Seminar "Success Stories in Formal Methods"

Introduction

Thomas Noll

Software Modeling and Verification Group

RWTH AACHEN UNIVERSITY

noll@cs.rwth-aachen.de

Summer Semester 2013; February 21, 2013

Outline

1. Overview
2. Aims of this Seminar
3. Important Dates
4. Seminar Topics

Formal Methods

Formal methods

- Rigorous, mathematically based techniques for the specification, development and verification of software and hardware systems
- Aim at improving correctness, reliability and robustness of such systems

Formal Methods

Formal methods

- Rigorous, mathematically based techniques for the specification, development and verification of software and hardware systems
- Aim at improving correctness, reliability and robustness of such systems

Classifications

- According to design phase
  - specification, development, verification, testing, ...
- According to underlying mathematical theories
  - process algebras, model checking, theorem proving, static analysis, ...

Outline

1 Overview

2 Aims of this Seminar

3 Important Dates

4 Seminar Topics

Goals

Aims of this seminar

- Independent understanding of a scientific topic
- Acquiring, reading and understanding scientific literature
- Writing of your own report on this topic
- Oral presentation of your results

Requirements on Report

Your report

- Independent writing of a report of 15–20 pages
- Complete set of references to all consulted literature
- Correct citation of important literature
- Plagiarism: taking text blocks (from literature or web) without source indication causes immediate exclusion from this seminar
- Font size 12pt with "normal" page layout
- Language: German or English
- We expect the correct usage of spelling and grammar
  - $\geq$ 10 errors per page $\Longrightarrow$ abortion of correction

Requirements on Talk

Your talk

- Talk of about 45 minutes
- Focus your talk on the audience
- Descriptive slides:
  - $\leq$ 15 lines of text
  - use (base) colors in a useful manner
- Language: German or English
- No spelling mistakes please!
- Finish in time. Overtime is bad
- Ask for questions

Final Preparations

Preparation of your talk

- Setup laptop and projector ahead of time
- Use a (laser) pointer
- Number your slides
- Multiple copies: laptop, USB, web
- Have backup slides ready for expected questions

Outline

1 Overview

2 Aims of this Seminar

3 Important Dates

4 Seminar Topics

Important Dates

Talks

The seminar will be held as a weekly meeting on Tuesdays at 16:00 (?) (see `http://www-i2.informatik.rwth-aachen.de/i2/fm13/`)

Important Dates

Talks

The seminar will be held as a weekly meeting on Tuesdays at 16:00 (?) (see `http://www-i2.informatik.rwth-aachen.de/i2/fm13/`)

Deadlines

You are requested to adhere to the following firm deadlines:

- immediately: obtain the required literature from the web or library
- eight weeks before your talk: present a table of contents
- six weeks before your talk: preliminary version of your report
- four weeks before your talk: final version of your report
- two weeks before your talk: preliminary version of your slides
- one week before your talk: final version of your slides

Important Dates

Talks

The seminar will be held as a weekly meeting on Tuesdays at 16:00 (?) (see `http://www-i2.informatik.rwth-aachen.de/i2/fm13/`)

Deadlines

You are requested to adhere to the following firm deadlines:

- immediately: obtain the required literature from the web or library
- eight weeks before your talk: present a table of contents
- six weeks before your talk: preliminary version of your report
- four weeks before your talk: final version of your report
- two weeks before your talk: preliminary version of your slides
- one week before your talk: final version of your slides

Missing a deadline causes immediate exclusion from the seminar

Outline

1 Overview

2 Aims of this Seminar

3 Important Dates

4 Seminar Topics

Selecting Your Topic

Procedure

- You obtain(ed) a list of topics of this seminar.
- Indicate the preference of your topics (first, second, third).
- We do our best to find an adequate topic-student distribution.
- Disclaimer: no guarantee for an optimal solution.
- Your topic will be published on our website by 15 February.
- Then also your supervisor will be indicated.
- Please give language preference
  - unsure $\Longrightarrow$ German

Selecting Your Topic

Procedure

- You obtain(ed) a list of topics of this seminar.
- Indicate the preference of your topics (first, second, third).
- We do our best to find an adequate topic-student distribution.
- Disclaimer: no guarantee for an optimal solution.
- Your topic will be published on our website by 15 February.
- Then also your supervisor will be indicated.
- Please give language preference
  - unsure $\Longrightarrow$ German

Withdrawal

You have up to three weeks to refrain from participating in this seminar.

Later cancellation (by you or by us) causes a not passed for this seminar and reduces your (three) possibilities by one.

Topic 1: Operating System Kernel

- Gerwin Klein, June Andronick, Kevin Elphinstone, Gernot Heiser, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch and Simon Winwood: seL4: Formal verification of an operating system kernel, Communications of the ACM, 53(6), 2010, 107-115
- seL4 microkernel comprising 8700 lines of C and 600 lines of assembler code
- proof of functional correctness
  - no code injection attacks,
  - no buffer overflows,
  - no NULL or ill-typed pointer access,
  - no memory leaks, ...
- formal verification in Isabelle/HOL theorem prover
- assumptions: correctness of C compiler, assembly code, hardware, and kernel initialization

Topic 2: Real-Time Operating System

- Verhulst, Eric and De Jong, Gjalt: OpenComRTOS: an ultra-small network centric embedded RTOS designed using formal modeling, Proceedings of the 13th international SDL Forum Conference on Design for Dependable Systems, LNCS 4745, 2007, 258-271
- real-time operating system for networked embedded systems
- design goals: trustworthiness, clean architecture, high performance, compactness of code
- parallel development of formal model (TLA+/TLC) and actual implementation
- rigorous formal verification of kernel algorithms (semaphores, ...)

Topic 3: Paris Metro

- Patrick Behm, Paul Benoit, Alain Faivre and Jean-Marc Meynadier: Météor: A Successful Application of B in a Large Project, Formal Methods (FM'99), LNCS 1708, 1999, 369-387
- Météor: first driverless metro in Paris
- automatic train operating system with different control units (ground, line, on-board)
- high requirements regarding dependability and safety
- developed using B formal method
- stepwise refinement from abstract model to (pseudo-)code

Topic 4: Railway Signaling

- Bacherini, S.; Fantechi, A.; Tempestini, M.; Zingoni, N.: A Story About Formal Methods Adoption by a Railway Signaling Manufacturer, FM 2006: Formal Methods, LNCS 4085, 2006, 179-187
- experiences with introduction of formal methods in the development process of a railway signaling manufacturer
- criteria for choosing a reference formal specification notation and related tools
  - application domain
  - company policies
  - legal regulations and guidelines
  - ...
- final choice: Matlab/Stateflow

Topic 5: New York Subway

- Sabatier, Denis and Burdy, Lilian and Requet, Antoine and Guéry, Jérôme: Formal Proofs for the NYCT Line 7 (Flushing) Modernization Project, Abstract State Machines, Alloy, B, VDM, and Z, LNCS 7316, 2012, 369-372
- installation of Communication Based Train Control (CBTC) system (including update of existing interlocking system)
- goal: formal proof of main safety properties of the system: no collision and no over-speeding
- carried out using Event-B formalism with Atelier-B toolkit

Topic 6: Air Traffic Control

- Hall, A.; Isaac, D.; Formal methods in a real air traffic control project, IEEE Colloquium on Software in Air Traffic Control Systems - The Future, pp. 7/1-7/4, June 1992
- introduction of new functionality in London Air Traffic Control Centre
- Central Control Function (CCF) based on sectorisation of airspace to improve air traffic throughput ("tunnels in the sky")
- central subsystem: CCF Display Information System (CDIS; distributed, real-time, dual redundancy)
- specification using VDM
- checking of various safety properties

Topic 7: Mars Rover

Aerospace

Topic 7: Mars Rover

- Brat, G.; Drusinsky, D.; Giannakopoulou, D.; Goldberg, A.; Havelund, K.; Lowry, M.; Pasareanu, C.; Venet, A.; Visser, W.; Washington, R.: Experimental Evaluation of Verification and Validation Tools on Martian Rover Software, Form. Methods Syst. Des. 25(2-3), 2004, 167-198
- application of different verification and validation technologies to NASA flight software
  - static analysis
  - runtime analysis
  - model checking
- controlled experiment using seeded errors in prototype of Mars Rover controller
- comparison with traditional testing

Topic 8: Validation of a Satellite System

Aerospace

Topic 8: Validation of a Satellite System

- Marie-Aude Esteve, Joost-Pieter Katoen, Viet Yen Nguyen, Bart Postma, Yuri Yushtein: Formal Correctness, Safety, Dependability and Performance Analysis of a Satellite. In 34th International Conference on Software Engineering (ICSE). pages 1022-1031. ACM and IEEE CS Press, 2012
- based on model of satellite platform in AADL
  - ˜ 50 million states, hybrid behavior
- analysis of failures and FDIR measures (esp. fault trees)
- using (probabilistic) model checking

Topic 9: Satellite Software

- Alexei Iliasov, Elena Troubitsyna, Linas Laibinis, Alexander Romanovsky, Kimmo Varpaaniemi, Dubravka Ilic, Timo Latvala: Developing mode-rich satellite software by refinement in Event-B, Science of Computer Programming, May 2012
- satellite's configuration characterized by system modes (launching, to orbit, in orbit, failsafe, ...)
- major requirement: correct implementation of mode transition scheme
  - states of system components consistent with global system mode
- approach: formal development by refinement in Event-B
- application to Attitude and Orbit Control System (AOCS)

Topic 10: Needham-Schroeder Public-Key Protocol

- G. Lowe: Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR, TACAS 1996, LNCS 1055, 1996, 147-166
- protocol to establish mutual authentication between two agents using public key cryptography
- CSP model for agents (initiator, responder) and intruder
- verified using FDR regarding correct authentication
- detection and fixing of security flaw

Topic 11: Mobile Communication Protocol

- M.A. Fecko, M.. Uyar, P.D. Amer, A.S. Sethi, T. Dzik, R. Menell, M. McMahon, A success story of formal description techniques: Estelle specification and test generation for MIL-STD 188-220, Computer Communications, Volume 23, Issue 12, July 2000, Pages 1196-1213
- communication protocol for mobile combat network radios
- specification in Estelle (description of protocol behavior by a set of communicating extended finite state machines)
- automatic generation of conformance test cases from formal specification
- several errors in implementations identified

Topic 12: Rotterdam Storm Surge Barrier

- Ken Madlener, Sjaak Smetsers and Marko van Eekelen: A Formal Verification Study on the Rotterdam Storm Surge Barrier, Formal Methods and Software Engineering, LNCS 6447, 2010, 287-302
- describes validation and verification of a crucial component of BOS
- large safety-critical system that controls a sturm surge barrier
- specified in formal language Z
- (lightweight) model of C++ implementation manually developed in PVS theorem prover
- identification of essential mismatches between specification and code

Some Final Hints

Hints

- Take your time to understand your literature.
- Be proactive! Look for additional literature and information.
- Discuss the content of your report with other students.
- Be proactive! Contact your supervisor on time.
- Prepare the meeting(s) with your supervisor.
- Forget the idea that you can prepare a talk in a day or two.

Some Final Hints

Hints

- Take your time to understand your literature.
- Be proactive! Look for additional literature and information.
- Discuss the content of your report with other students.
- Be proactive! Contact your supervisor on time.
- Prepare the meeting(s) with your supervisor.
- Forget the idea that you can prepare a talk in a day or two.

We wish you success and look forward to an enjoyable and high-quality seminar!