Safety analysis of train control system based on model-driven design methodology

Authors
Abdelhakim Baouya, Otmane Ait Mohamed, Djamal Bennouar, Samir Ouchani

Publication date
2019/2/1

Journal
Computers in Industry

Volume
105

Pages
1-16

Publisher
Elsevier

Description
Embedded system design is a complex process that demands an extensive system level modeling. Its implementation encompasses software and hardware components and its interconnections. In such systems, it is widely recognized that safety should be considered at the design stage itself, particularly at the architectural level to minimize the design effort. This paper presents a novel methodology based on model-driven specification and probabilistic model checking to automatically analyze safety based availability before synthesizing the embedded software product. Initially, the specification relies on the Architecture Analysis and Design Language (AADL) standard. Applying this standard, software components, communication links, and hardware platform are modeled. From the software components, a formal specification suitable for analysis and verification is extracted. When the verification is done and …