Einladung zum Vortrag

07. November 2017, 16.00 Uhr c.t.
Universität Bremen | Cartesium Rotunde

Dr.-Ing. Thomas Santen
Institut für Softwaretechnik und Theoretische Informatik, TU Berlin

Software-Verification:
From Research to Industrial Practice – and Back.

To enable the machine-supported verification of critical software properties has been a goal of academic research for decades. Many research results, as well as advances of technology, contribute to the state of the art that today allows realistic software artifacts to be formally verified. Transfer to the practice of industrial software production seems to be in close reach. At the same time the enormous complexity of the algorithms and implementations that make up an industrial software component today push classical quality assurance technology like testing to its limits. So has the time of industrial software verification eventually arrived?

This talk reports on the development and use of the verification tool VCC for concurrent C. VCC supports function- and thread-modular verification of industrial product code, which is instrumental for scaling to real products. After introducing the essential features of VCC, the talk discusses experience with applying VCC to code of industrial complexity and scale. It concludes with a discussion of technological and organizational challenges that still prevent formal verification from becoming a standard technology in software production.

Biografie

Dr.-Ing. Thomas Santen is Privatdozent at TU Berlin and independent consultant. From 2007 to 2016, he lead a team of researchers and software developers at the European Microsoft Innovation Center, in Aachen, Germany. Among other contributions, his team developed VCC, the Microsoft Verifier for Concurrent C, and formally verified large parts of the Microsoft Hyper-V kernel. Other than software verification, his research interests include model-based development of software-based systems, safe and secure systems, information flow analysis, privacy engineering, complex event processing and telemetry of large distributed systems.

After studying Computer Science at the universities of Erlangen-Nürnberg and Karlsruhe, Thomas Santen obtained a PhD summa cum laude and later a State Doctorate for Computer Science from TU Berlin. There he worked as an assistant professor at the chair of Software Engineering for several years before joining Microsoft.

Dieser Gast wurde von Dieter Hutter eingeladen.