The AAMP5/AAMP–FV Project

Steven P. Miller
Collins Commercial Avionics
Rockwell International
Cedar Rapids, IA 52498 USA
spmiller@pobox.cca.rockwell.com

Mandayam Srivas
Computer Science Laboratory
SRI International
Menlo Park, CA 94025 USA
srivas@csl.sri.com

Software and digital hardware are increasingly being used in situations where failure could be life threatening, such as aircraft, nuclear power plants, weapon systems, and medical instrumentation. Several authors have demonstrated the infeasibility of showing that such systems meet ultra–high reliability requirements through testing alone [1,2]. Formal methods are a promising approach for increasing our confidence in digital systems, but many questions remain on how it can be used effectively in an industrial setting.

This presentation describes a project, formal verification of the microcode in the AAMP5 microprocessor, conducted to explore how formal techniques for specification and verification could be introduced into an industrial process. Sponsored by the Systems Validation Branch of NASA Langley and by Collins Commercial Avionics, a division of Rockwell International, it was conducted by Collins and the SRI International Computer Science Laboratory. The project consisted of specifying in the PVS language developed by SRI [3] a portion of a Rockwell proprietary microprocessor, the AAMP5, at both the instruction set and register–transfer levels and using the PVS theorem prover to prove the microcode correct for a representative subset of instructions.

While this presentation includes a brief technical overview (see [4,5] for a detailed technical discussion), its emphasis is on the lessons learned in using PVS for an example of this size and the implications for using formal methods in an industrial setting. The central result of this project was to demonstrate the feasibility of formally specifying a commercial microprocessor and the use of mechanical proofs of correctness to verify microcode. This is particularly significant since the AAMP5 was not designed for formal verification, but to provide a more than three fold performance improvement, by pipelining instruction execution, while remaining object code compatible with the earlier AAMP2. As a consequence, the AAMP5 is one of the most complex microprocessors to which formal methods have been applied.

Another key result was the discovery of both actual and seeded errors. Two actual microcode errors were discovered and corrected during development of the formal specification, illustrating the value of simply creating a precise specification. Two seeded errors were systematically uncovered while doing correctness proofs. One of these was an actual error that had been discovered after first fabrication but left in the microcode provided to SRI. The other error was designed to be unlikely to be detected by walkthroughs, testing, or simulation.

Several other results emerged during the project, including the ease with which practicing engineers became comfortable with PVS, the need for libraries of general purpose theories, the usefulness of formal specification in revealing errors, the natural fit between formal specification and inspections, the difficulty of selecting the best style of specification for a new problem domain, the high level of assurance provided by proofs of correctness, and the need to engineer proof strategies for reuse.

Many of the costs of the AAMP5 project can be attributed to the overhead of applying an experimental method for the first time. To determine how much these costs can be reduced through reuse of the AAMP5 expertise, Collins, SRI, and NASA are conducting a follow–on project to verify the microcode in the AAMP–FV, a smaller microprocessor design similar to those actually used in autoland systems. A report on the status of this project is also presented.

[1] Butler, R. and G. Finelli, The Infeasibility of Experimental Quantification of Life–Critical Software Reliability, *Software Engineering Notes*, Vol. 16, No.5, pg. 66–76, December 1991.

[2] Littlewood, B. and L. Strigini, Validation of Ultra–High Dependability for Software–based Systems, *Communications of the ACM*, Vol. 36, No. 11, pg. 69–80, November 1993.

[3] Owre, S., J. Rushby, and N. Shankar, PVS: A Prototype Verification System, In Deepak Kapur, Editor, *11th International Conference on Automated Deduction, (CADE)*, pg. 748–752, Saratoga, NY, June 1992, Vol. 607 of Lecture Notes in Artificial Intelligence, Springer–Verlag.

[4] Srivas, M. and S. Miller, Formal Verification of the AAMP5: A Case Study in the Verification of a Commercial Microprocessor, to appear in *Applications of Formal Methods*, Michael G. Hinchey and Jonathan P. Bowen, Editors, Prentice–Hall International Series in Computer Science.

[5] Srivas, M. and S. Miller, *Formal Verification of an Avionics Microprocessor,* to be submitted as a NASA Contractor Report.