Safety Science 110 (2018) 313–323

Contents lists available at ScienceDirect

Safety Science

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

Evaluating Fault Tree by means of Colored Petri nets to analyze the railway system dependability

Haifeng Song[a,b,*], Eckehard Schnieder[b]

[a] School of Electronic and Information Engineering, Beijing Jiaotong University, China
[b] Institute for Traffic Safety and Automation Engineering, Technische Universität Braunschweig, Germany

ARTICLE INFO

Keywords:
Dependability analysis
Petri net modeling
Hazard analysis
Railway control system

ABSTRACT

Railway system is a safety critical and time-related system, the system's states and time parameters can be used to carry out the dependability and hazard analysis. Fault Tree is widely recognized as a standard evaluating method. However, restricted by the commercial products, the Fault Tree is limited to assess dynamic systems with event-repair operations and time-related attributions. Additionally, it is difficult to incorporate non-linear relationships such as feedback. The quality assurance for fault trees and events trees is mainly carried out by peer review. Combinatory limitations are encountered when modeling complex events with classical methods. Thus, this paper proposes a new method to represent and extend the Fault Tree in Colored Petri nets. Due to large calculation capabilities of CPNs, these limitations can be able to overcome. Additionally, it can be reused for customizations. The accuracy of the approach is verified by using model-based simulation and state space analysis. The performance and benefits of the new approach are demonstrated by investigating train to train collision failure models. To increase the safety demanding needs of railway transportation, we propose a new train movement authority plus system (MA+) in this paper. With the assistance of the wireless communication technology, MA+ can detect the condition of approaching switches and encountering trains within a certain range. The results indicate that the new MA+ can reduce the risk of train head to tail collisions. What is more, the new evaluation method can offer much more essential information, which involves maintenance components, model correctness verification, time factors, and mathematical calculation together, than the traditional Fault Tree Analysis.

1. Introduction

Despite developments in the automation technology, system faults exist at any time and in any situation. It is essential to evaluate the dependability and hazards of systems for the sake of maintaining an equivalent or a higher level security, after a new system is involved.

Fault Tree Analysis (FTA) can qualitatively and quantitatively evaluate the dependability, and represent the relationship between different events. Fault Tree Analysis (FTA) is highly recommended for software assessment in railway domain by the standard EN 50128 (Cenelec, 2011). In literature, a variety of (extended/varied) FTA methods have been introduced for analyzing railway system (Liu et al., 2015; Nguyen et al., 2015; Magott and Skrobanek, 2012; De Felice and Petrillo, 2011). In the general FTA, the binary states of events, the constant failure rates, the absence of repair events, and time duration limit the analysis ability of Fault Tree (FT) (Nguyen et al., 2015; Magott and Skrobanek, 2012). Some extended FTs are thereby proposed. For instance, publications (Buchacker, 2000; Lindhe et al., 2012) present a Multi-state Fault Tree, which involves repair events. Publication (Palshikar, 2002) introduces a Temporal Fault Tree, and it allows addressing dynamic behaviors that depend on time duration.

However, these aforementioned methods are not included in the correctness validation of the constructed fault trees, which are usually constructed manually and cost much time and effort, especially for large-scale systems. The quality assurance for fault trees is mainly carried out by peer review (e.g., by other fault tree experts or system designers) (Ericson, 1999). Hence, it is necessary to provide a methodology that can validate the model correctness when the system dependability is evaluated.

There are some commercial products, which can provide various functions, such as, Windchill FTA, ITEM ToolKit, Fault Tree++, and so on. However, the limitations of many commercial products used for fault tree analysis restrict the application of fault tree method. For example, as the FTA illustrates the accidents by means of linear event

* Corresponding author at: School of Electronic and Information Engineering, Beijing Jiaotong University, China.
E-mail addresses: songhaifeng2011@gmail.com, h.song@tu-braunschweig.de (H. Song), e.schnieder@tu-braunschweig.de (E. Schnieder).

https://doi.org/10.1016/j.ssci.2018.08.017
Received 19 January 2018; Received in revised form 22 May 2018; Accepted 23 August 2018

sequences, it is difficult to merge non-linear actions such as feedback. For quality analysis, the correctness of fault trees model is mainly implemented by peer review. The quantitative evaluation has disadvantages in dealing with flexible mathematical calculations. More importantly, for the dependability analysis of safety-critical complex systems, some mathematical calculation, which cannot be fully satisfied in the commercial software, is essential to quantify the dependability characteristic. Additionally, traditional FTA usually evaluates the systems that consist of non-maintenance process and time attributions (Wu and Zheng, 2018).

Motivated by the problems mentioned above, it is necessary to provide an efficient method satisfying the following requirements (R):

- **R1: Take different failure rates into account.** Given that the railway system is a combination of different subsystems, which have different failure distributions, different failure models should be taken into consideration. With the assist of random-variate generators in CPNs, the quality of the architectural information and the definition/precision of the failure rates are taken into consideration.
- **R2: Demonstrate the time attributions.** A practical system operates in the real-time space, but some time-related performances cannot be expected for a relatively long time (Song et al., 2017). However, this problem can be solved by involving time attributions in the modeling process.
- **R3: Carry out the flexible mathematical calculation.** For the dependability analysis and parameterization process, numerical calculations are necessary. Hence, the flexible mathematical calculation, which can be customized by implementers, is necessary.
- **R4: Consider subnet of components.** It is impractical to build a model of a large system as a single net, since it would become very large and inconvenient. However, it is time-consuming to produce a nice layout, which can not only give an overview of the system but also consist the details of components. By applying the subnet of component, it is possible to analyze the model in different abstraction levels, and reuse the components repeatedly.
- **R5: Verify the model's correctness.** Before any further analysis, the model represented system should be verified to ensure it precisely represents the system itself.

These requirements are essential for improving the flexibility and continuity in system dependability analyses. In this paper, we propose a methodology that can cover all these five requirements. Importantly, this solution is free and modifiable for special applications. The method is applied to describe practical systems and do qualitative and quantitative analyses.

Before the evaluation of FT is put forward, a suitable method is required to carry the aforementioned requirements. As suggested in EN 50128, in the area of railway application, the techniques of formal methods are suitable to do the system requirements specification, design, evaluation, as well as modeling. The system security analysis based on modeling is widely used in different research areas. The description refinement of a system depends on the formalization degree. The higher the formalization level used to describe the real system, the greater the possibility to mathematically verify the formalized concept system (Schnieder et al., 2009). In the railway domain, UML, B method, Petri nets and other varieties of modeling languages have been applied to describe railway application systems (Wu, 2014). UML is usually used to model and simulate the system's functionality, but is not suitable for structural analysis and formal proof. The B method is mainly used for the source code generation. Comparing with possible alternatives (Song and Schnieder, 2018), CPNs, as one of such formal methods, is more suitable to verify and formalize the FT.

The new method represents and analyzes the FT by using the CPN model. It has advantages of the aforementioned FTA for dependability analysis. Moreover, model correctness verification is carried out by applying state space analysis; events and conditions are represented by time durations but not considered as instantaneous; subnet of the event is proposed to implement other procedures, such as the maintenance.

The remainder of the paper is organized as follows: In Section 2, some preliminaries pertaining to the FT and CPNs notations are introduced. The main contribution of this work is discussed in Sections 3–5. For the sake of illustrating our process performance, a movement authority plus (MA+) system and the train to train collision accident model are proposed in Section 3. Section 4 is dedicated to discussing the modeling process, and verifying the model's calculation accuracy and structural correctness. Moreover, the evaluation approach is illustrated in Section 5, which presents an illustrative example applied to a railway system hazard. Finally, Section 6 presents the conclusion and future works.

Note that: the train collision model and parameters applied in this paper are only used to do the illustration, it maybe be different from the realistic situation.

2. Preliminaries

This section seeks to show some preliminary notions that are necessary for the discussion in the Sections 4 and 3. It is assumed that the readers have a knowledge of the CPNs and the software *CPN tools*. For starters publications (Jensen and Kristensen, 2009; Christensen and Mortensen, 1996) are highly recommended.

2.1. Elements in FT

Gates and events constitute the blocks of a fault tree. AND and OR gates are the fundamental logic gates in FT. In many cases, only these two fundamental gates are needed to build an FT model (Goble, 2010). In the following section, only these two gates are illustrated to introduce the gate structures in the CPN model.

An intermediate or top event (called "output event") happens when both input events' state and time duration meet the gate logic. As shown in Fig. 1, event $x1$ occurred at $n1$ period. The duration of the fault event relates to its maintenance time, and this fault event is activatable for the following steps during $[n1, n2]$. Given the event $OE$is the output of a gate and x_1, x_2 are inputs events, where OE, x_1, $x_2 \in [0, 1]$, 0 represents working and 1 represents failure, respectively. The probability relations between the input events and output event can be represented as formulas:

$$P_{AND}(OE) = \prod_{i=1}^{2} P(x_i) \tag{1}$$

$$P_{OR}(OE) = 1 - \prod_{i=1}^{2} (1 - P(x_i)) \tag{2}$$

where Eqs. (1) and (2) represent the AND and OR gates, respectively.

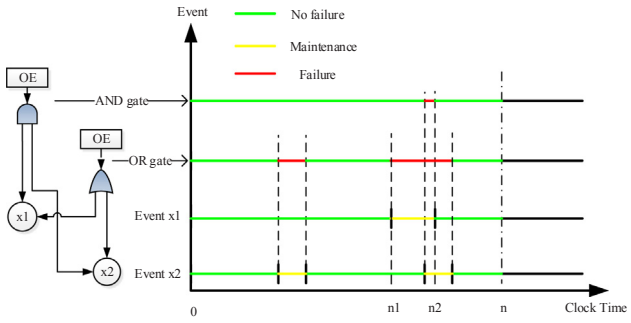

Fig. 1. A example of occurrence of service failure.