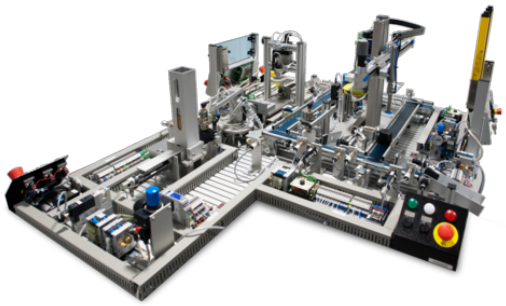
Karlsruher Institut für Technologie

Institut für Informationssicherheit und Verlässlichkeit (KASTEL)
Anwendungsorientierte Formale Verifikation
Prof. Dr. Bernhard Beckert

Praxis der Forschung

Automatisierung von Design-by-Contract bei reaktiven Systemen

Hintergrund. Eingebettete Systeme sind allgegenwärtig. Sie kommen beispielsweise als speicherprogrammierbare Steuerungen (SPS) zur Steuerung automatisierter Produktionssysteme, in medizinischen Geräten oder als Steuerungen (Motor, Bremsen, Fahrassistenz usw.) in Fahrzeugen vor. Diese Systeme sind speziell auf die Steuerung von Systemen zugeschnitten, die in unternehmens- und sicherheitskritischen Echtzeitumgebungen arbeiten. Eine Fehlfunktion kann schwere Schäden am System selbst oder an der Nutzlast verursachen oder sogar Personen in Reichweite des Systems schädigen. Sie sind ein lohnendes Ziel für die formale Verifikation, diese wird aber von den Entwickler in der Praxis jedoch aufgrund ihrer Komplexität nicht akzeptiert.



Eine etablierte Entwicklungsmethode ist die Design-by-Contract und die Verfeinerung. Bei Reaktiven Systemen findet eine Verfeinerung im Systementwurf in Form von Blockdiagrammen statt (vgl. Functional Block Diagrams, IEC 61131-3, oder Internal Block Diagram, SysML), in welchem die Funktionalität des übergeordnete Systems durch die Komposition einzelner Teilsysteme realisiert wird. Die Teilsysteme können wiederum komponiert sein. Hier helfen nun formale Verträge eine korrekte Verfeinerung der Anforderung des Gesamtsystems auf die unterliegende Komponenten nachzuweisen.
Normalerweise ist dies eine arbeitsintensive Aufgabe, in welcher die Entwickler Verträge der unteren und zwischenliegenden Systemen selbst beibringen müssen.

Ziel. Hier wollen wir einsteigen, indem wir (a) ein Verfahren aufstellen mit welchem *Minen* und Lernen von Spezifikation gelingt, und (b) Hilfsspezifikation für die Systemgrenzen automatisch inferiert. Als Spezifikationssprache soll auf Vertragsautomaten aufgebaut werden, und dadurch ebenso auf das Automatenlernen (vgl. L*-Algorithmus von Alduin).
Am Ende könnte ein Ansatz und ein Werkzeug entstehen, mit welchem ein Systementwurf vollautomatischer auf funktionale Korrektheit geprüft werden kann.

Kontakt
Dr. Alexander Weigl weigl@kit.edu Office: 50.34R225