European Research and Innovation

ADV.E.N.T.U.R.E.

ADVancEd iNtegraTed evalUation of Railway systEms

Advanced Integrated Evaluation of Railway Systems

by Davide Basile, Maurice ter Beek, Felicita Di Giandomenico (CNR-ISTI), Laura Carnevali and Alessandro Fantechi (University of Florence)

Researchers from the Software Technologies Lab (STLAB) of the University of Florence and the two research labs Formal Methods and Tools (FMT) and Software Engineering and Dependable Computing (SEDC) of CNR-ISTI join forces to work on innovative solutions for the evaluation of railway systems. The research is conducted in the context of the national project ADVENTURE funded by the Italian Ministry for Universities and Research (MUR) under the program for Projects of National Interest (PRIN).

The Railway domain is expected to contribute significantly to the European Green Deal by improved digitalisation and data analytics. Challenges include the goal to "increase the levels of safety, security, reliability, and comfort, thereby maintaining the EU's leadership in transport equipment manufacturing and services" [L1]. To this end, railway systems need to guarantee a set of expected Key Performance Indicators (KPIs) such as safety of the train movement, capacity (e.g. number of trains or passengers per time unit), energy efficiency, operating cost, etc. These KPIs are determined by the operation of innovative subsystems that cooperate towards the smooth performance of railway systems, supporting monitoring, command, and control of physical railway equipment.

The specific and complex interactions among these subsystems raise challenges that put at risk the accurate and efficient evaluation of the KPIs, as well as safe interoperability. First, to address them, it is necessary to overcome some current limitations of state-of-the-art hierarchical and compositional techniques for the estimation of non-functional attributes of component-based systems, in order to properly fit the railway needs. Second, advancements in formal specification of behavioural interfaces among heterogeneous components are required in order to improve the reliability of the composition of railway subsystems while reducing their cost.

The project ADVENTURE (ADVancEd iNtegraTed evalUation of Railway systEms) [L2] targets these challenges by developing innovative solutions for the evaluation of railway systems. The project focuses on the following three objectives, using Model-Driven Engineering (MDE) methods and multi-paradigm or multi-formalism approaches to help create bridges between different levels of abstraction:

- Qualitative evaluation of the safety of complex distributed railway systems, by means of diverse techniques like compositional model checking, synthesis of specifications provided as behavioural interfaces and tool support for relating specifications with implementations.

- Quantitative evaluation of dependability attributes despite of failures, in particular related to communication failures, by means of quantitative modelling and analysis of the timed failure logic of the system under analysis.
- Quantitative evaluation of trade-offs between availability/performance and energy efficiency, taking into account different smart policies of energy saving as well as failures, criticalities and priorities of the system under analysis.

The solutions developed during the project will be validated by their application to systems that are highly representative of the innovation trends in railways, namely decentralised interlocking, standard interfaces and smart de-icing systems.

A variety of formal methods and tools have successfully been applied to railway systems to address challenges in the railway domain, involving both qualitative and quantitative techniques [R1,R2,R3]. ADVENTURE aims to advance the state-of-the-art in the formal specification of railway interfaces as behavioural contracts, their formal verification and connection with implementations realised using a correct-by-design methodology. ADVENTURE also aims to advance the state-of-the-art in failure logic analysis of component-based systems. First, by the definition of an agile MDE approach tailored to the specific needs of the railway domain, concerning both the system structure and the mechanisms of failure propagation. Second, by the definition and integration of compositional analysis methods capable of handling the complexity of the railway systems being considered, in particular in terms of the number of components and failure modes. Finally, ADVENTURE aims to advance the modelling and analysis of smart deicing systems by introducing more comprehensive aspects, such as traffic load on individual railway switches.

ADVENTURE, funded by the European Union – NextGeneration EU, will run until November 2025 and is coordinated by Alessandro Fantechi from the University of Florence, who is moreover an expert member of the Scientific Steering Group of the Europe's Rail Joint Undertaking [L3].

Links:
[L1] https://kwz.me/hAQ
[L2] https://stlab.dinfo.unifi.it/pages/projects/adventure/
[L3] https://kwz.me/hAR

References:
[1] D. Basile, M. H. ter Beek, "Contract Automata Library," Sci. Comput. Program, vol. 221, 2022. doi: https://doi.org/10.1016/j.scico.2022.102841
[2] L. Carnevali, et al., "Stochastic modeling and analysis of road-tramway intersections," Innov. Syst. Softw. Eng., vol. 16, 2020. doi: https://doi.org/10.1007/s11334-019-00355-1
[3] S. Chiaradonna, et al., "Enhancing sustainability of the railway infrastructure: trading energy saving and unavailability through efficient switch heating policies," Sustain. Comput. Inform. Syst., vol. 30, 2021. doi: https://doi.org/10.1016/j.suscom.2021.100519

Please contact:
Maurice ter Beek, CNR-ISTI
maurice.terbeek@isti.cnr.it

Distributed Information Security Auditing Using Blockchains

by Lukas König, Martin Pirker, Simon Tjoa, Peter Kieseberg (St. Pölten University of Applied Sciences)

Information security is becoming increasingly important due to the growing threats in the digital space. In supply chains in particular, it is essential to ensure that all participating companies have achieved an adequate level of protection, as vulnerabilities in one organisation can jeopardise the entire supply chain. We present a concept for blockchain-based, distributed information security audits, where companies can prove their level of protection to each other and increase trust in supply chain security.

Information security audits, especially in the context of globally established standards such as ISO 27001, fulfil the purpose of an independent and objective assessment of a company's security level and serve as an important part of realising security strategies, especially when considering ICT-critical infrastructures. Still, the current approaches mainly focus on single organisations. As securing supply chains is increasingly becoming a central aspect of modern companies' overall risk assessment, the security and resilience of the underlying ICT systems of partners, suppliers as well as vendors, are playing an increasingly important role. This has also been recognised by the EU, which has addressed this issue at legislative level with the Cyber Resilience Act, as well as the NIS2 directive.

When it comes to the relationship between safe supply chains and the level of security that an individual organisation possesses, it is possible for vulnerabilities at a single point to put the entire supply chain in jeopardy over the course of time [1]. Consequently, it is not only essential for each single organisation to conduct routine security checks, but it is also essential for all of the organisations that are a part of a supply chain to participate in such checks.

Although securing supply chains is becoming increasingly important, there is still a lack of scientific work on this topic. Previous publications on distributed auditing deal with, for example, metrics for security maturity levels, records of network monitoring, or decentralised risk management. However, an actual decentralised system for securing and communicating information security audits has not yet been described, yet communicating actual threats, vulnerabilities and (successful and unsuccessful) attacks along a supply chain is key for enhancing its resilience.

One major concern is that any exchange of this kind of audit information might reveal sensitive information about an organisation's security gaps, which means that sharing these results is not in the organisation's own interest in terms of protection. Sharing information about security incidents, technical and organisational measures with external third parties requires a high level of trust, as such information can reveal ob-