Reliability Engineering and System Safety 96 (2011) 267–277

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Review

Algebraic determination of the structure function of Dynamic Fault Trees

G. Merle *, J.-M. Roussel, J.-J. Lesage

LURPA - ENS Cachan, 61 avenue du Président Wilson, Cachan 94230, France

ARTICLE INFO

Article history:
Received 3 April 2010
Received in revised form
2 October 2010
Accepted 4 October 2010
Available online 20 October 2010

Keywords:
Dynamic Fault Tree
Algebraic modeling
Structure function

ABSTRACT

This paper presents an algebraic framework allowing to algebraically model dynamic gates and determine the structure function of any Dynamic Fault Tree (DFT). This structure function can then be exploited to perform both the qualitative and quantitative analysis of DFTs directly, even though this latter aspect is not detailed in this paper. We illustrate our approach on a DFT example from the literature.

Contents

* Corresponding author. Tel.: +33 6 23 79 54 51; fax: +33 1 47 40 22 20.
E-mail addresses: guillaume.merle@lurpa.ens-cachan.fr (G. Merle), jean-marc.roussel@lurpa.ens-cachan.fr (J.-M. Roussel), jean-jacques.lesage@lurpa.ens-cachan.fr (J.-J. Lesage).

0951-8320/$ - see front matter
doi:10.1016/j.ress.2010.10.001

1. Introduction

The structure function of a Static Fault Tree (SFT) – a fault tree (FT) which only contains gates OR, AND, and K-out-of-N – is a Boolean function which represents the failure of the top event (*TE*) according to the failure of the basic events (*BEs*) of the FT. This algebraic model is classically used to perform both the qualitative and quantitative analysis of SFTs directly. For complex systems, these analyses are most often performed thanks to BDD-based methods [9,19] or other combinatorial techniques [1,17].

The introduction of dynamic gates – gates PAND, FDEP, and Spare – in FTs has changed the nature of the relation between the *TE* and the *BEs*. In a Dynamic Fault Tree (DFT), the failure of the *TE* depends not only on the failure of the *BEs* but also on the order of occurrence of these failures. As this last aspect is not taken into account in the Boolean model of failures (which only expresses whether a *BE* has occurred or not), a classical Boolean function cannot represent the dynamic relations between the *TE* and the *BEs* that exist in a DFT.

In a previous article, we presented the basics of an algebraic framework allowing to algebraically model dynamic gates PAND and FDEP, and determine the structure function of any Dynamic Fault Tree (DFT) containing these gates [13]. In this paper, we extend our previous work to Spare gates in order to be able to determine the structure function of any DFT. This structure function is based on a specific algebraic model of failures which allows to take into account the order of occurrence of failures. As this algebraic model is an extension of the Boolean model used for SFTs, all the results previously obtained for SFTs are preserved.

This paper is organised as follows. The most common approaches used to perform the analysis of DFTs are presented in Section 2. The algebraic framework that we introduce to model DFTs is detailed in Section 3, and the algebraic model of dynamic gates which can be determined from it is presented in Section 4. This algebraic model allows to determine the canonical form of the structure function of any DFT, as shown in Section 5, and our approach is illustrated on a DFT example in Section 6. Finally, we show how the qualitative analysis of DFTs can be performed directly from the canonical form of the structure function in Section 7.

2. State of the art

Several approaches have been used to avoid the problem of the determination of the structure function of DFTs. These approaches can be either modular or global.

Global approaches consist in solving the whole DFT directly, whereas modular approaches consist in:

- dividing the DFT into independent static and dynamic subtrees (or modules) prior to analysis: if a substree contains static gates only, it is considered as static; if a subtree contains at least one dynamic gate, it is considered as dynamic;
- solving the modules separately; and
- combining the results of the various modules to get the overall result for the entire tree.

Various methods exist to analyze the static and dynamic modules of DFTs. On the one hand, solving static modules can be done by using Binary Decision Diagrams (BDDs), other combinatorial techniques, or even some DFT Analysis models such as Markov Chains. On the other hand, solving dynamic modules is generally done using Input/Output Interactive Markov Chains [4–6], Stochastic Petri Nets (SPN) [1,7], or Temporal Bayesian Networks [2,3,15]. On the one hand, Markov Chains provide the cut sequences of the (sub)tree, which are the failure sequences that lead to the states of the Markov Chain in which the *TE* of the (sub)tree fails. They also provide the failure probability of the *TE* of the (sub)tree by solving the set of differential equations which is equivalent to the Markov Chain. On the other hand, the reachability graph of SPNs provides the cut sequences of the (sub)tree, and the failure probability of the *TE* can be computed after converting the SPN into its corresponding Markov Chain. However, in both cases, the failure of the components of the system is most often modeled by exponential time-to-failure distributions. Temporal Bayesian Networks allow to address this limit by allowing to consider other distributions. However, Bayesian Networks only allow to perform the quantitative analysis of the dynamic (sub)tree, and the inference algorithms used limit the distributions considered to Gaussian distributions [10] and mixtures of truncated exponentials [16].

An analytic approach was introduced in [23] to analyze DFTs by modelling the dynamic gate PAND and by determining simplification theorems. The authors focus on three temporal gates: gates PAND, Simultaneous-AND (SAND), and Priority-OR (POR). Gate SAND was created to address the ambiguity encountered in the definition of gate PAND regarding the simultaneity of input events, whereas gate POR was created from the definition of the Exclusive-OR gate found in [22]. Each event of the FT is assigned a sequence value which allows to know the order in which events occur. The authors propose an extension of truth tables, denoted as Temporal Truth Tables and based on these sequence values, to prove theorems allowing to simplify the FTs which contain the three temporal gates considered. Nevertheless, this approach allows to perform the qualitative analysis of FTs, only, and the only dynamic gate considered is gate PAND.

We have not found in the literature any attempt to provide an algebraic model for all dynamic gates allowing to determine the structure function of a DFT explicitly as it is currently the case for SFTs. The goal of the algebraic determination of the structure function of DFTs is to be able to perform their analysis directly whatever the distribution considered for basic events. We present such an algebraic framework in Section 3.

3. Algebraic framework for the modeling of Dynamic Fault Trees

3.1. Temporal model of non-repairable events

The structure function of SFTs is based on a Boolean model of events, and of basic events in particular. With this simple model, the only aspect which is taken into account is the presence or absence of failure. However, this Boolean model cannot render the order of occurrence of events which is necessary for the modeling of dynamic gates. To count on the temporal aspect of events, we consider the top event, the intermediate events, and the basic events as *temporal functions*, which are piecewise right-continuous