Domain: Programming-Testing-ProvingDomain

Model-based Testing of Concurrent Operating-System

Year: 2012
Starting: 1.10.2012
Advisor: WOLFF Burkhart, Co-advisors: Frederic Voisin
Laboratory: LRI,ForTesSE, University Paris-Sud

Collaborations: EU Project EURO-MILLS

Abstract:
System-level code (i.e. code referring to hardware such as CPU's, MMU's, and device-drivers typically written in C) are notoriously difficult to verify. Nevertheless they represent a rewarding target for formal verification, since components are fairly well-described, highly critical, and highly re-used. Based on prior experience of model-based generating test data with HOL-TestGen system, this Phd work attempts to adapt and extend model-based testing techniques to operating-system level functional tests. In particular, it has to be explored how reasonable abstractions can be found and how restricted forms of concurrency can be effectively tested.ContextThis Phd is part of the EU Integrated Project EURO-MILLS (consisting of 14 partners in Germany, Austria, Belgium, France, the Netherlands) whose primary goal is to provide a small virtualization platform (based on the operating system PikeOS) intended to allow the secure decomposition of complex embedded systems into independent components. The secondary goal is to achieve EAL7 certification for this virtualization platform by applying formal verification; for this purpose, a combination of proof and test techniques is envisaged, where the Partner U-PSud plays a major role.Objectives- Develop suitable, testable abstractions of the (in Isabelle developed) Pike-OS Model to be developed in the project.work

Workplan:

- Develop specific testing techniques and infrastructure for test-generation in the context of OS systems,
- possibly by exploiting explicit parallelism in the HOL-TestGen,
- integrate test-data generation into the industry-oriented, concretely used workflow in the project.

Publications:

- [1] Achim D. Brucker, Burkhart Wolff: On Theorem Prover-based Testing. Accepted the 07-08- 2011. In Formal Aspects of Computing (FAOC). DOI: DOI: 10.1007/s00165-012-0222-y. Springer, 2011.
- [2] Abderrahmane Feliachi, Marie-Claude Gaudel, and Burkhart Wolff. Isabelle/Circus: A process specification and verification environment. In VSTTE, LNCS 7152, pages 243-260, 2012.
- [3] Matthias Daum, Jan Dörrenbächer and Burkhart Wolff: Proving Fairness and Implementation Correctness of a Microkernel Scheduler. Journal of Automated Reasoning (JAR), DOI: 10.1007/s10817-009-9119-8. 42 (2-4), pages 349-388. Springer, 2009.
- [4]: Chalice: http://research.microsoft.com/en-us/projects/chalice/
- [5]Saswat Anand, Corina S. Pasareanu, and Willem Visser: JPF–SE: A Symbolic Execution Extension to Java PathFinder. TACAS 07.
- [6]]Daan Leijen, Wolfram Schulte, and Sebastian Burckhardt: The design of a task parallel library. In Oopsla 2009. The TPL became the corner stone of the Parallel Extensions.
- [7] Margus Veanes, Colin Campbell, Wolfgang Grieskamp, Wolfram Schulte, Nikolai Tillmann, and Lev Nachmanson: Model-based testing of object-oriented reactive systems with Spec Explorer. In Formal Methods and Testing 2008.
- [8] Nikolai Tillmann and Wolfram Schulte: Parameterized unit tests. In FSE 2005. Parametrized unit tests became the foundation for PEX/Moles for .NET

Prerequisite

- Knowledge in Formal Methods, Logic, Functional Programming
- Interest in Modeling and Programming with Isabelle/HOL
- English