NIC), the failure of the NIC makes the connected components inaccessible in the network [2]. For another example, in a computer system, peripheral devices are accessed through I/O controllers. If the I/O controller fails, the peripheral devices connected to it become unusable [5]. In general, functional dependence occurs when the failure of one component (referred to as the *trigger component*) causes other components (referred to as *dependent components*) within the same system to become inaccessible or unusable [2].

The functional dependence behavior can be modeled via a Functional DEPendence (FDEP) gate in the dynamic fault tree analysis [2,3]. As shown in Figure 1, the FDEP gate has a single trigger input, a non-dependent output reflecting the status of the input trigger event, and one or more dependent basic events. The trigger input can be either a basic event (representing the failure of a system component) or the output from another gate in the dynamic fault tree. When the trigger event occurs, all the dependent basic events are forced to occur. The separate occurrence of any of the dependent basic events has no effect on the trigger input. The FDEP gate has no logical output, thus it is connected to the top gate of the dynamic fault tree through a dashed line.

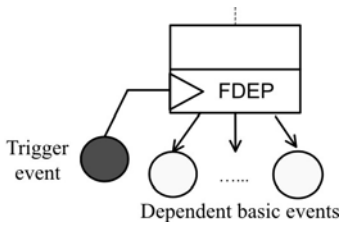

Fig. 1. The FDEP gate

The existing approaches for handling FDEP include an OR-gate replacement method and state-space-based approaches, in particular, continuous time Markov chain (CTMC)-based methods. In the OR-gate replacement method, the FDEP behavior is handled by replacing the FDEP gate with logic OR gate(s).

This is because each dependent component fails if it fails intrinsically, or if its trigger component fails. As an illustration, consider a system with FDEP represented in the dynamic fault tree model of Figure 2. Figure 3 shows the equivalent fault tree model after replacing the FDEP gate in Figure 2 with two OR gates, one for each dependent component. As a consequence of this OR-gate replacement, systems with FDEP can be analyzed using efficient combinatorial approaches for the dynamic fault tree analysis, such as inclusion-exclusion or sum-of-disjoint products based on minimal cut/path sets, and binary decision diagrams (BDD) [2]. However, the OR-gate replacement approach is limited to analyzing systems with perfect fault recovery mechanism and without FDEP loops.

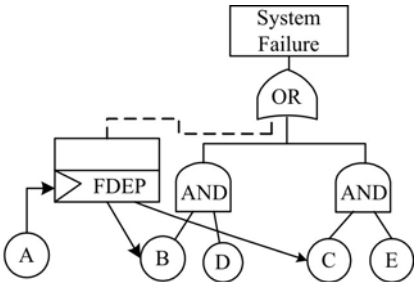

Fig. 2. Original dynamic fault tree with FDEP

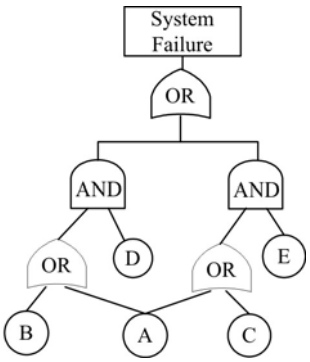

Fig. 3. Fault tree after OR-gate replacement

Amongst the functional dependencies there can be the existence of loops. That is, *A* brings down *B* which brings down *C* which can bring down *A* (Figure 4). In the case of loops existing in the dependencies, the OR-gate replacement method will not work because the loops represent feedback paths that fail most Boolean logic representation. In other words, if you try to do the OR-gate replacement, you will have loops between inputs and outputs of the OR gate that replaces the FDEP gate.

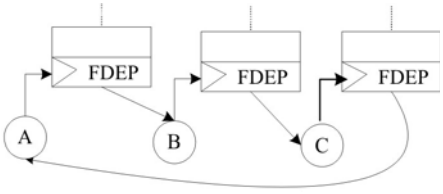

Fig. 4. An example of FDEP loops

The CTMC-based method is the existing approach for dealing with FDEP loops in the system reliability analysis. Unfortunately, the Markov-based method has a significant disadvantage that the model size grows exponentially as the size of the system increases. An illustration of this state-explosion problem is given in Section 4. The rapid growth of the number of states often leads to models that are computationally intensive and even intractable. Therefore, the CTMC-based methods can offer exact solution to the analysis of systems with only very limited size. Furthermore, the CTMC-based methods are typically not able to handle non-exponential time-to-failure distributions for trigger components and dependent components of FDEP.

To overcome the above mentioned problems of the existing methods, we propose a new and efficient method to the reliability analysis of systems with FDEP loops. The proposed method is combinatorial, and can be applicable to analyzing systems with general time-to-failure distributions.

The reminder of the paper is organized as follows: Section 2 presents our proposed approach for efficiently handling FDEP loops. In Section 3, a case study is performed to illustrate the application and advantages of the proposed combinatorial approach. Section 4 discusses the proposed method in comparison to the Markov-based approach. In the last section, we present our conclusions as well as directions for future work.

2. The Proposed Combinatorial Approach

Various transform methods have been used by mathematicians to simplify the calculation of probabilistic measures [1]. As an example, the logarithm function is one of the first transform methods used successfully. Using the identity of log (A*B) = log A + log B, the problem of multiplying two large numbers can be converted to a simpler problem of adding two small numbers. Motivated by this simple, yet insightful idea and based on the divide-and-conquer strategy, we propose to transform the original reliability problem involving FDEP loops into multiple reduced problems without FDEP or loops. The resultant reduced problems can be solved efficiently without using the inefficient Markov-based methods. The final solution can be obtained by integrating results of these reduced problems based on the total probability theorem.

Note that in this work we assume that if the system considered is a fault-tolerant system, then the system's fault recovery mechanism is perfect, *i.e.*, the system has perfect fault coverage. Also, we assume that the system is not subject to other dynamic behaviors such as sequence dependence, priorities, warm spares, and cold spares. Addressing FDEP in imperfect fault coverage systems as well as systems with those other dynamic behaviors is part of our future work.

In the following, the proposed combinatorial transformation method for handling FDEP loops is detailed as a three-step algorithm.

Step 1: Build a dependent trigger event (DTE) space. Assume a system with FDEP involves *m* trigger events (denoted by T_i, i=1…m). Based on these *m* elementary trigger events, we define a set of 2^m collectively exhaustive and mutually exclusive combined events that can occur in the system. Those combined events are termed as *dependent trigger events* (DTE) in this work. In particular, each DTE is a distinct and disjoint combination of elementary trigger events:

$$DTE_1 = \overline{T_1} \cap \overline{T_2} \cap ... \cap \overline{T_m},$$
$$DTE_2 = T_1 \cap \overline{T_2} \cap ... \cap \overline{T_m},$$
$$\dots\dots,$$
$$DTE_{2^m} = T_1 \cap T_2 \cap ... \cap T_m.$$

The complete set of DTE is termed as a "DTE space". The occurrence probability of DTE_i denoted by Pr(DTE_i) can be easily calculated based on the occurrence probability of elementary trigger events, as illustrated in the example analysis in Section 3.

Step 2: Generate and solve reduced problems. Based on the DTE space built in Step 1 and the total probability theorem [1], the occurrence probability of the event of the system failure, *i.e.*, the system unreliability can be calculated as Eq. (1).

$$U_{sys} = \sum_{i=1}^{2^m} [\Pr(\text{system fails}|DTE_i) \bullet \Pr(DTE_i)] \quad (1)$$

Using Eq. (1), the reliability problem for a system with FDEP loops is transformed into 2^m reduced reliability problems, Pr(system fails|DTE_i). To evaluate these reduced problems, it is necessary to obtain the fault tree model for each of them based on the original system dynamic fault tree model. The generation process of the reduced fault tree model is as follows:

1) Ignore all FDEP gates and the related trigger events.
2) Replace each basic event affected by DTE_i by a constant logic value '1' (True). Denote the set of components affected by DTE_i as S_{DTE_i}. And define a set of components that are functionally dependent on the same elementary trigger event as a functional dependence group (FDG). Then the set S_{DTE_i} can be obtained by performing the union operation on all related FDG whose corresponding trigger event(s) occur when the event DTE_i occurs. For example, consider a system with two elementary trigger events T_1 and T_2. For the event of $DTE_2 = \overline{T}1 \cap T_2$, the corresponding set S_{DTE_2} is simply FDG_{T_2} since the occurrence of DTE_2 implies the occurrence of T_2; for the event of $DTE_4 = T_1 \cap T_2$, the corresponding set S_{DTE_4} will be the union of FDG_{T_1}, FDG_{T_2}, and $FDG_{T_1 \cap T_2}$ (applicable when $T_1 \cap T_2$ serves as a trigger event of a FDEP gate) since the occurrence of DTE_4 implies the occurrence of both T_1 and T_2.
3) Apply a Boolean reduction to the system fault tree to generate a simpler fault tree in which all the components affected by DTE_i do not appear.

Note that a special treatment must be performed when some trigger events of FDEP gates in the original fault tree model also appear as basic events of other gates/parts of the system fault tree model. For example, the event *C* in Figure 5 serves as not only a trigger event of FDEP, but also an input event to the left AND gate. These events with two identities are termed as *dual events*. At this case, to generate the correct reduced fault tree model, in the above step 1) only the trigger event identity of a dual event will be ignored; the basic event identity of the dual event will be kept. In step 2) the basic event identity of the dual event will be replaced by a constant logic value '1' (*True*) if the event itself (e.g., *C*) appears in DTE_i; or by a constant logic value '0' (*False*) if the complement of the event (e.g., $\overline{C}$) appears in DTE_i.

The evaluation of the reduced fault tree models gives the solution to the reduced problems Pr(system fails|DTE_i). Note that since the effects of FDEP are out of picture, these reduced problems can be solved using efficient combinatorial methods, for example, the BDD-based method [2], [4], [7], [6]. Furthermore, since these reduced problems are independent, they could be solved in parallel given available computing resources.

Step 3: Integrate for the final system unreliability. After each reduced problem is separately conquered, lastly, using Eq. (1) the results of all the reduced problems are integrated with the occurrence probabilities of DTE_i to obtain the final unreliability of the system with FDEP loops.

3. Example Analysis and Results

3.1. An illustrative example

Figure 5 illustrates the dynamic fault tree model of an example system subject to a FDEP loop, where *A* brings down *B* that brings down *C* that brings down *A*. The loop is modeled using three cascaded FDEP gates, which form a *domino* chain.

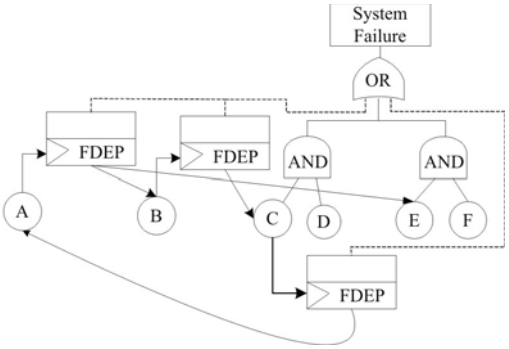

Fig. 5. An example of systems with FDEP loops

Two different sets of input failure parameters for system components will be used in the analysis:

Set 1: All the six components of the system fail exponentially with a constant failure rate of λ = 0.00001/hour. This set is used to verify the proposed approach using the existing Markov-based method.

Set 2: Components *A*, *C*, and *D* fail with different fixed probabilities: q_A=0.01, q_C=0.02, q_D=0.03. Components *B, E,* and *F* fail exponentially with constant failure rates: λ_B=0.00001/hr, λ_E=λ_F=0.0001. This set is used to illustrate that the proposed approach has no limitation on the type of time-to-failure distributions for the system components.

The mission times (t) of 1000 hours, 10000 hours, and 100000 hours are considered for both sets in the reliability analysis.

3.2. Example analysis

The three-step combinatorial method described in Section 2 can be applied to solve the example system in Figure 5 as follows.

Step 1: Build the DTE space. Because there are three elementary trigger events (*A*, *B*, and *C*), the DTE space for the example system in Figure 5 contains 8 DTE, which are shown in the first column of Table 1. The second column of Table 1 shows the calculation method of Pr(DTE_i) given that the three

trigger events are *s*-independent. Note that when a component, for example, A fails exponentially, $\Pr(A) = 1 - e^{-\lambda_A t}$ and $\Pr(\overline{A}) = e^{-\lambda_A t}$; when it fails with a fixed probability, $\Pr(A) = q_A$ and $\Pr(\overline{A}) = 1 - q_A$.

Tab. 1. DTE & calculation of Pr(DTE_i)

DTE_i	$\Pr(DTE_i)$
$DTE_1 = \overline{A} \cap \overline{B} \cap \overline{C}$	$\Pr(\overline{A})\Pr(\overline{B})\Pr(\overline{C})$
$DTE_2 = \overline{A} \cap \overline{B} \cap C$	$\Pr(\overline{A})\Pr(\overline{B})\Pr(C)$
$DTE_3 = \overline{A} \cap B \cap \overline{C}$	$\Pr(\overline{A})\Pr(B)\Pr(\overline{C})$
$DTE_4 = \overline{A} \cap B \cap C$	$\Pr(\overline{A})\Pr(B)\Pr(C)$
$DTE_5 = A \cap \overline{B} \cap \overline{C}$	$\Pr(A)\Pr(\overline{B})\Pr(\overline{C})$
$DTE_6 = A \cap \overline{B} \cap C$	$\Pr(A)\Pr(\overline{B})\Pr(C)$
$DTE_7 = A \cap B \cap \overline{C}$	$\Pr(A)\Pr(B)\Pr(\overline{C})$
$DTE_8 = A \cap B \cap C$	$\Pr(A)\Pr(B)\Pr(C)$

Step 2: Generate and solve reduced problems. According to Eq. (1), the unreliability of this example system can be calculated as Eq. (2).

$$U_{sys} = \sum_{i=1}^{8} [\Pr(\text{system fails} | DTE_i) \bullet \Pr(DTE_i)] \quad (2)$$

According to the approach described in Step 2 of the combinatorial approach in Section 2, the sets of components affected by the eight DTE are: $S_{DTE_1} = \phi$, $S_{DTE_k} = \{A, B, C, E\}$ for $k=2,3,\ldots,8$ since $FDG_A = FDG_B = FDG_C = \{A, B, C, E\}$. To generate the reduced fault tree models, because the event C is a dual event, the special replacement and reduction process (described in Step 2 of Section 2) will be applied. Figure 6(a) shows the fault tree model for the reduced problem #1, *i.e.*, Pr(System fails|DTE_1). The fault tree models for the reduced problems #2-8 are the same and shown in Figure 6(b).

With the FDEP loop removed, the two reduced fault tree models in Figure 6 can be solved using the efficient BDD-based combinatorial method [4], [7], [6]. Figure 7 shows the corresponding BDD models for those two reduced fault trees. The evaluation of the BDD models gives: Pr(System fails|DTE_1) = Pr(E)*Pr(F), Pr(System fails|DTE_i) = Pr(D) + (1-Pr(D))*Pr(F), for i = 2, 3, ..., 8.

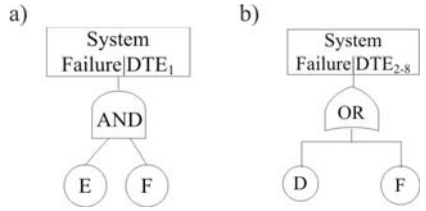

Fig. 6. Reduced fault tree models: a) For reduced problem #1, b) For reduced problems #2-8

Step 3: Integrate for the final system unreliability. According to Eq. (2), we obtain the final system unreliability for the example system in Figure 5 by combining the results of those reduced problems derived in Step 2 with the occurrence probabilities of 8 DTE as Eq. (3).

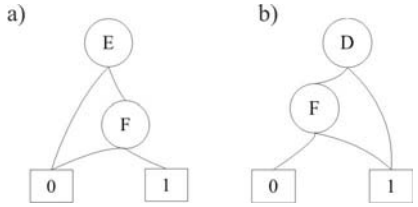

Fig. 7. BDD of reduced problems: a) For reduced problem #1, b) For reduced problems #2-8

$$U_{sys} = \Pr(\text{E})*\Pr(\text{F})*\Pr(DTE_1) + [\Pr(D) + (1 - \Pr(D))*\Pr(F)]*\sum_{k=2}^{8}\Pr(DTE_k) \quad (3)$$

Because $\sum_{k=1}^{8}\Pr(DTE_k) = 1$, Eq. (3) can be simplified as Eq. (4).

$$U_{sys} = \Pr(\text{E})*\Pr(\text{F})*\Pr(DTE_1) + [\Pr(D) + (1 - \Pr(D))*\Pr(F)]*[1 - \Pr(DTE_1)] \quad (4)$$

3.3. Example results

Using the two sets of input failure parameters given in Section 3.1, we obtained the system unreliability results for the mission times of 1000 hours, 10000 hours, and 100000 hours as shown in Table 2. All the unreliability results using parameters of Set 1 are consistent with those obtained using the Markov-based method. Note that the Markov-based approach cannot analyze the example system with the input parameters of Set 2 because some components have non-exponential time-to-failure distributions.

Tab. 2. Unreliability results of the example system

t (hrs)	1000	10000	100000
Set 1	6.812974e-4	0.053690	0.841509
Set 2	1.352411e-2	0.429324	0.999939

4. Discussions

In summary, using the proposed combinatorial method to solve the example system of Figure 5, we only need to analyze two reduced fault tree models both with 2 components (as shown in Figure 6) using efficient combinatorial approaches, for example, BDD (as shown in Figure 7).

In contrast, using the traditional Markov-based method, we must solve a compact Markov chain (after merging all failure states and related transitions) with 8 states and 15 transitions as shown in Figure 8. In Figure 8, the state "SF" represents the system failure state, and each of the other states is represented by its operational components. For example, the state (*ABCE*) represents a state in which components *A*, *B*, *C*, & *E* are operational and components *D* & *F* have failed. Additionally, the system with non-exponential failure distributions cannot be analyzed using the traditional Markov-based method, but can be analyzed using our proposed combinatorial method as illustrated in Section 3.

5. Conclusions and Future Work

In this paper, we presented an analytical and combinatorial method for the reliability analysis of systems with FDEP loops. Following the principle of the divide-and-conquer strategy, the method divides/transforms the original reliability problem with FDEP loops into several independent reduced problems without FDEP or loops. The resultant reduced problems can be conquered/solved using efficient combinatorial methods. Lastly, results of the reduced problems are integrated based on the total probability theorem to obtain the final system unreliability. As compared to the existing Markov-based methods, the proposed approach is computationally more efficient and can handle more general time-to-failure distributions. The proposed approach can also analyze systems with FDEP but without loops.

As mentioned in Section 2, in our future work, we will explore efficient approaches for considering functional dependence in imperfect fault coverage systems as well as systems with dynamic behavior of sequence dependence, priorities, warm spares, and cold spares.

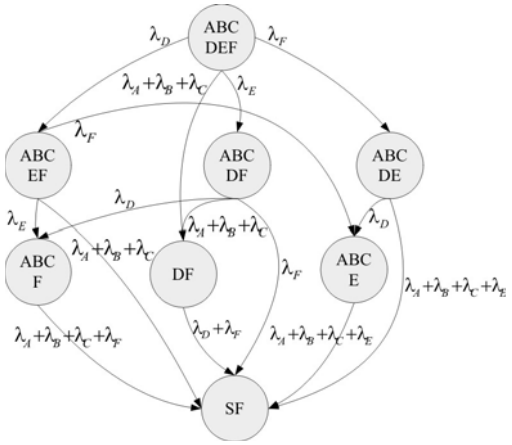

Fig. 8. CTMC in the equivalent Markov solution

6. References

1. Allen A. Probability, statistics and queuing theory: with computer science applications, 2nd edition. New York: Academic Press, 1990.
2. Dugan J B, Doyle S A. New results in fault-tree analysis. Tutorial notes of the Annual Reliability & Maintainability Symposium, 1997.
3. Huang H Z, Tong X, Zuo M J. Posbist fault tree analysis of coherent systems. Reliability Engineering and System Safety 2004; 84(2): 141-148.
4. Rauzy A. New algorithms for fault tree analysis. Reliability Engineering and System Safety 1993; 40(3): 203–211.
5. Stallings W. Computer organization and architecture, 8th edition. New York: Prentice Hall, 2009.
6. Xing L. An efficient binary decision diagrams based approach for network reliability and sensitivity analysis. IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans 2008; 38(2): 105-115.
7. Xing L, Dugan J B. Analysis of generalized phased-mission system reliability, performance and sensitivity. IEEE Transactions on Reliability 2002; 51(2): 199-211.

****

This work was supported in part by the US National Science Foundation under grant # 0832594. An earlier version of this paper was presented at the 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009). We appreciate the feedback given to us on this topic by reviewers.

****

Prof. Liudong XING, Ph.D.

Department of Electrical and Computer Engineering
University of Massachusetts – Dartmouth
Dartmouth, MA 02747, USA
tel.: +1 508 999 8883, fax: +1 508 999 8489
e-mail: lxing@umassd.edu

Prof. Joanne Bechta DUGAN, Ph.D.

Department of Electrical and Computer Engineering
University of Virginia
Charlottesville, VA 22904, USA
e-mail: jbd@virginia.edu

Brock A. MORRISSETTE, M.S.

Polaris Contract Manufacturing Division
Lockheed Martin MS2
Marion, MA 02738, USA
e-mail: brock.morrissette@lmco.com