brought to you by I CORE

Technical University of Denmark



Formal Development and Verification of Safe Railway Control Systems

Haxthausen, Anne Elisabeth; Vu, Linh Hong

Publication date: 2013

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):

Haxthausen, Á. E., & Vu Hong, L. (2013). Formal Development and Verification of Safe Railway Control Systems. Poster session presented at Danish Railway Conference 2013, Copenhagen, Denmark.

DTU Library

Technical Information Center of Denmark

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal



Formal Development and Verification of Safe Railway Control Systems

Challenges

Before 2021 all Danish signalling systems are going to be replaced with modern computer based systems. Central parts of these systems consist of safety-critical software.

Challenges: How to develop such new systems efficiently (i.e. cheap and fast) and at the same time ensure that they are safe?

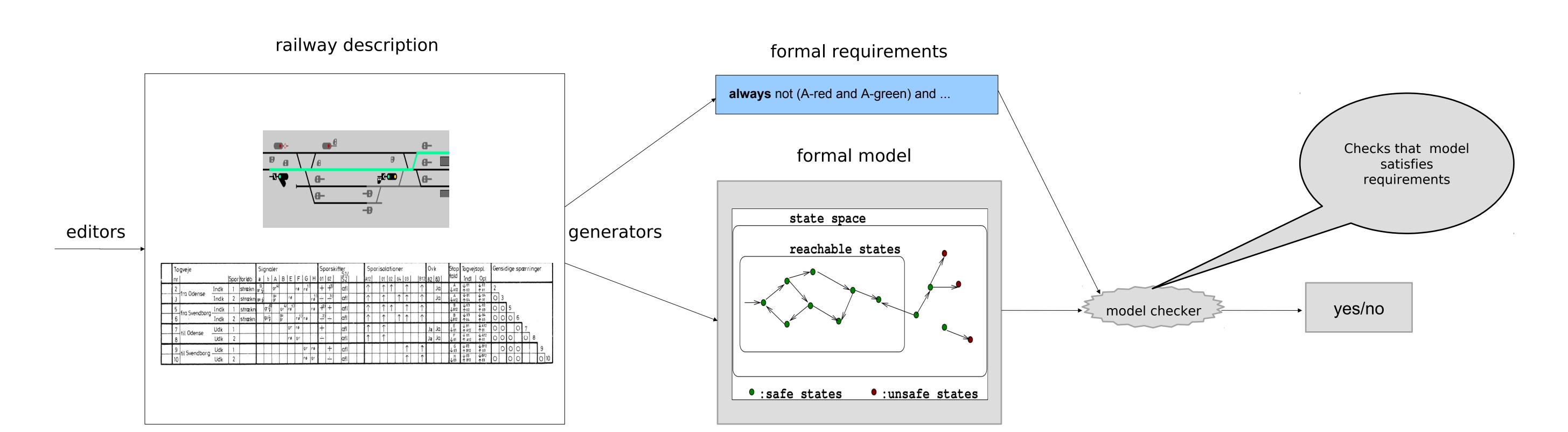


Research Goals of a Forthcoming PhD project

Research how to provide efficient methods and tools for development of safe railway control software.

The main approach to achieve this is to use of automation and formal methods.

Solution Ideas



Key idea is to provide:

- railway domain-specific language
- •re-usable formal requirements and models
- tools for automated generation of concrete, formal requirements and models from domain-specific descriptions
- techniques and tools for formal, automated verification







