Home   Publications   Search   My settings   My alerts   Shopping cart   Help

Export citation   Purchase   More options...

Search

Verification of the safety communication protocol in train control system using colored Petri net ☆

Chen Lijie[a] · ▲ · ✉, Tang Tao[a], Zhao Xianqiong[a], Eckehard Schnieder[b]

[a] State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China
[b] Institute for Traffic Safety and Automation Engineering, Technical University Braunschweig, Germany

View full text

Purchase $41.95

Abstract

This paper deals with formal and simulation-based verification of the safety communication protocol in ETCS (European Train Control System). The safety communication protocol controls the establishment of safety connection between train and trackside. Because of its graphical user interface and modeling flexibility upon the changes in the system conditions, this paper proposes a composition Colored Petri Net (CPN) representation for both the logic and the timed model. The logic of the protocol is proved to be safe by means of state space analysis: the dead markings are correct; there are no dead transitions; being fair.

Further analysis results have been obtained using formal and simulation-based verification approach. The timed models for the open transmit system and the application process are created for the purpose of performance analysis of the safety communication protocol. The models describe the procedure of data transmission and processing, and also provide relevant timed and stochastic factors, as well as time delay and lost packet, which may influence the time for establishment of safety connection of the protocol. Time for establishment of safety connection of the protocol in normal state is verified by formal verification, and then time for establishment of safety connection with different probability of lost packet is simulated. After verification it is found that the time for establishment of safety connection of the safety communication protocol satisfies the safety requirements.

Keywords

EURORADIO; The safety communication protocol; Colored petri net; Verification

Figures and tables from this article:
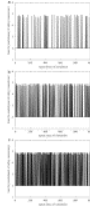

Fig. 1. Structure of EURORADIO [34].

Figure options

Fig. 2. State transition diagram of the safety layer entity in EURORADIO.

Fig. 3. CPN model of the safety layer Onboard.

Liveness Properties:
Dead Markings
7 [47, 29, 160, 159, 149, ...]
Dead Transition Instances
None
Live Transition Instances
None

Fig. 4. State space analysis report for the CPN model of the safety layer.

Fig. 5. Dead markings in the CPN of model the safety layer.

Fig. 6. Absence of self-loop terminal nodes.

Fig. 7. Absence of deadlock markings.

Fig. 8. CPN model of the channel.

Fig. 9. CPN model of application layer Onboard.

Fig. 10. Operational requirements and model checking results.

Fig. 11. Safety requirement and verification result (a).

Fig. 12. Safety requirement and verification result (b).

Fig. 13. Safety requirement and verification result (c).

Fig. 14. CPN model of channel with lost packet.

Fig. 15. Time for establishment of safety connection without lost packet.

Fig. 16. Time for safety connection with different lost packet probabilities: (a) 0.01 probability of lost packet, (b) 0.05 of lost packet and (c) 0.1 probability of lost packet.

Figure options

Table 1. Abbreviations and corresponding meanings.

View Within Article

Table 2. Tokens corresponding to service primitives.

View Within Article

Table 3. Simulation conditions

View Within Article

☆

Corresponding author.