ZUVERLÄSSIGE SOFTWARESYSTEME IN DER AUTOMOBILINDUSTRIE
PROF. DR. CARSTEN SINZ

Carsten Sinz ist 2008 ans KIT gekommen als Leiter der Forschungsgruppe „Verifikation trifft Algorithmik" am Institut für Theoretische Informatik. Seit 2018 bekleidet er die Professur „Zuverlässige Softwaresysteme in der Automobilindustrie". Er studierte bis 1998 Informatik an der Universität Tübingen, wo er 2003 auch promovierte. Seine Forschungsschwerpunkte sind Algorithmen für logische Erfüllbarkeitsprobleme (SAT/SMT), Produktkonfiguration und Software-Verifikation. In diesen Bereichen war er nach seiner Promotion freiberuflich in Projekten mit Daimler, T-Systems und Siemens Medizintechnik tätig, bevor er 2005 an der Universität Linz eine Stelle als Postdoktorand antrat. Darüber hinaus war er mehrmals als Visiting Researcher am NASA Langley Research Center in Hampton tätig.

Am KIT entwickelt die Forschungsgruppe das Statische-Analyse-Werkzeug LLBMC, das auch Grundlage der KIT-Ausgründung „QPR-Technologies" ist, die derzeit über das Programm „Junge Innovatoren" des Landes Baden-Württemberg gefördert wird.

Auf dem Gebiet der statischen Software-Analyse arbeitet die Forschungsgruppe eng mit der Daimler AG zusammen und ist seit 2015 am europäischen Verbundprojekt „ASSUME" im Rahmen des ITEA3-Programms beteiligt. Darüber hinaus ist Carsten Sinz Mitglied des Steering Committees der SAT Association und gehört dem Editorial Board des Journal on Satisfiability, Boolean Modeling and Computation an.

ÜBERBLICK UND ALLGEMEINES

Die Forschungsgruppe „Zuverlässige Softwaresysteme in der Automobilindustrie" am Institut für Theoretische Informatik befasst sich mit Verfahren zur Qualitätssicherung und Fehlervermeidung (Verifkation) in Softwaresystemen einschließlich der zugehörigen Grundlagenforschung (Algorithmik). Ein Schwerpunkt ist dabei die Weiterentwicklung von grundlegenden logischen Entscheidungsverfahren (z. B. SAT/SMT-Solver), die im Kern vieler Verifikationstools Verwendung finden. Hier beschäftigt sich die Gruppe insbesondere mit der Konstruktion neuer Algorithmen für in der Praxis auftretende Probleme sowie deren Anpassung auf moderne Hardwarearchitekturen (Multi-Core, Grid). Die Analyse der inneren Struktur solcher Probleme ist ein weiteres Forschungsthema, ebenso wie die Nutzbarmachung von Verifikationsmethoden für industrielle Probleme (Produktkonfiguration, Software-Verifikation), insbesondere für die Automobilindustrie.

ERGEBNISSE UND ERFOLGE

Die Forschungsgruppe entwickelt seit 2009 das Verifikations-Werkzeug LLBMC, mit dessen Hilfe sich schwer zu findende Software-Fehler (wie Speicherzugriffsfehler oder arithmetische Überläufe) mit hoher Präzision aufspüren lassen. Dazu wird das Verfahren „Bounded Model Checking" eingesetzt.

Im Jahr 2014 wurden erste Aktivitäten gestartet, LLBMC zu einem kommerziell nutzbaren Werkzeug weiterzuentwickeln, die im Rahmen einer Ausgründungsinitiative stattfinden und aktuell durch das Programm „Junge Innovatoren" des Landes Baden-Württemberg gefördert werden. Eine Weiterentwicklung der Kernalgorithmen von LLBMC findet parallel dazu auch im Rahmen des ITEA3-Verbundprojekts ASSUME (Affordable Safe and Secure Mobility Evolution) statt.

Dabei konnte eine deutliche Verbesserung der Skalierbarkeit erreicht werden durch Entwicklung eines neuen Algorithmus zur lokalen Prüfung. Dabei werden sichere Überapproximationen berechnet, die es erlauben, Programmeigenschaften anhand eines (relativ kleinen) Code-Fragments bereits zu entscheiden. Auf typischen Projekten lassen sich damit über 60% der zu beweisenden Eigenschaften bereits auf dem Programmfragment nachweisen. Darüber hinaus wurde die Bedienbarkeit von LLBMC/QPR-Verify deutlich verbessert, z.B. durch die Generierung von Fehlertraces auf Source-Code-Ebene.

Im Rahmen des 2016 gestarteten Projekts HIVES (Hochpräzise und hochperformante Verifikation von Fahrzeugsoftware), an dem auch das FZI und deie Forschungsgruppe von Professor Sanders beteiligt sind, wurden neue parallele Algorithmen zum SAT-Solving und zur statischen Programmanalyse entwickelt, insbesondere zum effizienten Scheduling von Analyse-Aufgaben auf einem High-Performance Compute-Cluster.

Auf der Summer School „Verification Technology, Systems & Applications“ 2018 in Nancy hat Carsten Sinz ein Tutorium zum Thema „Bounded Model Checking of Software for Real-World Applications“ abgehalten.

AUSGEWÄHLTE PUBLIKATIONEN

T. Balyo, C. Sinz: Parallel Satisfiability. In: *Handbook of Parallel Constraint Reasoning*. Springer-Verlag, S. 3-29, 2018.

B. Beckert, S. Bischof, M. Irda, M. Kirsten, M. Kleine Büning: Using Theorem Provers to Increase the Precision of Dependence Analysis for Information Flow Control. ICFEM 2018, S. 284-300, 2018.

S. Omri, P. Montag, C. Sinz: Static Analysis and Code Complexity Metrics as Early Indicators of Software Defects. Journal of Software Engineering and Applications, 11 (4). S. 153-166, 2018.

M. Iser, F. Kutzner, C. Sinz: Using Gate Recognition and Random Simulation for Under-Approximation and Optimized Branching in SAT Solvers. In: *Proceedings of the 29th Intl. Conf. on Tools with Artificial Intelligence (ICTAI 2017)*. S. 1029-1036, 2017.

T. Balyo, A. Biere, M. Iser, C. Sinz: SAT Race 2015. Artif. Intell. 241. S. 45-65, 2016.

MITARBEITERINNEN UND MITARBEITER

Verwaltungspersonal

Simone Meinhart

Wissenschaftliches Personal

David Farago
Robin Freyler
Markus Iser
Marko Kleine Büning
Felix Kutzner
Simon Silva Lauinger

Technisches Personal

Ralf Kölmel