Technical University of Denmark



Formal Development and Verification of Safe Railway Control Systems

Haxthausen, Anne Elisabeth

Publication date: 2016

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

Link back to DTU Orbit

Citation (APA): Haxthausen, A. E. (2016). Formal Development and Verification of Safe Railway Control Systems. Poster session presented at Kick Off for Transport DTU, Kgs. Lyngby, 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

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.





Formal Development and Verification of **Safe Railway Control Systems**

Research Question

Before 2021 all Danish signalling systems are going to be replaced with modern ERTMS niveau 2: Interoperabel jernbane uden 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 RobustRails WP 4.1

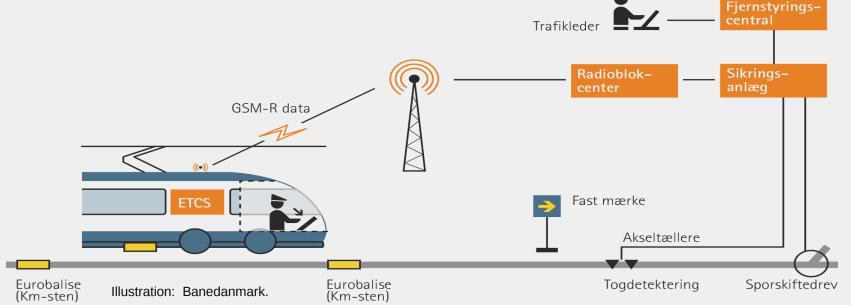
Goals: to provide efficient methods and tools for the development and safety verification of such systems.

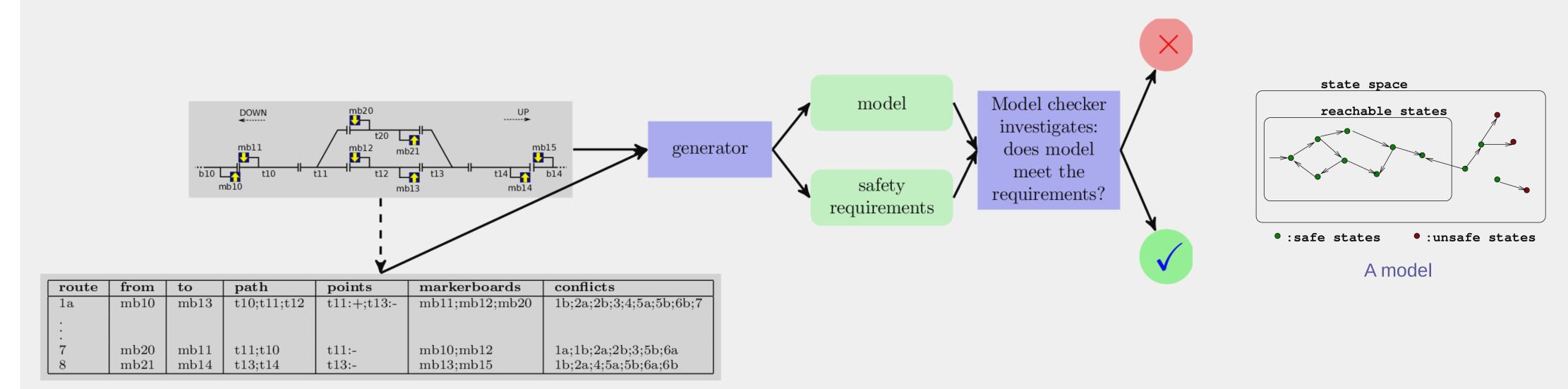
The main approach to achieve this is to make use of automation and formal (mathematically based) methods, as formal methods are strongly recommended by the CENELEC 50128 standard.

Case Study: Safety Verification of ERTMS/ETCS Level 2 Based Interlocking Systems

banedanmark

A tool chain for verifying control algorithms and train route control tables:





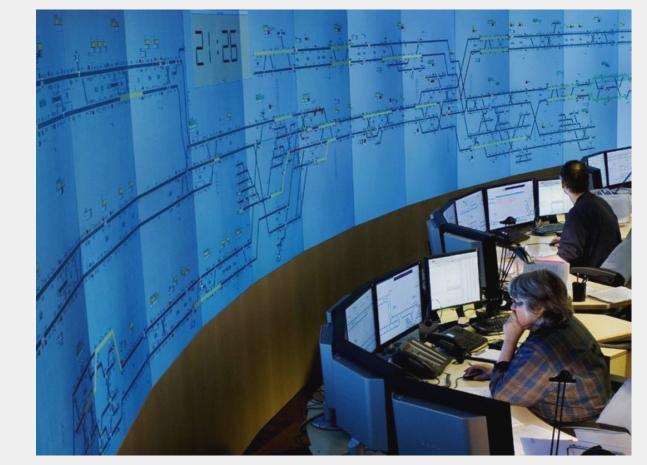


Foto: Banedanmark

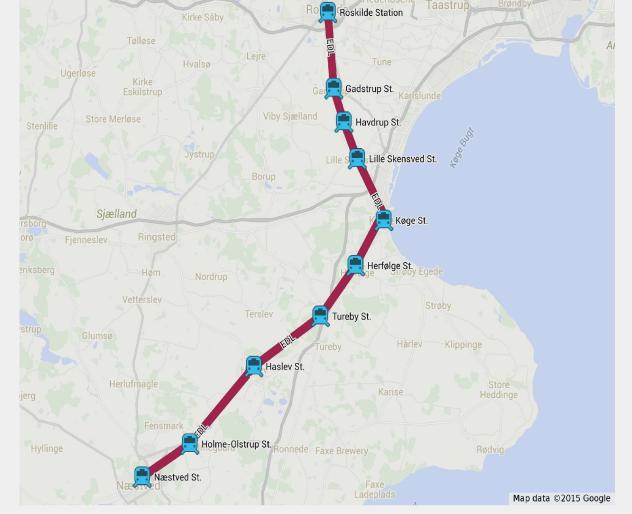
Method:

1. An interlocking system is specified by a track plan and a train route control table.

- 2. The train route control table can be automatically generated from the track plan.
- 3. A tool *automatically verifies* the specification for a number of correctness properties.

4. A tool automatically generates

(a) a *formal model* of all possible behaviours of the interlocking system and



(b) formal safety requirements (e.g no train collisions + no derailments). 5. A model checker automatically proves that the model satisfies the safety requirements. The proof is made combining advanced mathematical techniques and SMT solving.

Experiments:

The method has successfully been applied to the early deployment line in East Denmark.

Early deployment line East

InnovationsFonden Forskning, teknologi & vækst i danmark

RobustRailS Assoc. Professor Anne Haxthausen (aeha@dtu.dk)

The Railway Verification Group at DTU Compute For more info, see http://www.imm.dtu.dk/~aeha/Railway