International Journal of Software Science and Computational Intelligence
Volume 11 • Issue 2 • April-June 2019

Safe-Platoon:
A Formal Model for Safety Evaluation

Mohamed Garoui, UTBM, Sousse, Tunisia

ABSTRACT

Building a safety model to make expert decisions is an approach to improve the safety of a system. The issue of safe modeling and analyzing such domain is still an open research field. Providing quantitative estimation of a system's safety is an interesting method to study system complexity. This article explores the author's current methods and proposes a new formal model for quantitative estimation based on a stochastic activity network (SAN). This model is built based on some failure modes that affect platoon vehicles.

KEYWORDS

Platoon System, Quantitative Analysis, Safe, SAN

INTRODUCTION

Safety modeling and analysis are used in several dangerous industrial domain to explain safety of installations and operations. Such as defined by McDermid (2001): "System safety is a concept can be applied to this traditional field to help identify the set of conditions for safe operation of the system" or "The system safety concept calls for a risk management strategy based on identification, analysis of hazards and application of remedial controls using a systems-based approach". An important research work has also been initiated to provide plans to document safety modeling. The initial work is that developed by Arnaud Lanoix in (2008) wherein he uses the Event-B (Abrial, 2010) as a formal method to model and verify the behavior of platooning system. He needs the formal method that support and ensure the correctness and structuring of safety system development. The proposed technical by Event-B such as refinement which is used to progress towards implementation. An abstract model is transformed into a more concrete and elaborate model. The safety proprieties related the platoon system is specified in clause invariants in the model. Another research developed by Rugina (2005) in which aim to propose a formal modeling framework based AADL models (Bozzano et al., 2009) and GSPN models (Brenner, Fernandes, Sales, & Webber, 2005). Its framework allows the automatic generation of dependability oriented analytical models from high-level AADL models that are easier to handle for users. This framework is as stepwise approach for system dependability modeling and evaluation, using AADL and GSPNs.

In Bozzano et al. (2011), the authors propose an extension for AADL formalism and build so-called component-based modeling approach to system-software co-engineering of real-time embedded

DOI: 10.4018/IJSSCI.2019040102

sys-tems as aerospace system. The aims are then subject to different kinds of formal analysis such as model checking, safety and dependability analysis and performance evaluation. Now, we are interested to propose a formal framework based on only one formal language and subsequently helps us do analysis of system safety. For this reason, we have chosen the Stochastic Activity Network (SAN) as an extension of GSPN formalism. The SAN formalism supports the composition operators against the GSPN. These operators allow us to build a complex model.

In this article, our work addresses the problem of safeplatoon1. In this problem, our aim is to help the specialist to develop and install comprehensible and valid safe system (platoon) for a given application in a given environment. Here, we address safety of platooning system implemented as a transportation system, which has a mission within a specific context. A platoon is a series of organized vehicles that are moving in the same direction on a traffic lane.

Our work aims at developing assessment approaches and analyzable models that make it possible to study the vehicles platoon safety taking into account some phenomena, such as accidental fault occurrences, success and failures of the recovery maneuvers. The developed models are aimed at providing support to the designers for the analysis of possible solutions of platooning systems, based on safety evaluation.

The platoon safety is defined by "the system complete its mission without any disturbance which causes dangerous state to the system and its environment". The safety characterizes the confidence that can grant the absence of system failures that can have catastrophic consequences, for example in terms of loss of human lives. Several events such as the occurrence of accidental faults, mobility vehicles, and frequent loss of communications between the system entities are taken into account. This is a new problem in the context of transportation system safety analysis. The proposed architectures are based on the implementation of automatic maneuvers to ensure the safety of vehicles in the presence of perturbation events. The maneuvers are also planned to ensure the smooth functioning of the system following the occurrence of failures affecting the vehicles.

So, we have developed models, based on Stochastic Activity Network (SAN) to assess the impact of faulty vehicle as well as failure and success maneuvers on the Platooning Systems safety.

This paper is structured as follow: in Section 2 gives an overview about the formal method, Stochastic Activity Networks (SAN). Section 3 define the platooning system considered with its failure modes and its associated maneuvers. Section 4 presents the proposed safety modeling approach and its associated SAN model. Section 5 summarizes the results obtained and discusses their impact on the safety of platooning system. Finally, Section 6 concludes our approach and depicts future directions.

THE STOCHASTIC ACTIVITY NETWORK FORMALISM

Stochastic Activity Networks (SAN) are discrete events systems modeling formalism, like Petri Net. They are also able to model stochastic phenomena and are very similar to the Generalized Stochastic Petri Nets (GSPN). Additional SAN features will be explained the comparison with GSPN. Movaghar (n.d.) introduced the SAN to model a wide complex system and to make their analysis and performance and dependability assessment. Compared to Petri Net, they are characterized by the following elements as showing in Figure 1:

- **Places (small circle):** As for Petri nets, the set of places with their markings can be seen as state of the modeled system. In SAN formalism, places are of two types: ordinary and extended;
- **Activities:** Equivalent to transitions in Petri nets. Unlike GSPN, in SAN the timed activities can have either a deterministic or a stochastic duration. Stochastic ones are not necessarily exponentially distributed;
- **Input gates (red triangle):** Used to control the activation of activities. An input gate defines the condition on the marking of its input place to make the activity enabled. It also defines, thanks to the input function, the new marking of these places after the completion of its associated activity;