Available online at www.sciencedirect.com
ScienceDirect
Reliability Engineering and System Safety 93 (2008) 1577–1583
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

Quantitative analysis of a fault tree with priority AND gates

T. Yuge*, S. Yanagi

Department of Electrical and Electronic Engineering, National Defense Academy, 1-10-20 Hashirimizu, Yokosuka 239-8686, Japan

Received 1 December 2006; received in revised form 24 January 2008; accepted 9 February 2008
Available online 4 March 2008

Abstract

A method for calculating the exact top event probability of a fault tree with priority AND gates and repeated basic events is proposed when the minimal cut sets are given. A priority AND gate is an AND gate where the input events must occur in a prescribed order for the occurrence of the output event. It is known that the top event probability of such a dynamic fault tree is obtained by converting the tree into an equivalent Markov model. However, this method is not realistic for a complex system model because the number of states which should be considered in the Markov analysis increases explosively as the number of basic events increases. To overcome the shortcomings of the Markov model, we propose an alternative method to obtain the top event probability in this paper. We assume that the basic events occur independently, exponentially distributed, and the component whose failure corresponds to the occurrence of the basic event is non-repairable. First, we obtain the probability of occurrence of the output event of a single priority AND gate by Markov analysis. Then, the top event probability is given by a cut set approach and the inclusion–exclusion formula. An efficient procedure to obtain the probabilities corresponding to logical products in the inclusion–exclusion formula is proposed. The logical product which is composed of two or more priority AND gates having at least one common basic event as their inputs is transformed into the sum of disjoint events which are equivalent to a priority AND gate in the procedure. Numerical examples show that our method works well for complex systems.

Keywords: Dynamic FT; Priority AND gate; Top event probability; Markov analysis; Inclusion–exclusion

1. Introduction

The fault tree (FT) is used widely as a tool for quantitative risk assessments. Although obtaining the exact top event probability of an FT is one of the most important aims, it is a difficult problem for a reasonably large scale system with complex structure, such as a chemical plant, a nuclear reactor, an airplane and so on. The representative complex FT structures are caused by several types of dynamic behaviors such as transient recovery, intermittent error, and sequence dependency. A priority AND gate (PAG) is a typical logic gate to represent the order of dependency of the event sequence [1]. It is logically equivalent to an AND gate where input events must occur in a prescribed order for the occurrence of the output event. Fig. 1 shows a PAG. In Fig. 1, the output of the gate is true if both events A and B have occurred and if event A occurred before event B. If both events have not occurred or if event B occurred before event A, then the gate does not fire. Fig. 2 shows an example of a logic model for a non-repairable two unit redundant system with a switch control. The standby unit is instantaneously switched into operation upon failure of the main unit. This system fails if the main and standby units both fail or the switch control failed first then the main unit fails. In the later case, the standby unit cannot be in use because of the failure of the switch control.

Markov analysis is an alternative modeling technique for such dynamic systems [2–4]. The difficulty of the analysis comes from the existence of repeated events. If none of the input events of a PAG appear in other gates, the output probability of the gate can be derived by constructing a Markov transition diagram in which all possible states of the PAG are considered. However, if a PAG has a repeated

*Corresponding author.
E-mail addresses: yuge@nda.ac.jp (T. Yuge), shigeru@nda.ac.jp (S. Yanagi).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.02.016

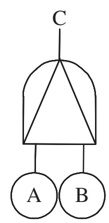

Fig. 1. Priority AND gate.

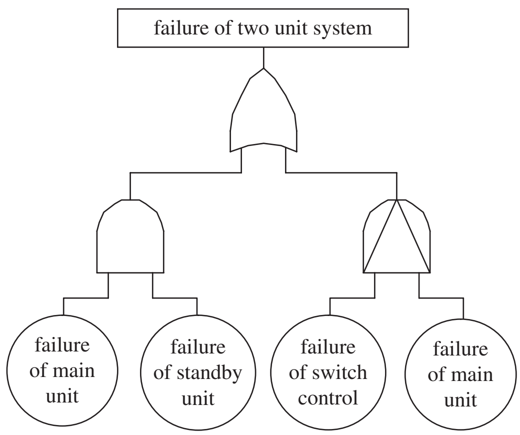

Fig. 2. Power supply system with standby unit.

input event, for example, the main unit failure in Fig. 2, we have to construct a large dimensional Markov transition diagram to obtain the top event probability. The dimensionality usually increases up to the number of the basic events. Therefore, the construction and calculation of a Markov diagram is tedious and error prone as the number of the basic events and/or the number of the repeated events increases. For such a complex system, one cannot get enough results with the related methods based on modularization [3] or BDD [4]. In fact, the well-known dynamic FT tool, Galileo [3], does not support a PAG having repeated events. However, it is considered that many FTs in the real world system have PAGs with repeated basic event as shown in Fig. 2. To overcome the shortcomings of the Markov model, it is necessary to develop a new analytical model that is flexible enough to capture the dynamic behaviors of the system. Other methods proposed for the analysis of dynamic FTs are a Bayesian network approach [5] and Monte Carlo simulation [6]. However, the former has a problem same as Markov analysis in complexity, the latter requires more computational time to achieve the desired accuracy.

The existence of repeated events makes analysis complicated even for conventional static FTs. For the static trees with repeated events, many researchers have proposed efficient algorithms to obtain exact or approximate top event probabilities [8]. The proposed methods are classified roughly into two groups. One approach uses factoring method [9,10] in order to eliminate the repeated events one by one. However, it is generally difficult to apply this approach to a dynamic FT. The conditional probabilities that have to be obtained when the factoring method is carried out cannot be readily obtained for a dynamic FT. The other uses a Boolean function. In this approach, the main effort is to find the structural representation of the top event in terms of the basic events. Finding the minimal cut sets is one way of accomplishing this step. Several algorithms [7,11,12] to find minimal cut sets are proposed. After all minimal cut sets are enumerated the inclusion–exclusion method is used to calculate the exact top event probability or its upper and lower bounds.

In this paper, we present a method for calculating the exact top event probability for a large scale FT containing many PAGs and repeated events when all the cut sets are given. Some cut sets are quite different from the traditional ones because these are the ordered cut sets where the basic events in the cut set have to occur in a prescribed order for the occurrence of the top event. The top event is represented by the union of the cut sets and the exact top event probability is given by the inclusion–exclusion expression as in the case of an FT without PAGs. An efficient procedure to obtain probabilities of logical products in the inclusion–exclusion formula is proposed. The logical product which is composed of two or more PAGs having at least one common basic event as their inputs is transformed into the sum of disjoint events which are equivalent to PAGs in the procedure. The output probability of the transformed PAG is given by Markov analysis. Numerical examples show that our method works well for complex systems such as a tree composed of 10 or more PAGs where almost all the basic events appear repeatedly.

2. Preparation

2.1. Acronyms and nomenclature

FT fault tree
PAG priority AND gate
Minimal cut set minimal set of basic events such that the incidence of all the events in a set directly causes the occurrence of the top event
Minimal ordered cut set minimal ordered set of basic events such that all the basic events in the set have to occur in a prescribed order for the occurrence of top event

2.2. Assumptions

(1) A system is composed of non-repairable components and does not have a cold standby component.
(2) The failure of a component which correspond to the occurrence of the basic event is *s*-independent and has an exponential failure time distribution.