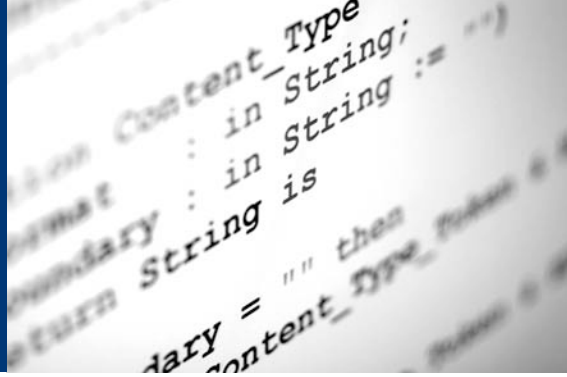
GNAT Pro insider

an AdaCore Publication
Fall 2008
www.adacore.com



newsflash

Ada Expert Stephen Baird on Board

Stephen Baird, an internationally recognized expert on Ada, has joined the GNAT Pro development team in the US. Previously with Rational and IBM, Mr. Baird has more than 25 years of experience on Ada compiler implementation technology, and he is an active member of the ISO working group that maintains the Ada language standard.

Public Courses at Paris Office

As part of its full complement of professional services, AdaCore will be offering public courses on Ada and the GNAT Pro toolset at its Paris headquarters starting in 2009. Similar to the training conducted at its New York office, all courses will combine lectures and hands-on workshops using the latest versions of the GNAT Pro tools. For a schedule and detailed course descriptions, please visit **www. adacore.com/home/gnatpro/professional_services/training** or contact **info@adacore.com**.

contents

NSA-Sponsored Tokeneer Software Available

The complete implementation of the high-security Tokeneer ID Station, developed in SPARK Ada by Praxis High-Integrity Systems using the GNAT technology, is available on the AdaCore website.

The release contains the entire set of project artifacts including requirements, specifications, source code, documentation, formal demonstrations of correctness, and tests. Software simulators for Tokeneer's peripheral devices are provided, and the system can be built and run on Windows platforms using any current version of GNAT.

Tokeneer is an unclassified experimental biometrics-based system for controlling physical access to a secure enclave. Under a contract from the National Security Agency (NSA) in the US, Praxis engineered one of the components—the Tokeneer ID Station (TIS)—using their Correctness by Construction methodology.

> **"We were able to implement the system in a cost effective and timely manner, and, most importantly, achieve demonstrably high reliability."**

The TIS software, approximately 10,000 lines of code, was completed by a team of 3 people part time over 9 months, and has had zero defects reported by the NSA since delivery. It was designed to comply with the TIS Kernel Protection Profile, which specifies Evaluation Assurance Level (EAL) 5 from the Common Criteria.

The public release is licensed by a Technology Transfer Agreement granted by the NSA, and the software has been submitted to the repository of the "Grand Challenge" in Dependable System Evolution.

"A commonly held view is that high-security software—at EAL 5 and higher—is intrinsically expensive and difficult to develop," said Rod Chapman, leader of the SPARK team at Praxis. "Our experience on the Tokeneer project indicates otherwise. By adhering to some sound engineering principles, and by using appropriate programming languages and tools, we were able to implement the system in a cost effective and timely manner, and, most importantly, achieve demonstrably high reliability. We are pleased that the project artifacts are now available on the AdaCore website, where they can serve as a working example to software and security practitioners and researchers."

The Tokeneer project artifacts are available at **www.adacore.com/tokeneer**.

For more information on Tokeneer, please see **www.praxis-his.com/pdfs/issse2006tokeneer.pdf**.

Project Coverage Launch Initiates Open AdaCore Series

The AdaCore Paris office hosted a kickoff meeting for Project Coverage on September 16. This research effort, funded by the French public authorities, will develop a Free Software coverage analysis toolset together with artifacts that can be reused in safety-critical systems undergoing DO-178B certification. The launch was attended by sponsors, project partners, researchers, and the press. It marked the first in a new series of planned events at the Paris office—the Open AdaCore Series—that will include a seminar in March 2009 featuring Jim Sutton, author of *Lean Software Strategies.* If you are interested in attending this seminar, or in learning about other Open AdaCore Series events, please contact **events@adacore.com**.

< new platforms >

Three new products have broadened GNAT Pro's support for the embedded system and real-time marketplace:

GNAT Pro for AVR

Expanding into the realm of commercial 8-bit processors, the GNAT Pro development environment is available for Atmel's AVR single-chip microcontroller. The compiler, hosted on Windows platforms, supports the ZFP (Zero Footprint) run-time profile for Ada and generates efficient, compact code that meets the constraints of small-footprint embedded applications.

GNAT Pro for ELinOS

GNAT Pro for SYSGO's x86 ELinOS Industrial Grade Embedded Linux environment is available on host platforms running GNU Linux. This product is aimed at Ada developers who are building large-scale Ada applications for Embedded Linux. The support for the Xenomai technology helps achieve hard real-time behavior in user-space applications together with seamless access to Linux services.

GNAT Pro for RTX

GNAT Pro is available for Ardence's RTX (Real-Time Extension for Windows), providing predictable, hard real-time performance for Windows programs without requiring source code changes. The product supports several development strategies:

- Using Windows plus RTX as a testing and development platform to verify an application's real-time properties before migrating to another real-time target;
- Using RTX to execute real-time applications in kernel mode, without passing through Windows for services such as device memory accesses.

< in the pipeline >

GNAT Pro 6.2

The next major release of the GNAT Pro toolset will be available on most platforms during Q1 2009 and will include the following enhancements:

Technology updates

- Compiler back end based on gcc 4.3
- Debugger engine based on gdb 6.8
- Improved support for safety-critical applications
  - Traceability to source code
  - Coverage analysis

Over 130 new features, including:

- Ability to associate pre- and post-conditions with subprograms
- Ability to selectively enable or disable groups of assertions
- Additional rules in gnatcheck, for coding standard verification
- More efficient implementation of stack checks, overflow checks, and validity checks
- Additional attributes and pragmas to ease generic programming
- Communication-related improvements
  - More efficient string streaming
  - Better support for serial communication and socket handling
- Additional compilation warnings on suspected errors
  - Missing overriding indicators
  - Assumption that string lower bound is 1

GPS 4.3

The next release of the GNAT Programming Studio IDE, scheduled for Q4 2008, will implement many new features, including:

Easy configurability for two toolchains

- Using a recent GNAT toolchain for purposes such as source navigation, coding standard enforcement, metrics computation
- Using an earlier (baselined) compiler for code generation

Enhanced support for gcov (code coverage tool), gnatcheck (coding standard checker) and compiler switches

A redesigned and fully customizable builder module

Improved documentation generation

- Ability to handle predefined tags, including comments, examples, and screenshots
- Ability to implement user-defined tags through python hooks

Support for VxWorks SMP

GNAT Pro 6.2 will support development of applications for Wind River Systems' VxWorks 6.6 SMP (symmetric multiprocessing) for multi-processor and multi-core processor hardware. Both kernel applications and real-time processes will be supported. Processor affinity will be controllable using the standard Ada task attributes package.

< academia corner >

Spotlighting a GAP Member
Mälardalen University (Västerås, Sweden)

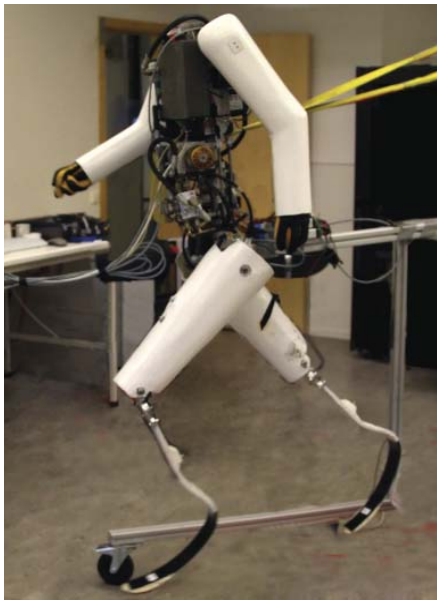
Run, Dasher, Run!
Swedish Students Implement Racing Robot in Ada

Under the direction of Professor Lars Asplund, graduate students at Mälardalen University are designing, building and programming the Dasher robot in a project that is pushing the limits of robotics technology. The software is being developed with AdaCore's GNAT toolset, furnished to the university under the GNAT Academic Program (GAP), on Wind River Systems' VxWorks real-time operating system.

The Dasher project's goal is to develop a humanoid (two-legged) robot that can run 100 meters in 9.5 seconds, which would break the human record. Among the many challenges are how to model the physics of sprinting, and how to manage the tradeoff between speed and stability so that the robot does not topple over or move into the lanes of other runners. Since safety is an important factor for robotics, Ada was selected as the implementation language, with concurrency usage adhering to the Ravenscar tasking profile. The project has adopted the Uppaal tool environment for modeling, validating and verifying the robotics software's real-time properties.

"We are very pleased with the progress on Dasher," said Professor Asplund. "Thanks to both the Ada language and the GNAT environment, the students have been highly productive and have learned a great deal about robotics, team software projects, and safety-critical system development. That was our goal, and we plan to continue with Ada and the GNAT tools on future projects."

For more information on Dasher, please see **www.dasher.se**.



Dasher photo: Lars Asplund

Interview with Ed Falis Senior Technical Staff, AdaCore US

Tell us about your background and how you came to be involved with Ada and AdaCore. What is your current role?

I was a graduate student at Stanford in the early 1980s. This was an exciting period for the computing industry, as the PC era was just beginning, and "the times, they were a-changin'" in the software arena also. Research advances from the 1970s—features for data abstraction, "programming in the large," concurrency—were showing up in new languages, with Ada in particular generating a lot of "buzz." I was studying program verification and formal methods, and my professor asked me to investigate efficient techniques for implementing Ada tasking. This was an enjoyable challenge, and after finishing my graduate work I joined Alsys in 1983. I started out designing and implementing Ada run-time libraries but later became a "jack of all trades," including engineering, management, sales, marketing and training.

Wearing my various hats I got to know the Ada vendor community well, and AdaCore impressed me with its people, business model, and long-term commitment to Ada. I joined the company in early 2000, and my role here is a bit diverse. On the engineering side I work on the GNAT Pro run-time libraries for Wind River Systems' VxWorks target platforms. I also designed and implemented the AUnit framework for automating Ada unit testing. On the other hand I also help with product planning and more generally handle a variety of issues where technology and business overlap.

You work from one of AdaCore's satellite locations but you need to coordinate with team members from the company's main offices and from other sites. How is that managed?

AdaCore has strict and well-defined processes for quality assurance, version control, and configuration management to make sure that a geographically distributed team can share development responsibilities on the same project. This was a case of necessity spawning invention, since from its outset the technical team has been spread across multiple locations. The details have evolved over time—for example we now have a web-based interface—but basically it's a matter of sound engineering practice assisted and enforced by automated tools. If I modify a component of the GNAT compilation system, my attempted check-in will trigger a regression suite run, and unless the run succeeds my check-in will fail. This is an example of an Extreme Programming "best practice" (constant integration) taken to the extreme—except that we were doing it before Extreme Programming hit the scene. We have major yearly releases of GNAT Pro and its add-on tools on dozens of platforms, and this sort of schedule would be impossible if we didn't have a well-specified and rigidly-enforced discipline for software development.

You've implemented Ada run-time libraries that need to meet stringent safety standards (DO-178B, Level A). What are some of the issues here?

In general, due to process costs associated with safety certification, restricted Ada profiles are defined. This results in a simpler, fully deterministic run-time library, which is less expensive to certify. However, there is a tradeoff in defining such a profile. On the one hand, customers often want to meet the needs of new systems by reusing large collections of existing code. On the other hand, more complex constructs in that code may be more expensive (or even impossible) to certify. So the challenge is to define a profile that maximizes the reusability of existing code resources while keeping certification costs manageable. Of course, the Ada run-time library itself also has to meet the certification requirements, and so it goes through the same kinds of rigorous checking and analysis as application code.

Any hobbies or outside interests that you'd like to share?

I just started playing saxophone again for the first time in almost 40 years. The dogs hate it; fortunately my wife is more forgiving.

Reminder: Ada Internship Program

The Ada Internship Program is a convenient GNAT Tracker-based resource for GNAT Pro customers and GAP members. Through this program customers can find students who are seeking Ada-related internship positions. Analogously, students at GAP member universities and students visiting **libre.adacore.com** can learn about organizations who are seeking interns for Ada projects. Companies like Eurocontrol in Belgium are taking advantage of this program, giving students the opportunity to contribute to state-of-the-art Ada development efforts. To find out more, go to **www.adacore.com/home/academia/intern**.

Webinar Schedule

On November 25 the GNAT Pro InSight Webinar series will continue with a presentation on the new features in the GPS 4.3 release. This webinar will include a tool demonstration and a question-and-answer session with AdaCore's GPS experts. To sign up for this event, please visit **www.adacore.com/home/gnatpro/webinars**.

Ed Falis photo: Gary Matoso

Traceability Analysis Expands Safety-Critical Ada

Helps Reduce Certification Costs

AdaCore has developed certification materials that can be used to help demonstrate compliance with safety-critical standards such as DO-178B, in particular to show the correctness of object code sequences generated from (but not directly traceable to) Ada source code constructs. These traceability analysis artifacts are customizable based on such factors as target platform, coding standards, and compiler options, and they allow broader use of Ada features than has historically been found in safety-critical systems.

Certifying safety-critical software under DO-178B requires, among other things, demonstrating that the requirements-based tests fully exercise the code structure. When this analysis is performed on the source code at the highest level of criticality (Level A), the developer must understand and analyze the correspondence between the source program and the object code. If any object code is not directly traceable to source code, then additional verification effort is required to establish the correctness of the generated object code.

One approach is to adopt a constrained programming style, avoiding language constructs that do not map directly to object code, for example features that generate implicit loops or conditionals. However, the resulting subset may be uncomfortably restrictive, and the directness of the mapping is target dependent. Furthermore, the concept of a "direct" mapping is somewhat subjective.

A more flexible alternative is to identify a useful set of source constructs and the generated "untraceable" object code, and then to verify the correctness of the object code through the following steps:

- Specifying the requirements describing the intended behavior of the generated code,
- Defining the test cases and procedures to verify the compliance against the requirements,
- Executing the tests and collecting the test results and coverage information, and
- Verifying the test results and assessing object code coverage.

This is the approach that AdaCore has taken. It fully complies with DO-178B, allows a less restrictive coding style, and helps reduce the certification effort by providing an analysis that would otherwise need to be performed by the customer. To learn more, please contact **info@adacore.com**.

newsflash

GNATbench 2.2 for Eclipse

With the release of GNATbench 2.2, AdaCore is synchronizing its GNATbench release cycle with that of Eclipse itself. In addition to supporting the latest versions of Eclipse and the C/C++ Development Toolkit (CDT), GNATbench 2.2 includes a new project explorer view that simplifies resource and project management.

Conferences / Events ■ September 2008 – April 2009

SAFECOMP 2008
22–25 September / Newcastle, UK

AdaCore is the main industrial sponsor of this event. Robert Dewar, AdaCore CEO and President, is presenting a talk at the Safety and Security workshop on 25 September.
www.safecomp2008.org/index.html

MODELS 2008
29 September / Toulouse, France

Matteo Bordin from AdaCore is presenting a paper on model-based development of embedded systems.
www.artist-embedded.org/artist/ACES-MB-08.html

SCADE User Group Conference
9 October / Toulouse, France

AdaCore is an invited partner and exhibitor at this event.
estereltechnologies.com/news-events/events/2008/sugc-2008

IET International Conference on System Safety 2008
20–22 October / NEC, Birmingham, UK

AdaCore is a major sponsor of this event.
conferences.theiet.org/safety/

ESC Boston 2008
27–30 October / Boston MA, US

AdaCore is exhibiting at this conference.
www.embedded.com/esc/boston/

SIGAda 2008
27–30 October / Portland OR, US

Ben Brosgol from AdaCore is delivering a tutorial and a keynote address, and AdaCore is a platinum level sponsor of this conference.
www.sigada.org/conf/sigada2008

Eclipse Summit 2008
19–20 November / Ludwigsburg, Germany

AdaCore is a sponsor of this event.
www.eclipsecon.org/summiteurope2008/

Avionics 2009
11–12 March / Amsterdam, Holland

AdaCore is a sponsor of this event.
www.avionics-event.com

ESC Silicon Valley 2009
29 March–3 April / San Jose CA, US

AdaCore is exhibiting at this event.
www.cmp-egevents.com/web/esv/home

SSTC 2009
20–23 April / Salt Lake City UT, US

AdaCore is exhibiting at this conference.
www.sstc-online.org/

The GNAT Pro insider is published twice a year simultaneously in New York and Paris by AdaCore

104 Fifth Avenue, 15th floor
New York, NY 10011-6901, USA
tel +1 212 620 7300
fax +1 212 807 0162

46 rue d'Amsterdam
75009 Paris, France
tel +33 1 49 70 67 16
fax +33 1 49 70 05 52

info@adacore.com
www.adacore.com

AdaCore
The GNAT Pro Company