**Scalable Formal Analysis of Real-Time Systems**

Peter Ölveczky, Ifi, UiO

**Main objective and summary of the project:**

The proposed PhD project aims at developing formal verification methods that scale up to the large and complex real-time and cyber-physical systems encountered today.

**Project background and scientific basis:**

Computer systems are becoming ever more complex, yet we are ever more dependent on their correct behavior. Formal methods have been advocated to verify such reliability/safety/security-critical computing systems. However, there is a tension between the expressiveness needed to capture today’s large and complex systems and the expressive power of many automated verification methods. Rewriting is an intuitive and expressive formalism that has been applied to a wide range of complex real-time and cyber-physical systems, including large network protocols, wireless sensor networks, industrial cloud storage systems, and avionics and railway systems [1,2,3].

**Research questions and scientific challenges:**

This PhD project addresses the challenge of providing verification methods that scale up to today’s complex computing systems. Some ways of achieving this scalability is to integrate symbolic methods into model checking analysis [4,5], design systems composed by verified components [6], and so on. There is also a need for efficiently combining probabilistic and timed reasoning.

**Scientific method:**

One part of the project is to extend promising new symbolic analysis methods to the real-time setting. These will be inspired and validated by concrete systems in areas such as avionics, railway systems, and multi-core and cloud computing. The new analysis methods should be integrated into well-known modeling and analysis tools.
Ethics:

It is not expected that non-standard ethical challenges will arise in the project. Nevertheless, the candidate will be required to take a mandatory ethics course administered by the University of Oslo.

Project timeline:

4 years, with 25% teaching duty, and a midterm evaluation during the third semester. 1st year: literature study; extend symbolic techniques to the real-time setting, and smaller case studies. 2nd year: tool development and larger case studies. 3rd year: combining real-time and probabilistic reasoning. 4th year: finish thesis.

Proposed collaboration partner institutions:

University of Illinois at Urbana-Champaign
POSTECH, Korea

Applicant Background and Competence:

The applicant should preferably have a background in formal methods or related fields (logic, term rewriting, program verification, probabilistic analysis, etc.).

References:


