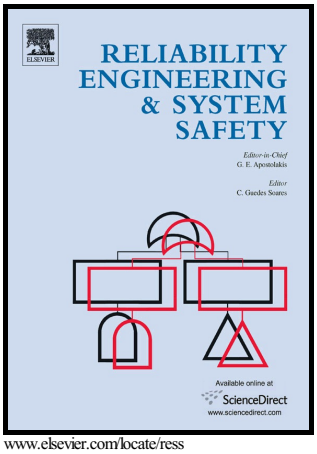

www.elsevier.com/locate/ress

Validation, Verification and Evaluation of a Train to Train Distance Measurement System by means of Colored Petri Nets

Haifeng Song, Jieyu Liu, Eckehard Schnieder

PII: S0951-8320(17)30258-2
DOI: http://dx.doi.org/10.1016/j.ress.2017.03.001
Reference: RESS5761

To appear in: *Reliability Engineering and System Safety*

Received date: 6 March 2016
Revised date: 17 January 2017
Accepted date: 2 March 2017

Cite this article as: Haifeng Song, Jieyu Liu and Eckehard Schnieder, Validation Verification and Evaluation of a Train to Train Distance Measurement System by means of Colored Petri Nets, *Reliability Engineering and System Safety* http://dx.doi.org/10.1016/j.ress.2017.03.001

Validation, Verification and Evaluation of a Train to Train Distance Measurement System by means of Colored Petri Nets

Haifeng Song[1*], Jieyu Liu[1], Eckehard Schnieder[1]

[1]Institute for Traffic Safety and Automation Engineering, Technische Universität Braunschweig, Germany

[*]Corresponding author, Institute for Traffic Safety and Automation Engineering, Technische Universität Braunschweig, Germany. Tel.: +49 0531/391-66320, Fax: +49 0531/391-66399, h.song@tu-braunschweig.de

Abstract:

Validation, verification and evaluation are necessary processes to assure the safety and functionality of a system before its application in practice. This paper presents a Train to Train Distance Measurement System (TTDMS), which can provide distance information independently from existing onboard equipment. Afterwards, we proposed a new process using Colored Petri Nets to verify the TTDMS system functional safety, as well as to evaluate the system performance. Three main contributions are carried out in the paper: Firstly, this paper proposes a formalized TTDMS model, and the model correctness is validated using state space analysis and simulation-based verification. Secondly, corresponding checking queries are proposed for the purpose of functional safety verification. Further, the TTDMS performance is evaluated by applying parameters in the formal model. Thirdly, the reliability of a functional prototype TTDMS is estimated. It is found that the procedure can cooperate with the system development, and both formal and simulation-based verifications are performed. Using our process to evaluate and verify a system is easier to read and more reliable compared to executable code and mathematical methods.

Keywords:

formal method, Colored Petri net, evaluation, performance analysis, ASK-CTL

1. Introduction

The train control system is a safety-critical system. The development of train control system has been to reduce the reliance upon and the responsibility placed on train drivers to maintain safe separation between trains. It has been done by providing different improved signaling systems. The issues related to system safety are of primary importance [1]. To assure security and functionality of each system before its application in practice, an efficient analysis procedure that can perform evaluation and verification analysis is essential.

Various methods can be applied to evaluate the reliability performance of the safety-related system. For instance, fault tree analysis [2], Bayesian network [3], and Markov Analysis [4]. However, fault tree analysis is based on the assumption that all items obey Bernoulli distribution, which is not suitable to represent practical systems [5]. Bayesian network cannot deal with system functional safety evaluation. Markov chain does not allow the use of non-exponential statistical. Importantly, real systems require a higher formalization level to describe.

The aim of this paper is to validate, verify and evaluate the TTDMS by means of Colored Petri Nets (CPN). Hence, an approach is proposed in this paper for the evaluation and verification of system description and development. Importantly, different from most analysis methodologies for systems that only perform simulations to verify the systems' performance or the correctness of system functions, this approach provides both functional safety evaluation and simulation-based verification. CPN can carry out these requirements.

There are several motivations using CPN such as: CPN is a discrete-event modeling language, which