


AdaCore alTran 
PRAXIS

———— PARTNERSHIP ————

SPARK Pro 9 and Beyond

An Update from SPARK Team

Rod Chapman

Agenda

- Praxis/AdaCore partnership news
- SPARK Pro Release 9
- Other on-going activities of interest

Praxis/AdaCore partnership news



- Reminder: We have completely transformed SPARK into the “FLOSS” business model.
 - Very permissive licence for you.
 - No restriction/locking/counting of licences or “seats” – we just trust you.
 - Aligns our focus on innovation and support.
 - Remember “free” means “free speech” not “free beer” in this context.

Praxis/AdaCore partnership news

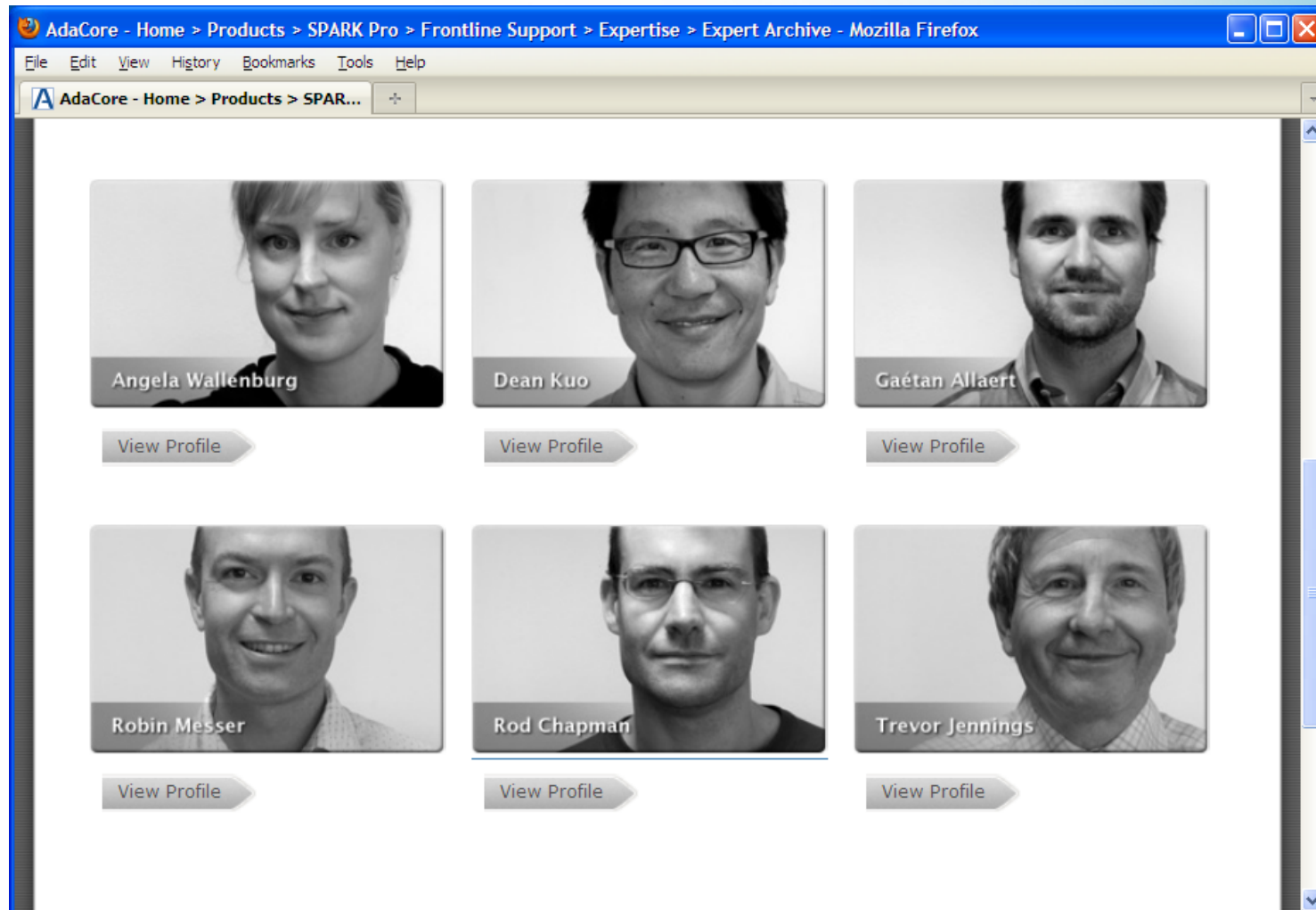


- In short: it's working.
- We have made a major leap in capability in marketing, sales, support etc.
 - Tokeneer FLOSS release made a big impact
 - Tokeneer Tutorial on web
 - Webinars
- New customers since SPARK Pro launch: CESG, Thales Underwater, plus 2 major new ones in security.
- Some really interesting new customers in the pipeline.

Praxis/AdaCore partnership news



- The team is growing, and stable...



SPARK Pro Release 9

- SPARK Pro 9 shipped on 24th March. Here are some of the major new features:
- SPARK2005 – new language switch and SPARK2005 profile.
 - Most of Ada2005 is still out-of-scope for SPARK, but a few interesting and useful things:
 - ‘Mod and ‘Machine_Rounding attributes
 - “overriding” and “not overriding” static semantics
 - New reserved words
 - Official standardization of Ravenscar tasking profile, so RavenSPARK is supported in both SPARK95 and SPARK2005 modes.

SPARK Pro Release 9

- “SLI” file generation – like the compiler’s “ALI” file, but contains cross-reference info for SPARK contracts.
 - Enables navigation inside GPS and GNATBench.
- VC Generator: Function “return” contract is now substituted into the caller’s VC hypotheses.
- Casing checks: Examiner can now check for consistency of identifier casing inside contracts – complements GNAT’s style checks.

SPARK Pro Release 9

- New tool for finding dead paths and dead code
 - Checks VCs for dead paths by finding contradictions in path-traversal conditions.
 - A dead path is not always a bug, but usually suspicious...
 - One bug in Tokeneer would have been prevented if we'd had this at the time...
- POGS Tool
 - New output format, hopefully both easier to read and easier to search automatically. Reports both proof and dead-path status for each VC.
 - GPS plug-in recognizes status of each VC and offers navigation to the appropriate file(s).

SPARK Pro Release 9

- New Examiner switch
 - -policy=[security | safety]
- Allows package-level own variables to have an “Integrity” property – a Natural number.
 - “security” mode implements simple policy – i.e. Secret input may not affect Unclassified output.
 - “safety” mode reverses the relationship – “Not Critical” input may not affect “Critical” output.
- Most important catch: *constants* are not modelled in the IFA engine.

SPARK Pro Release 9

- Simplifier
 - Yet more tactics improvements, particularly for record types and quantified predicates that arise from array types.
- Documentation
 - New “Proof Manual” merges all proof related stuff into one manual.
 - New “Global Index” (one page) in PDF and HTML with links to all the other docs.
 - All available from the GPS help menu too...

SPARK Pro Release 9

- New Course: “Introduction to the Proof Checker”
 - 1 day, usually following the Advanced SPARK Program Design & Verification course.
 - Full set of courses running in September 2010 in Bath, or on demand at customer site,

SPARK Pro Release 9

- New One-Day Course: “Refresh your SPARK!”
 - Learnt SPARK years ago? Forgotten it?
 - You last used the Examiner on VAX/VMS?
 - Never tried to use the VC Generator?
 - Then this course is for you...

Other on-going activities

- Partnerships with other tools/companies.
 - MATLAB/Simulink – Open-Source “GeneAuto” project building a code-generator.
 - Esterel SCADE. European Space Agency “Full MDE” project funding the development of a new SPARK code-generator for SCADE, in collaboration with EADS Astrium Space and Praxis.

Other on-going activities

- Partnerships with universities
 - Edinburgh Uni – Theorem proving research.
 - York – Tokeneer re-engineering and model-checking.
 - Oxford and Aston Unis – decision procedures for floating-point arithmetic.
 - KSU – value-dependent flow analysis, refactoring, Eclipse integration.
 - Virginia – Specification refinement and proof.
 - Bath – Counter-Example Finding using answer-set-programming. We are seeking funding to support this work in late 2010.

Other on-going activities

- Hi-Lite Project
 - Three-year French-funded research partnership with AdaCore, EADS Astrium, and others.
 - Aims to lower the hurdle for formal methods and static verification.
 - Main effort from SPARK Team: language expansion (generics, discriminated types etc.), standard container library, link to new theorem proving tools.

Other on-going activities

- High Assurance Software Symposium and SPARK User Group 2010
 - October 13th, Bath, UK
 - This year: both a “management” and a “technical” track.
 - Invited speakers from industry, academia, and government.
 - Invitations are going out now to our supported customers, tool partners, GAP members, regulators, and distinguished guests.

Altran Praxis Limited

20 Manvers Street

Bath BA1 1PX

United Kingdom

Telephone: +44 (0) 1225 466991

Facsimile: +44 (0) 1225 469006

Website: www.altran-praxis.com

Email: rod.chapman@altran-praxis.com

Email: andrew.proctor@altran-praxis.com