Reliability Engineering and System Safety 133 (2015) 300–313

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Method for evaluating an extended Fault Tree to analyse the dependability of complex systems: Application to a satellite-based railway system

T.P. Khanh Nguyen [a,*], Julie Beugin [a], Juliette Marais [b]

[a] Univ Lille Nord de France, IFSTTAR, COSYS, ESTAS, Villeneuve d'Ascq, France
[b] Univ Lille Nord de France, IFSTTAR, COSYS, LEOST, Villeneuve d'Ascq, France

ARTICLE INFO

Article history:
Received 12 March 2014
Received in revised form
12 August 2014
Accepted 21 September 2014
Available online 19 October 2014

Keywords:
Dynamic & time dependent Fault Tree
Repairable & multi-state components
Petri net modelling
Monte Carlo simulation
Dependability analysis
GNSS-based localisation unit

ABSTRACT

Evaluating dependability of complex systems requires the evolution of the system states over time to be analysed. The problem is to develop modelling approaches that take adequately the evolution of the different operating and failed states of the system components into account. The Fault Tree (FT) is a well-known method that efficiently analyse the failure causes of a system and serves for reliability and availability evaluations. As FT is not adapted to dynamic systems with repairable multi-state components, extensions of FT (eFT) have been developed. However efficient quantitative evaluation processes of eFT are missing. Petri nets have the advantage of allowing such evaluation but their construction is difficult to manage and their simulation performances are unsatisfactory. Therefore, we propose in this paper a new powerful process to analyse quantitatively eFT. This is based on the use of PN method, which relies on the failed states highlighted by the eFT, combined with a new analytical modelling approach for critical events that depend on time duration. The performances of the new process are demonstrated through a theoretical example of eFT and the practical use of the method is shown on a satellite-based railway system.

1. Introduction

In order to satisfy user requirements, the configuration of technical systems becomes more and more complex and is the combination of multiple sub-systems. In the railway context for example, the Global Navigation Satellite System (GNSS) is an advantageous solutions for on-board localisation units as it offers an interoperable worldwide solution and as it reduces infrastructure costs. However, numerous studies [1,7] emphasised the necessity of reinforcing the performances of GNSS localisation units by other sensors when they are used in safety applications. Numerous combinations between GNSS and other kinds of sensors, such as odometer/ tachometer, Inertial Navigation System (INS) or Eddy Current Sensor (ECS) are considered. In this context, the GaLoROI project (Galileo Localisation for Railway Operation Innovation), which aims at developing a certifiable, safety-relevant, and satellite-based localisation unit for low density railway lines, is ongoing. The operation principle of GaLoROI is to combine satellite positioning data with satellite-independent data, here provided by an ECS. This combination poses multiple challenges when analysing and evaluating the system dependability. In fact, it is necessary to provide an efficient analysis method that can evaluate the behaviour of complex systems.

Using popular, simple and standard notation, the Fault Tree (FT) [6] method provides an ideal framework for deductive analyses of causal relationships between a system fault and associated failure events. It also allows the calculation of probabilities related to the combinatorial logic of several associated gates. Therefore, it is suitable for both qualitative, quantitative analyses and is widely used in reliability and safety studies. For example, a recent study [25] uses the FT approach with customer weighted values of component failures frequencies and downtimes for predicting customer reliability of a distribution power. However, FT analysis is based on the assumption that all components must be in boolean state (working or failed) and that component failure events are pairwise stochastically independent. These assumptions allows the evaluation of the system unreliability using the combinatorial method but is not sufficient to capture real behaviours of complex systems.

By defining additional gates, an extension of the FT, called *Dynamic Fault Tree* (DFT), was first proposed in [5] to attain a higher level of system dependability analysis. This method that was then developed in numerous studies [2,18,10,19,26] allows failure sequences, functional dependent failures and presence of spare

E-mail addresses: khanh.nguyen@ifsttar.fr, nguyenthipk85@gmail.com (T.P.K. Nguyen), julie.beugin@ifsttar.fr (J. Beugin), juliette.marais@ifsttar.fr (J. Marais).

http://dx.doi.org/10.1016/j.ress.2014.09.019
0951-8320/

Notation in this paper.

S	State space of the component
i	Degraded state whose the sojourn time that satisfies duration time condition can lead to a critical event (CE)
n	Number of sojourn periods in a degraded state, which lead to a critical event (CE)
m	Discretisation period
$Q_{CE}(m)$	Probability that the critical event, CE is available at the m-th period, $m \geq n$
T_0	Observation period of the subsystem output
n_{miss}	Last period of the mission time (T_{miss})
n_{CE}	First occurrence period of the critical event (CE)
$p(n_{CE})$	Probability distribution function (pdf) of n_{CE}
$P(n_{CE})$	Cumulative distribution function (cdf) of n_{CE}
$p(n_{lCE})$	The probability that the component leaves state i after n_{lCE} periods
p_{ii}	Probability for staying in state i after T_0 s
P_{to_i}	Column vector of size $\|S\| \times 1$ that presents the transition probabilities from all states of the component to state i
P_{from_i}	Be the row vector, of size $1 \times \|S\|$, that represents transition probabilities from state i to all states of the component
P_{occ}	Row vector of size $1 \times \|S\|$ that presents the probability vector of initial states of the component at $t=0$
$P_{occ}(i)$	Occurrence probability of state i at the initial instant
P_{trans}	Transition matrix of size $\|S\| \times \|S\|$
$D1(a)$	Probability that CE occurs for the first time at the a-th period $(n+1 \leq a \leq 2n+1)$ and lasts until the (m)-th period
$D2(a)$	Probability that CE occurs for the first time at the a-th period $(n+2 \leq a \leq m)$ and also is available at the m-th period
N	Large number of transition step, such as $P_{trans}^{N} \simeq P_{trans}^{N+1}$

components to be captured. However, these studies do not consider the components having multi-states due to degradation processes and time conditions of the causes that lead to critical consequences.

Refs. [4,11,12] presented another extended FT, called *multi-state Fault Tree* (mFT). This mFT allows considering degraded components whose states are stochastically dependent and also allows taking into account the repair events [4].

On the other hand, extensions of *FT with time parameters* (time conditions of event duration that lead to critical consequences, delay time between cause and effect) are useful for the dependability analysis of technical systems. Ref. [22] expressed quantitative time relations between causes and effects by defining numerous additional temporal gates. This extension is called *Temporal Fault Tree* (TFT). Ref. [13] also considered the time relation between causes and effects using *State-Event Fault tree* (SEFT). For this extended FT, inputs of gates are both instantaneous events and states that last over a period of time. It allows addressing dynamic behaviours that depend on event sequences and considers the duration time conditions of events. Ref. [15] presented *Time dependencies Fault Tree* (TdFT) and focused on the timing analysis of the hazard events. In this last paper, events are not considered as instantaneous but are expressed by their duration times. The authors then define the causal gates characterised by the delay times between causes and consequences.

For dependability analysis of complex technical systems, such as the GaLoROI localisation system, it is necessary to provide an efficient method that permits to:

1. consider the repairable multi-state components,
2. take into account sequence dependent behaviours of a system,
3. examine duration conditions of the causes that lead to critical events.

Therefore, we follow the research directions of [2,4,5,13,15,22] and present in this paper *the extended Fault Tree* (eFT) that combines advantages of these above FT models for qualitative dependability analysis. In order to find the most appropriate method for evaluating this eFT, a survey of existing methods is examined in Section 2. After a discussion, the necessity for developing a new evaluation process, which is based on the Petri net (PN) modelling of critical events due to the duration of degraded states of sub-system, is highlighted. This modelling process is presented in Section 3 and is performed by two steps:

1. An analytical approach is developed in order to directly calculate the probability distribution function (pdf) of critical events stemming from the duration of a particular state.
2. Based on the pdf, an algorithm is proposed to sample the occurrence time of these critical events.

Then, the last part of Section 3 aims at proving the accuracy and at showing the efficiency of our new evaluation process. Moreover, the performance of our approach is illustrated one more time when considering a practical example, the GaLoROI system in Section 4. Finally, Section 5 presents the conclusion and the further research works.

2. Methods for evaluating extended Fault Trees

2.1. Overview of existing methods for evaluating the Fault Trees and extended Fault Trees

Two main approach types are employed in order to evaluate the FT and its extensions:

1. Analytic approaches aim at giving precise and reliable results, but it is not enough efficient for taking into account multiple complex behaviours of systems.
2. Modelling and simulation approaches aim at capturing the behaviours of complex systems, but their results are less precise.

2.1.1. Analytic approaches

2.1.1.1. Combinatorial methods for evaluating mFT. As long as there are no additional stochastic interdependencies between the components, the multi-state Fault Tree (mFT) can still be qualitatively analysed using the combinatorial methods. In earlier studies [11,12], the authors extended the combinatorial method of FT. For that, they defined discrete function characterising the relations between inputs and outputs of combinatorial gates in order to quantitatively analyse mFT. This method is only appropriate for a static system, i.e. a system that is examined without considering the possible evolution of its states over time.

2.1.1.2. Methods for evaluating DFT. When considering stochastic interdependencies between components, such as the order in which stochastic fault events occur, the combinatorial models are not appropriate. In order to quantitatively evaluate a DFT, [5,19] generate all the possible system states and stochastic transitions between states, i.e. the Continuous Time Markov Chain (CTMC) of the system. This is an efficient method to examine the dependencies of stochastic events or component states. However, this method presents the following drawbacks:

1. the number of basic events of the DFT can lead to an explosion of the state space of the CTMC.
2. the analytic evaluation is based on the assumption that all transitions between states follow exponential probability distributions.
3. it is difficult to take into account the maintenance information.

In order to reduce the state space explosion problem of CTMC, [10] presented a modular approach for identifying and solving the independent sub-trees. This approach is appropriate for fault trees whose a small part is dynamic in nature. Different techniques are applied to each sub-tree depending on its characteristics (static or dynamic) and the solutions are integrated to get the results for the