Karlsruher Institut für Technologie

Application-oriented Formal Verification Research Group
Institute of Information Security and Dependability (KASTEL)
Am Fasanengarten 5
76131 Karlsruhe
https://formal.kastel.kit.edu

Fallstudie: Verifikation von Java Controller Software für Cyber-Physische Systeme

Bachelorarbeit

Hintergrund. In unserer Gruppe entwickeln wir seit einiger Zeit ein (theoretisches) Framework für die Kombination von Modellierungs- und Verifikationstechniken, genannt *Heterogene Dynamische Logik*. Dieses Framework baut auf den Ideen von *Dynamischer Logik* auf. Beispiele für erfolgreiche Dynamische Logiken, die am KIT entwickelt werden, sind JavaDL [1] (implementiert im Theorembeweiser KeY) und Differenzielle Dynamische Logik [2] (implementiert im Theorembeweiser KeYmaera X). Unser Framework ermöglicht es, Garantien für Systeme zu beweisen, die bspw. teilweise in Java und teilweise in hybriden Programmen modelliert sind.

Aufgabenstellung. In der ausgeschriebenen Bachelorarbeit soll eine Fallstudie für Heterogene Dynamische Logik entwickelt werden. Hierzu gilt es zunächst, die Umgebung eines cyber-physischen Systems als hybrides Programm in Differenzieller Dynamischer Logik zu modellieren. Im Anschluss soll ein Controller für das vorliegende System in Java prototypisch implementiert werden. Hauptaugenmerk der Arbeit ist es, Eigenschaften über das Gesamtsystem (Java+hybrides Programm) im Framework der Heterogenen Dynamischen Logik zu beweisen. Hierbei gilt es insbesondere, gute Primitive für die Kommunikation zwischen Java und hybriden Programmen zu entwickeln.

Untersuchungsgegenstand der Fallstudie. Grundsätzlich ist es Ihnen freigestellt, sich einen eigenen möglichen Anwendungsfall zu suchen. Unser Vorschlag ist die Betrachtung von adaptiver Geschwindigkeitsregelung auf Straßen mit vielen Fahrzeugen.

Stichworte: Dynamische Logik, KeY, KeYmaera X, cyber-physische Systeme

Referenzen

[1] Bernhard Beckert et al. *Dynamic Logic for Java*. In: *Deductive Software Verification - The KeY Book - From Theory to Practice*. Vol. 10001. Lecture Notes in Computer Science. Springer, 2016, pp. 49–106.

[2] André Platzer. *Differential Dynamic Logic for Hybrid Systems*. In: *J. Autom. Reason.* 41.2 (2008), pp. 143–189.

Betreuung:

Samuel Teuber, teuber@kit.edu, Raum 203 (Geb. 50.34)
Mattias Ulbrich, ulbrich@kit.edu, Raum 229 (Geb. 50.34)