Degree project specification

Adam Renberg
adamre@kth.se

June 12, 2012

School: School of Computer Science and Communication (CSC) at KTH
Company: Valtech, http://www.valtech.se/

Supervisor, Valtech:	Erland Ranvinge	erland.ranvinge@valtech.se
Supervisor, CSC:	Narges Khakpour	nargeskh@kth.se
Examiner:	Johan Håstad	johanh@kth.se
Coordinator, KTH:	Ann Bengtsson	ann@csc.kth.se

Contents

1 Short Background

Runtime verification (RV) is a dynamic approach to checking program correctness, in contrast to the more traditional formal static analysis techniques of *model checking* (or its bounded form) and *theorem proving*. These are often very useful, but suffer from severe problems such as the state explosion problem, incompleteness, undecidability etc., when they are used for verification of large-scale systems. Moreover, static analysis only verifies an abstract model of the program, and cannot guarantee the correctness of the implementation or the dynamic properties of the executing code.

Runtime verification is a light-weight formal verification technique, see e.g. [1, 2]. It verifies whether some specified properties hold during the execution of a program. It operates on a *trace* of the *current execution*, either during the execution (*online monitoring*), or at some other time and/or place (*offline monitoring*).

The specification that should be verified is written in a formal language, often a logic/calculus, such as linear temporal logic [3]. To build a *system model* for verifying the properties of the specification, the target program needs to emit and expose certain events and data. Many RV frameworks use *code instrumentation* to generate *monitors* for this end.

When a violation against the specification occurs, simple actions can be taken (e.g. log the error, send emails, etc.), or more complex responses initiated, resulting in a *self-healing* or *self-adapting* system (see e.g. [4]).

On the other end of the program-correctness-checking spectrum is *testing*, which is the practical approach of checking that the program, given a certain input, produces the correct output. Testing is not complete, and lacks a formal foundation, so it cannot be used for formal verification. Testing can be a complement to more formal techniques, such as RV (but is in many cases the sole correctness-checking tool).

Unit testing is the concept of writing small tests, or test suites, for the units in a program, such as functions, classes, etc. These tests are used during development to test the functionality of the units. They aim to reduce the risk of breaking existing functionality when developing new features or modifying existing code (by preventing regression).

Writing unit tests, often using unit testing *frameworks* such as JUnit [5] for Java and unittest [6] for Python, is a common practice on many development teams.

2 Problem

2.1 Problem Definition

How can runtime verification specifications be written in a manner that uses the syntax of the target program's programming language, and resembles the structure of unit tests?

Suggested title: *Test-inspired runtime verification - using a unit test-like specification syntax for runtime verification.*

2.2 Motivation

Checking that a program works correctly is of great interest to software developers, and formal verification techniques can often help. As mentioned above, traditional approaches can be impractical with larger programs, and verification by testing is informal and incomplete. Runtime verification can here be a lightweight addition to the list.

The specification languages used by RV approaches are often based on formal languages/formalisms (e.g. logic or algebra) and not written in the target program's programming language. This means that writing the specifications require specific knowledge and expertise in mathematics. It also requires mental-context switching and special tools to support this specialised language syntax. In contrast, unit testing frameworks often utilize the programming language to great effect, and their use is wide spread.

If RV specifications more resembled unit tests, and were written in the target program's programming language, it might popularize the use of runtime verification for checking the correctness of software systems.

3 Literature

3.1 Previous Research

Runtime verification is a somewhat new area of research, but the research on verification and formal methods goes back several centuries. Research of interest include the early work on formal methods, e.g. by Hoare [7] and Floyd [8], and work on logics suitable for runtime verification, e.g. LTL by Pnueli [3]. Relevant work on runtime verification include [9] on instrumenting code

and transforming specifications into automata, [10] on runtime verification through *aspect-oriented programming* [14], and more.

Unit testing is also quite young, perhaps having begun in earnest in the 90s, and it is not as much researched as formal methods. Testing in general is very old.

The work on the linear temporal logic (and other logics), on runtime verification in general and its applications, on code instrumentation (e.g. [14, 15]), and on unit testing and their frameworks will lay the foundation of this work. Interesting research also include the work by Meyer on the "Design by Contract" methodology [11] and on programming with assertions in general, see e.g. [12, 13].

I have already studied several papers, mostly in runtime verification, verification tools, logics, etc. A list of these can be found at the project's website: `http://tgwizard.github.com/thesis/`.

3.2 Examination

The literature study will be examined as a part of the report, as the report will contain both a general description of RV and unit testing, and more detailed sections on research related to the problem.

4 Method

The work will consist of two parts:

4.1 Approach

I will do a background and state-of-the-art inventory of RV and unit testing. The focus will lie on the syntax used for writing the specifications, how the properties are verified against the system model, and how code instrumentation is done. For unit testing the structure and syntax, and purpose thereof, will have relevance.

I will also answer the following questions:

1. How should the syntax for the specification be defined, so that it looks

similar to that for unit tests, but works for RV? Which language could be used? Which unit testing framework to take inspiration from?

2. How can it be provided with a formal foundation (e.g. by translating it into a formal logic)?
3. How should the code be instrumented to monitor the system and build the system model?
4. How will this be used to (online) verify the system against the specification? (e.g. which techniques should be used to verify the monitored system against the specification?)

Item one and three are of most interest to this project, but all four items are important and required parts of runtime verification.

4.2 Evaluation

In this part I will implement an RV framework prototype, based on the previous investigation.

If possible, I will also attempt to use the resulting framework to enable runtime verification on a project at Valtech.

5 Resources

If I attempt to try the prototype framework on a project at Valtech, I need to get access to such a project. One suggested possible project is the Valtech Intranet.

6 Working Procedure

6.1 Overview

I will work on the degree project 50% and 50% on projects at Valtech, in periods of two weeks degree project, two weeks work. This fits well into the iteration-planning at Valtech. During the summer I will almost exclusively work on the degree project, and also use some of my vacation hours to work on it.

Other required work related to the degree project, such as doing the opposition of another student's work, will take time from the work above and require flexibility in planning. The periods outlined below will of course overlap somewhat, especially in the investigation and implementation parts.

I will keep a diary, `http://tgwizard.github.com/thesis/`, in which I will write on my progress.

6.2 Approximate Time Plan

Start	Weeks		Work
May	*1w in May/June*	**1w**	Writing, and doing the research for, this specification.
May	*2w in May*, v23[1], v26, v27	**5w**	Doing background & research.
9/7	v28	**1w**	Writing the background part of the report.
16/7	v29, v30, v31, v32, v33	**5w**	Investigating and evaluating the questions section of the approach part.
13/8	v34	**1w**	Writing about the investigation.
20/8	v35, v36, v37, v38	**4w**	Implementing and evaluating the RV framework. Possibly testing and analysing the RV framework on a project.
24/9	v39, v40, v41	**3w**	Writing and finishing the report.

Table 1: Time plan week-by-week

I will take the weeks v24 and v25 off, as well as about 1 week in august (not planned). **The weeks I will be working at Valtech haven't been written into the time table.**

Total: 20 weeks. End date: **12 October 2012** (very optimistic).

[1] vXX means week-of-the-year XX, calculated in the Swedish way. i.e., week 23 starts on the 6th of June

7 Licensing

I will license any resulting code under some open source license, and any documentation, including the report, under Creative Commons Attribution 3.0 Unported License [16] (or something similar).

References

[1] Martin Leucker, Christian Schallhart. A brief account of runtime verification. In *The Journal of Logic and Algebraic Programming 78*. 2009, pages 293-303.

[2] Nelly Delgado, Ann Q. Gates, Steve Roach. A Taxonomy and Catalog of Runtime Software-Fault Monitoring Tools. In *IEEE Transactions on Software Engineering*. IEEE, 2004.

[3] Amir Pnueli. The temporal logic of programs. In *Proceedings of the 18th IEEE Symposium on the Foundations of Computer Science (FOCS-77)*. IEEE, 1977

[4] Markus C. Huebscher, Julie A. McCann. A survey of Autonomic Computing degrees, models and applications. In *ACM Computing Surveys*, Volume 40 Issue 3. ACM, 2008.

[5] Kent Beck, Eric Gamma, David Saff. JUnit. `http://junit.sourceforge.net/`, June 2012.

[6] Python Software Foundation. unittest. `http://docs.python.org/library/unittest.html`, June 2012.

[7] C. A. R. Hoare. An Axiomatic Basis for Computer Programming. In *Communications of the ACM*, Volume 12 Issue 10. ACM, 1969

[8] Robert W. Floyd. Assigning meaning to programs. In *Proceedings of Symposium on Applied Mathematics*, Vol. 19. A.M.S., 1967

[9] Andreas Bauer, Martin Leucker, Christian Schallhart. Monitoring of real-time properties. In *Proceedings of the 26th Conference on Foundations of Software Technology and Theoretical Computer Science* (FSTTCS), volume 4337 of LNCS. Springer, 2006.

[10] Eric Bodden. Efficient and Expressive Runtime Verification for Java. In Grand Finals of the ACM Student Research Competition 2005. ACM, 2005.

[11] Bertrand Meyer. Applying "Design by Contract". In *Computer (IEEE)*, 25, 10. IEEE, 1992.

[12] Davis S. Rosenblum. A Practical Approach to Programming With Assertions. in *IEEE Transactions on Software Engineering*, Vol. 21, No. 1. IEEE, 1995.

[13] Detlef Bartetzko, Clemens Fischer, Michael Möller, Heike Wehrheim. Jass - Java with Assertions. In *Electronic Notes in Theoretical Computer Science*, Volume 55, Issue 2. Elsevier 2001.

[14] AspectJ. `http://www.eclipse.org/aspectj/`, June 2012

[15] Martin Matusiak. Strategies for aspect oriented programming in Python. 2009

[16] Creative Commons. Creative Commons Attribution 3.0 Unported License. `http://creativecommons.org/licenses/by/3.0/`