Bridging the Gap Between Specifications and Compliance Tests
R-Check® SCA

James Ezick
Jonathan Springer

Reservoir Labs, Inc.
New York, NY

SDR-WInnComm 2013
WIF Conference on Wireless Communications Technologies & Software Defined Radio

8 January 2013
Thought Experiment

If a specification is written, but software written to it cannot be tested for compliance, does it make an impact?

US DARPA

- Approximately 1–5 bugs per 1000 lines of code
- In the United States, approximately 1000 experts in formal verification

Woodcock et al. "Formal Methods: Practice and Experience,”
ACM Computing Surveys. Volume 41 Issue 4, October 2009
Innovation #2: Certification Process for Third Party Waveform Software

The ability to certify software implementations of waveforms for use on various radio computing platforms promises to significantly reduce development cost and time to market of software based radios.
Holy Grail

The dream ...

Automatic Process

Plain Text Specification Document

Fast Automated Test

Pass: Compliant!

Fail: And here’s why ...

The reality ...

Testing is a time-intensive, expensive, imprecise process that requires a combination of tools – tools that require significant domain expertise to construct and certify
R-Check SCA

Draw from the most successful ideas in static analysis to develop a solution customized to the SCA

Version 1.17.3

- SCA structure and context aware
- Expanded support for XML, CORBA IDL
- Scales to enterprise code
- Push–button support for SCA 2.2.2 tests

R-Check SCA has been verified by the JTRS Test and Evaluation Laboratory (JTEL) to correctly test SCA 2.2 and 2.2.2 requirements [AP0]603, [AP0]604, [AP0]607, and [OE0]620. JTEL anticipates utilizing R-Check SCA to verify these requirements as a part of the process of record (currently manual MASTD/MOESTD testing) for requirements [AP0]603, [AP0]604, [AP0]607, and [OE0]620 as of 1 Dec 2011.

JTEL has found that utilizing R-Check SCA has provided up to a 90% reduction in the time required to test [AP0]603, [AP0]604, [AP0]607, and [OE0]620.

Statement Approved for Public Release by:
Benefits of Static Analysis

Static Analysis seeks to *find bugs* through *inspection of source code* rather than through the execution of the program

- Analyzes all possible program paths without bias
- Can be run on code in an intermediate state
- Integrates with development environments

What can it do?

- Provide reproducible, automated tests
- Explain specifications, answer “what ifs”
- Generate counter-examples

Based on a rich theory of analysis with specific applicability to the SCA

  *Outstanding Paper Award, Design, Manufacture, and Deployment (DMD) track*
Challenges to Bridging the Gap

Advantages of Domain-specific Testing

- Speak the language of the specification
- Exploit domain knowledge
- “Teaches” the specification throughout the development process

How do we further automate the process of domain-specific test tool development?

Key Challenges

- Translate prose to working tests
- Specify tests that span file types
- Conversing in domain language

R-Check SCA GUI with named tests for SCA requirements
Translating Prose Requirements to Working Tests

Two Phase Process

Sticky Patterns: Abstract Analyses

- Built on the theory of data-flow analysis
- State machines with patterns that “stick” the first time they are matched

Query Interface: Templates for Abstract Analyses

- English-like sentences
- Syntax is bound to a pre-formed state machine with blanks being used to complete the patterns

“On all paths, if X occurs then Y shall eventually occur.”

X, Y: API calls, pointer-based memory allocation, error check, etc.
Specifying Tests that Span Files Types

R-Check SCA Workflow
Enabled by GNU Make
Conversing in the Domain Language

Reading the Domain Language
- Understand the domain and use knowledge to affect rules (e.g., SCA Components)
- Take advantage of model-based development environments and automatically generated code

Speaking the Domain Language
- Present options in the language of the domain (e.g., GUI)
- Special cases (e.g., waivers)
- Explain counter-examples & remedies not just as code, but using domain

*Challenge is to abstract this knowledge!*

Automatically Generated

Generated from Scratch
*The Toaster Project*, Thomas Thwaites, 2011
Bringing it All Together

"Walking on water and developing software from a specification are easy if both are frozen."

- Edward V Berard

Cooperative Process

Design tools with automation in mind
- Components that can be automatically generated (e.g., GUI, Tests, Makefiles)
- Philosophy of providing clear, correct information where a yes/no result can not be determined

Design specification with automation in mind
- Write statements that are testable
- Be clear about where domain knowledge is applicable and how it impacts the test
What’s coming with R-Check SCA?

More than a dozen new requirements in approval testing now
- Expanded SCA XML coverage
- Consolidated heap memory reporting
- Linux support

Adding more than 100 new source code requirements
- Exception handling constructs
- Consistency tests across XML, IDL, and source code
- APIs

Anticipate first SCA 4.0 support in Q3’13
- Full support through GUI

Automatic test generation: 2014
- Write English-like specification statements and test them with the benefit of SCA domain knowledge
What is the Wireless Forum Doing?

Coordinating Committee on International SCA Standards
The Test & Certification Group Working Document
“SCA Test, Evaluation and Certification”
Chair: Randy Navaro (SAIC)

SCA Test Lab: Accredited facility for reproducible testing
• Responsibilities
• Structure
• Business Case

Expecting document submission first-half of 2013

Looking for volunteers!

Working sessions: Wed 1600 (Coolidge), Fri 830 (Hoover)
Takeaways

*We are passionate about testing!*
- Strive to build the best tool for the SCA

**Testing is integral to specification writing**
- Deep connection between spec and tool

**There is value in domain-specific testing**
- Speak the language of the specification
- Teach the specification

**Domain knowledge can be used to sharpen the testing process**
- Use deep-knowledge of the domain to produce better tests than can be achieved with “customizable” generic tools
Takeaways

The SCA is a great test case for driving research in this area

• Complex software requirements
• Span multiple file types

Tools should be developed with automation in mind

• Open formats, COTS utilities
• Provide information rather than conclusions

The WIF is active in this area

• #2 Most Wanted Innovation
• Test & Certification Group: SCA Test Lab Document
About Reservoir Labs

Privately owned, Reservoir Labs has been providing leading-edge consulting and contract R&D to the computer industry, business, end-users, and the US Government since 1990

Expertise
- Custom verification solutions
- Applied compiler research for emerging high-performance and embedded architectures
- Reasoning, constraint solving, and mathematics
- High-bandwidth network cyber security

Technologies
- R-Check Static Analysis Platform
- R-Stream Mapping Compiler
- R-Solve Reasoning and Planning Technology
- R-Scope Network Security Technology

Reservoir Labs’ offices in New York, NY and Portland, OR
Acknowledgements

Development funded by SPAWAR under Navy Phase II.5 SBIR Contract “Static Analysis Tool for Interface Compliance Verification and Program Comprehension”

Thanks!

John Thom, TPOC (SPAWAR)

JTEL Test Execution Team

Jim Kulp, Parera Information Services
Bridging the Gap Between Specifications and Compliance Tests

For more information on R-Check SCA

- https://www.reservoir.com/rchecksca

Contact us by email

- rcheck-support@reservoir.com

Visit our booth!