



[Prof. Dr. Ina Schaefer // Test, Validierung und Analyse Software-intensiver Systeme]

104

Prof. Dr.-Ing. Ina Schaefer ist seit 1. April 2022 Professorin für Software Engineering am KIT. Sie studierte Informatik an der Universität Rostock und an der Universität Oxford, United Kingdom. Sie promovierte in 2008 zur Modell-basierten Verifikation von adaptiven Systemen an der TU Kaiserslautern. Als Forschungstipendiatin der DFG arbeitete sie in ihrer Postdoc-Zeit an der Chalmers University, Göteborg, zur formalen Verifikation von feature-orientierten Systemen. Von 2012–2022 war sie Professorin für Softwaretechnik und Fahrzeuginformatik an der TU Braunschweig und seit 2015 Vorstandsmitglied im Niedersächsischen Forschungszentrum für Fahrzeugtechnik (NFF).

Schwerpunkt ihrer Forschungsarbeit ist die Integration von formalen Methoden in die Softwareentwicklung, damit Software besser werden kann, als sie aktuell ist. Dabei interessieren sie besonders Aspekte von Skalierbarkeit, Modularität und Wiederverwendbarkeit. Anwendungen für diese Arbeiten finden sich in einer Vielzahl von Systemen, unter anderem in den Bereichen Automotive, Aviation und Automation. Ab 1. Oktober 2022 übernimmt sie die Leitung des Mobilitätslabors im Helmholtz-Programm Engineering Secure Systems.

Ina Schaefer ist Co-Chair des IFIP Technical Committee 2 „Software and Databases“. Sie war 2021 Co-Vorsitzende des Expertenausschusses zum Zukunftsfonds Automobilindustrie im BMWi. Im Juli 2022 wurde sie zur Co-Vorsitzenden des Expertenkreises Transformation der Automobilwirtschaft im BMWK gewählt.

// **Forschungsvision**

Unsere Forschung zielt auf die Entwicklung von Konzepten, Methoden und Werkzeugen für die ganzheitliche ingenieurmäßige Entwicklung von vertrauenswürdigen und sicheren software-intensiven Systemen ab. Dabei müssen diese Softwaresysteme robust und resilient sein im Hinblick auf geplante und ungeplante Änderungen im Rahmen von Konfiguration, Re-Konfiguration oder Evolution. Die Systeme müssen zuverlässig und sicher dynamisch an neue Anwendungsszenarien und Umgebungen anpassbar sein und die systematische Wiederverwendung unterstützen. Dabei sind präzise, mathematisch fundierte Garantien für kritische funktionale und nicht-funktionale Systemeigenschaften unabdingbar. Anwendungsbereiche für diese Forschungsarbeiten finden sich vor allem im Bereich des Automotive Software und Systems Engineering und in der Automatisierungstechnik.

// **Einblicke in die Forschung**

Security-by-Design und By-Construction Engineering
Software-intensive Systeme in sicherheits- und missionskritischen Bereichen stellen hohe Anforderungen an ihre Sicherheit (Safety und Security) und Zuverlässigkeit. Diese essentiellen Systemeigenschaften

genschaften müssen bereits im Entwicklungsprozess betrachtet werden, um sie im Betrieb garantieren zu können. Die Vorgehensweise des By-Construction Engineerings zielt darauf ab, Softwaresysteme ausgehend von einer (formalen) Spezifikation ihrer funktionalen und nicht-funktionalen Eigenschaften so zu entwickeln, dass sie diese Eigenschaften per Konstruktion erfüllen.

Post-hoc Quality Assurance:

Komplementär zum By-Construction Engineering zielen Post-hoc Qualitätssicherungstechniken darauf ab, kritische funktionale und nicht-funktionale Eigenschaften von Systemen nach Systementwicklung zu garantieren. Ein besonderer Fokus der Forschungsarbeiten sind effiziente und effektive Testverfahren auf Basis von systematischer Testfallgenerierung, Testfallselektion und Testfallpriorisierung vor allem für variantenreiche und evolvierende Softwaresysteme. Dazu gehören auch Absicherungsverfahren für intelligente Systeme, in denen Teile der Funktionalität durch trainierte KI-Komponenten realisiert werden. Ein aktuelles Forschungsprojekt beschäftigt sich mit dem Ende-zu-Ende Test von intelligenten Fahrfunktionen im Rahmen des Automatischen Fahrens.

Software Diversity (Variability & Adaptability)

Moderne Softwaresysteme sind hochkonfigurierbar, um an verschiedene Anforderungen und Umgebungskontexte angepasst werden zu können. Diese Konfigurierbarkeit zur Entwicklungszeit kann auch als Anpassungsfähigkeit (Adaptability) zur Laufzeit genutzt werden, so dass sich Systeme selbständig an neue Bedingungen anpassen können. Damit kann die Robustheit und Resilienz von Softwaresystemen durch Diversität verbessert werden, was besonders für die Härtung von Systemen zur Abwehr von Angriffen genutzt werden kann.

Quantum Software Engineering

Der Einsatz von Quantencomputern verspricht einen Vorteil gegenüber klassi-

schen Rechnern bei der Lösung rechenintensiver Probleme. Das BMBF-Projekt QuBRA bringt Expertinnen und Experten aus Forschung und Industrie zusammen, um diesen Vorteil durch geeignete Benchmarks für Optimierungsprobleme aus der industriellen Praxis zu quantifizieren. Im BMWK-Projekt ProvideQ wird eine Toolbox entwickelt, mit welcher Optimierungsprobleme durch den Einsatz von hybriden Quantenalgorithmien gelöst werden. Die ProvideQ Toolbox bietet hierbei eine Schnittstelle zwischen Optimierungsdienstleistern, Entwicklern von Optimierungsalgorithmen und der eigentlichen Quantenhardware.

// Ausgewählte Publikationen

Tobias Runge, Alexander Kittelmann, Marco Servetto, Alex Potanin, Ina Schaefer: Information Flow Control-by-Construction for an Object-Oriented Language, SEFM 2022.

Tabea Bordis, Tobias Runge, David Schultz, Ina Schaefer: Family-Based and Product-Based Development of Correct-by-Construction Software Product Lines. J. Comput. Lang. 70: 101119 (2022)

Tobias Runge, Alex Potanin, Thomas Thüm, Ina Schaefer: Traits: Correctness-by-Construction for Free. FORTE 2022: 131–150

Lukas Birkemeyer, Tobias Pett, Andreas Vogelsang, Christoph Seidl, Ina Schaefer: Feature-Interaction Sampling for Scenario-based Testing of Advanced Driver Assistance Systems. VaMoS 2022: 5:1–5:10

Elias Kuitert, Alexander Knüppel, Tabea Bordis, Tobias Runge, Ina Schaefer: Verification Strategies for Feature-Oriented Software Product Lines. VaMoS 2022: 12:1–12:9

// Mitarbeiterinnen und Mitarbeiter

Verwaltungspersonal

Petra Ufer

Wissenschaftliches Personal

Joshua Ammermann

Lukas Birkemeyer

Tim Bittner

Tabea Bordis

Domenik Eichhorn

Dr. Alexander Kittelmann

Christoph König

Tobias Pett

Tobias Runge

Technische Mitarbeitende

Andrea Scheller

// Website

tva.kastel.kit.edu