Reliability Engineering and System Safety 96 (2011) 1515–1526

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Dynamic fault trees resolution: A conscious trade-off between analytical and simulative approaches

F. Chiacchio [a,*], L. Compagno [b], D. D'Urso [b], G. Manno [a], N. Trapani [b]

[a] Dipartimento di Matematica e Informatica—DMI, Università degli Studi di Catania, Italy
[b] Dipartimento di Ingegneria Industriale e Meccanica—DIIM, Università degli Studi di Catania, Italy

ARTICLE INFO

Article history:
Received 4 August 2010
Received in revised form
7 June 2011
Accepted 30 June 2011
Available online 13 July 2011

Keywords:
Risk assessment
Combinatorial models
Markov chains
Hierarchy
Spreadsheet modeling

ABSTRACT

Safety assessment in industrial plants with 'major hazards' requires a rigorous combination of both qualitative and quantitative techniques of RAMS. Quantitative assessment can be executed by static or dynamic tools of dependability but, while the former are not sufficient to model exhaustively time-dependent activities, the latter are still too complex to be used with success by the operators of the industrial field.

In this paper we present a review of the procedures that can be used to solve quite general dynamic fault trees (DFT) that present a combination of the following characteristics: time dependencies, repeated events and generalized probability failure.

Theoretical foundations of the DFT theory are discussed and the limits of the most known DFT tools are presented. Introducing the concept of weak and strong hierarchy, the well-known modular approach is adapted to study a more generic class of DFT. In order to quantify the approximations introduced, an ad-hoc simulative environment is used as benchmark.

In the end, a DFT of an accidental scenario is analyzed with both analytical and simulative approaches. Final results are in good agreement and prove how it is possible to implement a suitable Monte Carlo simulation with the features of a spreadsheet environment, able to overcome the limits of the analytical tools, thus encouraging further researches along this direction.

1. Introduction

The RAMS techniques offer qualitative analyses and quantitative techniques for risk assessment. The former (such as HAZOP and FMEA [1]) concern the context analysis (kind of process, geographic issues, internal specifications and rules, etc.) and are used to reveal potential hazards and consequences. The latter concern the risk assessment, computed as the probability of occurrence of undesired events (which are often highlighted by the qualitative analyses).

Two main classes of analytical stochastic models are used for quantitative evaluations:

- combinatorial models (also known as static) that are straightforward, but unable to describe dynamic dependencies among the components of the system and
- state-space models, mostly based on the Markov Chain representation (DTMC, CTMC, MRM, MRGP and GSMP), that overcome many of the limits of the static models but can become too large to be handled [2–4].

In the last years researchers have proposed several techniques, which combine the best properties of the previous models [4,7,8] such as the BDMP [5,6], the DRBD [9], the DFT [10], the SPN [11], etc. These powerful techniques of modeling are implemented using many reliability tools [2,5,12,13,14,17] that can be used according to their own hypotheses and features, which, often, are not suitable to design and solve any possible type of model.

Abbreviations: BDD, Binary Decision Diagram; BDMP, Boolean logic Driven Markov Process; BE, Basic Event; CDF, Cumulated Distribution Function; CTMC, Continuous Time Markov Chain; DAG, Direct Acyclic Graph; DCS, Decision Support System; DFT, Dynamic Fault Free; DRBD, Dynamic Reliability Block Diagram; DTMC, Discrete Time Markov Chain; ExpD, Exponential Distribution of Probability; FDEP, Functional Dependency; FMEA, Failure Mode and Effects Analysis; FT, Fault Tree; FT-A, Fault Tree Analysis; GD, Generalized Distribution of Probability; GSMP, Generalized Semi-Markov Process; HAZOP, Hazard and Operability Study; MCS, Minimal Cut Sets; MOE, Multiple Occurring Event; MOE-FT, Fault Tree with repeated events; MRGP, Markov Regenerative Process; MRM, Markov Rewards Model; (N)HCTMC, (Non) Homogenous Continuous Time Markov Chain; PAND, Priority AND; RAMS, Reliability, Availability, Maintainability and Safety; RBD, Reliability Block Diagram; SEQ, Sequence Enforcing; SFT, Static Fault Tree; SPN, Stochastic Petri Net; TE, Top Event; UnMOE-FT, Fault Tree with no repeated events; Wysiwyg, What you see is what you get

* Corresponding author. Tel.: +39 95 7382412; fax: +39 95 337994.
E-mail addresses: chiacchio@dmi.unict.it (F. Chiacchio), lco@diim.unict.it (L. Compagno), ddurso@diim.unict.it (D. D'Urso), gmanno@dmi.unict.it (G. Manno), ntrapani@diim.unict.it (N. Trapani).

0951-8320/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2011.06.014

In this paper we focused on the Fault Tree analysis because nowadays it is the most used quantitative technique for accident scenario assessment in the industry. The aim of this paper is to review briefly the improvements of the DFT over the SFT and provide a useful scheme to approach the resolution of a quite general class of DFT that includes nested dynamic gates, events with generalized distributed time to failure and MOE [40] (also known as repeated events). Intentionally, we will not cover other approaches (i.e. SPN, SAN, BDMP, etc.) because they are too general [5,6] and their use requires notions that go over the capability covered by the DFT approach.

A significant part of this work is devoted to reason about the hierarchical approach for DFT [15,16,18,19]. The concepts of weak and strong hierarchy are introduced and used to estimate what approximations arise when DFT with nested dynamic gates are analyzed.

This paper is organized as follows: in the first part we present an overview of the fault tree analysis, introducing the SFT of the presented case of study and its enhanced model by the mean of the DFT technique. In the second part, the most common analytical techniques of resolution are discussed, in particular the state-space models and an adapted modular approach for general DFTs. The aim of this section is to provide a reference framework to analyze a generic DFT, what techniques apply and what software uses (or combine) to obtain reasonable results.

In the final section, the case of study is solved in several manners, according to the scheme of resolution suggested. Among the traditional analytical tools, a novel simulative approach—developed under a well-known commercial spreadsheet [44]—is used as a benchmark to compare the final results. In the end conclusions are drawn and future works are indicated.

2. Research framework

The study is developed with reference to the FT model of Fig. 1: an accident scenario in an alkylation plant, as it is reported in the Safety Report required by the Seveso Directive. The SFT was designed by the experts according to the HAZOP report. Although SFTs are very common in the industrial field, DFTs are desirable because some reliability schemes and the integration with real time technology of monitoring (like the DCS [20]) introduce temporal dependencies that the static models are unable to treat.

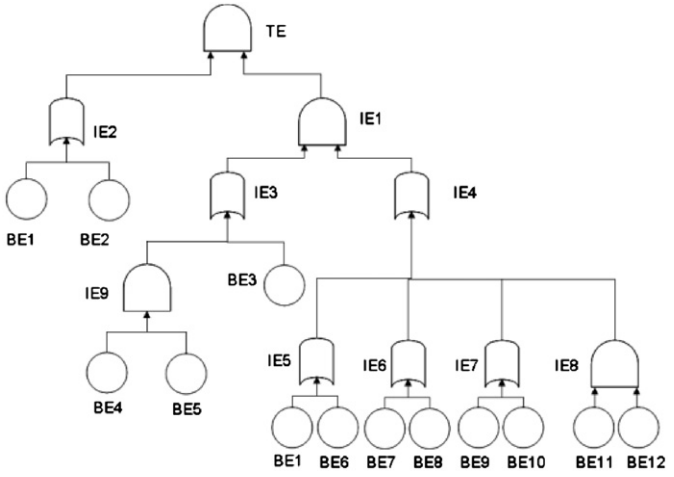

Fig. 1. SFT of a real industrial plant (alkylation plant).

2.1. Static Fault Tree (SFT)

The TE of a SFT [21] is described through the well-known structure function:

$$\phi(t) = f(\underline{X}(t)) = \begin{cases} 1, & \text{if the system is working} \\ 0, & \text{if the system is failed} \end{cases} \quad (1)$$

where $\underline{X}(t) = [X_1(t), X_2(t), \ldots, X_n(t)]$ is the vector of the states of the system and $X_i(t)$ represents the ith component that can be in a working or in a failed condition. Several methods of resolution exist and their usability depends on the complexity of the tree. In fact, a simple model without repeated events can be solved with the equivalent RBD [22]. Nevertheless, in the industrial applications it is usual to deal with large SFT composed by BEs characterized by a very low probability of occurrence. In these cases, exact methods such as factorization [23] or BDD [24] can be unfeasible; therefore the MCS technique is combined with the rare event approximation renouncing to exact results. The choice of what is the optimal truncation limit is discussed in many regulatory guides of PRA and it has been the objective of further elaborations through a technique that considers the important measures and the sensitivity of the CDF [25]; however, there is no certainty about the accuracy that can be reached and this can cause the underestimation (or the overestimation) of the sources of risk [26] and consequently can invalidate the safety or optimization strategies, which are based on these evaluations. The SFT models are constrained to the following assumptions [27]:

- binary nature of the components, which can only be in the operative or in the failure state;
- BEs are independent;
- transition between the working and the failed state is instantaneous;
- maintenance restores components as good as new and
- if the failure of a component influences other events on superior levels, its repair restores these events to the normal operative condition.

The algorithms for the resolution of the SFT are easy to implement because they make use of the Boolean algebra.

2.2. Dynamic Fault Tree (DFT) and analytical resolution

State-space models have been used to overcome the limits of the SFT, but

- unlike the FT, they are not systemic oriented;
- construction of the schema can become difficult and error prone;
- readability of the model is less intuitive than the combinatorial representation and
- complexity of the model can make the analytical resolution hard (or even unfeasible).

DFT methodology is a technique for the reliability assessment that was born to overcome the state-space complications but keeps the powerful representation of the SFT. In fact, the structure function of these models is time dependent since the dynamic gates (Fig. 2) establish interactions among the components (FDEP, PAND) and modify their failure attitude (SPARE, SEQ) [4], but the resolution of a DFT is not as simple as in the SFT because it cannot be performed with the rules of the Boolean algebra.

After a careful review of the most important literature about DFT models, we have realized the need to list and discuss the