An Investigation into Proof Automation for the SPARK Approach to High Integrity Ada

Andrew Ireland Bill J. Ellis Julian Richardson

Department of Computing & Electrical Engineering
Heriot-Watt University
Edinburgh, Scotland
E-mail: a.ireland@hw.ac.uk

Position Statement

We are currently investigating[1] the application of proof planning to the SPARK[2] approach to developing high integrity Ada. The SPARK approach advocates *correctness by construction* – where the development of code and verification proofs go hand-in-hand. Proof planning involves the use of high-level patterns of reasoning in constraining the automatic search for verification proofs.

Our investigation began in September 2001. An evaluation of the potential use of existing proof plans within this new application is currently under-way. This evaluation will also inform our development of new proof plans. In addition, we are currently building a first prototype of NuSPADE, an experimental proof planning system. NuSPADE will extend the SPADE Proof Checker[3], an interactive theorem proving environment designed to support the proof of verification conditions arising from software written in SPARK. This extension will build upon earlier work implemented within the Clam proof planning system. We believe that NuSPADE will significantly increase the level of proof automation that is currently supported by the SPADE Proof Checker.

[1]The research outlined here is funded under the EPSRC Critical Systems Programme – EPSRC grant GR/R24081.

[2]Praxis Critical Systems Ltd – `http://www.praxis-cs.co.uk`

[3]The SPADE Proof Checker is part of the SPARK Examiner tool-set and is a product of Praxis Critical Systems Ltd.