Reliability Engineering and System Safety 176 (2018) 62–79

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Formal model-based quantitative safety analysis using timed Coloured Petri Nets

Daohua Wu*, Wei Zheng

National Research Center of Railway Safety Assessment, Beijing Jiaotong University, Beijing 100044, China

ARTICLE INFO

Keywords:
Quantitative safety analysis
Timed Coloured Petri Nets
Systems theory
Mean time to hazardous event
Probability of keeping in normal and safe states
Railway control system

ABSTRACT

Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) are by far the most frequently used qualitative and quantitative approaches in system reliability and safety analysis such as in the railway domain. FTA and ETA explain the causalities and consequences of hazards or accidents (e.g., rail traffic accidents) in terms of linear event sequences, which are difficult to incorporate none-linear relationships such as feedback. For quantitative analysis, FTA and ETA have disadvantages in dealing with dependent failure events. The quality assurance for fault trees and events trees is mainly carried out by peer review. In addition, traditional FTA and ETA are usually applied to systems that consists of non-repairable components. For systems that comprise repairable components, Markov models are widely used, which suffer however intensively from the state space explosion.

Considering all these issues, we propose a formal model-based approach for quantitative safety analysis using timed Coloured Petri Nets (CPNs). There are three main contributions in this paper: firstly, a modelling method based on the specifications of timed message sequence charts, systems theory and decision tables for system components is raised for establishing timed hierarchical CPN models of systems that are appropriate for quantitative safety analysis. Secondly, state-space-based methods by exploring standard state space reports, and applying standard as well as non-standard queries to state spaces are presented to verify the untimed CPN models. Finally, methods of evaluating the safety characteristics of mean time to hazardous event and the probability of keeping in normal and safe states on the basis of the data collected during the simulation of the timed CPN models are provided. To illustrate our approach, a case study of a railway level crossing control system is presented as a running example throughout the paper.

1. Introduction

For many safety-critical systems, e.g., railway control systems, in addition to qualitative safety analysis, quantitative safety analysis is desirable. Qualitative safety analysis is used to locate possible hazards and to identify proper precautions (design changes, administrative procedures, etc.) that will reduce the frequencies or consequences of such hazards. Quantitative safety analysis aims at quantifying the probability of occurrence of each critical failure condition and the associated consequences [1]. Fault Tree Analysis (FTA) [2] and Event Tree Analysis (ETA) [3] are highly recommended for software assessment in railway domain by the standard EN 50128 [4]. In literature, a variety of (extended/varied) FTA methods have been introduced for analysing railway systems [5–11]. However, fault trees and event trees explain the causalities and consequences of hazards or accidents in terms of events sequenced as chains over time. Such event chains emphasize linear causality relationships, and they are difficult to incorporate non-linear relationships, including feedback [12]. Given the increasing complexity of today's systems, many hazards arise due to unsafe interactions between components (even when the components have not necessarily failed) [13]. This is, in particular, vital for railway distributed control systems such as the radio-based level crossing control system studied in this work; FTA is currently mainly applied to hardware whose events must be considered as statistically independent [14]. When it is applied to software, functional independence is required, namely, there are neither systematic nor random faults, which cause a set of functions to fail simultaneously [15]. Special attention to common cause failures therefore must be paid while implementing FTA; fault trees are usually constructed manually, which cost much time and effort, especially for large-scale systems. The quality of the constructed fault trees depend heavily on the experiences and abilities of the engineers who develop them. The quality assurance for fault trees is mainly carried out by peer review (e.g., by other fault tree experts or system designers) [16]; FTA is only applicable to systems that consist of non-repairable components.

For quantitative safety analysis, works [17–19] employ approaches that are based on extended/varied fault trees, i.e., dynamic fault trees in [17,18] and State/Event Fault Trees in [19]. Works [19–23] propose to use intermediate models to describe system behaviour/states, and then translate them into formal models that are appropriate for

[*] Corresponding author.
E-mail address: wudaohua@bjtu.edu.cn (D. Wu).

https://doi.org/10.1016/j.ress.2018.03.035
Received 31 October 2017; Received in revised form 26 March 2018; Accepted 31 March 2018
Available online 4 April 2018

probabilistic analysis i.e., PRISM models in [20–22] and Petri net models in [19,23]. Although fault tree based approaches are capable of modelling the aspect of dynamic behaviour of systems, fault trees still need to be constructed in the first place. Therefore, these approaches share some common disadvantages raised in FTA. For the formal-based approaches, a complicated translation process between different kinds of models which is error-prone and time-consuming, is necessary.

Taking all the aforementioned issues into consideration, we present a formal model-based approach for quantitative safety analysis using timed Coloured Petri Nets (timed CPNs or timed CP-nets) [24]. Firstly, the untimed hierarchical CPN model of a system is established based on the specification of timed Message Sequence Charts (timed MSC), system control structure and decision tables for system components. Secondly, the correctness of the untimed CPN model is verified by analysing standard state space report and applying standard as well as non-standard queries to the state space. Finally, the timing information is added to the CPN model and safety characteristics of Mean Time To Hazardous Event (MTTHE) and Probability of keeping in normal and safe states ($P_{N,\,S}$) is evaluated on the basis of the data collected during model simulations.

In this paper, a modelling method of developing timed hierarchical CPN models that are suitable for quantitative safety analysis is proposed in the first place. And then state-space-based methods by means of exploring standard state space reports, and applying standard as well as non-standard queries to state spaces are presented for the purpose of verifying the untimed CPN models. Last, methods of evaluating the safety characteristics of mean time to hazardous event and the probability of keeping in normal and safe states based on the data collected during the simulation of the timed CPN models are provided. In addition to these major contributions, the proposed approach has following advantages: (1) Scenarios [25] in the form of timed MSC and decision tables for system components are employed as specifications for developing CPN models of systems. Timed MSC and decision tables are easily understood by both customers and system engineers. This shall lay a solid foundation for developing desired system models for safety analysis. (2) The formal language of CP-nets are adopted as the modelling language. The CPN models for safety analysis could be verified by animation/simulation and/or model checking, while fault trees and event trees are checked mainly by peer review. (3) The system control structure based on systems theory [26] is utilized to capture hazards emerged due to the occurrences of non-linear-related events like feedback and unsafe interactions between system components (which is difficult to incorporate with FTA and ETA). (4) It is convenient to include repairable system components in the CPN models, which implies that it is possible to evaluate the dependability/availability and safety of systems that comprise repairable components without establishing Markov models which might suffer from the state space explosion problem intensively [27,28]. (5) Quantitative safety analysis is performed by analysing the data collected during the simulation of CPN models, which avoids the construction of large-scale fault trees or event trees, and thus avoids the dependency issue raised in dealing with fault trees.

The motivation of adopting CP-nets as the means of description for this work is as following: as standard Petri nets (or called low-level Petri nets [29,30]), CP-nets are graphical and mathematical means of descriptions that are well-known in describing systems characterized as being concurrent, asynchronous and distributed (e.g., railway control systems). When we use low-level Petri nets to model large-scale and complex systems such as the railway level crossing control system studied in this work, the system models often end in unmanageable scale. But with CP-nets, it is possible to work with different levels of detail and abstraction by specifying hierarchical CPN models. These hierarchical models consist of a set of modules and each module can have submodules. This will be of great benefit when modelling large-scale and complex systems. Besides, mature tools (e.g., CPN Tools [31] adopted in this work) for editing CPN models and associated techniques for model analysis are available. Moreover, Petri nets have been successfully applied to reliability and safety engineering in recent years [32–35].

The rest of the paper is organized as follows. Section 2 presents some basics of CP-nets and a radio-based railway level crossing control system. In Section 3, the modelling approach to develop untimed hierarchical CPNs is proposed. State-space-based verification of the untimed CPN models is carried out in Section 4. In Section 5, quantitative safety analysis methods based on the simulation of CPN models are provided. We conclude our work in Section 6.

2. Preliminaries

To illustrate the proposed approach, we present a case study of a simplified radio-based railway level crossing control system throughout the paper. Therefore, an brief introduction (textual description) of the level crossing control system is provided following the introduction of Coloured Petri Nets in this section.

2.1. Coloured Petri Nets

Coloured Petri Nets (CPNs or CP-nets) [24] are high-level Petri nets. Similar to low-level Petri nets, CPN models are directed graphs containing two types of nodes: places (ellipses or circles) and transitions (rectangular boxes), where edges that connect only nodes of different types are denoted as *arcs*. Each place is assigned a type called *color set* which determines the set of token colors (data values) that the tokens on that place are allowed to have. A transition is *enabled* if each variable that appears in any of the input arc expressions can be bound to a token color that is present on the corresponding *input place* (those places that have an arc leading to the transition), such that with respect to this variable binding, the number of tokens contained in each input place is no less than that determined by the arc expression, while satisfying the guard of the transition if there is any. When an enabled transition *fires* (which represents an event occurs in the system), it removes tokens from its input places and adds tokens to its *output places* (those places that have an arc coming from the transition). The colors and quantity of the tokens that are removed from input places and added to output places are determined by the arc expressions.

With the CPN modeling language, it is possible to work with different levels of detail and abstraction because of the capability of specifying hierarchically structured models of CPNs. These hierarchical models allow a *module* to have *submodules*, a set of modules to form a new module, and the reuse of submodules in different parts of the model. A module exchanges tokens with its environment (i.e., other modules) through interfaces which are port places. Port places can be recognized by rectangular port tags (“In”, “Out” or “I/O”) positioned next to them specifying whether the port place is an *input, output*, or *input/output port*. In CPN models, a module is usually represented by a substitution transition in its superior hierarchical level. A *substitution transition* has a rectangular substitution tag positioned next to it. The substitution tag contains the name of a submodule which is related to the substitution transition. The input places of substitution transitions are called *input sockets*, and the output places are called *output sockets*. To obtain a complete hierarchical model, it must be specified how the interface of each submodule is related to the interface of its substitution transition. This is done by means of a *port-relation*, which relates the port places of the submodule to the socket places of the substitution transition. Beside specifying port-relations, fusion sets can also be utilized for relating/synchronizing modules. A *fusion set* is comprised of a group of *fusion places*. It allows places in different modules to be glued together into one compound place across the hierarchical structure of the model. The fusion places that are members of a fusion set represent a single compound place. More information about CPNs (e.g., graphical examples) can be found in [24].