Presentation of the Chalmers Team

Reiner Hähnle
Chalmers Tekniska Högskola, Gothenburg

First Management Committee Meeting of COST Action IC0901
Brussels

2009-10-30
## Team Members

- Reiner Hähnle, professor, group leader
- Wolfgang Ahrendt, lecturer
- Richard Bubel, postdoc
- Crystal Din, research assistant
- Ran Ji, PhD student
- Ann Lillieström, PhD student
- Gabriele Paganelli, PhD student
- Ina Schaefer, postdoc
- Niklas Sörensson, postdoc
- Angela Wallenburg, PhD student
Research Group:
Formal Methods in Software Engineering

Research Topics Relevant for COST Action IC0901

- State-of-art source code verification for imperative OO languages
  - Floating point arithmetic
  - Memory model of safety-critical JAVA
- Automated deduction technology tailored to needs of verification:
  - Arithmetic beyond linear/Presburger
  - Finding counter examples that violate contract
  - SAT and extensions
- Behavioral Modeling of OO Concurrent Software Components
- Debugging and symbolic state visualization
- Combining symbolic execution and abstract interpretation

Verification Tools Developed

- KeY software verification tool
  - Main version for JAVA
  - KeY-Hoare (education)
  - KeY-TestGen
  - Visual Symbolic State Debugger based on KeY
- MiniSat, Paradox (with K. Claessen)
- Contributions to SPEC#

Verification Tools Used

- Maude (used to verify KeY-rules)
- Coq (used in MOBIUS)
- JML tools, Lustre, SPIN used in teaching
- Various SMT solvers used in KeY (SMT interface)
Current European Projects

- **CHARTER**: Critical and High Assurance Requirements Transformed through Engineering Rigour
  ARTEMIS Embedded Computing Systems Initiative

- **COST Action IC0701**: Formal Verification of Object-Oriented Software

- **FP7 Integrated FET Project: HATS**: Highly Adaptable and Trustworthy Software using Formal Models

- **FP7 Coordination Action: ETERNALS**: Trustworthy Eternal Systems via Evolving Software, Data and Knowledge
## Interest in Working Groups of Action

| WG 1  | - Realization of import/export between KeY and RML  
|       | - Contribution to RM benchmark collection  
|       | - Contribution to design requirements for RML  

| WG 3  | - Abstraction-based symbolic execution with abstract domain tailored to given RML fragment  

Potential for Collaboration with other IC0901 Teams

- Linz (SAT)
- Graz (verification, debugging)
- Copenhagen (specification, verification)
- Helsinki (SAT, automated testing)
- Munich (verification)
- Saarbrücken (program analysis)
- Verona (SMT)
- Barcelona (abstract interpretation)
- Madrid (distributed systems)