Domain	Programming-Testing-Proving
Domain - extra	

Model-Based testing of Concurrent JAVA Programs

Year	2012
Starting	1.10.2012
Status	Open
Subject	Model-Based testing of JAVA Programs with Isabelle/HOL-TestGen.
Thesis advisor	WOLFF Burkhart
Co-advisors	Marie-Claude Gaudel
Laboratory	LRI ForTesSE
Collaborations	Biotronik AG Berlin
Abstract	The widely used programming language JAVA supports concurrency by allowing thread creation and synchronization on objects. Concurrent programs are notoriously difficult to verify, be it by proof or testing techniques. Some approaches, however, have been explored based on symbolic test-case generation techniques, mostly based on symbolic evaluation (JavaPathFinderSE (sequential algorithms), Pexx (sequential algorithms), Chalice (Proofs of concurrent programs)). In this thesis, the Isabelle/HOL-TestGen system should be extended by a component that allows to model JAVA-like concurrent programs and to generate tests for them. One potential approach is to extend the existing Monad-library in HOL-TestGen (used for sequence testing) by suitable combinators for interleaving and synchronization; a particular emphasis will have to be put on bounding the number of thread-switches in an interleaving of threads as additional test hypothesis and to find suitable reduction principles to "relevant thread switches" (concerning shared state and locks; thread-switches on distinct state are considered "irrelevant".) Another potential approach is to use the Isabelle/CIRCUS language, which provides process-algebraic modeling approach to concurrency, and to extend it by support for similar

	mechanisms.
Context	This thesis is in the context of a collaboration with the Biotronik Gmbh that is a major producer of medical systems. Biotronik underlies particularly high standards of software quality and certification; the company therefore wishes to extend its expertise in model-based testing techniques. An integral part of this Phd is therefore to apply the test-generation tools developed above to Testing critical components of the Biotroniks Pace-maker Home-Monitoring System. As an example, the Home-Monitoring System contains an efficient communication multiplexer (which is basically a prioritized multi-level Queue), which must satisfy critical security properties (a FIFO-Principle of ingoing/outgoing information packages must be preserved) as well as dead-lock and lifeness properties.
Objectives	- Develop a new method to symbolic test-case generation of concurrent program of non-trivial size (2000 loc) - Apply the approach for a realistic case-study provided by Biotronik Gmbh - The goal is not to support full Java - rather a small subset containing the essentials defined for the case studies.
Work program	- Selecting a means to represent and abstract concurrent JAVA programs - Building theories - building tactic support for the exploration of trace interleavings in Isabelle
Extra information	Publications: BW11 Achim D. Brucker, Burkhart Wolff: On Theorem Prover-based Testing. Accepted the 07-08-2011. In Formal Aspects of Computing (FAOC). DOI: 10.1007/s00165-012-0222-y. Springer, 2011. FGW12Abderrahmane Feliachi, Marie-Claude Gaudel, and Burkhart Wolff. Isabelle/Circus: A process specification and verification environment. In VSTTE, volume 7152 of Lecture Notes in Computer Science, pages 243-260, 2012. [Leino 12]: Chalice: http://research.microsoft.com/en-us/projects/chalice/ [APV 07]Saswat Anand, Corina S. Pasareanu, and Willem Visser: JPF–SE:

	A Symbolic Execution Extension to Java PathFinder. TACAS 07. [LSB 09]]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. [VCGSTN08] 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. SpecExplorer was adopted by Windows for testing 200+ protocols, requiring more than 200+ man years. [TS05] Nikolai Tillmann and Wolfram Schulte: Parameterized unit tests. In FSE 2005. Parametrized unit tests became the foundation for PEX/Moles for .NET
Prerequisite	- Interest in functional programming and formal modeling - Interest in proof techniques (in Isabelle) - Interest in working at least part-time (a few months over the duration of the project) at the site of the project partner - knowledge in english.
Details	
Expected funding	Research contract