Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 327 (2016) 27–47

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Dynamic Fault Trees with Rejuvenation: Numerical Analysis and Stochastic Bounds

Jean-Michel Fourneau

DAVID, Université de Versailles-St-Quentin
Versailles, France

Nihal Pekergin

LACL, Université Paris Est
Créteil, France

Abstract

This paper presents an extension of a methodology that we have introduced recently to analyze Dynamic Fault Trees (DFT). The failure time distributions of the components are obtained from measurements leading to discrete failure time distributions. The gate outputs in a DFT are numerically analyzed from the input failure time distributions. This paper presents one major extension in which maintenance operations are considered such that some components are replaced by new ones to increase the availability of the system.

Keywords: Fault Trees, Stochastic Bounds, Maintenance, Rejuvenation, Discrete Distributions.

1 Introduction

Fault Tree (FT) analysis is a standard technique used in reliability modeling [15]. Dynamic Fault Trees (DFT) are an extension of Fault Trees to model more complex systems where the duration and the sequences of events are taken into account (see for instance [2] or [16] for a presentation). Because of this representation of time and sequence of events, DFTs are much more difficult to analyze than static Fault Trees. The standard numerical approach combines the static analysis based on cut sets for static gates and a Markov chain approach to model dynamic gates. New techniques have been proposed (Monte Carlo simulation [11], process algebra [3]) but there is still a need for some efficient methods of resolution for large and complex DFTs.

Indeed, the Markovian approach leads as usual to the state space explosion which prevents the analysis of large systems while simulations of transient processes need a large number of replications of the sample-path computation to obtain an accurate estimator for the reliability (see [7] and references therein for a statement

http://dx.doi.org/10.1016/j.entcs.2016.09.022
1571-0661/

of the problem and [14] for a tool based on the same set of methods). Thus, new resolution methods still have to be investigated.

We have proposed in [6] a numerical procedure to compute the distribution of the time to failure of a DFT or some stochastic bounds of this distribution which relies on the description of component failure processes by some discrete distributions, our model is not Markovian and it is not state-based unlike most of the tools (see [12] for a survey). Here we allow some rejuvenation process for the system components and we extend the numerical methods to take into account this maintenance activity.

Fault Trees are composed of a set of leaves which model the system components and some gates whose inputs are connected to the leaves or to the outputs of other gates. The value of the leaves is a boolean which is True, if the component is down, and False otherwise. The whole topology, when there is no replicated events, must be a tree. The root of the tree is a boolean value which must be True when the system has failed. The fault trees contain 3 types of gates: OR, AND and K/N (K out of N, or voting) gates. All of them are logical gates which are not needed to be presented here.

DFTs also contain four new gates: PAND (priority AND), FDEP (functional dependency), SEQ (sequential failures) and SPARE gates:

- SPARE gate. It is used to represent the replacement of a primary component by a spare with the same functionality. Spare components may fail even if they are dormant but the failure time distribution of a dormant component is lower in some sense than the failure time distribution of the component which is operational. A spare component may be "cold", if it cannot fail while it is dormant, or "hot" if the dormant has the same failure time distribution as an operating one, or "warm" otherwise. CSP, HSP and WSP gates are associated respectively with the cold, hot, and warm spare behaviors.
- FDEP. The FDEP gate has one main input connected to a component or to another gate and it has several links connected to components. When the main input becomes True, all the components connected by the links become True, irrespective of their current values. If a DFT contains a FDEP gate, its topology is not a tree anymore.
- PAND and STRICT-PAND (SPAND). The output of these gates becomes True when all of its inputs have failed in a preassigned order (from left to right in graphical notation). When the sequence of failures is not respected, the output of the gate is False. As discrete time models are considered, a distinction is made between PAND and SPAND when inputs become True at the same time.
- SEQ. The output of the SEQ gate becomes True when all of its inputs have failed in a preassigned order but it is not possible that the failure events occur in another order.

The DFT is represented by a function F (the so-called structure function [8]) which returns True when the system is down and False when it is operational. It is the value carried by the root of the DFT. The analysis of the DFT consists in computing the value of the structure function from the initial time (i.e. 0) up to