COMPUTER SCIENCE REVIEW 15–16 (2015) 29–62

Available online at www.sciencedirect.com

ScienceDirect

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

Survey

Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools

*Enno Ruijters**, *Mariëlle Stoelinga*

Formal Methods and Tools, University of Twente, The Netherlands

ARTICLE INFO

Article history:
Received 2 December 2014
Received in revised form
22 March 2015
Accepted 28 March 2015
Published online 5 May 2015

Keywords:
Fault trees
Reliability
Risk analysis
Dynamic Fault Trees
Graphical models
Dependability evaluation

ABSTRACT

Fault tree analysis (FTA) is a very prominent method to analyze the risks related to safety and economically critical assets, like power plants, airplanes, data centers and web shops. FTA methods comprise of a wide variety of modeling and analysis techniques, supported by a wide range of software tools. This paper surveys over 150 papers on fault tree analysis, providing an in-depth overview of the state-of-the-art in FTA. Concretely, we review standard fault trees, as well as extensions such as dynamic FT, repairable FT, and extended FT. For these models, we review both qualitative analysis methods, like cut sets and common cause failures, and quantitative techniques, including a wide variety of stochastic methods to compute failure probabilities. Numerous examples illustrate the various approaches, and tables present a quick overview of results.

Contents

* *Correspondence to:* Universiteit Twente, t.a.v. Enno Ruijters, Vakgroep EWI-FMT, Zilverling, P.O. Box 217, 7500 AE Enschede, The Netherlands.
E-mail addresses: e.j.j.ruijters@utwente.nl (E. Ruijters), m.i.a.stoelinga@utwente.nl (M.I.A. Stoelinga).

http://dx.doi.org/10.1016/j.cosrev.2015.03.001
1574-0137/

1. Introduction

Risk analysis is an important activity to ensure that critical assets, like medical devices and nuclear power plants, operate in a safe and reliable way. Fault tree analysis (FTA) is one of the most prominent techniques here, used by a wide range of industries. Fault trees (FTs) are a graphical method that model how failures propagate through the system, i.e., how component failures lead to system failures. Due to redundancy and spare management, not all component failures lead to a system failure. FTA investigates whether the system design is dependable enough. It provides methods and tools to compute a wide range of properties and measures.

FTs are trees, or more generally directed acyclic graphs, whose leaves model component failures and whose gates failure propagation. Fig. 1 shows a representative example, which is elaborated in Example 1.

Concerning analysis techniques, we distinguish between *qualitative* FTA, which considers the structure of the FT; and *quantitative* FTA, which computes values such as failure probabilities for FTs. In the qualitative realm, *cut sets* are an important measure, indicating which combinations of component failures lead to system failures. If a cut set contains too few elements, this may indicate a system vulnerability. Other qualitative measure we discuss are path sets and common cause failures.

Quantitative system measures mostly concern the computation of failure probabilities. If we assume that the failure of the system components are governed by a probability distribution, then quantitative FTA computes the failure probability for the system. Here, we distinguish between discrete and continuous probabilities. For both variants, the following FT measures are discussed. The *system reliability* yields the probability that the system fails with a given time horizon t; the *system availability* yields the percentage of time that the system is operational; the *mean time to failure* yields the average time before the first failure and the *mean time between failures* the average time between two subsequent failures. Such measures are vital to determine if a system meets its dependability requirements, or whether additional measures are needed. Furthermore, we discuss sensitivity analysis techniques, which determine how sensitive an analysis is with respect to the values (i.e., failure probabilities) in the leaves; we also discuss importance measures, which give means to determine how much different leaves contribute to the overall system dependability.