Generating Code Review Documentation for Auto-Generated Mission-Critical Software

Ewen Denney and Bernd Fischer

***Abstract*— The AutoCert tool takes a set of mission safety requirements, and formally verifies that auto-generated code satisfies these requirements. It generates human-readable and traceable safety documentation in the form of a hyper-linked report that provides a high-level traceable structured argument for why the code complies with the specified requirements.**

Index Terms— automated code generation, model-based design, verification and validation, code reviews

I. Introduction

Model-based development and automated code generation are increasingly used by NASA missions (e.g., Constellation uses MathWorks' Real-Time Workshop), but the V&V situation remains unsatisfactory for several reasons:

- Code reviews are still necessary for mission-critical software, but auto-generated code is often difficult to understand, and requires reviewers to match subtle details of textbook formulas and algorithms to model and/or code.
- Common modeling and programming languages do not allow important requirements to be represented explicitly (e.g., units, coordinate frames, quaternion handedness); consequently, such requirements are generally expressed informally and the generated code is not traced back to these requirements.
- Writing documentation is tedious and therefore often not completed or kept up to date.

In this paper, we describe a new tool that generates human-readable and traceable safety documentation from the results of an automated analysis of auto-generated code. It is based on the AutoCert code analysis tool, which takes a set of mission safety requirements, and formally verifies that the code satisfies these requirements. AutoCert exploits the idiomatic nature of auto-generated code in order to automatically infer logical annotations which allow the fully automatic formal verification of the required properties. AutoCert can verify both simple execution-safety requirements (e.g., variable initialization before use, array out of bounds, etc.), as well as domain- and mission-specific requirements such as the consistent use of Euler angle sequences and coordinate frames.

The results of the code analysis are used to generate a hyper-linked report that provides a high-level traceable structured argument for *why* the code complies with the specified requirements. The report makes the following information explicit: assumptions (e.g., the physical units and constraints on input signals), assumptions on intermediate variables in the computation (representing intermediate signals in the model), the algorithms used by the code generator to implement the various blocks, the dependencies between variables, and the chain of reasoning which allows the requirements to be concluded from the assumptions. The tool matches against candidate algorithms for various mathematical operations, and then uses theorem proving to check that they really are correct implementations. The report links to the source code, giving traceability between verification artifacts (e.g., verification conditions), documentation, and code. In order to construct a justification that code meets its requirements, a diligent code reviewer must "rediscover" all the information which is automatically generated by AutoCert, so our tool can result in substantial savings in effort.

Our approach, both to the formal verification and the construction of the review reports, is independent of the particular generator used, and we have applied it to code generated by several different in-house and commercial code generators, including MathWorks' Real-Time Workshop. In particular, we have applied our tool to several subsystems of the navigation software currently under development for the Constellation program, and used it to generated review reports for mission-specific requirements such as the consistent use of Euler angle sequences and coordinate frames.

Manuscript received December 1, 2008.

E. Denney is with USRA/RIACS, NASA Ames Research Center, Mountain View, CA 94035, USA (650-604-2274; e-mail: Ewen.W.Denney@nasa.gov).

B. Fischer is with the University of Southampton, UK (e-mail: b.fischer@ecs.soton.ac.uk).

Filename: 59.doc
Directory: D:\F Drive_new\www-smcit09\abstracts-contri_papers
Template: C:\Documents and Settings\klittle\Application Data\Microsoft\Templates\Normal.dot
Title: .
Subject: IEEE Transactions on Magnetics
Author: -
Keywords:
Comments:
Creation Date: 9/3/2008 9:34:00 AM
Change Number: 11
Last Saved On: 12/1/2008 7:49:00 PM
Last Saved By: Ewen Denney
Total Editing Time: 25 Minutes
Last Printed On: 5/27/2009 11:21:00 AM
As of Last Complete Printing
Number of Pages: 1
Number of Words: 593 (approx.)
Number of Characters: 3,384 (approx.)