Editorial

Ernst-Rüdiger Olderog*, Martin Fränzle, Oliver Theel, and Paul Kröger

System correctness under adverse conditions

https://doi.org/10.1515/itit-2021-0043
Received September 8, 2021; accepted September 9, 2021

Abstract: This special issue presents seven overview articles on research conducted in the Research Training Group "System Correctness under Adverse Conditions" (SCARE) at the University of Oldenburg.

1 System correctness

The quest for correctness started in the early days of computing, with landmark papers by Alan Turing, Robert Floyd, and Tony Hoare. Then program correctness expressed by flow charts annotated with assertions or by Hoare triples $\{p\}S\{q\}$ was in the focus of interest, where S is a program, p a precondition, and q a postcondition. Today, we are concerned with *system correctness*. It can be expressed by the formula $Asm \vdash (Env \parallel Sys)$ `sat` $Spec$. Here a system *Sys* interacts with its environment *Env*. Correctness means that their parallel composition $(Env \parallel Sys)$ should satisfy a specification *Spec*, where the satisfaction relation `sat` can have different definitions ranging from Boolean yes/no to probabilistic interpretations. The correctness may depend on certain assumptions *Asm* on the interaction between system and environment. System correctness is an ongoing concern because the notion of system is advancing, for example a system may comprise multiple cars moving along a road. Application contexts induce adverse conditions, for example limited sensing in traffic manoeuvres.

Examples for such systems can be found in any flavour of the domain of embedded control: in addition to many household appliances of daily use, automated transportation systems, Industry 4.0 applications, or smart health systems are prominent instances thereof. Such systems often implement safety-critical applications which are required to be robust against unexpected situations or component failures. Thus, correctness guarantees are desirable or even mandatory. This is where the Research Training Group on "System Correctness under Adverse Conditions", abbreviated SCARE, at the University of Oldenburg made and makes its contribution.

A rigorous analysis of the system behaviour under adverse conditions is required in order to prove system correctness, i. e. to prove that the joint behaviour of the system and its environment satisfies a given specification of safety, stability, or liveness properties. In SCARE, we concentrate on the following adverse conditions:

- *limited knowledge*, i. e. systems interacting with an environment that is only partially known or imprecisely observed via error afflicted measurements,
- *unpredictable behaviour*, i. e. systems that a) exhibit sporadic or persistent errors or component failures caused by design errors, aging effects, or environmental effects occurring at runtime, or that b) interact with an environment that develops unexpected behaviour, and
- *changing system environment and system structure*, i. e. systems interacting with an environment changing due to, e. g., physical positions changing over time and thereby changing the ego system's context which in turn might cause a change of the system structure by enabling or disabling components.

In SCARE, we pursue the following research themes:

- formal modeling,
- verification and analysis,
- constructive techniques, where formal methods are combined with engineering techniques, in particular the use of machine learning.

Each PhD thesis in SCARE addresses one or more adverse conditions in one or more of these research themes.

2 Contents

This special issue comprises seven overview papers authored by current or past PhD students of SCARE, often together with their supervisors. Each paper has undergone two reviewing and revision rounds.

***Corresponding author: Ernst-Rüdiger Olderog,** University of Oldenburg, Department of Computing Science, D-26129 Oldenburg, Germany, e-mail: olderog@informatik.uni-oldenburg.de
Martin Fränzle, Oliver Theel, Paul Kröger, University of Oldenburg, Department of Computing Science, D-26129 Oldenburg, Germany, e-mails: fraenzle@informatik.uni-oldenburg.de, theel@uni-oldenburg.de, p.kroeger@uni-oldenburg.de

The topic of safe transportation is addressed in the paper *Proving Properties of Autonomous Car Manoeuvres in Urban Traffic* by Maike Schwammberger. It defines an abstract model to logically reason about properties of autonomous manoeuvres at intersections in urban traffic. The approach introduces extended timed automata Crossing Controllers that use the traffic logic Urban Multi-lane Spatial Logic to reason about traffic situations. Safety in the sense of collision freedom is mathematically proven. Liveness and fairness properties are examined using the model checker UPPAAL for timed automata.

The analysis of analog and hybrid-state circuits and systems is addressed by three papers.

The paper *Bayesian Hybrid Automata: Reconciling Formal Methods with Metrology* by Paul Kröger and Martin Fränzle presents a revised formal model for hybrid systems, which combine discrete actions and continuous behaviour. A natural domain of such systems are emerging smart technologies which add elements of intelligence, co-operation, and adaptivity to physical entities. The new model is able to represent state tracking and estimation in hybrid systems and thereby enhancing precision of verification verdicts.

The paper *Functional Verification of Cyber-Physical Systems Containing Machine-Learnt Components* by Farzaneh Moradkhani and Martin Fränzle addresses the problem of automatically reasoning about systems with artificial neural networks (ANNs) as a major part. The focus is on dealing with activation functions that cannot be modelled any more with piecewise linear functions supported by the majority of satisfiability modulo theories (SMT) solvers and specialized solvers for ANNs. The research uses the SMT solver iSAT which aims at solving Boolean combinations of linear and non-linear constraint formulas, and therefore is suitable to verify the safety properties of deep neural networks which contain non-linear transfer functions.

The paper *A Sampling-based Approach for Handling Delays in Continuous and Hybrid Systems* by Erzana Berani Abdelwahab and Martin Fränzle considers a more realistic setting for feedback loops in dynamical systems where delays are explicitly modelled. It demonstrates that for continuous systems such as delay differential equations, a major part of the delay-induced complexity can be reduced effectively when adding natural constraints to the model of the delayed feedback channel, namely that it transports a band-limited signal and implements a non-punctual, distributed delay. The reduction is based on a sampling approach which is applicable when the above conditions on the feedback are satisfied.

Aging hardware is studied in the paper *Abstraction NBTI Model* by Stephan Adolf and Wolfgang Nebel. It addresses one of the major transistor aging effects called Negative Bias Temperature Instability, NBTI for short. This can lead to timing failures during the run-time of a system. The paper proposes an abstract model reducing the state space of trap based NBTI models using two abstraction parameter, applying a state transformation to incorporate variable stress conditions. This transformation is faster than traditional approaches.

The correctness of graph transformation systems is addressed in the paper *Infinite-state Graph Transformation Systems under Adverse Conditions* by Okan Özkan. To model adverse conditions, it constructs joint graph transformation systems which involve a system, an interfering environment, and an automaton modeling their interaction. For joint graph transformation systems, it presents notions of correctness under adverse conditions that are expressible in LTL (linear temporal logic) or CTL (computation tree logic), respectively. The automatic verification of these correctness conditions, in particular under the concept of well-structuredness of transition systems, is then discussed.

The topic of system synthesis is addressed in the paper *Exploiting Symmetries of High-Level Petri Games in Distributed Synthesis* by Nick Würdemann. It deals with the problem of automatically generating correct controllers for individual agents in a distributed system. Petri games model this problem by a game between two teams of players on a Petri net structure. The concept of symmetries in Petri nets is transferred to Petri games, and used to create concise high-level representations of Petri games. Petri games can be solved by a reduction to a two-player game. Applying symmetries to the states in this game results in a significant state space reduction.

Acknowledgment: We thank Prof. Anne Koziolek for inviting us to this special issue on the topic of the Research Training Group "System Correctness under Adverse Conditions" (SCARE).

Funding: The German Research Foundation (DFG) funded this group as GRK 1765 from October 2012 until September 2021, with individual extensions until March 2022.

Bionotes

Prof. Dr. Ernst-Rüdiger Olderog
University of Oldenburg, Department of Computing Science, D-26129 Oldenburg, Germany
olderog@informatik.uni-oldenburg.de

Prof. Dr. Ernst-Rüdiger Olderog obtained his diploma, doctoral degree (Characterization of Hoare's Logic for ALGOL-like Programming Languages), and habilitation (Nets, Terms and Formulas: Three Views of Concurrent Processes and Their Relationship) in Computer Science from the University of Kiel in the years 1979, 1981 and 1989. A postdoctoral stay 1981–1983 at the Programming Research Group in Oxford led by Tony Hoare initiated his research on communicating processes. He had positions as a visiting professor at the universities of Saarbrücken and Amsterdam, and at ETH Zürich. In 1989 he was appointed associate professor and in 1994 full professor of Theoretical Computer Science at the University of Oldenburg. His research interests include program verification, communicating processes, real-time systems, correct system design, and more recently games based on concepts of Petri nets. In 1994 he was awarded the Leibniz Prize of the German Research Foundation (DFG). He is the speaker of the DFG-funded Research Training Group SCARE.

Prof. Dr. Martin Fränzle
University of Oldenburg, Department of Computing Science, D-26129 Oldenburg, Germany
fraenzle@informatik.uni-oldenburg.de

Prof. Dr. Martin Fränzle is a Professor for Hybrid Systems within the Department of Computing Science at the University of Oldenburg since 2004 and the university's Vice President for Research, Transfer, and Digitalization since 2020. He holds a diploma and a doctoral degree in Computer Science from the University of Kiel and was an associate professor and a Velux visiting professor at the Technical University of Denmark. Further visiting professorships and extended research stays led him to Freiburg, Saarbrücken, Copenhagen, Tallinn, Grenoble, Oxford, and the Chinese Academy of Sciences. Fränzle's research focuses on the mathematical modelling as well as the verification and synthesis of secure and reliable cyber-physical systems, i. e., the merging of physical objects with information technology into "smart" infrastructures such as autonomous vehicles, production facilities, or supply networks. His research interests thereby span from theoretical foundations to applications and industrial transfer, the latter often pursued within the associated research institute OFFIS e. V., where he is long-standing member of the executive board of the R&D division Transportation. He is co-speaker of the DFG-funded Research Training Group SCARE.

Prof. Dr.-Ing. Oliver Theel
University of Oldenburg, Department of Computing Science, D-26129 Oldenburg, Germany
theel@uni-oldenburg.de

Prof. Dr.-Ing. Oliver Theel received the MSc and PhD degrees in computer science from the Darmstadt University of Technology in 1990 and 1993, respectively. Since 2002, he is professor in the computer science department at the University of Oldenburg, holding the chair for system software and distributed systems. From 1995 till 1996, he visited the research group of Michel Raynal at IRISA Rennes, France, under a research fellowship granted by the Commission of the European Union in the scope of the Basic Research Action Program (ESPRIT Network of Excellence in Distributed Computing Architectures). He spent 1994–1995 as a visiting researcher at the computer science department of the University of California, Riverside. From 1992–1993, he worked for Digital Equipment Corp.'s Campus-based Engineering Center in Karlsruhe, where he participated in multiple projects jointly funded by universities and industry. His research interests are distributed systems, fault-tolerance, replication techniques, properties of distributed algorithms, control theory, hybrid systems, and self-stabilization. He is co-speaker of the DFG-funded Research Training Group SCARE.

Paul Kröger
University of Oldenburg, Department of Computing Science, D-26129 Oldenburg, Germany
p.kroeger@uni-oldenburg.de

Paul Kröger is a PhD student in the Hybrid Systems group at the Department of Computing Science of the Carl von Ossietzky Universität Oldenburg (CvO). He studied Computer Science at CvO and completed his MSc in 2017. His research focusses on modelling and verification of cyber-physical systems. He has been a member of the DFG-funded Research Training Group SCARE.