



Verification of the safety communication protocol in train control system using colored Petri net $_{\star}$

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

http://dx.doi.org/10.1016/j.ress.2011.12.010, How to Cite or Link Using DOI



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 in normal state is verified by formal verification, and then time for establishment of safety connection of the time for establishment of safety connection of the safety connection protocol satisfies the safety communication protocol satisfies the safety requirements.

Keywords

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

Figures and tables from this article:



Ouglang controls and information and Alforent work or Society and the second and	
inst F O ANNY ACCES THE CONTRACT CONTRACT OF THE CONTRACT OF T	
VI 08	
mille fa BATAng (-975abBC)	
Fig. 2. State transition diagram of the safety layer entity in EURORADIO.	
	Figure options
128mm40 • (200)	
Mail Total Concentration	
Fig. 3. CPN model of the safety layer Onboard.	
	Figure options
	- ight of the
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.	
	Figure options
lat List of our trackinge	
via film, all "Instrumentation and the state of the st	
Fig. 5. Dead markings in the CPN of model the safety layer.	
	Figure options
	· ·g··· · ·
(as haf any formal or (ASNAN) (b) as the second of the sec	
(a) A. S. Y. Jiao Languagi, and an analysis of the state of the sta	
Fig. 6. Absence of self-loop terminal nodes.	
	Figure options
fen Valsfloward - Oslek Studiowiller Valsien I of 1011 (1996) Neb Strafficient Studiowiller (1997), obser Mark Studiowiller (1	
n (f. μ The start and the	
Fig. 7. Absence of deadlock markings.	
·	Figure options
	90.0 001010
(194549) (194549) (19454) (194549) (194569) (196	
100g 100g [01:66:4.0.40] 100g Toss 100g 100g 100g 100g 100g 100g 100g	
Fig. 8. CPN model of the channel.	
	Figure options

<pre>Fg.1. Safety requirement and welficiation result (a). fgire options fgire</pre>	Figure options Figure	Fig. 9. CPN model of application layer Onboard.	
Image: Second			Figure options
Image: second		Restart - 2016 Restart/File of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million - Restart of art - 8: Not - 1- Million	Figure options
Image: set in the set is a set if if if if is a set if if if is a set if if if is a set if			
image: state in the state	image: state in the state	Strands Mah.TrankgP001111+-:17(); In Dependencia: - Reduction Trankstratic Stranger not: Stranger not: Stranger no: Stranger no: Stranger no:	Figure options
Image: State in the state	Image: State in the state		
		Immunity -Obstachused/per/AULT11 (==10) Immunity Immun	Figure options
<figure><figure><figure></figure></figure></figure>	$eq:selected_s$	Fig. 13. Safety requirement and verification result (c).	Figure options
<figure><figure><figure><figure><figure><figure></figure></figure></figure></figure></figure></figure>	<figure><figure></figure></figure>		
$\label{eq:rescaled_statistic} \begin{split} & \int_{a}^{b} \int_{a}^{d} $	figure options	The function of the function o	Figure options
$f_{ij} = \frac{1}{2} \int_{-\infty}^{0} \int_{$	figure options		
		Fig. 15. Time for establishment of safety connection without lost packet.	Figure options

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

 \Rightarrow This work is supported by the frame of the project (no. RCS2008ZZ005) and National Science Foundation of PR China under grant no. 60736047 in State key laboratory of rail traffic control and safety in Beijing Jiaotong University.

Corresponding author. Copyright © 2011 Elsevier Ltd. All rights reserved.