Karlsruhe Institute of Technology
Institute for Theoretical Computer Science
Am Fasanengarten 5
76128 Karlsruhe

Task Description
for a minor thesis (Studienarbeit/Bachelorarbeit)

Analyzing Alloy Models using KeY

Lightweight formal methods describe and analyse high-level models of software systems using concepts and calculi from mathematical logic. Alloy, developed by MIT's Software Design Group, is a modeling language particularly tailored for this purpose. It has been widely used in academia and industry for verifying network protocols, schedulers, file systems, and for program analysis.

The Alloy Analyzer is a fully automatic tool for checking properties and simulating Alloy models. The tool, however, can perform the analysis only with respect to finite domains; unrestricted quantification is not covered.

The task of this thesis project is to design and implement a translation of the Alloy modeling language to the input language of the software verification system KeY developed at our institute. The translation shall only cover the core constructs of Alloy, and will be guided by a couple of concrete case studies.

Requirement: Basic knowledge of first order predicate logic as, e.g., taught in the "Formal Systems" lecture.

This thesis is a joint project between *Automated Software Analysis* group (led by Mana Taghdiri), and *Logic and Formal Methods* (led by Peter H. Schmitt).

If interested, please contact:

Peter H. Schmitt	Mattias Ulbrich	Mana Taghdiri
`pschmitt@ira.uka.de`	`mattias.ulbrich@kit.edu`	`mana.taghdiri@kit.edu`