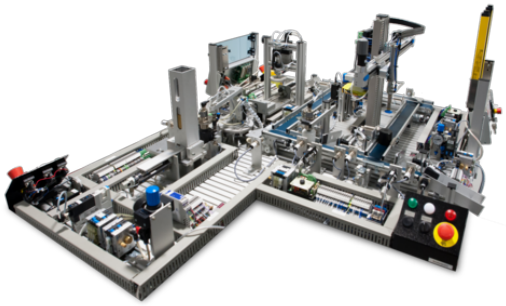
Karlsruher Institut für Technologie

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

Master Thesis

Real-time Specification with Contract Automata

Background. Embedded systems are ubiquitous. For example, they appear as *Programmable Logic Controllers* (PLCs) controlling automated production systems, medical devices, or as controllers (motor, breaks, assisted driving, . . .) in cars. These systems are specially tailored to control system which operate in a mission- and safety-critical **real-time** environments. A malfunction may cause severe damage to the system itself or to the payload, or even harm persons within the reach of the system. They are worthy goal for formal verification.
At the chair of Prof. Beckert, we develop a new specification language for the reactive system called Contract Automata. A Contract Automaton is a finite automaton describing the possible contracts (pre- and post-condition) at every step of the reactive system. Currently, it is based on a discrete-time semantic, in which the time is replaced by number of steps in the system.



Specification and Modeling languages for real-time behavior are known, e.g, UPPAAL models behavior with Timed Automata, and MTL, STL or TCTL allows the specification of real-time properties.

Goal & Task. In this work, we want to extend the current notion of Contract Automata with elements to allows real-time properties. This also includes revisited definition of the semantics and the final goal of the generation of monitors for the runtime verification.

Your Profile. Programming skills are required. Furthermore, you should be interested in Model Checking, Temporal Logics and Automata Theory. You should have completed the Formal Methods (Formale Systeme) Course at KIT or equivalent.

SofCar

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