Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 44 (2015) 599 – 608

Procedia Computer Science

2015 Conference on Systems Engineering Research

Integrated Matrix-Based Fault Tree Generation and Evaluation

Michael Roth*[a], Moritz Wolf[a], Udo Lindemann[a]

a Technische Universität München, Institute of Product Development, Boltzmannstr. 15, 85748 Garching, Germany

Abstract

Increasing complexity of products and safety regulations combined with an increasing amount of variants complicates the process of safety analysis within systems engineering. Moreover, it is known that the early avoidance or prevention of failures saves costs and improves the quality. As methods of safety analysis, i.e. fault tree analyses require immense manual efforts and expert knowledge, the efficiency of these analyses has to be improved. Our paper thus presents an approach to generate and evaluate fault trees by the usage of matrix-based models. It is an approach tailored to the early phases of system design and provides a preliminary fault tree analysis. It automatically generates fault trees and evaluates them. Thus, it facilitates the efficient identification of safety critical elements and the assessment and comparison of alternative system architecture concepts. This paper provides a brief introduction to fault tree analysis and presents existing approaches to automate the generation or synthesis of fault trees. The limitations of these approaches during early stages of design are discussed and the need for a tailored approach is derived. The developed approach consists of four phases and six steps which each are explained in detail. The whole approach is validated within a small industrial case study and its benefits and limitations are discussed. The case study shows, that the approach successfully improves the efficiency of a preliminary fault tree analysis.

Peer-review under responsibility of the Stevens Institute of Technology.

Keywords: Fault Tree Analysis; Design Structure Matrix; Functional Modeling; Safety;

1. Introduction

Customers' expectations and requirements as well as their variance are steadily increasing. This is one reason, why the complexity of products and systems grows[1]. Thus, companies are under pressure to offer even more variants, which increases the size of their product portfolio. As a result we observe a hardly manageable amount of variants and evolutionary grown complex systems in the industry[2]. Combined with stricter safety regulations this leads to immense efforts for safety analysis and approval. For each new system variant, the process of safety analysis and approval has

* Michael Roth. Tel.: +49-89-289-15129; fax: +49-89-289-15144.
E-mail address: michael.roth@pe.mw.tum.de

Peer-review under responsibility of the Stevens Institute of Technology.
doi:10.1016/j.procs.2015.03.027

to be repeated. However, traditional deductive methods of safety analysis strongly rely on the experience of expert analysts[3] and focus on the design validation stage[4]. This limitations become more and more critical with increasing complexity of the system[3].

Recent publications in systems engineering acknowledge, that the consideration of safety aspects should be shifted to the early stages of the system design process and develop suitable methods and support (such as[3,4,5]). Safety analyses in early stages provide large value adding potential, but are difficult to perform due to the high level of uncertainty[6]. A challenge thus is, how classical methods like fault tree analysis (FTA) or failure mode and effect analysis (FMEA) can efficiently serve for a preliminary safety analysis in the early stages of design. To cope with uncertainty and a wide solution space, the required experience and manual efforts of these methods have to be reduced to facilitate the analysis and assessment of alternative concepts[7]. Thus, the objective of this paper is how the generation of preliminary fault trees and their evaluation can be automated to reduce the required efforts during the early stages of design.

In this paper we first provide a brief introduction to FTA and point out the interconnections between FTA and FMEA. We then discuss existing approaches to automate the generation of fault trees and their limitations. Based on that, we develop our approach which founds on established matrix-based models and methods. We apply and validate the approach in a simple case study on a cordless screwdriver. The paper concludes with the discussion of the findings and applicability of our approach as well as recommendations for further work.

2. Failure Analysis in Early Stage

2.1. Safety Analysis in Design – Classical Methods

The fault tree analysis (FTA) is a classical and standardized method applied to the safety analysis of systems (IEC61025[8]). It identifies conditions that may cause or contribute to the occurrence of an undesired top event and represents them in a graphical form[7,8]. Being a deductive method, it identifies an undesired top event and starting from there creates a tree structure of possible causes. The dependencies of multiple causes are modeled by Boolean logic gates. The tree's branches are followed down to the basic events. They represent failures in the system's components or elements. Thereby, the impact of a failure on multiple events, called common cause, can be identified[8]. Using analytic methods, all possible combinations of basic events that cause the top event can be determined. These combinations are called cut sets[8]. If the removal of one basic event will break the impact on the top event, a cut set is considered a minimal cut set[8]. As limitations, many researchers name the usually high manual efforts and experience, which are needed to perform the fault tree analysis[3,7,9].

Moreover, international norms recommend the combination of the deductive FTA with inductive methods like FMEA (IEC60812[10]) in order to ensure a comprehensive safety analysis[8]. The link between FMEA and FTA is provided by the basic events: each basic failure mode in the FMEA which causes a system failure has to be represented by a minimal cut set in the fault tree. Also each basic failure of the fault tree has to be considered in a complete FMEA[8]. Thus, the challenge is not only to automate the generation of the fault tree but also to derive the minimal cut sets and automatically evaluate them to identify the most relevant system elements and to improve safety.

2.2. Model-Based Generation of Fault Trees – Existing Approaches

Due to the large complexity of systems, the manual activity of generating fault trees usually requires immense efforts. During the last years various approaches to automate the generation of fault trees based on system models have been published. A condensed overview on the most relevant approaches can be found in Mhenni et al.[9] and Majdara et al.[7] give an extensive reference list of approx. 20 approaches. We thus just provide a short overview on the most relevant concepts in the context of complex systems engineering. In the following they are classified by their modeling approach and we point out their advantages and limitations from our point of view.

SYSML-based Approaches

SysML is one of the main modeling languages used in the field of systems engineering, yet only few approaches to generate fault trees from these models are published.