Report from Dagstuhl Seminar 23041

Integrated Rigorous Analysis in Cyber-Physical Systems Engineering

Erika Abraham[*1], **Stefan Hallerstede**[*2], **John Hatcliff**[*3], **Danielle Stewart**[*4], **and Noah Abou El Wafa**[†5]

1 **RWTH Aachen University, DE.** abraham@informatik.rwth-aachen.de
2 **Aarhus University, DK.** stefan.hallerstede@wanadoo.fr
3 **Kansas State University – Manhattan, US.** hatcliff@ksu.edu
4 **Galois – Minneapolis, US.** danielle@galois.com
5 **KIT – Karlsruher Institut für Technologie, DE.** noah.abouelwafa@kit.edu

Abstract

This report documents the program and the outcomes of the Dagstuhl Seminar 23041 "Integrated Rigorous Analysis in Cyber-Physical Systems (CPS) Engineering".

This seminar brought together academic and industry representations from a variety of domains with backgrounds in different techniques to develop a roadmap for addressing the current challenges in the area of CPS engineering. An overarching theme was the potential use of integrated models and associated methodologies that support cross-technique information/results sharing and smooth workflow hand-offs between individual tools and methods.

Seminar January 22–27, 2023 – https://www.dagstuhl.de/23041
2012 ACM Subject Classification Computer systems organization → Embedded and cyber-physical systems; Security and privacy → Logic and verification
Keywords and phrases cyber-physical systems, formal methods, rigorous modelling and analysis, systems engineering
Digital Object Identifier 10.4230/DagRep.13.1.155

1 Executive Summary

Erika Abraham (RWTH Aachen University, DE)
Stefan Hallerstede (Aarhus University, DK)
John Hatcliff (Kansas State University – Manhattan, US)
Danielle Stewart (Galois – Minneapolis, US)

Overview

The design of cyber-physical systems (CPSs) typically balances requirements that concern function, performance and interaction between discrete and continuous subsystems. In the big picture CPS design must be considered in the context of systems engineering. When engineering a CPS, modelling plays a central role during early stages of the development. Depending on objectives and purpose different models are produced, say, for a concept of operation, a trade study, a preliminary design, and a detailed design. In recent years modelling methods and tools have been developed that can contribute to the development of CPSs.

[*] Editor / Organizer
[†] Editorial Assistant / Collector

Integrated Rigorous Analysis in Cyber-Physical Systems Engineering, *Dagstuhl Reports*, Vol. 13, Issue 1, pp. 155–183
Editors: Erika Abraham, Stefan Hallerstede, John Hatcliff, and Danielle Stewart
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Each method has a limited view of CPS development, say, focusing on correctness verification, scenario validation or evaluation of design alternatives. Each method is specialised on specific kinds of analyses depending on its purpose and objectives. Of course, this is necessary for reasons of effectiveness and efficiency. Unfortunately, then the outcomes of different analyses carried out on the various models of a CPS are not systematically exploited in the other models. The arguments connecting the different outcomes of independent methods and tools can be intricate and complex, potentially causing erroneous reasoning but missed opportunities when relevant outcomes remain unused.

This Dagstuhl Seminar explored systems engineering processes and methodology as a framework for rigorous reasoning to alleviate the problem of bridging different modelling methods, opening up a possibility to reason across method and stage barriers. The seminar brought together academic and industry representations from a variety of domains with backgrounds in different techniques. We developed a roadmap for addressing CPS challenges both in industry and academia, and identified ways that we can help each other overcome these challenges.

Outcomes of the Seminar

- Identified new techniques, tool capabilities and methodology improvements that will improve the ability to develop, assure, deploy, and evolve modern CPS.
- Identified gaps and needs that enumerates desired tool capabilities and methodology improvements that if successfully addressed, would improve the ability to develop, assure, deploy, and evolve modern CPS.
- Identified criteria and resources for community-based example systems that enable the interplay of multiple techniques to be evaluated across the life-cycle of system development.
- Created an activity plan for future meetings and smaller collaborative groups to build on the outcomes of the seminar.

The organizers thank all participants for their interesting ideas and viewpoints presented in talks, discussions, and informal meetings. Moreover, we would like to express our gratitude towards Schloss Dagstuhl and its staff for all the support before and during the seminar, which contributed to making this seminar a successful one.

2 Table of Contents

3 Overview of Talks

3.1 How to Prove That We Do Not Prove a Faulty Controller Safe

Wolfgang Ahrendt (Chalmers University of Technology – Göteborg, SE)

Joint work of Wolfgang Ahrendt, Yuvaraj Selvaraj, Jonas Krook, Martin Fabian

Cyber-physical systems are often safety-critical and their correctness is crucial, as in the case of automated driving. Using formal mathematical methods is one way to guarantee correctness. Though these methods have shown their usefulness, care must be taken as modeling errors might result in proving a faulty controller safe, which is potentially catastrophic in practice. This talk deals with two such modeling errors in differential dynamic logic. Differential dynamic logic is a formal specification and verification language for hybrid systems, which are mathematical models of cyber-physical systems. The main contribution is to express conditions that, when fulfilled, show the absence of certain modeling errors that would cause a faulty controller to be proven safe. The problems are illustrated with an example of a safety controller for automated driving, and it is shown that the formulated conditions have the intended effect both for a faulty and a correct controller. It is also shown how the formulated conditions aid in finding a loop invariant candidate to prove properties of hybrid systems with feedback loops. The results are proven using the interactive theorem prover KeYmaera-X.

3.2 Surrogate Verification – Neural Networks and Koopman Operator Approximations

Stanley Bak (Stony Brook University, US)

Main reference Stanley Bak, Hoang-Dung Tran: "Neural Network Compression of ACAS Xu Early Prototype Is Unsafe: Closed-Loop Verification Through Quantized State Backreachability", in Proc. of the NASA Formal Methods – 14th International Symposium, NFM 2022, Pasadena, CA, USA, May 24-27, 2022, Proceedings, Lecture Notes in Computer Science, Vol. 13260, pp. 280–298, Springer, 2022.
URL https://doi.org//10.1007/978-3-031-06773-0_15

Many systems are black-box in nature or too complex to directly verify. To work with such systems, surrogate model approaches can be used to create models that approximate system behaviors. We discussed two approaches for this problem, one for neural network approximations and one for approximations of nonlinear dynamical systems based on Koopman Operator approximations.

In Koopman Operator approximations a nonlinear system is approximated using a higher-dimension linear system. While reachability and verification of linear systems is usually much easier, the problem involves complex nonlinear initial sets of states. We overcome this using polynomial zonotopes, data structures originally designed for nonlinear reachability analysis. Further, to accommodate for the error in the model approximation, we explore conformant synthesis approaches. We are working toward developing scalable formal analysis methods that can still be applied towards complex and black-box systems.

3.3 Validation and verification approaches for safe and secure cyber-physical systems

Stylianos Basagiannis (Raytheon Technologies – Collins Aerospace – Cork, IE)

Ensuring the security and safety of cyber-physical systems (CPS) while reducing systems' environmental impact, fuel consumption, and operational cost is forcing a rethinking of future cyber-physical systems design cycles. In a continuously growing global market, next-generation CPS development requires methods and tools to promote early cross-discipline collaboration, allowing a system-wide accurate analysis, validation, and verification. Collaborative model-based design is a promising approach, in which diverse digital model representations of system elements are combined and analyzed in a virtual setting, but its full benefits have not been fully realized in the sector. At the same time, the multi-diverse engineering background of CPS teams forces requirements to be easily corrupted or misinformed from the (abstract) design till the (granular) prototype generation phase.

In this presentation, we will introduce some of our recent validation and verification approaches being applied in aerospace cyber-physical systems. The first (top-down) approach will involve the usage of simulation-based verification techniques through interval analysis approaches [1] for the safety verification of advanced engine control solutions. The second (bottom-up) approach will involve the usage of theorem-proving techniques at the instruction set level for embedded (RISC-V) micro-architectures for verifying security requirements. Activities described in this presentation are part of two European-funded projects in which Collins Aerospace Ireland is participating; namely the ECSEL VALU3S (2020-2023) [2] and Horizon Europe REWIRE (2022-2025) [3].

References

1 Vassilios A. Tsachouridis and Georgios Giantamidis and Stylianos Basagiannis and Kostas Kouramas, Formal analysis of the Schulz matrix inversion algorithm: A paradigm towards computer aided verification of general matrix flow solvers, In Journal of Numerical Algebra, Control and Optimization, v10 (2), pp. 177-206, 2020.
2 ECSEL VALU3S: Verification and Validation of Automated Systems' Safety and Security, 2020-2023, https://valu3s.eu/
3 Horizon Europe REWIRE: REWiring the ComposItional Security VeRification and AssurancE of Systems of Systems Lifecycle, 2022-2025, https://www.rewire-he.eu/

3.4 Developing a prototype of a mechanical ventilator controller from requirements to code with ASMETA

Andrea Bombarda (University of Bergamo – Dalmine, IT)

Joint work of Andrea Bombarda, Silvia Bonfanti, Angelo Gargantini, Elvinia Riccobene
Main reference Andrea Bombarda, Silvia Bonfanti, Angelo Gargantini, Elvinia Riccobene: "Developing a Prototype of a Mechanical Ventilator Controller from Requirements to Code with ASMETA", Electronic Proceedings in Theoretical Computer Science, Vol. 349, pp. 13–29, Open Publishing Association, 2021.
URL https://doi.org//10.4204/eptcs.349.2

Rigorous development processes aim to be effective in developing critical systems, especially if failures can have catastrophic consequences for humans and the environment. Such processes generally rely on formal methods, which can guarantee, thanks to their mathematical foundation, model preciseness, and properties assurance. However, they are rarely adopted in practice.

In this talk, I report the experience of my research group in using the Abstract State Machine formal method and the ASMETA framework in developing a prototype of the control software of the MVM (Mechanical Ventilator Milano), a mechanical lung ventilator that has been designed, successfully certified, and deployed during the COVID-19 pandemic.

Although due to time constraints and lack of skills, no formal method was applied for the MVM project, later we wanted to assess the feasibility of developing (part of) the ventilator by using a formal method-based approach. Our development process starts from a high-level formal specification of the system to describe the MVM main operation modes. Then, through a sequence of refined models, all the other requirements are captured, up to a level in which a C++ implementation of a prototype of the MVM controller is automatically generated from the model, and tested.

Along the process, at each refinement level, different model validation and verification activities are performed, and each refined model is proved to be a correct refinement of the previous level. By means of the MVM case study, we evaluate the effectiveness and usability of our formal approach.

3.5 Monitoring distributed cyber-physical systems: opportunities and challenges

Borzoo Bonakdarpour (Michigan State University – East Lansing, US)

CPS is becoming increasingly distributed, where a set of asynchronous agents deal with continuous signals that do not share a global clock. We advocate for runtime verification (RV) of distributed CPS as a complementary method, but a roadmap for enhancing its effectiveness and efficiency is much needed. This brief talk will go over the challenges, recent advances, open problem problems and opportunities in RV for distributed CPS. We will first explain the challenges of verification of a set of continuous signals subject to clock drifts against specifications expressed in the signal temporal logic (STL). We then explain how a practical assumption, namely, an off- the-shelf clock synchronization algorithm such as NTP, can drastically contribute to efficiency and effectiveness of RV. Finally, we show how exploiting

special characteristics of CPS such as the knowledge of dynamics of physical processes can reduce the runtime overhead and discuss a roadmap of open problems, applications, and opportunities.

3.6 Optimizing different flavours of nondeterminism in hybrid automata with random clocks

Joanna Delicaris (Universität Münster, DE) and Anne Remke (Universität Münster, DE)

Joint work of Joanna Delicaris, Anne Remke, Carina da Silva, Stefan Schupp
Main reference Carina Pilch, Stefan Schupp, Anne Remke: "Optimizing Reachability Probabilities for a Restricted Class of Stochastic Hybrid Automata via Flowpipe-Construction", in Proc. of the Quantitative Evaluation of Systems – 18th International Conference, QEST 2021, Paris, France, August 23-27, 2021, Proceedings, Lecture Notes in Computer Science, Vol. 12846, pp. 435–456, Springer, 2021.
URL https://doi.org//10.1007/978-3-030-85172-9_23

Stochastic hybrid automata (SHA) are a powerful tool to evaluate the dependability and safety of critical infrastructures. However, the resolution of nondeterminism, which is present in many purely hybrid models, is often only implicitly considered in SHA. This paper instead proposes algorithms for computing maximum and minimum reachability probabilities for singular automata with *urgent* transitions and random clocks which follow arbitrary continuous probability distributions. We borrow a well-known approach from hybrid systems reachability analysis, namely flowpipe construction, which is then extended to optimize nondeterminism in the presence of random variables. Firstly, valuations of random clocks which ensure reachability of specific goal states are extracted from the computed flowpipes and secondly, reachability probabilities are computed by integrating over these valuations. We compute maximum and minimum probabilities for history-dependent prophetic and non-prophetic schedulers using set-based methods. The implementation featuring the library Hypo and the complexity of the approach are discussed in detail. Two case studies featuring nondeterministic choices show the feasibility of the approach.

3.7 Application of Reachability Analysis to MAPE-K Loops

Cláudio Gomes (Aarhus University, DK)

Joint work of Cláudio Gomes, Hao Feng, Casper Thule, Kenneth Lausdahl, Peter Gorm Larsen, Thomas Wright, Jim Woodcock
Main reference Thomas Wright, Cláudio Gomes, Jim Woodcock: "Formally Verified Self-adaptation of an Incubator Digital Twin", in Proc. of the Leveraging Applications of Formal Methods, Verification and Validation. Practice – 11th International Symposium, ISoLA 2022, Rhodes, Greece, October 22-30, 2022, Proceedings, Part IV, Lecture Notes in Computer Science, Vol. 13704, pp. 89–109, Springer, 2022.
URL https://doi.org//10.1007/978-3-031-19762-8_7

The performance and reliability of Cyber-Physical Systems are increasingly aided through the use of digital twins, which mirror the static and dynamic behaviour of a Cyber-Physical System (CPS) in software. Digital twins enable the development of self-adaptive CPSs which reconfigure their behaviour in response to novel environments. It is crucial that these self-adaptations are formally verified at runtime, to avoid expensive re-certification of the reconfigured CPS.

In this talk, I discuss formally verified self-adaptation in a digital twinning system, by constructing a non-deterministic model which captures the uncertainties in the system behaviour after a self-adaptation. We use Signal Temporal Logic to specify the safety requirements the system must satisfy after reconfiguration and employ formal methods based on verified monitoring over Flow* flowpipes to check these properties at runtime. This gives us a framework to predictively detect and mitigate unsafe self-adaptations before they can lead to unsafe states in the physical system.

3.8 Systems engineering with formal methods: darpa case successes, challenges, and gaps

David Hardin (Collins Aerospace – Cedar Rapids, US)

This talk provides a summary of experiences in the development of a Systems Engineering Environment using Formal Methods-based tools on the DARPA CASE program, highlighting notable successes, research and development challenges, as well as technology gaps.

3.9 Heterogeneous Approaches to Safety of Automated Driving Systems: Search-based Testing and Refinement-based Verification

Fuyuki Ishikawa (National Institute of Informatics – Tokyo, JP)

In this talk, I will introduce our research for safety of automated driving systems (ADS).

We had our intensive work on automated testing and debugging for the path planning function in ADS via simulation. Multiple requirements need to be satisfied such as safety, comfort, and compliance with traffic rules. Violations may occur in very specific traffic scenarios or simulator configurations such as positions of other cars. Our technical approach is to make use of automated testing and debugging techniques, originally for program code, by adapting them to the continuous and uncertain ADS problems. We employed search-based testing techniques to explore simulation configurations that lead to violations, e.g., [1]. We also applied fault localization techniques to analyze possible causes of detected violations [2]. Our techniques were evaluated with a simulator provided by our partner Mazda.

To complement these heuristics or search-based approaches, we are also working on a formal approach called Responsibility-Sensitive Safety (RSS). Intuitively, RSS is an approach to define rules such that no crash occurs if all the traffic participants obey them. We formulated RSS with Hoare-like pre-post decomposition and made a case study of refinement-based safety verification with the Event-B formalism for ADS that switches between a black-box AI-based controller and a conservative safe controller [4].

These studies have considered the control aspect of ADS while the emerging difficulties lie in the perception aspect, especially using deep neural networks (DNN). After interviews with industrial partners, our "Engineerable AI" project tackles the problem of safety-aware DNN update. We may want to "fix" our DNN component to mitigate the risk by specific

errors, e.g., misclassifying pedestrian to something else. However, re-training with additional dataset can shuffle the millions of DNN parameters. We may not have intended improvement or even have unintended degradation for other error types. We defined benchmarks with our industry partners that evaluate many (10+) of fine-grained safety metrics for the prediction performance. We are tackling them by unique techniques to apply fault localization techniques to identify "suspicious neurons" in DNN for safety-aware, regression controlled update, e.g., [3].

We believe integrating these heterogeneous approaches is essential to deal with complexity and uncertainty of safety-critical CPS such as ADS.

References

1 Yixing Luo, Xiao-Yi Zhang, Paolo Arcaini, Zhi Jin, Haiyan Zhao, Linjuan Zhang, Fuyuki Ishikawa, Targeting Requirements Violations of Autonomous Driving Systems by Dynamic Evolutionary Search, The 36th IEEE/ACM International Conference on Automated Software Engineering (ASE 2021), pp.295-305, November 2021
2 Xiao-yi Zhang, Paolo Archani, Fuyuki Ishikawa, An Incremental Approach for Understanding Collision Avoidance of an Industrial Path Planner, IEEE Transactions on Dependable and Secure Computing, March 2023
3 Davide Li Calsi, Matias Duran, Xiao-Yi Zhang, Paolo Arcaini, Fuyuki Ishikawa, Distributed Repair of Deep Neural Networks,The 16th IEEE International Conference on Software Testing, Verification and Validation (ICST 2023), April 2023
4 Tsutomu Kobayashi, Martin Bondu, Fuyuki Ishikawa, Formal Modelling of Safety Architecture for Responsibility-Aware Autonomous Vehicle via Event-B Refinement, The 25th International Symposium on Formal Methods (FM 2023), March 2023

3.10 Data-Driven Verification for Dynamical Systems Under Uncertainty

Nils Jansen (Radboud University Nijmegen, NL)

Joint work of Thom S. Badings, Licio Romao, Alessandro Abate, Nils Jansen
Main reference Thom S. Badings, Licio Romao, Alessandro Abate, Nils Jansen: "Probabilities Are Not Enough: Formal Controller Synthesis for Stochastic Dynamical Models with Epistemic Uncertainty", CoRR, Vol. abs/2210.05989, 2022.
URL https://doi.org//10.48550/arXiv.2210.05989

Capturing both aleatoric and epistemic uncertainty in models of robotic systems is crucial to designing safe controllers. Most existing approaches for synthesizing certifiably safe controllers exclusively consider aleatoric but not epistemic uncertainty, thus requiring that model parameters and disturbances are known precisely. We present a novel abstraction-based controller synthesis method for continuous-state models with stochastic noise, uncertain parameters, and external disturbances. By sampling techniques and robust analysis, we capture both aleatoric and epistemic uncertainty, with a user-specified confidence level, in the transition probability intervals of a so-called interval Markov decision process (iMDP). We then synthesize an optimal policy on this abstract iMDP, which translates (with the specified confidence level) to a feedback controller for the continuous model, with the same performance guarantees. Our experimental benchmarks confirm that accounting for epistemic uncertainty leads to controllers that are more robust against variations in parameter values.

References

1 Badings, T., Abate, A., Nils Jansen, Parker, D., Poonawala, H. & Stoelinga, M. Sampling-Based Robust Control of Autonomous Systems with Non-Gaussian Noise. *AAAI*. pp. 9669-9678 (2022)

2 Badings, T., Romao, L., Abate, A., Parker, D., Poonawala, H., Stoelinga, M. & Jansen, N. Robust Control for Dynamical Systems with Non-Gaussian Noise via Formal Abstractions. *Journal Of Artificial Intelligence Resesarch*. **76** pp. 341-391 (2023)

3 Badings, T., Romano, L., Abate, A. & Jansen, N. Probabilities Are Not Enough: Formal Controller Synthesis for Stochastic Dynamical Models with Epistemic Uncertainty . *AAAI*. (2023)

3.11 Dynamic Model Composition in Digital Twins

Einar Broch Johnsen (University of Oslo, NO)

Digital twins are currently revolutionizing industry [9] and are entering into the world of medicine (e.g., [7]) and natural science (e.g., [1]). A digital twin is an information system that analyzes the behavior of a physical or cyber-physical system by connecting streams of observations of this twinned system to dynamic (e.g., simulation) and static (e.g., asset management) models. In complex settings, the digital twin will often need to manage several models that reflect different subsystems or different aspects of the twinned system. To analyze such complex systems, digital twins must ensure the correct composition of these models. However, the composition problem for models in digital twins remains unresolved [8]; e.g., models may be at different levels of abstraction, at different granularities or scales, and use different modeling concepts.

In this talk, we discuss this problem for digital twins, with a focus on the composition of heterogeneous dynamic models. For the integration and transfer of information between subsystems, digital twins may profit from a formalization of domain knowledge using ontologies, which has proven effective to unify data models. We have started to explore this approach to correctness and compositionality in digital twins by combining formalized asset models [2] with dynamic behavioral models [4, 6]. This has been done in the context of SMOL [5], a small object-oriented orchestration language[1] which can (a) dynamically create models and integrate them into a program and (b) lift the runtime configuration of a program into a static asset model which can be queried from inside the programs using semantic technologies [3].

Climate barometer for the Oslo Fjord. In a recently started project in collaboration with natural sciences, we tap into on-going efforts to equip the Oslo Fjord (see Fig. 1) with sensors. Our purpose is to combine these sensor streams with digital twin technology to analyze the effects of climate change on ecosystems in the fjord in "real time". During intense precipitation periods (extreme weather), the circulation in the fjord system will change, but it is not known how extreme weather changes the circulation in the fjord. We study this problem by combining two kinds of models. First, a low-resolution circulation model of the fjord. Second, a high-resolution hydro-dynamical models of turbulence in riverine floods

[1] https://smolang.org/

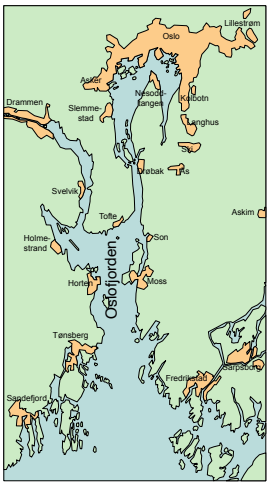

Figure 1 The Oslo Fjord System.

Figure 2 Extreme weather floods.

Figure 3 Custom drifter sensor.

(see Fig. 2). The composition of these models will be decided by sensor data from mobile sensors (using an "openSensor" solution, see Fig. 3), tracking the water from the river into the fjord. This composition poses several challenges: (a) the difference in scale between the models needs to be addressed and (b) the exact positioning of the models with respect to each other needs to be decided by the sensor data. Our aim is to formalize this notion of correct composition in a "fjord asset model" of the digital twin, such that the twin can use it together with the sensor data to dynamically compose and adjust the models.

Acknowledgment. This work is a collaboration with Atle Jensen (Dept. of Mathematics, Univ. of Oslo), Kai H. Christensen (Norwegian Meteorological Institute), and Eduard Kamburjan, S. Lizeth Tapia Tarifa, Rudolf Schlatte, Vidar Klungre, David Cameron, Martin Giese and Ingrid Chieh Yu (SIRIUS, Dept. of Informatics, University of Oslo).

References

1 P. Bauer, P. D. Dueben, T. Hoefler, T. Quintino, T. C. Schulthess, and N. P. Wedi. The digital revolution of earth-system science. *Nature Computational Science volume*, 1:104–113, 2021.

2 J. Heaton and A. K. Parlikad. *Asset information model to support the adoption of a digital twin: West Cambridge case study.* IFAC-PapersOnLine 53(3): 366–371, 2020.

3 P. Hitzler, M. Krötzsch, and S. Rudolph. *Foundations of Semantic Web Technologies*. Chapman and Hall/CRC Press, 2010.
4 E. Kamburjan and E. B. Johnsen. Knowledge structures over simulation units. In *Proc. Annual Modeling and Simulation Conference (ANNSIM 2022)*, pages 78–89. IEEE, 2022.
5 E. Kamburjan, V. N. Klungre, R. Schlatte, E. B. Johnsen, and M. Giese. Programming and debugging with semantically lifted states. In *Proc. 18th Intl. Conf. on the Semantic Web (ESWC 2021)*, *LNCS* 12731, pages 126–142. Springer, 2021.
6 E. Kamburjan, V. N. Klungre, R. Schlatte, S. L. Tapia Tarifa, D. Cameron, and E. B. Johnsen. Digital twin reconfiguration using asset models. In *Proc. 11th Intl. Symp. on Leveraging Applications of Formal Methods, Verification and Validation. Practice (ISoLA 2022)*, *LNCS* 13704, pages 71–88. Springer, 2022.
7 J. Masison, J. Beezley, Y. Mei, H. Ribeiro, A. C. Knapp, L. Sordo Vieira, B. Adhikari, Y. Scindia, M. Grauer, B. Helba, W. Schroeder, B. Mehrad, and R. Laubenbacher. A modular computational framework for medical digital twins. *Proceedings of the National Academy of Sciences*, 118(20), 2021.
8 J. Michael, J. Pfeiffer, B. Rumpe, and A. Wortmann. Integration challenges for digital twin systems-of-systems. In *Proc. 10th Intl. Workshop on Software Engineering for Systems-of-Systems and Software Ecosystems (SESoS 2022)*, pages 9–12. ACM/IEEE, 2022.
9 F. Tao and Q. Qi. Make more digital twins. *Nature*, 573: 490–491, 2019.

3.12 Assurance-based Learning-enabled Cyber-Physical Systems: A project summary

Gabor Karsai (Vanderbilt University – Nashville, US)

Joint work of Gabor Karsai, Ted Bapty, Abhishek Dubey, Taylor Johnson, Xenofon Koutsoukos, Janos Sztipanovits and many others
URL https://assured-autonomy.isis.vanderbilt.edu/

Cyber-Physical Systems (CPS) are increasingly incorporating what one can call Learning-Enabled Components (LEC) to implement complex functions. By LEC we mean a component (typically, but not exclusively, implemented in software) that is realized with the help of data-driven techniques, like machine learning. For example, an LEC in an autonomous car can implement a lane follower function such that one trains an appropriate convolutional neural network with a stream of images of the road as input and the observed actions of a human driver as output. The claim is that such LEC built via supervised learning is easier to implement than building a very complex, image processing driven control system that steers the car such that it stays on the road. In other words, if the straightforward design and engineering is too difficult, a neural network can do the job – after sufficient amount of training. For high-consequence systems the challenge is to prove that the resulting system is safe: it does no harm, and it is live: it accomplishes its goals. Safety is perhaps the foremost problem in autonomous vehicles, especially for ones that operate in a less-regulated environment, like the road network. The traditional technology for proving the safety of systems is based on extensively documented but often informal arguments – that are very hard to apply to CPS with LEC. The talk will focus on a recent project that aims at changing this paradigm by introducing (1) verification techniques whenever possible (including proving properties of the "learned" component), (2) monitoring technology for assurance to indicate when the LEC is not peforming well, and (3) formalizing the safety case argumentation process so that it can be dynamically evaluated. The application target is autonomous vehicles, with significant, but not exclusively used LECs. The goal is to construct an engineering process and a supporting toolchain that can be used for the systematic assurance of CPS with LECs.

3.13 Revisiting the challenges in combining requirements engineering and formal methods for CPS

Régine Laleau (IUT Sénart-Fontainebleau, FR)

Joint work of Marc Frappier, Amel Mammar, Tueno Fotso, Steve Jeffrey

Main reference Steve Jeffrey Tueno Fotso, Régine Laleau, Marc Frappier, Amel Mammar, Francois Thibodeau, Mama Nsangou Mouchili: "Assessment of a Formal Requirements Modeling Approach on a Transportation System", in Proc. of the Formal Methods and Software Engineering – 21st International Conference on Formal Engineering Methods, ICFEM 2019, Shenzhen, China, November 5-9, 2019, Proceedings, Lecture Notes in Computer Science, Vol. 11852, pp. 470–486, Springer, 2019.

URL https://doi.org//10.1007/978-3-030-32409-4_29

Main reference Steve Jeffrey Tueno Fotso, Amel Mammar, Régine Laleau, Marc Frappier: "Event-B Expression and Verification of Translation Rules Between SysML/KAOS Domain Models and B System Specifications", in Proc. of the Abstract State Machines, Alloy, B, TLA, VDM, and Z – 6th International Conference, ABZ 2018, Southampton, UK, June 5-8, 2018, Proceedings, Lecture Notes in Computer Science, Vol. 10817, pp. 55–70, Springer, 2018.

URL https://doi.org//10.1007/978-3-319-91271-4_5

A well-known rule says that the sooner a problem is identified in the development process, the better it is for the success of a project, its costs, time delivery and residual default rate. That is why requirements engineering (RE) is getting higher responsibility in the development of systems. RE, always, has to manage some tradeoffs between methods, languages, models and tools to capture well the initial goals defined in a natural language and the need to produce a clear, complete, unambiguous model of the specification for design and implementation phases. On the other hand, when developing critical systems, formal methods are used to strengthen the development process and to increase the level of confidence of the final product. In the last decade, several research works have been developed to combine requirements engineering and formal methods, mainly for software or embedded systems. Cyber-Physical Systems (CPS) combine interconnected computational and physical elements, possibly including human interactions. They are most often critical systems, especially in industrial domains like automotive, aeronautics, space, energy, medical, etc. Clearly, RE for CPS is more complex than RE for traditional embedded or software systems. Indeed, CPS design necessarily involves different engineering disciplines, such as mechanical, electrical, software engineering, relying on different sets of modeling languages. Similarly, different kinds of formal methods (e.g. logic for computational components, differential calculus for physical components) are essential to verify critical requirements such as consistency, safety, security, reliability, performance, while taking into account requirements involved by human interactions. In this talk I will introduce some of the challenges surrounding the modeling and verification of requirements for CPS through an illustrative example of a road transportation system.

3.14 Increasing Dependability of Cyber-Physical Systems by using Digital Twins

Peter Gorm Larsen (Aarhus University, DK)

Joint work of John S. Fitzgerald, Peter Gorm Larsen, Ken G. Pierce
Main reference John S. Fitzgerald, Peter Gorm Larsen, Ken G. Pierce: "Multi-modelling and Co-simulation in the Engineering of Cyber-Physical Systems: Towards the Digital Twin", in Proc. of the From Software Engineering to Formal Methods and Tools, and Back – Essays Dedicated to Stefania Gnesi on the Occasion of Her 65th Birthday, Lecture Notes in Computer Science, Vol. 11865, pp. 40–55, Springer, 2019.
URL https://doi.org//10.1007/978-3-030-30985-5_4

This presentation demonstrated the personal journey moving from formal modelling to using such models to realise digital twins for Cyber-Physical Systems (CPSs). There are many considerations that needs to be considered in order to make such a journey successful and many of these involve interdisciplinary engineering and research. Coupling models together with different mathematical backgrounds we are conducting using co-simulation. Here it is important to note that many mathematically-based models of the physical phenomena does not just have an anlytic solution and thus when simulating such models we get approximations, and these are not necessarily refinements of each other (and many of them need to be calibrated to be close to what happens in reality). Another challenge that needs to be overcome is the fact that receiving data from the physical system can be a complicated process and this will also result in discretations with approximations of the real values (e.g. due to noise). In case data is received wirelessly there will also be a time delay and this matters in a digital twin setting, in particular if one wish to control the physical twin from the digital side. Being able to estimate the state (and state transitions) of a physical twin can also be challenging when it needs to be done purely on the data that is accessible from the outside. Finally, since the models of a CPS will never be having a behaviour which will be identical to the physical system, so it is likely that there will be drifting and thus one will need to calibrate the models once in a while and determining when and how to do this is also not obvious.

3.15 Functional, Safe, Secure CPS In contact with human beings

Thierry Lecomte (CLEARSY – Aix-en-Provence, FR)

Main reference Thierry Lecomte, David Déharbe, Paulin Fournier, Marcel Oliveira: "The CLEARSY safety platform: 5 years of research, development and deployment", Sci. Comput. Program., Vol. 199, p. 102524, 2020.
URL https://doi.org//10.1016/j.scico.2020.102524

This presentation reports on the return of experience collected during the last two decades, while applying formal methods for software-based safety critical systems, from design to exploitation. These systems, legacy or brand new, are in close contact with people. Forthcoming systems have to be analysed through a huge number of dimensions (safety, security, cybersecurity, AI, autonomy, etc.). Who is going to specify, design, V&V, certify, qualify them ? We need tools, standards, and people to achieve this – people from the 30% of the population, able to use abstraction, are required. Target customers are those who do not sleep well at night – the financial argument (FM are going to save money) is quite usually ignored.

3.16 ProB after 20 Years

Michael Leuschel (Heinrich-Heine-Universität Düsseldorf, DE)

ProB has been developed over around 20 years and was initially developed in SICStus Prolog. In this talk I will discuss various lessons learned over this period, touching development, maintenance, certification and reaching industrial users.

3.17 Integrated Rigorous Analysis of CPS: Examples from the Airspace Domain

Paolo Masci (NASA Langley – Hampton, US)

This talk discusses a range of verification and validation approaches employed by the research team at NASA Langley for the analysis of new automated navigation systems for general aviation. Concrete examples will be given based on Detect-And-Avoid (DAA) systems. DAA is the capability of an aircraft to remain well clear of other aircraft and avoid collisions. The idea behind DAA is to define a safe region around the aircraft and use the current position and velocity vector of the aircraft to compute possible route conflicts with other aircraft flying nearby. DAA was originally created for Unmanned Aerial Vehicles (UAVs). The research team at NASA Langley has created a reference implementation of a DAA system [1], and is now adapting the DAA concept to manned aircraft. The ultimate goal is to create a technology that can be used by pilots in the cockpit to enhance traffic awareness and support maneuver guidance when required to comply with see and avoid regulations [2]. This research is carried out within NASA's Air Traffic Management Exploration (ATM-X) project [3], which is looking into the future of airspace operations and services.

References

1 NASA Detect and AvoID Alerting Logic for Unmanned Systems (DAIDALUS) https://shemesh.larc.nasa.gov/fm/DAIDALUS/
2 NASA Detect and Avoid in the cockpit (DANTi) https://shemesh.larc.nasa.gov/fm/DANTi/
3 NASA Air Traffic Management Exploration (ATM-X) Project https://www.nasa.gov/aeroresearch/programs/aosp/atm-x

3.18 Generative Engineering: A Paradigm for the Development of Cyber-physical Systems

Andrei Munteanu (Siemens PLM Software, BE)

Generative engineering is a new paradigm for developing cyber-physical systems. Rather than developing, increasingly more detailed model of a system, multiple architectural system variants are computationally generated and evaluated, which would be prohibitively expensive

to do by hand. The components and parameters that make up this system model optionally maps to library components in various simulations and analytics tools, with architectural models for those tools then automatically generated. This methodology was successfully applied to different use cases, from vehicle transmission design and hybrid vehicles to safety in avionics.

3.19 Logic of Autonomous Dynamical Systems

André Platzer (KIT – Karlsruher Institut für Technologie, DE)

Main reference André Platzer: "Logical Foundations of Cyber-Physical Systems", Springer, 2018.
URL https://doi.org//10.1007/978-3-319-63588-0

This talk highlights some of the most fascinating aspects of the logic of dynamical systems which constitute the foundation for developing cyber-physical systems (CPS) such as robots, cars and aircraft with the mathematical rigor that their safety-critical nature demands. Differential dynamic logic (dL) provides an integrated specification and verification language for dynamical systems, such as hybrid systems that combine discrete transitions and continuous evolution along differential equations. In dL, properties of the global behavior of a dynamical system can be analyzed solely from the logic of their local change without having to solve the dynamics.

In addition to providing a strong theoretical foundation for CPS, differential dynamic logics as implemented in the KeYmaera X prover have been instrumental in verifying many applications, including the Airborne Collision Avoidance System ACAS X, the European Train Control System ETCS, automotive systems, mobile robot navigation, and a surgical robotic system for skull-base surgery. dL is the foundation to provable safety transfer from models to CPS implementations and is also the key ingredient behind autonomous dynamical systems for Safe AI in CPS.

References

1 Platzer, A.: Logical Foundations of Cyber-Physical Systems. Springer, Cham (2018). 10.1007/978-3-319-63588-0
2 Platzer, A.: Logics of dynamical systems. In: LICS. pp. 13–24. IEEE, Los Alamitos (2012). 10.1109/LICS.2012.13

3.20 Inspiration from NASA Formal Methods Success Stories

Kristin Yvonne Rozier (Iowa State University – Ames, US)

This invited talk offers inspiration from the significant history of successful integration of formal methods into NASA projects. We highlight the differences between software and flight software, overview lessons learned from practical experience, and identify the limits of, and future challenges for, formal verification of aerospace systems. After drawing on examples from design-time verification of automated Air Traffic Control and runtime verification on-board Robonaut2, we visit the current full-system-lifecycle verification plans published for the NASA Lunar Gateway. We conclude with a collection of real-life, full-scale, open-source resources for the formal methods research community.

References

1. H. Erzberger, K. Heere, Algorithm and operational concept for resolving short-range conflicts, Proc. IMechE G J. Aerosp. Eng. 224 (2) (2010) 225–243
2. Zhao, Yang, and Rozier, Kristin Yvonne. "Formal Specification and Verification of a Coordination Protocol for an Automated Air Traffic Control System." In AVoCS 2012
3. Y. Zhao and K.Y. Rozier. Formal specification and verification of a coordination protocol for an automated air traffic control system. *Science of Computer Programming Journal*, volume 96, number 3, pages 337-353, Elsevier, December, 2014
4. Zhao, Yang, and Rozier, Kristin Yvonne. "Probabilistic Model Checking for Comparative Analysis of Automated Air Traffic Control Systems." In IEEE/ACM 2014 International Conference on Computer-Aided Design (ICCAD), 2014
5. C. von Essen & D. Giannakopoulou"Analyzing the Next Generation Airborne Collision Avoidance System" *TACAS* 2014
6. Marco Gario, Alessandro Cimatti, Cristian Mattarei, Stefano Tonetta and Kristin Y. Rozier."Model Checking at Scale: Automated Air Traffic Control Design Space Exploration." In *Computer Aided Verification (CAV)*, 2016
7. Rohit Dureja and Kristin Yvonne Rozier. "FuseIC3: An Algorithm for Checking Large Design Spaces." In Formal Methods in Computer-Aided Design (FMCAD), IEEE/ACM, Vienna, Austria, October 2-6, 2017
8. Rohit Dureja and Kristin Yvonne Rozier. "More Scalable LTL Model Checking via Discovering Design-Space Dependencies (D^3)." In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, part I, volume 10805 of Springer LNCS, pages 309-327, Springer-Verlag, Thessaloniki, Greece, 14-21 April 2018
9. B.Kempa, P.Zhang, P.H.Jones, J.Zambreno, K.Y.Rozier. "Embedding Online Runtime Verification for Fault Disambiguation on Robonaut2." FORMATS, LNCS vol 12288, 2020
10. Dabney, James B., Julia M. Badger, and Pavan Rajagopal. "Adding a Verification View for an Autonomous Real-Time System Architecture." In AIAA Scitech 2021 Forum, p. 0566. 2021
11. James Bruster Dabney, "FSW 2021: Using Assume-Guarantee Contracts In Autonomous Spacecraft." Online: `https://www.youtube.com/watch?v=zrtyiyNf674`
12. James Bruster Dabney, "FSW 2022: Using Assume-Guarantee Contracts for Developmental Verification of Autonomous Spacecraft." Online: `https://www.youtube.com/watch?v=HFnn6TzblPg`
13. B. Kempa, C. Johannsen, K.Y.Rozier. "Improving Usability and Trust in Real-Time Verification of a Large-Scale Complex Safety-Critical System." *Ada User Journal*, 2022
14. Alexis Aurandt, Phillip Jones, and Kristin Yvonne Rozier. "Runtime Verification Triggers Real-time, Autonomous Fault Recovery on the CySat-I." In *Proceedings of the 14th NASA Formal Methods Symposium (NFM 2022)*, Caltech, California, USA, May 24-27, 2022
15. Zachary Luppen, Michael Jacks, Nathan Baughman, Benjamin Hertz, James Cutler, Dae Young Lee, and Kristin Yvonne Rozier. "Elucidation and Analysis of Specification Patterns in Aerospace System Telemetry." In *Proceedings of the 14th NASA Formal Methods Symposium (NFM 2022)*, Springer, Caltech, California, USA, May 24-27, 2022
16. Benjamin Hertz, Zachary Luppen, and Kristin Yvonne Rozier. "Integrating Runtime Verification into a Sounding Rocket Control System." In *Proceedings of the 13th NASA Formal Methods Symposium (NFM 2021)*, Springer, Virtual, May 24-28, 2021
17. Abigail Hammer, Matthew Cauwels, Benjamin Hertz, Phillip Jones, and Kristin Yvonne Rozier. "Integrating Runtime Verification into an Automated UAS Traffic Management System." In *Innovations in Systems and Software Engineering: A NASA Journal*, Springer, July, 2021

3.21 All Eyes on Extra-functional System Properties: On the Formalisation and Analysis of Explainability and Morality for Autonomous Traffic Agents

Maike Schwammberger (KIT – Karlsruher Institut für Technologie, DE)

Joint work of Maike Schwammberger, Verena Klös
Main reference Maike Schwammberger, Verena Klös: "From Specification Models to Explanation Models: An Extraction and Refinement Process for Timed Automata", in Proc. of the Proceedings Fourth International Workshop on Formal Methods for Autonomous Systems (FMAS) and Fourth International Workshop on Automated and verifiable Software sYstem DEvelopment (ASYDE), FMAS/ASYDE@SEFM 2022, and Fourth International Workshop on Automated and verifiable Software sYstem DEvelopment (ASYDE)Berlin, Germany, 26th and 27th of September 2022, EPTCS, Vol. 371, pp. 20–37, 2022.
URL https://doi.org//10.4204/EPTCS.371.2

Motivation. During the last years, autonomous cars are increasingly capturing the markets worldwide. As such autonomous cars involve both software and hardware aspects, these systems can be summarised as Cyber-Physical Systems. Often, these systems also involve cooperation or interaction with human operators or end-users, thus leading to *Human Cyber-Physical Systems (HCPS)*. Ensuring functional properties of these HCPS is of the utmost importance to allow for a desirable future with them. Examples for functional properties are safety (e.g. collision freedom for moving HCPS) or liveness (a desired goal is finally reached). Fortunately, different research directions for analysing and proving functional system properties exist.

Apart from functional system properties, a variety of important *extra-functional* system properties must be ensured, which is the focus of this talk. In our case, we consider self-explainability and morality to be such extra-functional properties. Both fields have gained more and more attention within the last years of success for autonomous systems. With *self-explainability*, we describe the capability of a system to self-explain its actions and decisions to an addressee. Such an addressee may, e.g., be an engineer, an end-user or another HCPS. When we say that an HCPS *acts morally*, we mean that it can follow a given set of moral rules, as is, e.g., presented through the societal, cultural or legal context of the HCPS.

Approach. We introduce the modular MAB-EX framework for self-explainability[1]. The framework comprises four phases: First, the system is **M**onitored, e.g. through an observer mechanism. In the second phase, **A**nalyse, the monitored data is examined w.r.t. unusual behaviour that needs explaining. If the need for an explanation is identified, the formal core of an explanation is extracted from an *explanation model* in the **B**uild phase. An explanation model is a structure that we extract from formal system models and that contains formalised versions of explanations[3]. In the last phase, **EX**plain, the extracted, formal, explanation is translated into an explanation that fits for the intended addressee.

For morality, we envision a step-wise procedure to include morality into *autonomous traffic agents (ATAs)*, thus gaining moral ATAs[2]. For this, we will analyse a formalised set of traffic rules for conflicts and solve them by introducing moral rules to the ATAs. Conflicts could exist between different traffic rule in different contexts, or between an agent's goals and traffic rules. For instance, if a traffic sign demands that cars drive only at 50km/h, while an agents goal is to drive faster, a moral rule might be used to implement that the agent (temporarily) adapts their own goal.

Challenges. We perceive and discuss a variety of challenges in the field of formal analysis of extra-functional system properties of ATAs:

- How far can we go with formal methods in the area of extra-functional system properties?
- The endeavour of proving extra-functional system properties like self-explainability will be an interdisciplinary operation. What disciplines need to be involved and how can we bridge potential gaps between different disciplines?
- What types of extra-functional properties must be analysed and ensured?
- What are the further challenges that exist?

References

1 Mathias Blumreiter, Joel Greenyer, Francisco Javier Chiyah Garcia, Verena Klös, Maike Schwammberger, Christoph Sommer, Andreas Vogelsang, Andreas Wortmann. *Towards Self-Explainable Cyber-Physical Systems*. In: MODELS Companion, IEEE, pp. 543–548, 2019.

2 Astrid Rakow, Maike Schwammberger. *Brake or Drive: On the Relation Between Morality and Traffic Rules when Driving Autonomously*. In: 20th Workshop on Automotive Software Engineering (ASE), 2023.

3 Maike Schwammberger, Verena Klös. *From Specification Models to Explanation Models: An Extraction and Refinement Process for Timed Automata*. In: FMAS@SEFM, volume 371 of EPTCS, pp. 20–37, 2022.

3.22 Modeling and Analysis of Cyber-Physical Systems Using Actors

Marjan Sirjani (Mälardalen University – Västerås, SE)

Main reference Marjan Sirjani, Edward A. Lee, Ehsan Khamespanah: "Verification of Cyberphysical Systems", Mathematics, Vol. 8(7), 2020.
URL https://doi.org//10.3390/math8071068
Main reference Marjan Sirjani, Luciana Provenzano, Sara Abbaspour Asadollah, Mahshid Helali Moghadam, Mehrdad Saadatmand: "Towards a Verification-Driven Iterative Development of Software for Safety-Critical Cyber-Physical Systems", J. Internet Serv. Appl., Vol. 12(1), p. 2, 2021.
URL https://doi.org//10.1186/s13174-021-00132-z
Main reference Marjan Sirjani: "Power is Overrated, Go for Friendliness! Expressiveness, Faithfulness, and Usability in Modeling: The Actor Experience", in Proc. of the Principles of Modeling – Essays Dedicated to Edward A. Lee on the Occasion of His 60th Birthday, Lecture Notes in Computer Science, Vol. 10760, pp. 423–448, Springer, 2018.
URL https://doi.org//10.1007/978-3-319-95246-8_25

Our world has become a network of connected software systems, communicating with each other, and controlling physical systems. We have autonomous cars driving around, interoperable medical devices monitoring and controlling the health of patients and collaborating robots interacting with humans without separating fences. These systems are generally concurrent, distributed, and dynamic, with critical timing properties.

I will present our approach for analysis of timing properties of interoperable systems, using actor models and formal verification. Rebeca was designed more than 20 years ago as an imperative actor-based language with the goal of providing an easy-to-use language for modelling concurrent and distributed systems, with formal verification support. It was extended a few years later to support modelling real-time network and computational delays, periodic events, and required deadlines; and then extended to Hybrid Rebeca to support hybrid systems.

At the dagstuhl, I will briefly present our work that may be of interest for the audience. I will reflect on how we used Rebeca, its extensions, and its toolset for timing analysis and safety assurance of different systems, for example sensor network applications, and medical

interoperable systems. I will present Hybrid Rebeca and our design decisions in extending Rebeca to support hybrid systems. I will present our work on model checking CPS by connecting Timed Rebeca and Lingua Franca (of Edward Lee from UC Berkeley). I will also explain our work on anomaly detection of CPS using formal verification at design time, and runtime monitoring during operation using an abstract digital twin that we call Tiny Twin.

3.23 Rigorous Development & Certification of Complex, Software Intensive Systems – My Wish List

Alan Wassyng (McMaster University – Hamilton, CA)

The talk tackled the question "Can we achieve the safety & dependability we need for extremely complex systems of systems that combine hardware & software, and may even include machine learning components?" I presented my personal wish list for techniques and approaches that I believe can help us answer the question in the affirmative.

Top of my wish list is "Incremental Product Family Assurance" to complement "Incremental Product Family Development", which I think is already well established. To support this we need effective and practical "Change Impact Analysis & Bi-directional traceability". I presented our work on the Workflow+ modeling framework as one approach that can help in this regard.

I also presented 8 Support Wishes ranging from "Systematic Methods To Explore Emergent Behaviour" to "Integrated Methods", with an emphasis on Model Driven Engineering. I ended the presentation with 5 Foundational Wishes ranging from "Separation Of Concerns" to "[building the] Assurance Case Before Start [of development]".

References

1 Nicholas Annable, Thomas Chiang, Mark Lawford, Richard F. Paige and Alan Wassyng. *Generating Assurance Cases using Workflow+ Models*. In Computer Safety, Reliability, and Security, Munich, Germany, September 6–9, pp. 97–110. Springer, 2022

3.24 Towards a Unifying Framework for Uncertainty in Cyber-Physical Systems

James C. P. Woodcock (University of York, GB)

Main reference Kangfeng Ye, Ana Cavalcanti, Simon Foster, Alvaro Miyazawa, Jim Woodcock: "Probabilistic modelling and verification using RoboChart and PRISM", Softw. Syst. Model., Vol. 21(2), pp. 667–716, 2022.
URL https://doi.org//10.1007/s10270-021-00916-8

There are many challenges to the satisfactory operation of cyber-physical systems (CPSs). They include architectural issues, real-time properties, human interaction, autonomy, privacy, safety, security, and uncertainty. Researchers who have analysed CPSs cite problems linked to security and uncertainty as the most common causes of failure [1]. We focus on uncertainty, a lack of knowledge about a system's state.

Computer scientists have proposed several formalisms for dealing with uncertainty. Probabilistic and statistical model checkers, such as Prism [5] and Storm [4], analyse a range of semantic models for these formalisms. These include discrete and continuous-time Markov chains and their nondeterministic extensions. These tools are good at interoperability. Verification-oriented formalisms include the following: Hehner's probabilistic predicative programming [3], the conditional probabilistic guarded command language [7], probabilistic Hoare logic [2], and partially observable Markov decision processes [6].

Research on describing and analysing uncertainty raises many questions. What does a unifying theory for uncertainty look like? What are the connections between semantics and tools that support the different approaches? Can we establish more connections? Can we support probabilistic and statistical model checking with theorem proving? Contrariwise, can we support theorem proving with probabilistic and statistical model checking? Can we establish uncertainty properties using correctness by construction? What about probabilistic refinement-based model checking? Can we qualify one analysis tool (as in DO-178C) and then map soundly into that tool for high assurance? What is the formal testing theory for a CPS with (say) unknown MDP semantics? What are the testability hypotheses (in Gaudel's sense)? How do we exploit the interplay between testing, proof, and model checking? What about uncertainty modelling and runtime verification? What role can unifying uncertainty formalisms and tools play in the development, application, and evaluation of CPSs?

We describe some preliminary work towards answering these questions.

References

1 Mah Asmat, Saif Ur Rehman Khan, and Shahid Hussain. Uncertainty handling in cyber–physical systems: State-of-the-art approaches, tools, causes, and future directions. Journal of Software: Evolution and Process, 2022.

2 Jerry den Hartog and Erik P. de Vink. Verifying probabilistic programs using a Hoare-like logic. Int. J. Found. Comput. Sci., 13(3):315–340, 2002.

3 Eric C. R. Hehner. Probabilistic predicative programming. In Dexter Kozen and Carron Shankland, editors, Mathematics of Program Construction, 7th International Conference, MPC 2004, Stirling, Scotland, UK, July 12-14, 2004, Proceedings, volume 3125 of Lecture Notes in Computer Science, pages 169–185. Springer, 2004.

4 Christian Hensel, Sebastian Junges, Joost-Pieter Katoen, Tim Quatmann, and Matthias Volk. The probabilistic model checker Storm. Int. J. Softw. Tools Technol. Transf., 24(4):589–610, 2022.

5 Marta Z. Kwiatkowska, Gethin Norman, and David Parker. PRISM 4.0: Verification of probabilistic real-time systems. In Ganesh Gopalakrishnan and Shaz Qadeer, editors, Computer Aided Verification – 23rd International Conference, CAV 2011, Snowbird, UT, USA, July 14-20, 2011. Proceedings, volume 6806 of Lecture Notes in Computer Science, pages 585–591. Springer, 2011.

6 George E. Monahan. A survey of partially observable Markov decision pro- cesses: Theory, models, and algorithms. Management Science, 28(1):1–16, 1982.

7 Federico Olmedo, Friedrich Gretz, Nils Jansen, Benjamin Lucien Kaminski, Joost-Pieter Katoen, and Annabelle McIver. Conditioning in probabilistic programming. ACM Trans. Program. Lang. Syst., 40(1):4:1–4:50, 2018.

4 Working Groups

4.1 Formal methods for hybrid systems: Challenges and research directions

Erika Abraham (RWTH Aachen University, DE), Wolfgang Ahrendt (Chalmers University of Technology – Göteborg, SE), André Platzer (KIT – Karlsruher Institut für Technologie, DE), Marjan Sirjani (Mälardalen University – Västerås, SE), Frank Zeyda (Zapopan, MX)

Hybrid and *cyber-physical systems* started to attract the interest of the *formal methods* community in the 90s, followed by a diversity of great ideas, elegant methods and impactful tools. However, till today, these methods and tools did not find their way into regular industrial usage. What are the major problems delaying a wider adoption?

Model building: As a crucial enabling factor for verification, we first need formal models for these systems.

- A hybrid system is typically composed of a controller and a continuous dynamical system controlled by it. Whereas models for the controller are developed at relatively early design phases, the modeling process considers the dynamics often too late. There is a communication problem between engineers constructing the system and modeling people making it difficult to get the right starting point for realistic dynamical models on the suitable level of abstraction.
- Often, different sources offer different information (e.g. on the dynamics, control, uncertainty, environment, requirements, etc.) that needs to flow together for model building. However, there is no clear methodology for synthesizing models from partial information from different sources.
- A related problem is the scarcity of notion of compositionality/composability/modularity for hybrid systems. Compositionality of hybrid systems modeling and reasoning works in logic per operator, but it needs good design to succeed for larger system components. Furthermore, there is no established way to jointly represent models together with their specifications and verification results, which would ease their adoption and maintenance during the system's life cycle.
- In general, for modeling we might not yet have the right interface between the hybrid and the discrete world. Here, research may benefit from further novel principles.
- For the modeling, no standard language exists. Different languages differ in their semantics (if a semantics is defined at all) and expressivity, which makes model transformation challenging. Consequently, applying different tools on the same problem requires a lot of effort, or may even be impossible. For instance the system time-horizon has a huge impact on the performance of some tools but not on others.
- The model is often not sufficiently maintained during system construction, leading to major differences between the system implementation and the current model. Consequently, previous verification results are not applicable any more, and the whole modeling and verification process needs to be carried out anew.

Specification: What is still missing is a specification formalism that is easier to use for engineers than the formal languages but still captures assumptions as well as guarantees of (hybrid) components, composition operators, and composability constraints (relative to the desired properties of the composed system). Education and training enables engineers to use the required logic, but more gentle specification languages may make that specification process easier for engineers who are novice in formal techniques.

Verification: Intensive research efforts in the last decades have led to a number of formal verification techniques and tools, but only a few of them are used by a larger community.

- The verification problem for hybrid systems is inherently hard. People might change research direction such that available tools are not maintained any more.
- The development of usable tools requires both strong science and significant engineering effort that is often impossible to find funding for.
- Industrial applications are doable, but often need a PhD student's help. Bachelor's students can also do impressive verification studies but of more medium complexity.
- The combined analysis of the discrete-continuous behavior of hybrid systems is hard. Separating discrete behavior and continuous dynamics for the verification process is only partially possible, because the hybrid system's safety conditions impact the needs of the discrete controllers.
- Abstractions (e.g. discrete abstractions combined with a counterexample-guided abstraction refinement approach) are possible but they do not always solve the problem, unless clever problem-specific insight is given to the tools.
- Rigorous verification needs a stack of rigorous tools that is hard to sustain.
- Most techniques are developed to compute (or approximate) the set of all states that a system can reach from a given set of initial states during its execution. However, there is nearly no support for more complex (e.g. temporal or spatial) properties except in deductive logic approaches.
- The controller is discrete, coupled with the physical world in the time dimension; it would be great to find a way to exploit this fact to simplify the analysis.

4.2 Human models for human cyber-physical systems

Maike Schwammberger (KIT - Karlsruher Institut für Technologie, DE), Borzoo Bonakdarpour (Michigan State University - East Lansing, US), Simon Thrane Hansen (Aarhus University, DK), Joseph Roland Kiniry (Galois - Portland, US), Régine Laleau (IUT Sénart-Fontainebleau, FR), Ken Pierce (Newcastle University, GB)

Cyber-Physical Systems (CPSs), often acting autonomously, are used in more and more application domains of our daily lives: Driving assistance systems, smart factories and smart homes are just some examples. While the level of autonomy of these systems increases, so also does the need for these systems to interact with human end-users, operators or engineers. A new type of system is born: Human Cyber-Physical Systems (HCPSs). With that, one question comes to the fore: How we can capture, analyze and formally verify human behavior in CPS models?

Challenges and Opportunities: We discuss a selection of topics and challenges that need to be addressed for ensuring a satisfying and safe interaction of human and CPS.

- Human models for self-explainability: The capability of a Cyber-Physical System to self-explain its actions is a crucial feature for HCPS, especially if shared and safety-critical tasks of the CPS and the human exist. However, such explanations must be targeted towards a variety of addresses: E.g., end-users, engineers, operators or lawyers. For different addressees of explanations, we need different human models. What techniques do we have to model humans?

- To answer the previous question, cognitive models as they are used by psychologists come to our minds. However, how do we translate psychologists' cognitive models into formal models? A widely used approach to specify knowledge is, e.g., to use an (auto) epistemic logic.
- Should a human's behavior be modeled as a continuous-time or hybrid process?
- What assumptions do we need about human behavior? For this, literature often uses a notion of *rational agents*. A rational agent is an entity that generally tries to use optimal actions based on some given knowledge, rules and goals. Nonetheless, also notions of irrational or even evil agents should be taken into account for worst-case analyses.

4.3 Formal Methods and Certification

Danielle Stewart (Galois - Minneapolis, US), Kristin Yvonne Rozier (Iowa State University – Ames, US), Stefan Hallerstede (Aarhus University, DK), Stanley Bak (Stony Brook University, US), John Hatcliff (Kansas State University - Manhattan, US), David Hardin (Collins Aerospace – Cedar Rapids, US), Andrea Bombarda (University of Bergamo – Dalmine, IT), Fuyuki Ishikawa (National Institute of Informatics – Tokyo, JP), Gabor Karsai (Vanderbilt University, US), Thierry Lecomte (CLEARSY – Aix-en-Provence, FR), Michael Leuschel (Heinrich-Heine-Universität Düsseldorf, DE), Alan Wassyng (McMaster University – Hamilton, CA)

Notetaker: Danielle

Summary

Different regulatory agencies have different expectations and requirements for certification processes. Certain agencies are more comfortable with formal methods and verification approaches, such as the NSA. Dave described a Type I crypto system called Janus that required accreditation through the NSA. They were able to provide formal evidence of various code properties and the NSA gave approval for the system. Other agencies are not familiar enough with formal method approaches to understand the artifacts, let alone the benefit of the approach. Safety and security are totally different. The security process (Common Criteria) is fully defined, and formal methods – along with penetration testing – is part of the process. The certification authorities are well equipped to evaluate the formal methods artifacts. The nuclear regulation in Canada is more serious about formal methods artifacts. They decide where they think problems exist and focus on those parts of the system. But any discussion about formal methods in certification needs to also look at the problem of tool qualification. If you want to certify a system to a certain point, any formal methods tools must be qualified to that standard as well. This is a difficult and expensive process. Formal methods can, however, provide insight into the system during certification, even if to the developer alone. It can aid in understanding and documentation, even if those artifacts are not used directly within the certification process.

4.4 Stochastic cyberphysical systems

Cláudio Gomes (Aarhus University, DK), James C. P. Woodcock (University of York, GB), Joanna Delicaris (Universität Münster, DE), Noah Abou El Wafa (KIT - Karlsruher Institut für Technologie, DE)

Our group focused on the discussion of what barriers are there for the integration of stochastic behavior into formal methods. One barrier is that, currently, formalisms traditionally used to model stochastic behavior, like Discrete Time Markov Chains (DTMC), have no formal semantics, that enables them to be used in, e.g., theorem provers. Just like their deterministic counterparts, stochastic formalism have relationships between them. For example, each step of a DTMC is a simple Markov chain, and each transition in a Markov chain is a statistical distribution. Another barrier is therefore to represent the links between these formalisms by, e.g., defining Galois connections between these formalisms. Another barrier: What are the methodologies to build stochastic models from physical prototypes. This might be well known to statisticians, but not to computer scientists. Finally, we need methodologies on how to identify the sources of uncertainty. Barrier: how are uncertainties propagate through a coupled system, and do they affect the software elements' formal models? Here we can draw from a huge body of literature with formalisms to quantify and propagate uncertainty: sensitivity analysis, monte-carlo simulations, stochastic differential equations, etc.

4.5 Technology Needs – Self-Explainability of Cyber-Physical Systems

Maike Schwammberger (KIT – Karlsruher Institut für Technologie, DE), Thierry Lecomte (CLEARSY – Aix-en-Provence, FR), Alan Wassyng (McMaster University – Hamilton, CA)

As autonomous systems get more and more complex, we need to ensure that they remain or get understandable. For instance, if an AV needs to change a driving strategy unexpectedly, this should be explained to a passenger to retain usability and trustworthiness into the AV. Using formal methods, we can automatically generate formal explanations from specification models (e.g. UML diagrams, timed automata,...). Such *formal cores of explanations* allow for formal verification. From these explanation cores that have been extracted at design time, explanations may be translated at run-time whenever an explanation is needed.

Challenges and Solutions:

- **There is a need to identifying different addressees:** Different addressees mean that differently grained and detailed explanations are needed. For instance, an engineer needs a different explanation than an end-user. For this, expertise from requirements engineering could be taken into account (e.g. "Personas" or "User Classes") or different user models might be learned using AI techniques.
- **Verification and validation of formalized explanations:** A validation of explanations cannot be done isolated from the addressees, as , e.g., it is necessary to know what is relevant for different addressees. A formalization and verification of different addressee's mental models is needed for a joint verification of formalized explanations and user models.

- **Structure of formalized explanations:** Safety explanations could be produced from the discovery of why a system was designed in a certain way. Explanations start from feared events. These events are refined into assumptions agreed on by all experts and measures taken to avoid these events, to produce a tree. All leaves are either assumptions or functions that are sufficient when combined to avoid these events.
- **Automatically extractable explanations can help in system debugging:** If a formalized explanation has been automatically extracted from a specification model in a provably correct manner, and the explanation is still wrong or does not make sense, this means that something is wrong with the system specification. This can be especially helpful for very complex systems that are hard to understand or verify even by experts. This approach could be a fast way to identify some system faults before we start time and resource costly verification mechanisms.

4.6 Digital Twins

Peter Gorm Larsen (Aarhus University, DK), Einar Broch Johnsen (University of Oslo, NO), Leo Freitas (Newcastle University, GB), William Earl Scott (ScubaTx – Newcatle upon Tyne, GB), Andrei Munteanu (Siemens PLM Software, BE), Klaus Kristensen (Bang & Olufsen – Struer, DK)

This group worked to identify the main research challenges for Digital Twins (DT). This also involved assessing how Formal Methods (FM) may be incorporated to enhance the engineering and assurance of DT.

Requirements for the overall twin system:

- Who is responsible for what at different stages of the lifecycle of a digital twin system?
- The requirements of a DT system need to include the main purpose of the DT.
- Would it make sense to create new special DSLs for configurations, monitors and/or what-if scenarios?
- Declare properties of interest to be true of the system/module/unit.
- How to formally specify and evaluate hypothetical (what-if) scenarios?

Applications of FM in Digital Twins:

- Some engineering challenges are related to getting data (in a filtered form) into formal models in a satisfactory manner.
- When we need humans in the DT loop we also need human models. How do we get those models?

Challenges for applying FM in Digital Twins:

- What are the pros and cons of using FM inside DTs?
- How to determine the collection of different models to be included inside the DT (and consider how to select between them)?

Challenges in Digital Twins that would benefit from applying FM:

- Providing evidence of the "goodness" of the digital twin.

- The composition of DTs will benefit from an analysis from FM stakeholders.
- The placement of simulation models in a distributed setting will require different analysis.

Correctness criteria for Digital Twins:
- How to define the assumptions required before being able to verify properties?

Experiences with rigorous engineering of Digital Twins:
- How to discover calibration options/needs?
- Different case studies are important here (some of these will be reported about in a new book on engineering digital twins).

Models for safety and security of Digital Twins:
- Most likely these shall be indicated in some of the monitors.
- How can we trust the results from services considering what-if scenarios?

Fidelity of Digital Twins:
- How accurate does the DT models need to be in relation to the performance of the physical twin?

Validation of Digital Twins:
- Start with historical data and use this as arguments to FM models (potentially in a co-simulation context).
- Determine how it is possible to get data transferred from a physical twin to its digital twin (there can be significant challenges with respect to handling of data because of noise and the fact that the input to models may need to be derived from data that can be extracted).

Achievements applying FM to Digital Twins:
- FM has numerous opportunities for having impact on the DT domain in semantics for different notations, clarification of different concepts.
- Run-time verification is essentially the core of the monitors here.

Participants

- Noah Abou El Wafa
KIT – Karlsruher Institut für Technologie, DE
- Erika Abraham
RWTH Aachen University, DE
- Wolfgang Ahrendt
Chalmers University of Technology – Göteborg, SE
- Stanley Bak
Stony Brook University, US
- Ezio Bartocci
TU Wien, AT
- Stylianos Basagiannis
Raytheon Technologies – Collins Aerospace – Cork, IE
- Andrea Bombarda
University of Bergamo – Dalmine, IT
- Borzoo Bonakdarpour
Michigan State University – East Lansing, US
- Joanna Delicaris
Universität Münster, DE
- Leo Freitas
Newcastle University, GB
- Cláudio Gomes
Aarhus University, DK
- Stefan Hallerstede
Aarhus University, DK
- Simon Thrane Hansen
Aarhus University, DK
- David Hardin
Collins Aerospace – Cedar Rapids, US
- John Hatcliff
Kansas State University – Manhattan, US
- Fuyuki Ishikawa
National Institute of Informatics – Tokyo, JP
- Nils Jansen
Radboud University Nijmegen, NL
- Einar Broch Johnsen
University of Oslo, NO
- Gabor Karsai
Vanderbilt University – Nashville, US
- Joseph Roland Kiniry
Galois – Portland, US
- Klaus Kristensen
Bang & Olufsen – Struer, DK
- Régine Laleau
IUT Sénart-Fontainebleau, FR
- Peter Gorm Larsen
Aarhus University, DK
- Thierry Lecomte
CLEARSY – Aix-en-Provence, FR
- Michael Leuschel
Heinrich-Heine-Universität Düsseldorf, DE
- Paolo Masci
NASA Langley – Hampton, US
- Monica Moniz
Cambridge University Press, GB
- Andrei Munteanu
Siemens PLM Software, BE
- Ken Pierce
Newcastle University, GB
- André Platzer
KIT – Karlsruher Institut für Technologie, DE
- Anne Remke
Universität Münster, DE
- Kristin Yvonne Rozier
Iowa State University – Ames, US
- Maike Schwammberger
KIT – Karlsruher Institut für Technologie, DE
- William Earl Scott III
ScubaTx – Newcatle upon Tyne, GB & Newcastle University, GB
- Marjan Sirjani
Mälardalen University – Västerås, SE
- Danielle Stewart
Galois – Minneapolis, US
- Alan Wassyng
McMaster University – Hamilton, CA
- James C. P. Woodcock
University of York, GB
- Frank Zeyda
Zapopan, MX