Expert Systems With Applications 77 (2017) 114–135

Contents lists available at ScienceDirect

Expert Systems With Applications

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

Review

An overview of fault tree analysis and its application in model based dependability analysis

Sohag Kabir

School of Engineering and Computer Science, University of Hull, Hull, HU6 7RX, UK

ARTICLE INFO

Article history:
Received 30 June 2016
Revised 18 January 2017
Accepted 29 January 2017
Available online 4 February 2017

Keywords:
Fault tree analysis
Reliability
Risk analysis
Safety analysis
Dynamic fault trees
Model based dependability analysis
Expert systems

ABSTRACT

Fault Tree Analysis (FTA) is a well-established and well-understood technique, widely used for dependability evaluation of a wide range of systems. Although many extensions of fault trees have been proposed, they suffer from a variety of shortcomings. In particular, even where software tool support exists, these analyses require a lot of manual effort. Over the past two decades, research has focused on simplifying dependability analysis by looking at how we can synthesise dependability information from system models automatically. This has led to the field of model-based dependability analysis (MBDA). Different tools and techniques have been developed as part of MBDA to automate the generation of dependability analysis artefacts such as fault trees. Firstly, this paper reviews the standard fault tree with its limitations. Secondly, different extensions of standard fault trees are reviewed. Thirdly, this paper reviews a number of prominent MBDA techniques where fault trees are used as a means for system dependability analysis and provides an insight into their working mechanism, applicability, strengths and challenges. Finally, the future outlook for MBDA is outlined, which includes the prospect of developing expert and intelligent systems for dependability analysis of complex open systems under the conditions of uncertainty.

1. Introduction

Safety critical systems are extensively used in many industries, including the aerospace, automotive, medical, and energy sectors. Systems that fall into this category range from airbags in cars to propulsion systems on spacecraft; however, they all share a common property — their failure has the potential to cause catastrophic effects on human life as well as the environment. For this reason, it is expected that safety critical systems possess a high level of dependability. Dependability is the capability of avoiding failures that are more frequent and more severe than is acceptable, and thus dependability assessment should be carried out early in the design phase to avoid unacceptable costs in terms of loss of life, environmental damage, and loss of resources by identifying and rectifying potential hazards as soon as possible. The dependability of a system includes, but is not limited to the following characteristics: safety, reliability, and maintainability.

There are many widely used classical safety assessment methods available to assist safety analysts in performing dependability analysis of systems. One such widely used method is Failure Modes Effects and Criticality Analysis (FMECA). FMECA was initially specified in US Military Procedure MIL-P-1629 and then updated in MIL-STD-1629A (US Department of Defense, 1980). It is an inductive analysis method that considers all possible combinations of effects of a single component failure mode(s). This method also provides ways to perform probabilistic analysis to determine criticality of failure modes.

The Fault Tree Analysis (FTA) (Vesely, Goldberg, Roberts, & Haasl, 1981) is another well-established and well-understood technique, widely used to determine system dependability. In fault trees, the logical connections between faults and their causes are represented graphically. FTA is deductive in nature meaning that the analysis starts with a *top event* (a system failure) and works backwards from the top of the tree towards the leaves of the tree to determine the root causes of the *top event*. The results of the analysis show how different components failures or certain environmental conditions can combine together to cause the system failure. After construction of a fault tree, the analyses are carried out in two levels: a qualitative level and a quantitative level. Qualitative analysis is usually performed by reducing fault trees to minimal cut sets (MCSs), which are a disjoint sum of products consisting of the smallest combinations of basic events that are necessary and sufficient to cause the top event.

In quantitative analysis, the probability of the occurrence of the top event and other quantitative reliability indexes such as importance measures are mathematically calculated, given the failure rate or probability of individual system component. The results of quantitative analysis give analysts an indication about system relia-

E-mail addresses: s.kabir@hull.ac.uk, s.kabir@2012.hull.ac.uk

http://dx.doi.org/10.1016/j.eswa.2017.01.058
0957-4174/

bility and also help to determine which components or parts of the system are more critical so analysts can put more emphasis on the critical components or parts by taking necessary steps, e.g., including redundant components in the system model. The usual quantification methods for classical static fault trees do not consider uncertainty in failure data. As the outcome of quantitative analysis is entirely dependent on the precision of the numerical data used in the analysis, if uncertainties are left unresolved then there is a chance of producing misleading results. Different methodologies, mainly based on fuzzy numbers, have been proposed to tackle the issue of uncertain failure data in FTA.

The standard fault tree (SFT) can only evaluate safety and reliability of static systems. Static systems are those which only experience a single mode of operation throughout the duration of their lifetimes, and thus exhibit constant nominal and failure behaviours. However, modern large-scale and complex systems can operate in multiple phases, e.g. an aircraft can operate in take-off, flight, and landing modes. One important characteristic of such systems is their dynamic behaviour, i.e., the behaviour of the system (both nominal and potential failure behaviour) can change according to what state or mode of operation the system is in. Dynamic system behaviour leads to a variety of dynamic failure characteristics such as functional dependent events and priorities of failure events. Although SFTs are widely used for dependability analysis, they are unable to capture dynamic failure behaviour of a system.

Dynamic dependability assessment overcomes many of the limitations of the static dependability analysis by allowing the dependability assessment of dynamic systems. It can capture system behaviour for multiple states and can model many possible interactions between system components and variables. In addition to that, it can capture time- or sequence-dependent behaviour of systems. To facilitate dynamic dependability analysis, the SFTs have been extended in different ways such as dynamic fault trees (DFTs) (Dugan, Bavuso, & Boyd, 1992), state-event fault trees (Kaiser, Gramlich, & Förster, 2007), and Stochastic Hybrid Fault Tree Automaton (SHyFTA) (Chiacchio et al., 2016) etc. DFT is the most widely used dynamic extensions of the SFT and it can capture sequence dependent behaviour, behaviour of functionally dependent components and also the priorities of the events. SHyFTA is a recent approach that combines DFT and the Stochastic Hybrid Automaton (Aubry & Brînzei, 2015; Castaneda, Aubry, & Brînzei, 2011) techniques to perform dynamic reliability assessment.

FTA is primarily a manual process and often performed on informal system models. As the system design evolves, these informal models could rapidly become outdated, which has the potential to make the dependability assessment process inconsistence and incomplete. Over the past two decades, research has focused on simplifying dependability analysis by looking at how we can synthesise dependability information from system models automatically. This has led to the field of Model-Based Dependability Analysis (MBDA) (Joshi, Heimdahl, Miller, & Whalen, 2006). Several tools and techniques such as Hierarchically Performed Hazard Origin & Propagation Studies (HiP-HOPS) (Papadopoulos & Mcdermid, 1999), AADL (Feiler, Lewis, & Vestal, 2006), and AltaRica (Arnold, Point, Griffault, & Rauzy, 2000) etc. have been developed as part of MBDA. Many of these techniques use fault tree analysis as their primary means of system dependability analysis and automate the fault tree generation process.

A survey on standard fault tree analysis and its extensions is represented in Ruijters and Stoelinga (2015). This survey covered technical details of different types of fault trees and their analyses (both qualitative and quantitative) approaches. A literature review on different model based dependability analysis approaches is available in Aizpurua and Muxika (2013), and Sharvia, Kabir, Walker, and Papadopoulos (2015). As described in these reviews, many of the MBDA approaches use fault tree analysis as their primary means of analysis and automate the fault tree generation process from system models. In this paper, at first, I review the standard FTA and describe the limitations of this approach with an example. Afterwards, I review different extensions of the standard fault tree. Finally, different model based dependability analysis approaches where fault trees are used as an analysis technique is reviewed and the concepts of the application of FTA in these approaches are discussed with examples. In doing this, I have reviewed more than 200 papers on fault tree analysis, extensions of fault trees and model-based dependability analysis concepts.

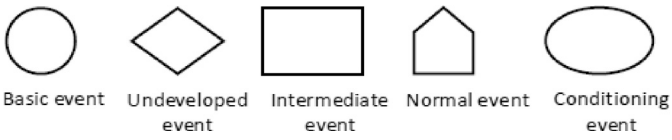

Fig. 1. Fault tree event symbols.

I have used different bibliographical research tools such as Google Scholar (https://scholar.google.co.uk/), ScienceDirect (http://www.sciencedirect.com/), IEEEXplore (http://ieeexplore.ieee.org/), SpringerLink (http://link.springer.com/), Web of Science (https://webofknowledge.com/), ACM Digital Library (http://dl.acm.org/), and Scopus (https://www.scopus.com/), to obtain the relevant articles. Although an extensive effort has been made to find all the relevant articles, no explicit guarantee can be given that this paper has found every relevant paper.

The remainder of this paper is organised as follow: Section 2 reviews the classical fault tree analysis technique and describes the limitation of this technique. Section 3 presents a bibliographical review of different extensions of the standard FTA. The concept of model based dependability analysis, different MBDA techniques, and the application of FTA in MBDA are reviewed in Section 4. Section 5 presents a thorough discussion and future outlook for MBDA. Finally, the concluding remarks are presented in Section 6.

2. Standard fault trees

FTA was invented in 1961 in Bell Laboratories by H.A. Watson, with the support of M. A. Mearns. The intention behind this invention was to help in the design of US Air Force's Minuteman missile system. The approach was successfully used by David Haasl from the Boeing Company to analyse the whole system. Several papers on fault tree analysis were presented at the first System Safety Conference in 1965 (Ericson, 1999). After the creation of FTA, it has been used in variety of fields, including but not limited to: automotive, aerospace, and nuclear industries (Kabir, Azad, Walker, & Gheraibia, 2015; Walker & Papadopoulos, 2009). The Fault Tree Handbook (Vesely et al., 2002) provides a broad introduction to standard fault trees.

2.1. Fault tree symbology

Fault tree consists of three types of nodes: events, gates and transfer symbols. Symbols used in SFTs to represent different events are shown in Fig. 1.

A basic event is an initiating or basic fault that does not require any further development or expansion and is graphically represented by a circle. Basic events are represented as leaf nodes in the fault tree and they combine together to cause intermediate events. To facilitate quantitative analysis basic events are usually given failure rates and/or repair rates. In the qualitative analysis, cut sets are the combination of different basic events.