International Journal on Software Tools for Technology Transfer (2024) 26:127–129
https://doi.org/10.1007/s10009-024-00744-3

GENERAL

Special Issue: FMICS 2022

Formal Methods for Industrial Critical Systems

Jan Friso Groote[1] · Marieke Huisman[2]

Accepted: 6 February 2024 / Published online: 15 February 2024
© The Author(s) 2024

Abstract
To stimulate the development and application of formal methods in industry, we need to promote research and development for the improvement of formal methods and tools for industrial applications, and we need to exchange experiences of the industrial usage of these methods and tools. This special issue of Software Tools for Technology Transfer presents various tools and experience reports that are targeting the use of formal methods in industry. The papers in this special issue are extended versions of selected conference papers from the proceedings of the 27th International Conference on Formal Methods for Industrial Critical Systems (FMICS 2022).

Keywords Deductive verification · Smart contracts · Interactive validation · Spatio-temporal logics · Autonomous driving · Avionic software · Monotony analysis stochastic specifications · Real-time operating systems

1 FMICS

This special issue of the journal Software Tools for Technology Transfer (STTT) contains revised and extended versions of six papers selected out of 13 papers accepted for presentation at the 27th International Conference on Formal Methods for Industrial Critical Systems (FMICS 2022) [4].

The aim of the FMICS conference series is to provide a forum for researchers interested in the development and application of formal methods in industry. FMICS brings together scientists and engineers who are active in the area of formal methods and are interested in exchanging their experiences of the industrial usage of these methods. The FMICS conference series also strives to promote research and development for the improvement of formal methods and tools for industrial applications.

Topics of interest for FMICS are:

- Case studies and experience reports on industrial applications of formal methods, focusing on lessons learned or identification of new research directions.
- Methods, techniques, and tools to support automated analysis, certification, debugging, descriptions, learning, optimization and transformation of complex, distributed, real-time, embedded, mobile, and autonomous systems.
- Verification and validation methods (model checking, theorem proving, SAT/SMT constraint solving, abstract interpretation, etc.) that address shortcomings of the existing methods with respect to their industrial applicability (e.g., scalability and usability issues).
- Impact of the adoption of formal methods on the development process and associated costs. Application of formal methods in standardization and industrial forums.

2 This Special Issue

The peer-reviewed papers collected in this special issue have been invited by the guest editors among the top papers presented at FMICS 2022.

The papers in this special issue all develop tool-supported verification and validation techniques. The first two papers describe how verification and validation techniques can be made adapted and extended to make them usable in an industrial context. The next two papers focus in particular on verification and validation techniques that can be used on safety-critical applications. The last two papers investigate how verification can be made more scalable by exploiting compositionality.

Below we give a short summary of each paper.

✉ M. Huisman

[1] Eindhoven University of Technology, PO Box 513, 5600 MB
Eindhoven, The Netherlands

[2] University of Twente, P.O. Box 217, 7500 AE Enschede,
The Netherlands

2.1 Industrial verification and validation

Deductive verification of smart contracts with Dafny [2]

The paper presents a methodology for verifying Ethereum smart contracts using Dafny. The methodology is developed in several steps. First, support for reasoning about closed contracts that do not depend on external calls is developed. In addition, support to reason about code using external calls is added, by modeling (potential) callbacks explicitly (and nondeterministically) in Dafny. As a result, it is possible to prove properties that are preserved by arbitrary callbacks, e.g., using a global invariant and additional specifications. The paper demonstrates the approach on verified versions of a token contract (with and without external calls and locks) and an auction contract.

Generating interactive documents for domain-specific validation of formal models [7]

The paper describes tool support for the validation of B specifications by improving domain-specific visualizations of animation traces and interactive models. These visualizations are important to get the feedback from stakeholders and domain experts in an early stage of the development. The paper focuses on how this visualization support is developed.

2.2 Safety-critical applications

Monitoring of spatio-temporal properties with nonlinear SAT solvers [6]

This paper presents a runtime verification approach for monitoring spatio-temporal properties with a demonstration in the setting of autonomous driving. Spatio-temporal logic combines temporal logic with metric spaces. It is shown how this logic can be encoded in the first-order logic over the Reals (FOL_R), which can be reasoned about using SMT. The approach has been integrated with a simulation test-bed based on the CARLA simulator allowing for real-world testing with images from a traffic camera.

Certification of avionic software based on machine learning: the case for formal monotony analysis [3]

This paper discusses how the use of machine learning impacts certification for avionic software. It focuses on one particular case, the monotony guarantees that ensure the correspondence with the underlying physics. The paper proposes an approach for the analysis of monotony of neural networks, by proposing an algorithm for splitting the input space into increasingly smaller partitions, to give lower and upper bounds on the nonmonotonic space coverage. The algorithm identifies a partition as not satisfying monotony, partially satisfying it, or totally satisfying it (meaning that each point within it satisfies monotony). The approach uses logical encoding in linear real arithmetic and MILP solving in an incremental loop that refines the space partitioning. To illustrate the approach, an aeronautical use case is presented where a pretrained neural network is used to estimate brake distance for airplanes (based on the status of different brakes).

2.3 Compositional verification

Formally verifying decompositions of stochastic specifications [5]

This paper presents a new framework for compositional verification by means of refinement analysis of real-time probabilistic systems, where traces are used to describe the continuous-time evolution of the system. This is relevant for industrial safety-critical applications, as their behaviors are often of stochastic nature, for example, giving a bound on the probability that a system failure will occur before a given time. The paper specifies the behavior of such systems using timed automata combined with probabilistic acceptance conditions. It then shows how such systems can be verified in a compositional manner by reducing the verification problem to checking emptiness of the solution space for a system of linear inequalities.

Reusable formal models for concurrency and communication in custom real-time operating systems [1]

This paper proposes a reusable set of UPPAAL timed automata templates that can be used to model and verify concrete processes that are scheduled for their execution using a real-time operating system (RTOS), in particular, the templates model tasks, events, scheduler, sensor inputs, data queues, and so on. Timing constraints (BCET and WCET) for individual steps of tasks are encoded as location invariants and transition guards. The resulting verification framework is applied to a model of a search-and-rescue robot application.

Acknowledgements We are grateful to all the authors for their contributions and to the program committee of FMICS 2022 for their help in selecting the papers for the conference program, including the papers for this issue. We are especially grateful to the FMICS 2022 program committee and external referees who reviewed the extended versions of the papers that appear in this special issue.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Adelt, J., Gebker, J., Herber, P.: Reusable formal models for concurrency and communication in custom real-time operating systems. Int. J. Softw. Tools Technol. Transf. (2024). In this issue
2. Cassez, F., Fuller, J., Quilles, H.M.A.: Deductive verification of smart contracts with Dafny. Int. J. Softw. Tools Technol. Transf. (2024). In this issue
3. Ducoffe, M., Gabreau, C., Ober, I., Ober, I., Vidot, E.G.: Certification of avionic software based on machine learning: the case for formal monotony analysis. Int. J. Softw. Tools Technol. Transf. (2024). In this issue
4. Groote, J.F., Huisman, M. (eds.): Formal Methods for Industrial Critical Systems – 27th International Conference, FMICS 2022, Warsaw, Poland, September 14–15, 2022. Proceedings, Lecture Notes in Computer Science, vol. 13487. Springer, Berlin (2022). https://doi.org/10.1007/978-3-031-15008-1
5. Hampus, A., Nyberg, M.: Formally verifying decompositions of stochastic specifications. Int. J. Softw. Tools Technol. Transf. (2024). In this issue
6. Pedro, A.M., Silva, T., Sequira, T., Lourenço, J., Seco, J.C., Ferreira, C.: Monitoring of spatio-temporal properties with nonlinear SAT solvers. Int. J. Softw. Tools Technol. Transf. (2024). In this issue
7. Vu, F., Happe, C., Leuschel, M.: Generating domain-specific interactive validation documents. Int. J. Softw. Tools Technol. Transf. (2024). In this issue

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.