Reliability Engineering and System Safety 145 (2016) 169–182

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Model-based verification method for solving the parameter uncertainty in the train control system ☆

Ruijun Cheng [a], Jin Zhou [b], Dewang Chen [c,*], Yongduan Song [a]

[a] State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China
[b] School of Information Science and Engineering, Jinan University, Shandong 250022, China
[c] College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350116, China

ARTICLE INFO

Article history:
Received 23 January 2015
Received in revised form
11 September 2015
Accepted 16 September 2015
Available online 28 September 2015

Keywords:
Parameter uncertainty
System safety verification
Linear hybrid automata
Reachable state analysis
Stochastic time petri nets
High-speed train control system

ABSTRACT

This paper presents a parameter analysis method to solve the parameter uncertainty problem for hybrid system and explore the correlation of key parameters for distributed control system. For improving the reusability of control model, the proposed approach provides the support for obtaining the constraint sets of all uncertain parameters in the abstract linear hybrid automata (LHA) model when satisfying the safety requirements of the train control system. Then, in order to solve the state space explosion problem, the online verification method is proposed to monitor the operating status of high-speed trains online because of the real-time property of the train control system. Furthermore, we construct the LHA formal models of train tracking model and movement authority (MA) generation process as cases to illustrate the effectiveness and efficiency of the proposed method. In the first case, we obtain the constraint sets of uncertain parameters to avoid collision between trains. In the second case, the correlation of position report cycle and MA generation cycle is analyzed under both the normal and the abnormal condition influenced by packet-loss factor. Finally, considering stochastic characterization of time distributions and real-time feature of moving block control system, the transient probabilities of wireless communication process are obtained by stochastic time petri nets.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

The train control system is a typical safety-critical system, in which the safety is one of the most important issues. How to improve the design of the train control system, including shorten the development cycle and reduce design cost, to ensure the safe operation of the train has become an essential problem in scientific researches and engineering applications. The main methods of checking the system's correctness are dependent on simulation, testing or model checking approaches [1–3]. However, both simulation and testing methods are time-consuming and it is very difficult to develop a collection of test cases or scenarios that covers all dynamic behaviors of the system. Different from simulation and testing, the model-based verification method can examine all possible behaviors of the formal model. In last few years, the model-based method [4–6] is proposed and plays an important part in the safety modeling and verification. By modeling and verifying the top-level safety requirements with non-temporal nature, [7] proposed a top-level framework for analyzing the segment control mechanism of a distributed railway control system that includes the train, signal points and switch boxes. [8] established a model-based development approach that integrates SysML and Simulink/Stateflow to rigorously handle complex system requirements when projects grew in size and studied the transformation mechanism from the SysML to Simulink/Stateflow to realize the code automatic generation of used models. On the basis of CSP∥B modeling and verification method, [9] proposed a structured way to refine track plans by analyzing the collision and derailment freeness problem of interlocking railway system.

For reliability analysis and dependability evaluation, Petri Nets (PN), Colored Petri Nets (CPN) and Stochastic Petri Nets (SPN) are proposed and applied [10–15]. For example, [16] modeled the procedure of data transmission and processing using CPN and proposed a unifying approach that includes both formal and simulation-based verification of the protocol to verifying the safety communication protocols in European Train Control System (ETCS). [17] modeled plant and primary-to-secondary leaking safety procedure with CPN and verified it with formal and simulation-based methods to ensure the safety of a nuclear power

☆This paper is a collaborative effort.

* Corresponding author.
E-mail addresses: 14111052@bjtu.edu.cn (R. Cheng), ise_zhouj@ujn.edu.cn (J. Zhou), dwchen@fzu.edu.cn (D. Chen), ydsong@bjtu.edu.cn (Y. Song).

http://dx.doi.org/10.1016/j.ress.2015.09.014
0951-8320/© 2015 Elsevier Ltd. All rights reserved.

plant. [18] modeled the failure and recovery behavior of the communication link with SPN and evaluated the performance of ETCS by simulation results of construed SPN models. Considering stochastic characterization of time distributions and real-time feature of moving block control system (MBCS), the stochastic time petri nets (STPN) proposed by Vicario [19–21], is used to model the wireless communication process of MBCS. The transient probabilities of reachable state classes are obtained to monitor the wireless communication situation online. For parameters' uncertainty in the control process of high-speed trains (HSTs), many researchers use control theory to obtain the parameters evaluation on the basis of constructing the precise dynamic model of the train control system [22–24]. The main function of automatic train operation (ATO) is to automatically control the train speed to follow the computed optimal speed-distance trajectory, by regulating the traction and braking forces. In order to track the optimal speed profile, research has been done to enhance the performance of ATO. For example, [25] proposed intelligent train control algorithms to adjust the control parameters online for Subway using expert system and reinforcement learning algorithms. Based on Lyapunov stability theory, [26] designed the robust cruise controller for HST based on sampled-data to make the HST track the desired speed and ensure the safety and comfort of the operating of HST. For the ATO system under actuator saturation caused by constraints from serving motors, [27] proposed a robust adaptive control law to online estimate the unknown system parameters and stabilize the closed-loop system. However, because the unknown resistance and the nonlinearity of train control model cannot be ignored, modeling the accurate model is impossible. Control methods are only an estimation method with time-delay and disturbance.

Admittedly, the research and implementation of the existing methods have greatly improved the performance of high-speed train operation. However, there are still some drawbacks that exist in traditional analysis methods for safety-critical system in published papers:

- Simulation and testing have an important role in the overall verification of a system but are not suitable for complete verification, because only a limited number of system behaviors can be analyzed due to time limitation.
- Most formal verification methods are off-line verification methods that cannot be applied in the real-time safety-critical systems. Online verification method [28] is more meaningful for the real-time characteristic of the train control system.
- Due to the limitations of the formal models, a lot of formal models are unable to describe time-related requirements. The correlation of some key time-related parameters is difficult to determine in distributed system.
- Most top-level formal models cannot verify the correctness of hybrid system very well for satisfying the safety requirements of the system when the formal model contains uncertain parameters.
- It is difficult to construct the precise dynamic model of the train control system, the evaluation method based on control theory is so complex and difficult to predict the uncertain parameters. Train control system is inevitably influenced by time-delay of control process and disturbance of the operation environment.

As a complex, real-time, distributed system, the train control system is a hybrid system, which contains both the continuous movement behavior and the discrete control process [29,30]. Due to the hybrid property, we use linear hybrid automata (LHA) to accurately describe the dynamic process of the train control system. Because that LHA is a mathematical model, which can not only describe the discrete control through automation transitions, but also capture the continuous movement process with differential [5,6]. So, it is very suitable for analyzing and modeling the train control system. For the reasons given above, the contributions of this paper are described below:

- To begin with, in order to improve the reusability of the abstract control model, we propose a parameter analysis method to analyze an abstract LHA control model that contains uncertain parameters for satisfying the system's safety requirements.
- Then, different from the traditional ATO control method, we want to use model-based verification method to solve the parameters' uncertainty of MBCS from a new perspective. And, we also propose an online verification method to solve the state space explosion problem and improve the real-time quality of formal verification method in MBCS.
- Furthermore, in order to improve the performance of the distributed system, the correlation of key parameters is obtained based on the verification data by analyzing the movement authority (MA) generation process.
- Finally, considering stochastic characterization of time distributions, we analyze wireless communication process between RBC and HSTs by STPN model.

The remainder of this paper is organized as follows. In Section 2, we present an overview of the basic process of parameter analysis method. Section 3 provides an example of train tracking model in train control domain to illustrate the application of proposed method for solving uncertain control parameters. In order to solve the verification problem of the real-time system, two algorithms of online verification method are designed to obtain all possible executable paths of LHA within bounded time intervals in the immediate future. In Section 4, we present another case of MA generation process and the wireless communication process. Then, we discuss the MA generation cycle (MGC) under the normal and packet-loss circumstances and obtain the transient probabilities of reachable state classes. Finally, the conclusions and future works are given in Section 5.

2. Parameter analysis approach and online verification algorithms

The basic flowchart of parameter analysis approach is depicted in Fig. 1. In order to ensure the safety specification of the train control system, the proposed method comprises two parts. In the first part, the constraint sets of uncertain parameters of the abstract LHA model is obtained by using reachable set computation method. After obtaining the constraint sets of uncertain parameters, the abstract LHA model can be transformed into the concrete LHA model, which will be analyzed in the second part. Abstract LHA means it includes some uncertain parameters, and the concrete LHA means the model only contains constant parameters.

(A) The main steps in the first part are described as follows:

Step 1: Select a set of requirements or a communication protocol from the specification document, and transform them into LHA model through extracting these requirements. So, the constructed LHA model is an abstract LHA model, which contains uncertain control parameters and describes the whole dynamic control process of the system. In the transformation process, the consistency between the requirements and the corresponding LHA model must be ensured.

Step 2: The verification tools, such as HYTECH or PHAVer, can be used to check whether all locations of the model are

Download English Version:

https://daneshyari.com/en/article/805400

Download Persian Version:

https://daneshyari.com/article/805400

Daneshyari.com