DisCoRail 2019 - International Workshop on Distributed Computing in Future Railway Systems

Distributed Interlocking

Jan Peleska, University of Bremen, Germany: **New Distribution Paradigms for Railway Interlocking**
Abstract: We discuss a new "flavour" of distributed interlocking systems, where the proper interlocking logic is allocated on cloud computers using conventional (i.e. commercial-off-the-shelf) multi-core hardware and operating systems. The servers in the cloud communicate with intelligent track elements over internet connections. Interlocking logic may even be geographically distributed on more than one server farm, introducing a new dimension of fault tolerance. This technology has been announced 2018 by Siemens Mobility, and a first application is expected to become operative this year. In this talk, it is analysed how the new distribution concept both presents opportunities for significantly higher reliability and availability, and at the same time introduces new threats to safety and security that had not been present in more conventional interlocking system architectures. We explain the basic mechanisms how safety and security are achieved in such a system, including means to safely re-use legacy interlocking software. It is shown how formal methods can be used to verify crucial safety mechanisms and allows for testing strategies with exceptional test strength. The material presented here is based on a collaboration between Siemens and Verified Systems International, a company specialised on verification and validation of safety-critical systems.

Signe Geisler, DTU Compute, Denmark (joint work with Anne Haxthausen):
Stepwise Development and Model Checking of a Distributed Interlocking System - Using RAISE
Abstract: We consider the challenge of designing and verifying control protocols for geographically distributed railway interlocking systems. We describe for a real-world case study how this can be tackled by stepwise development and model checking of state transition models in an extension of the RAISE Specification Language (RSL). This method also allows different variants of the control protocols to be explored.

Per Lange Laursen and Van Anh Thi Trinh, DTU Compute, Denmark:
Modelling and Verification of a Distributed Interlocking System - Using UPPAAL and UMC
Abstract: This presentation investigates the modelling and model checking of an existing distributed railway control system algorithm using two different model checkers: UPPAAL and UMC. Control systems for specific railway networks are verified by providing a generic model with configuration data that describes the network and involved trains. Other variants of the control system with additional features or different modelling techniques have also been developed. Experiments are carried out on all versions in order to compare them with each other. These show that the models can handle networks of various sizes and layouts as well as verifying a real-world railway network.

Paulius Stankaitis, Newcastle University (joint work with Alexei Iliasov, Tsutomu Kobayashi, Yamine Aıt-Ameur, Fuyuki Ishikawa, and Alexander Romanovsky - SHORT contribution):
Formal distributed protocol development for reservation of railway subsections
Abstract: This paper presents the rigorous development of a distributed resource allocation protocol in Event-B. The work is motivated by the challenges of ensuring safety and improving capacity of modern and emerging railway control systems. The development consists of several complementary verification steps. Ensuring deadlock freedom of the protocol is the main challenge of this work and by using proof and stochastic simulation techniques we demonstrate the continuous progress of the protocol. Protocol performance is evaluated in stressed situations by using the stochastic simulation approach.

Formal methods and tools

Thierry Lecomte, Clearsy, France: **Formal Techniques for Safer Signalling Systems**
Abstract: Designing safety critical railways signalling systems is a difficult task, given the number of dimensions to analyse, the heterogeneity and the interdependency of the devices composing these systems, and the ongoing replacement of history-based nationwide signalling systems with a unique interoperable one. To address all these issues, formal methods have been experimented on real life systems to ensure safety demonstration at system, software and data levels. The combination of existing formal proof techniques and innovative modelling approaches makes possible the discovery of specification errors (even for systems already deployed), the completion of safety cases with a higher level of confidence and the seamless development of safety critical functions.
This talk is going to present several applications of this kind, describing the technical frameworks, the added value and the results obtained so far.

Anne Haxthausen DTU Compute, Denmark (joint work with Jan Peleska and Linh Hong Vu - SHORT contribution)
The RobustRailS verification tool set
Abstract: This presentation describes the RobustRailS verification method and tool set for automated, formal modelling and verification of ERTMS Level 2 based interlocking systems, and reports on its successful application to a Danish line. The tool set is centered around a domain-specific language (DSL) for describing application specific parameters (track layout and route control tables) and provides support for an automated 3 step verification and testing approach: (1) First a static check is performed on the domain-specific description, (2) then a formal, behavioural system model is automatically generated and model checked using an induction scheme by means of bounded model checker, and (3) finally model based testing of the implemented system is done using test cases, test oracles etc. automatically generated from the formal model. The static check is able to catch errors in the control tables, while the model checking is used to check that the system model is safe and can be used to catch errors in the designed control algorithms. The testing is used to catch errors in the implemented system.

Security and Blockchain technology

Jens Braband, Siemens Mobility GmbH, Germany: **A Survey of Cybersecurity in Signaling**
Abstract: The presentation covers main developments in Railway Signaling from the early 90s e. g. specification of ERTMS and the introduction of public networks for safety-related data transmission up to today's challenges, e. g. IP based interlocking, use of COTS HW and SW, remote access etc. Also main developments in standardization as well as future developments are addressed.

Michael Kuperberg, Deutsche Bahn Systel Gmbh, Germany (partially based on joint work with Daniel Kindler and Sabina Jeschke):
Towards a Systematic Selection of a Blockchain Implementation for a Decentralized Rail Control System
Abstract: Conventional railway operations employ centralized custom software and hardware to ensure safe and secure train operations. A research project to make this setup more distributed and dynamic has created a blockchain-based prototype for decentralized train operations, train-to-train communications and usage billing. By using a tamper-resistant blockchain with smart contracts, the prototype enables the trains to find routes and make booking decisions which are conflict-free, safeguarded and protocolled in an auditable manner. In this talk, we present an approach for the systematic selection of a scalable and robust blockchain/DLT implementation for a Decentralized Rail Control System.

Moving block, Virtual coupling and positioning systems

Francesco Flammini, Linnæus University, Sweden (joint work with Stefania Santini and Valeria Vittorini):
Towards Railway Virtual Coupling
Abstract: Railway infrastructure operators need to push their network capacity up to their limits in high-traffic corridors. Virtual Coupling is considered among the most relevant innovations to be studied within the European Horizon 2020 Shift2Rail Joint Undertaking as it can drastically reduce headways and thus increase line capacity by allowing to connect dynamically two or more trains in a single convoy. This talks addresses a proof of concept of Virtual Coupling by introducing a specific operating mode within the European Rail Traffic Management System / European Train Control System (ERTMS/ETCS) standard specification, and by defining a coupling control algorithm accounting for time-varying delays affecting the communication links. To that aim, one ploy is defined to enrich ERTMS/ETCS with Virtual Coupling without changing its working principles and a numerical analysis methodology is borrowed from the automotive field

where it is used to study platooning. The numerical analysis supports the proof of concept with quantitative results in a case-study simulation scenario.

Davide Basile, Univ. of Florence, Italy (joint work with Alessandro Fantechi, Gianluca Mandò, Luigi Rucher):
Statistical model checking of hazards in an autonomous tramway positioning system
Abstract: A promising option to improve performance and contain costs of current tramway signalling systems is to introduce an Autonomous Positioning System (APS) in substitution of traditional occupancy detecting sensors. APS is an onboard system that uses a plurality of sensors (such as GPS or inertial platform) and a Sensor Fusion Algorithm (SFA) to autonomously estimate the position of the tram with the needed levels of uncertainty and protection. Au- tonomous positioning however introduces, even in absence of faults, a quantita- tive uncertainty with respect to traditional sensors. This paper investigates this issue in the context of an industrial project: a model of the envisaged solution is adopted, and the UPPAAL Statistical Model Checker is used to study possible hazards induced by the substitution of legacy track circuits with on-board satellite positioning equipment.

Franco Mazzanti, ISTI-CNR, Italy: **Modelling a Moving Block train control system: different techniques and tools**
Abstract: UML behavioral diagrams (e.g. statecharts) are often accepted and encouraged as a standard communication mechanism among stakeholders. Event B machines are often exploited for the refinement of a system into an actually executable model, and for verifying its safety properties. Process Algebras are probably the most flexible specification mechanism that allows for a compositional verification of liveness properties of system of systems.
These different points of view are illustrated with respect to the same case study represented by a skeleton of moving block train control system.

Markus Roggenbach, Swansea University (joint work with Aled Walters, Yong Zhang, Phillip James, and Monika Seisenberger - SHORT contribution):
Modelling and Verification of ERTMS – A Comparison of KeYmaera, Real-Time Maude, and UPPAAL
Abstract: The European Rail Traffic Management System (ERTMS) is a modern state-of-the-art railway control system which is based on the communication between trains and interlocking via a radio block centre. In the ERTMS standard level 2, the system is described using discrete control logic as well as differential equations when it comes to, e.g., braking curves. Thus, in its technical definition, the system is a hybrid one. The question now is what this means for modelling: either one provides a hybrid model, or one works with a timed model with explicit solutions of the differential equations. Both approaches are possible. In our presentation we compare how ERTMS can be modelled and verified with the three formal methods that come with verification tools: KeYmaera, Real-Time Maude, and UPPAAL. Here, KeYmaera allows us to formulate a hybrid model, which can be verified with theorem proving. Modelling with UPPAAL and Real-time Maude is done with timed models, where verification is performed through model-checking. Starting from a simple railway scenario, in all three methods we model ERTMS entailing elements of all components participating in its control cycle. Furthermore, we demonstrate that it is feasible to prove safety. Following previous work on comparing railway modelling approaches, we analyse commonalities and differences between the three tools w.r.t. modelling the ERTMS. The most prominent differences found concern: Simulation, Ability to cope with real world braking and acceleration curves, Ease of expressing control logic (control tables), Modelling without making a maximal progress assumption, Scalability.