Student Project Announcement:

Driver Verification Concept for Embedded Platforms

Development of concepts and adaption of verification tools to provide formal verification of device drivers for a particular embedded platform.

Device drivers are the original cause of operating system crashs. For this reason, operating system vendors are currently working on tools for device driver programmers which employ formal verification techniques to exclude certain generic errors, such as NULL pointer dereference or overflows.

For critical embedded systems, crashs in this sense are even more severe, so there is a natural need for such tools also in the embedded systems domain. Yet small embedded controllers typically don't even run an operating system, so one cannot expect the existing methods to be applicable without further investigation.

In this project, the candidate should (at hand of a USB driver) develop a concept of driver verification for a certain embedded systems platform. The concept shall be evaluated using the existing tools for driver verification, possibly after necessary adaptations.

The candidate should have interest in software development for embedded systems (in C), and at best a good background in formal methods.

Note: This is a joint project with company SeCa GmbH (http://www.seca-online.de). The project can be conducted as part of a 9 month internship ("Werkstudent") where the candidate is employed as a student worker at SeCa.

Degree: MSc

Tutor(s): Dr. B. Westphal, Prof. Dr. A. Podelski

URL: http://swt.informatik.uni-freiburg.de/research/theses

8. Dezember 2009