Tool support for automated traceability of test/code artifacts in embedded software systems


Published in:
Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
Copyright 2011 IEEE. This work is made available online in accordance with the publisher’s policies. Please refer to any applicable terms of use of the publisher.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen’s institutional repository that provides access to Queen’s research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person’s rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Download date: 25. Mar. 2022
Abstract— Development, testing and maintenance of software for embedded systems is a complex task. Analysis of the traceability between different software artifacts (e.g., source code, test code and requirements) is an enabling capability for better development, testing and maintenance of software systems. However, there is a general lack of tool support for automating traceability analysis for embedded systems. We demonstrate in this paper how to extend an existing unit test and test coverage framework to produce a hard-ware assisted tool framework capable of automatically deriving and visualizing traceability links between source code and test code artifacts. To demonstrate the applicability and usefulness of the framework, we report the application of the framework on realistic embedded software for vehicle gear transmission control built and deployed on the Analog Devices Blackfin® ADSP-5XX family of DSP processors.

I. INTRODUCTION

Many products today contain embedded software, for example: mobile phones, DVD players, cars, airplanes, and medical systems. Because of rapid changes in this field, future products will likely contain even more embedded software.

Development, testing and maintenance of embedded software systems is a complex task [1-3]. Embedded software engineering [1, 3] is an emerging and active area for both researchers and practitioners that aims at addressing various challenges in this domain, e.g., requirements engineering, reengineering and reverse engineering of existing systems, quality, maintenance, program comprehension, management of development process.

Analysis of traceability between different software artifacts (e.g., source code and test code) is a widely used practice in the embedded industry [1] and an enabling factor for better development, testing and maintenance of embedded systems.

In its beginnings, traceability in embedded software development was driven mainly by obligatory regulations such as DoD 2167a/ML-STD-498 for US military systems [4]. Later, quality standards which recommended traceability such as IEEE Standard #1219, ISO 9000ff, ISO 15504, and SEI CMM/CMMI have gained more and more attention.

In a survey of eight European embedded system companies (including major firms such as Nokia and Philips), Graaf et al. [1] found that embedded software engineers see traceability among software artifacts as an essential aspect of embedded software development and project management. To keep all development products and documents consistent, the project engineers had to analyze the new features’ impact (by utilizing automated tools and also manually). However, in the projects surveyed it was reported that the relationship between requirements and other artifacts were frequently not explicitly documented which made impact analysis quite difficult. Tracing artifacts to each other was difficult because the relations were too complex to specify manually (for example, between requirements and architectural components) [1]. Note that in software engineering, (change) impact analysis is defined as follows [6]: If the interdependencies between artifacts are documented and maintained, proposed changes of earlier (later) artifacts can be traced to necessary changes in downstream (up-stream) artifacts, supporting product development time and cost.

The industrial survey reported in [1] also revealed that the embedded system companies need more specific, yet flexible, development and support tools (including traceability tools).

In our current on-going Collaborative Research and Development (CRD) project funded by the Canadian government, we are finding that our industrial embedded systems partners are interested in traceability tools in their projects. By searching in the literature and also the software products (either open-source or commercial), we have found a general lack of tool support for automating traceability analysis in the context of the embedded software systems.

To address the above need, we have recently designed and built a tool-set to automatically derive and visualize traceability links between source code and test code artifacts in embedded software. Our development platform are the families of DSP processors offered by Analog Devices Inc., namely Blackfin®, SHARC® and TigerSHARC® [7].

Our traceability analysis tool-set is referred to as Automated Embedded Traceability Framework (AutoETF) constructed as an extension of an existing unit testing and test coverage framework developed by the third author and several
other colleagues (reported in several earlier papers [8-10]. An advantageous novel feature of those frameworks is that they perform test coverage analysis using processor hardware features rather than software, thus they have low overhead and are efficient for embedded systems.

In this report, we report how the *AutoETF* framework has been developed, its features and uselessness, and its application/evaluation on real embedded software.

The rest of this article is structured as follows. A review of the related work and a brief background on traceability analysis is presented in Section II. Since some knowledge about our existing embedded unit testing [9] and code coverage measurement framework [8] is important for the presentation of the *AutoETF*, an overview of those two frameworks is presented in Section III. *AutoETF* itself is presented in Section IV. To demonstrate the applicability and usefulness of the *AutoETF* framework, we report in Section V its application on realistic embedded software we have designed and built for automated control of vehicle gear transmission. Finally, Section VI concludes this article and points out future works.

II. BACKGROUND AND RELATED WORK

The area of traceability analysis in software engineering is quite well developed and active research area. For example, a recent 2010 survey paper [6] reported extensively on widespread developments and usage of traceability in conventional software engineering across 202 key publications. Analysis of traceability links across software artifacts can be performed in various stages of the software development lifecycle (SDLC).

An example hypothetical traceability graph showing traceability links among artifacts in five typical phases of the SDLC is depicted in Fig. 1. In this graph, an edge (arrow) denotes a traceability link, meaning either usage of an earlier artifact in developing a later artifact, or an artifact depending on another (e.g., a test case testing a code artifact). The areas shaded by gray are the focus and contributions of the current work in the embedded system’s context.

![Traceability Graph](image)

Fig. 1-An example hypothetical traceability graph showing traceability links among artifacts.

Although tools for automated traceability in the software engineering literature [6] exist, there is a lack of tool support focusing in the context of embedded software. Many companies and embedded software developers feel the need for automated tool support traceability [2].

To the best of the authors’ knowledge, works in [11, 12] are the key traceability methodologies for embedded software and the toolset reported in [13] is the only tool environment to support traceability in this domain.

Von Knethen [11] has proposed a set of models and a working environment [13] in the domain of embedded systems. The approach supports change-impact analysis (as an application of traceability) and semi-automatic propagation of changes through these models based on previously-recorded traceability links. However, the tool-set does not support automated extraction of traceability links between application and test code as proposed in our work.

III. AN OVERVIEW OF OUR EXISTING EMBEDDED UNIT TEST AND COVERAGE MEASUREMENT FRAMEWORK

The third author of this paper and several other colleagues have developed and reported previously [8-10] an embedded unit framework (called *E-Unit*) and a hardware-assisted framework for efficient code coverage analysis in embedded environments. We provide an overview of those two frameworks in Fig. 2 since our traceability framework is built on top of them. For details, the interested reader is referred to [8-10].
The diagram in Fig. 2 shows where each component is deployed (i.e., on the embedded device under test, or the desktop computer). The top figure depicts the actual connection to the embedded device (Blackfin® DSP board in this case) of the development tool installed and running on a PC. To clarify the contributions of the current work versus [8-10], note the three shades present for the modules in the legend of the bottom figure in Fig. 2.

In our current platform, the desktop computer runs the development tool, Analog Devices VisualDSP++®, which is an Integrated Development and Debugging Environment (IDDE) for embedded software. We extended VisualDSP++® to add support for embedded unit (E-Unit) testing features [8] and code coverage [9].

E-Unit capabilities include creation, build, executions, and results reporting of the unit test suite running on the hardware under test. The coverage engine [9] calculates two types of test coverage metrics: function (method) and statement. The coverage framework was developed using a hardware feature in processors called the branch vector buffer. Use of the hardware performance monitoring unit (containing the above buffer) has been demonstrated to reduce code coverage profiling overheads by moving much of the logging process into hardware [8, 14]. While a basic version of this can found on some PC-oriented processors such as the Itanium 2 by Intel [14], this feature has much greater flexibility and power with embedded systems where it forms a fundamental part of the embedded processor’s debugging sub-system [8].

The desktop computer lets the engineer build and deploy the Software Under Test (SUT) and its automated test suite using the IDDE. The E-Unit library is automatically deployed on the embedded device by VisualDSP++®.

After executing the test suite on the embedded device, the test results of the test suite are brought back from embedded device to the desktop computer using the automation API of VisualDSP++® and the results displayed in the IDDE [8]. The coverage plug-in embedded inside the IDE then generates the test coverage reports. Of particular interest is the fact that the test coverage analysis is performed with low overhead (near real-time) using hardware features present in the Analog Device’s families of DSP processors rather than the customary software analysis.

With our additions in the current work, the coverage plug-in produces also, in addition, the traceability data from each execution of test suites. In other words, the current work adds to the existing platform [8-10] an automatic traceability between test and code artifacts.

IV. EMBEDDED TRACEABILITY FRAMEWORK

Our Automated Embedded Traceability Framework (AutoETF) has two modules: (1) automated traceability extraction, and (2) traceability visualization tool, which are described next.

A. Automated Traceability Extraction

Automated traceability extraction is the process of extracting traceability links between source and test code artifacts. Recall from Fig. 1 that traceability links can be among artifacts in different phases of the SDLC, e.g., requirements, design, development, testing and maintenance. In our first attempt in this work, we have currently developed automated extraction of traceability links between source (production) code and test code artifacts.

Fig. 3 depicts a detailed view of part of Fig. 2 showing the software tools we have developed and deployed on a desktop computer to perform automated traceability extraction. We have extended the E-Unit test and embedded coverage engine to extract traceability links while measuring code coverage of test suites.

Automated extraction of traceability links works as follows. During the post-build of the test suite code in the IDDE, a VisualDSP++ utility called ElfDump generates the symbol table of the code-base (shown as symtab in Fig. 3) and source code line data (debug_line, details in [15]) into two text files (symtab.txt and linetab.txt). After test suite executions, the E-Unit test and embedded coverage engine reads, using the Automation API from IDDE, addresses of the program’s control flow stored in the memory of embedded device. Those addresses are mapped to functions and source lines data, using respectively symtab.txt and linetab.txt data to create test/code traceability links.
Fig. 3- Detailed view of part of Fig. 2 showing the software tools deployed on desktop computer that perform automated traceability extraction.

Building traceability links between artifacts is realized by identifying the position (start, inside or end) of methods to determine when each test artifact calls a source code artifact. The extended embedded coverage engine generates an XML file containing traceability links between source code and test code. Since our next step is to visualize the traceability links using a graph visualization framework (Gephi [16]), we have designed the embedded coverage engine in a way that the XML file is created in the Graph Exchange XML Format (GEXF) [17].

For traceability links between artifacts, different granularities for either source code or test code must be supported. To formally present this concept, a UML meta-model showing traceability links between different granularities of source (production) code and test artifacts is shown in Fig. 4. A source (production) code artifact can be a namespace, class, method, line or a target memory address. On the other hand, a test artifact can either be a test suite, test method, test line of code, or a memory address storing the code.

This hierarchical scheme allows our framework to support 20 (5x4) granularities of traceability links between the two artifact types. An example of the traceability links extracted by our tool-set is provided in the next section. A larger example and application of the AutoETF framework on a real large-scale embedded software is discussed in Section V.

B. Traceability Visualization Tool

We have developed a traceability visualization tool by adapting the popular Gephi graph visualization framework [16]. The entire source code of our visualization tool is available online in the Google Code repository [18] and can be used by researchers and practitioners.

A workflow diagram showing how the traceability visualization tool works and how it is used is shown in Fig. 5.

With the XML file containing traceability links among the source and test artifacts generated, our traceability visualization tool is used to visualize the traceability data as a traceability graph (TRG).

As an example of a TRG, let us present simple embedded software with two classes: Addition and Subtraction. Code listing for the example classes Addition and Subtraction is shown in Fig. 6. Four example test cases (methods) for these two classes are shown in Fig. 7.

As mentioned above, a TRG can be generated for different granularities of source code and test artifacts. Two example TRGs rendered in our visualization tool for the above example system are shown in Fig. 8. In both TRGs, the test artifact
Different artifacts are related and trace to each other. Panning, moving nodes around, etc. to understand how to perform standard graph browsing tasks such as zooming, automatically generated these example TRGs and the user can source code artifact granularities are methods and lines of granularity is test method. In the top and bottom TRG, the example (Fig. 6 and Fig. 7).

Test redundancy detection

As Winkler and von Pilgrim discuss in their survey paper [6], recording, extracting, storing and visualizing software traces only makes sense if the traces can be used later. In fact, a project’s traceability goals should generally drive the activity of extracting traces.

Winkler and von Pilgrim aggregate [6] from the existing traceability literature that traceability links have been used for many purposes in software engineering including the following (refer to [6] for references to articles on each type of usage): estimating change impact, showing system’s adequateness, validating artifacts, supporting audits, improving changeability, monitoring progress, assessing the development process, understanding the system, documenting reengineering, and finding reusable elements.

In our own industrial collaborations, we have frequently observed that software engineers and testers (especially in the embedded context) have considerable challenges in the following scenarios:

1. Test coverage (adequacy) improvement
2. Test suite maintenance as the software under test (SUT) evolves
3. Fault localization
4. Test redundancy detection

Our proposed AutoETF framework aims at addressing all the above challenges as is discussed next. For usage scenario #1 above (test coverage improvement), testers need to find the uncovered parts of the SUT and attempt to cover them by creating new test cases. For this purpose, testers only require to find the SUT nodes with no incoming edges when using TRG. Using the conventional code-coverage tools to show the coverage information, multiple files should need to be inspected manually for this purpose so that extensive time from human testers is required to find uncovered parts of the SUT.

As an example of the usage scenario #2 above, consider the following scenario. As a result of SUT evolution, source code modifications can make a number of test methods invalid for regression testing and thus testers need to modify them appropriately. TRG can help testers to find all the tests related to the modified part of the system. For this purpose, the tester needs to find the modified SUT node in the graph and consider all those tests which are covering these items.

In the usage scenario #3 above by referring to TRGs, testers can find which part of the system is covered more frequently by failing tests. The number of incoming edges to a SUT item and the number of the calls shown on each of those edges can be used to find more suspicious fault prone parts of the SUT [27]. Again, using the conventional code-coverage tools to show the progress-bar like coverage information, multiple files must be inspected manually at extensive effort.

To detect redundant test cases (usage scenario #4 above), testers need to find the tests that cover part of the system which are also covered by other test cases in the test suite. For this purpose, TRG can be useful to find which parts of the system are covered by each test and compare the covered parts by various test cases with each other.

C. Making Use of Traces (i.e., Traceability Links)
Last but not least, from a higher-level perspective, we can qualitatively estimate the cost of test maintenance (entailed by a change in the SUT) by visually analyzing the volume of edges from the test suite domain to the SUT domain.

V. EVALUATION ON AN EMBEDDED CONTROLLER SOFTWARE FOR VEHICLE GEAR TRANSMISSION (EMBEDDEDGEAR)

To demonstrate the applicability and usefulness of our traceability framework, we applied the tool on a realistic embedded software that we have developed for vehicle gear transmission control (referred to as EmbeddedGear in the rest of paper). The software was built and deployed on Blackfin ® ADSP-BF533, BF561 and BF548 DSP processors [7] made by Analog Devices Inc.

We discuss next an overview of the EmbeddedGear software, its automated test suite, our initial attempt to conduct traceability analysis of this system, and as a result of our initial evaluations, some discussions on the usefulness of AutoETF for development, testing and maintenance of this system.

A. An Overview of the EmbeddedGear Software

The Matlab Simulink platform provides as a demo (tutorial) a fully-implemented and executable model for automotive power transmission control [19]. We reverse engineered this model and used it as the requirements and design document to develop the EmbeddedGear system.

A typical automotive power train system is shown in Fig. 9 [19]. It is composed of the following four blocks: engine, transmission, transmission control unit and vehicle dynamics.

The UML use case diagram of EmbeddedGear is shown in Fig. 10 (reverse engineered from the Matlab Simulink model [19]). Driver has the ability to manipulate the throttle and brake only. The automatic transmission control unit will then set the appropriate gear, will update the vehicle speed and set the engine RPM (revolutions per minute).

The main logic of the transmission control is carried by classes Gear, GearState, TransmissionGearRatio and TorqueConverter. The GearState class has four child classes denoting gears 1 to 4 (we have only modelled a 4-gear transmission system in this software, but more gears can be added).

The ShiftState class has three child classes (designed based on the state design pattern [20]) denoting the shifting states down and up and also the steady state for no shifting.

Each thread class (except SchedulerThread) has another (runner) class inside itself which is executed by the thread class. Class SchedulerThread itself acts a runner class and an object of this class performs the scheduling of all the other threads by setting execution times among different objects.

The class diagram of the EmbeddedGear software is shown in Fig. 11. There are eight thread classes which inherit from the Thread class in the VisualDSP++ Kernel (VDK) library. Thread classes are responsible for parallel execution of different components (objects) of EmbeddedGear system, and input/output synchronization of their signals.
To verify and validate the behavior of EmbeddedGear, an executable Matlab Simulink model [19] was compared with the output of the Matlab Simulink model [19].

Breakdown of the number automated tests for each class of the EmbeddedGear generated by each of the above three black-box test approaches is provided in Table 2. To manage the efforts on creating test cases for each class, we used the guidelines of value-based software testing [25], i.e., classes under test were prioritized so that high priority classes would have more test cases.

Table 2- Information about the Automated Unit Test Suite of the EmbeddedGear

<table>
<thead>
<tr>
<th>Class under test</th>
<th>Type of test generation activity</th>
<th>Breakdown of the number automated tests for each class of EmbeddedGear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine</td>
<td>Category partitioning</td>
<td>47 102 6 6 155</td>
</tr>
<tr>
<td>Vehicle</td>
<td>Contract-based unit testing</td>
<td>0 53 0 53</td>
</tr>
<tr>
<td>ShiftLogic</td>
<td>Contract-based integration testing</td>
<td>1 0 6 7</td>
</tr>
<tr>
<td>Gear</td>
<td>Sum</td>
<td>1 0 2 3</td>
</tr>
<tr>
<td>Transmission</td>
<td></td>
<td>0 0 20 20</td>
</tr>
<tr>
<td>TransmissionGearRatio</td>
<td></td>
<td>0 37 4 41</td>
</tr>
<tr>
<td>Total number of test cases</td>
<td></td>
<td>97 269 47 413</td>
</tr>
</tbody>
</table>

C. Traceability Analysis of EmbeddedGear

We applied our toolset to the EmbeddedGear by running its test suite on a Blackfin® model BF548 DSP processor [7] and used our tool to visualize several types of traceability graphs (TRGs).

Due to space constraints, it is not possible to report all combinations of different granularities of a TRG in this paper. Thus, we only report four selected types of TRGs here (Fig. 13 and Fig. 14). To provide more details, we have prepared a screen-cast video demo of traceability analysis of EmbeddedGear using our visualization tool which can be viewed online at [26].

To provide a few examples, Fig. 13 and Fig. 14 depict three selected TRGs for the classes Engine and Transmission as two important classes in this system. In Fig. 13, the granularity of the SUT artifacts (in left side) are methods and lines (of class Engine) in the top and bottom TRGs, respectively. In both TRGs, test artifacts are unit test methods.

In the TRG shown in Fig. 14, the granularity of the SUT artifacts (in left side) is methods (of class Transmission). Test artifacts are unit test methods. Usefulness of the AutoETF framework based on these three TRGs is discussed next. The width of the edges in a TRG denotes the frequency of calls from the involved test artifact to the code artifact.

D. Usefulness of AutoETF

After developing the AutoETF framework, our goal was to evaluate its usefulness based on the usage scenarios of...
traceability links from the literature [6] and also based on our own experience in working with industrial partners.

Fig. 13. Two TRGs for the class Engine.

Fig. 14. A TRG for class Transmission.

During development, testing and maintenance of EmbeddedGear, we extensively used different views of TRGs to facilitate the tasks on hand. More specific usage scenarios were test coverage improvement and test suite maintenance as the software under test (SUT) evolved. For example, the TRG shown in Fig. 14 shows that only six of the methods of class Transmission are covered by the existing test suite. Thanks to the information provided by these TRG, we were able to effectively develop new test code to cover the other uncovered methods.

Traditional code coverage information (in text and number format, e.g., 80%) can be of help in this challenge. However we have found in the current work and also a previous study [27] that a visual representation of coverage is better for these purposes since it can provide a high-level bird-eye view for the test engineer on both the SUT code and test artifacts without overwhelming the test engineer with details.

VI. CONCLUSIONS AND FUTURE WORKS

We presented in this paper a tool framework to automatically derive and visualize traceability links between source code and test code artifacts in embedded software. To demonstrate the applicability and usefulness of the framework, we reported the application of the tool on an embedded software called EmbeddedGear.

The traceability framework has been helpful for our project so far in development, testing and maintenance of EmbeddedGear, e.g. in test coverage improvement and test suite maintenance. As a future work, we plan to conduct more usage scenarios of the proposed traceability framework based on the needs of our industrial partners.

ACKNOWLEDGMENT

This project was financially supported by the Discovery Grant no. 341511-07 and also the Collaborative Research and Development (CRD) grant no. 365295-08, provided by the Natural Sciences and Engineering Research Council of Canada (NSERC) and also by Analog Devices Inc.

REFERENCES


