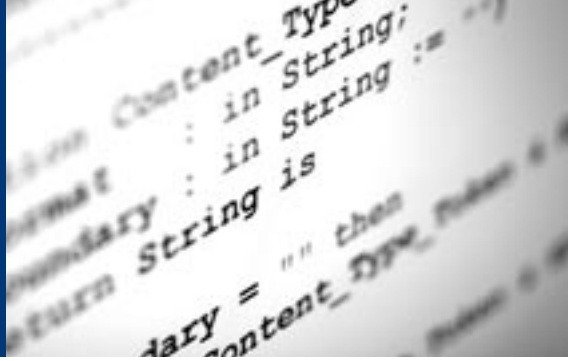
GNAT Pro insider

an AdaCore Publication
Autumn 2010
www.adacore.com



newsflash

New SPARK course

Altran Praxis and AdaCore have introduced a SPARK refresher course for engineers. The course first reviews SPARK basics — the language subset, Examiner usage, information-flow analysis, and diagnosing and correcting common design errors. It then goes on to cover more recent developments including the various language profiles (SPARK95, SPARK2005, and RavenSPARK), the INFORMED design style for SPARK, the basic use of the proof tools to establish the absence of runtime errors, and the impact of SPARK on other areas of the software process, such as reviewing and testing. For more information on this course and others, please visit **www.adacore.com/home/products/sparkpro/professional_services/training/**.

SPARK Implementation of Skein Algorithm

Altran Praxis and AdaCore have released a new reference implementation of the Skein algorithm, written and verified using the latest version of the SPARK language and toolset. Skein, a cryptographic hash function, is an entrant in the National Institute of Standards and Technology (NIST) hash function competition to design what will become the new Secure Hash Algorithm (SHA-3) standard. Such hash functions are used to compute short "digests" of long messages and are one of the key building blocks of digital communication and cryptographic systems. Altran Praxis and AdaCore are distributing the SPARKSkein reference implementation under an open source license; it is available through the Skein website **www.skein-hash.info/**.

contents

GPS 5.0 Now Available

Major New Release of GNAT Programming Studio IDE

The latest version of the GPS graphical Integrated Development Environment offers numerous enhancements in a wide range of areas. Key improvements or new features have been implemented in GPS's multi-language support, source editing, tool support/integration, documentation generation, and ease of use.

GPS's multi-language support, incorporating an upgraded technology that has been under development for the past several years, will be of particular benefit in writing applications that use C or C++ along with Ada. Enhancements include more accurate and complete source navigation based on a new cross reference engine, better outlining and indentation, and navigation through #include directives.

GPS 5.0 makes source editing easier through features such as additional syntax highlighting, annotations on the side of editing windows (for compilation messages and search results), automatic compilation, error highlighting, improved code completion, and better automated code fixes.

GPS 5.0 offers integration with GNATstack and improved support for CodePeer. GNATstack, a static analysis tool that determines a program's maximum stack requirements, is included with the GNAT Pro High-Integrity Edition and is also available as a GNAT Pro add-on. CodePeer, a static analysis tool that automates code review and validation, is available as a standalone tool.

Documentation generation enhancements include detecting entity names in comments and producing links to their definitions, and handling lists and intentional line returns in structured comments.

Easier usage is evident in improvements such as simple target toolchain selection, faster processing for large projects, better handling of the desktop via perspectives, and the ability to quickly create projects from existing templates.

GPS is written in Ada using the GtkAda toolkit. Its source-code navigation and analysis tools can generate useful information such as call graphs, source dependencies, project organization, and complexity metrics. GPS also supports configuration management through an interface to third-party Version Control Systems, and it is available on a variety of platforms. GPS is highly extensible; a simple scripting approach enables additional tool integration. It is also customizable, allowing programmers to specialize various aspects of the program's appearance in the editor for a user-specified look and feel.

GPS 5.0 is available as part of the GNAT Pro Ada Development Environment as well as the SPARK Pro and CodePeer Pro toolsets, and customers can download it via the GNAT Tracker tool. Please contact AdaCore (**info@adacore.com**) for information on pricing or supported configurations.

GNAT Pro High-Integrity Edition for DO-178B: Partitioning for Safety on VxWorks 653

The GNAT Pro High-Integrity Edition for DO-178B is available for Wind River's VxWorks 653, a Real-Time Operating System that complies with the time- and space-partitioned ARINC 653 architecture and thus allows applications at different safety levels to run without interference on the same processor. GNAT Pro High-Integrity Edition for DO-178B provides several run-time libraries, at different degrees of generality, to meet the variety of safety certification requirements that might be imposed by different applications running on this platform.

For the highest level (DO-178B, Level A) the GNAT Pro "Zero Footprint" (ZFP) library is appropriate since it is the simplest; it corresponds to sequential Ada without features such as exceptions and dynamic storage management. For additional generality the product supplies a richer run-time library, also certifiable to DO-178B Level A, integrated with and interfacing to ARINC-653 facilities such as multi-threading and intra- or inter-partition communication. With this library, a programmer may use either a small deterministic Ada tasking model (Ravenscar) or ARINC-653 processes. Certification material for this library, and for ZFP, is available. For maximum generality, a full Ada run-time library is provided, which is appropriate for components that do not have significant safety certification requirements.

For further information about this or related products (such as the GNAT Pro High-Integrity Edition for DO-178B on the Wind River VxWorks Cert platform), please visit **www.adacore.com/home/products/gnatpro/development_solutions/safety-critical/do-178b/**.

< current releases >

SPARK Pro 9.1

The latest release of SPARK Pro includes the following features:

- **Enhancements for GPS and GNATbench** A specialized auto-fix for an unexpected or misplaced '~' or '%' character in SPARK annotations is offered, to either remove the character or replace it correctly. In addition, there is better highlighting of SPARK keywords in SPARK annotations.
- **Full range array subtypes** Full-range array subtypes may be used in all contexts. This provides a convenient way to rename an array type locally, and may also be of use for tools that automatically generate code from languages (such as Lustre) that employ structural type equivalence.
- **Relaxation of aliasing rules for record fields** Non-overlapping record fields may be used as different actual parameters to a procedure where the corresponding formal parameters are exported.
- **Specifying Verification Condition generation on a per-file basis in metafiles** Verification Conditions may be specified on a file-by-file basis using metafiles. Any file followed by -vcg in a metafile will have VCs generated.
- **SPARK library packages** SPARK versions of the Ada library packages Ada.Strings and Ada.Text_IO are available.
- **SPARKBridge technology preview** SPARKBridge, a ViCToR-based technology bridge between the SPARK tools and Satisfiable Modulo Theories (SMT) solvers such as Alt-Ergo, provides access to additional provers for automatically discharging Verification Conditions. A preview will be available as part of the SPARK Pro 9.1 release, and support for the technology will be included in future releases of the Black Belt edition.

< academia corner >

Spotlighting a GAP Member
Telecom ParisTech (France)

The Telecom Robotics club at the French engineering college Telecom ParisTech is using Ada and the GNAT technology for its projects.

Telecom Robotics' mission is to provide a robotics-focused forum where students can learn, share knowledge, and innovate. To help realize this goal, the group competes in European Robotics Cup contests where they explore all aspects of the subject: mechanics, electronics (embedded electronics, microprocessors, FPGAs), computer science (programming, image processing) and project management. In 2010, Telecom Robotics finished in the top ten (out of 150 competitors) and came in 3rd place in the Czech cup.

Ada was selected as the language for programming the robot. As explained by Samuel Mokrani, this year's president of the Telecom Robotics club: "We chose Ada because of its reliability, safety, and efficiency, and because the various checks enforced by the compiler make it easier to maintain code as the system evolves or requirements change. And thanks to AdaCore's GNAT Academic Program, universities have a top-quality Ada development environment, including support, at no cost." The issues that the team encountered during the European Robotics Cup contests were mechanical and not software related; the embedded Ada code was completely reliable.

> "We chose Ada because of its reliability, safety, and efficiency."

The target configuration is an SH4 processor running GNU Linux. The software for this year's robot processed sensor data to locate its opponents, used camera data to detect items on the table, and adapted its strategy accordingly. The image and data analysis, traction control, and artificial intelligence represent over 15,000 lines of Ada code.

In light of their successful experience on this project, Telecom Robotics is continuing with Ada and GNAT for future efforts, including a robot based on LEGO Mindstorms.

< in the pipeline >

GNAT Pro 6.4

The next major release of the GNAT Pro development environment will offer a wide variety of enhancements, many based on customer comments and requests. The new features fall into several areas:

- Ada 2012 preview, including most of the currently finalized Ada Issues (AIs) and in particular conditional/case/parameterized/quantified expressions, aspect specifications (including pre/postconditions and type invariants), subtype predicates, and improved support for multiprocessors
- Improved code generator based on GCC 4.5
- New switch (-fdump-xref) to generate cross reference information for C and C++
- More detailed exception messages (-gnateE switch)
- New gnatcheck rules
- New warnings
- Better debugger performance
- More flexible and more efficient project manager in gnatmake/gprbuild
- More aggregates recognized as static
- Support for GNATbench 2.5, which will work with a new version of Eclipse

GNAT Pro 6.4.1 will be available on most platforms during Q1 2011.

CodePeer 2.0

A major new release of the CodePeer source code analyzer / reviewer for Ada will include the following features:

- Support for access-to-subprogram types
- Much more efficient SCIL generation, with faster processing and simpler (and fewer) SCIL files. In addition, CodePeer will require fewer partitions by default to perform an analysis.
- Support for parallel SCIL generation. Users can now take advantage of the gnatmake -jxx switch to generate SCIL files in parallel on multiple cpus/cores.
- New warning, "useless self assignment", when an assignment does not modify the destination variable.
- Fewer "false positives" (false alarms)
- Improved integration with the GPS IDE.

CodePeer 2.0 will be available during Q1 2011.

GNATemulator

GNATemulator, a new tool based on QEMU, offers an efficient and flexible emulator solution for Ada, C and C++ applications. It allows developers to compile code directly for their target architecture and run it on their host platform, through a technology that translates from the target object code to native instructions on the host. This approach avoids the inconvenience of managing an actual board, while offering an efficient testing environment compatible with the final hardware. GNATemulator runs on Windows and Linux host environments, and it supports target architectures including PowerPC and LEON. The tool can be used either in bareboard mode or with an operating system such as VxWorks 653 for the target. GNATemulator will be available during Q1 2011.

GNATcoverage

The GNATcoverage tool, known earlier as XCov, performs coverage analysis on both object code (including branch coverage) and source code (including decision coverage and MC/DC). It does not require instrumentation of the executable code. Instead, the tests can be run either on GNATemulator, which is instrumented for collecting coverage data, or directly on a board with a suitable debugger interface. The tool has full DO-178B qualification material and is being used for avionics systems with Level A certification requirememts. Supported processors include the PowerPC and LEON. A new version of GNATcoverage will be available during Q1 2011.

Interview with Steve Baird
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've been involved with the implementation and design of Ada since the language's origins in the early 1980s, when I joined Rational. For my first job there I helped design the instruction set and wrote microcode for Rational's proprietary Ada-specific hardware. After that I pretty much became a "compiler guy" and was one of the principal engineers working on the Ada compilers for Rational Apex. On the language standardization side, I've been a member of the ARG (the ISO/IEC JTC1/SC22/WG9 Ada Rapporteur Group) since 2002, participating in language maintenance work and the development of new revisions of the language (Ada 2005, Ada 2012).

In 2008 I left Rational (actually part of IBM at that point) and joined AdaCore. My primary focus here has been on CodePeer, integrating that tool with the GNAT front end. I have also continued my work with the ARG and am getting immersed in the SPARK language and technology. In keeping with AdaCore's "frontline support" approach, I have enjoyed a good amount of direct contact with customers. Because of my background, I can help users who are interested in porting their applications to GNAT Pro.

Ada is continuing to evolve, as evidenced by the upcoming Ada 2012 enhancements. What are your favorite new language features and why?

This may put me out of the mainstream, but I'm going to pass over what might seem the obvious feature — subprogram pre- and postconditions — and choose membership predicates for subtypes. Although details of this proposal are still being ironed out, it essentially allows the programmer to specify a boolean condition for objects of a given subtype — for example membership in a given set of values — and thus generalizes Ada's existing mechanism for specifying contiguous ranges of scalar values. One of Ada's fundamental advantages over other languages is how it allows programmers to express their intentions via explicit syntax, and subtype predicates are an important step forward in this area.

I'm also looking forward to many of Ada 2012's "creature comfort" changes. Although features like conditional and case expressions, iteration over containers, and quantified expressions don't let you do anything that wasn't already expressible, the new syntax makes them much more convenient to use. Case expressions in particular will help make code more maintainable when an enumeration type is changed, while at the same time revealing the programmer's intent more concisely and more understandably. It's always good when a language feature makes programs both easier to write and easier to read.

As one of the engineers working on CodePeer, you have an "insider's" perspective on this tool. What do you find to be its most useful features?

Although the idea behind detecting run-time errors (and more generally, deriving program properties) at compile time is not new, CodePeer's great strength is that it does such a good job of it. What's most useful is obviously a subjective judgment, but I'll single out the tool's ability to synthesize subprogram pre- and postconditions, to perform partial analysis on incomplete programs, and to generate incremental reports relative to an established baseline. And although the advantages of an automated tool over manual code review seem obvious, they are still very real. CodePeer is just as effective on, say, the 173rd version of the program as it was on the first, whereas a human reviewer could easily miss something after so many iterations over code that might have changed only slightly at each step.

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

I like to take my dog Trumbull, a Poodle-mix, to a nearby park where he can run around off-leash with his canine friends. The shelter where we found him had named him Prince, so you could say that he is the dog "formerly known as Prince".

Webinar Schedule

The GNAT Pro InSight series continues this Autumn with two webinars, featuring the newly released GPS 5.0 and SPARK Pro 9.1. The webinars, presented by the tools' developers, discuss and demonstrate the new features of these major releases and include a question and answer session. The SPARK 9.1 webinar will be held on Tuesday, December 7, and the GPS 5.0 webinar will be held on December 14.

AdaCore and Wind River are delivering a joint Open Systems E-Cast webinar on Tuesday, January 18, 2011, on the topic *Developing Security-Critical Applications for Multi-level Secure (MLS) Platforms*. Among other topics the webinar will summarize Wind River's VxWorks MILS architecture and present a case study in which the SPARK language was used on the VxWorks MILS separation kernel to meet high-assurance requirements.

For more information about both webinars, or to register, please visit **www.adacore.com/home/products/gnatpro/webinars/**.

Steve Baird photo by Gary Matoso

Multi-language Solutions Available

Wide range of tools and support for customers using Ada with other languages

AdaCore has enhanced its product line with comprehensive solutions for Ada projects that are using multiple programming languages. At the heart of the technology is a flexible and general-purpose tool, the GNAT Project Builder, that comes with GNAT Pro and allows users to specify options for multi-language builds. A variety of products then address the use of specific languages:

- **GNAT Pro C and GNAT Pro C++ supply the needed compilation tools plus support to assist C and C++ development. The --fdump-ada-spec switches for these products are especially useful, providing an automated binding generator from C or C++ to Ada.**
- **The GNAT Ada-Java Interfacing Suite allows communication between Java and natively compiled Ada, and GNAT Pro for the JVM compiles Ada into bytecodes. Please visit www.adacore.com/home/products/gnatpro/multi-language/ada-java/ for links to tutorials and examples.**
- **GNAT Pro for .NET allows smooth interfacing, through managed code, between Ada and C# or other languages that compile to Common Language Runtime assemblies. The product includes the cil2ada binding generator, which produces Ada package specifications from .NET assemblies and thus allows access to the C# API from Ada.**
- **The GNAT Component Collection (GNATcoll), a set of packages supplied with the standard GNAT Pro subscription, supports applications that combine Ada and Python, for example to drive Ada test suites through Python scripts.**

These complement GNAT Pro's existing support for the foreign language interfacing facilities specified in the Ada standard, for example to invoke code written in C, Fortran or COBOL.

Conferences / Events ■ October 2010 – April 2011

IRILL Days 2010
October 4–5, 2010 / Paris, France
Yannick Moy is presenting "Hi-Lite: a Verification Toolkit for Unit Test and Unit Proof".
www.irill.org/events/irill-days-2010

High Assurance Software Symposium and SPARK User Group 2010
October 13, 2010 / Bath, UK
Robert Dewar is presenting "Open Source Software and Formal Methods". Videos from this event are available at
www.adacore.com/home/ada_answers/lectures/spark_2010/

Wind River - Multi-core Regional Conference
October 20, 2010 / Waltham MA, US
AdaCore is exhibiting at this event.
www.windriver.com/announces/ad-tech-forum-2010/

Fraunhofer FIRST
October 21–22, 2010 / Berlin, Germany
Yannick Moy is delivering an invited talk, "Formal Verification in Aeronautics: Current Practice and Upcoming Standard", at the workshop on C Program Quality Assurance using ACSL.
www.first.fraunhofer.de/veranstaltung/Workshop_DEVICE_SOFT

SCADE User Group
October 21–22, 2010 / Paris, France
AdaCore is exhibiting at this event.
www.esterel-technologies.com/news-events/events/2010/sugc/

ACM SIGAda 2010
October 24–28, 2010 / Fairfax VA, US
Ben Brosgol is conducting a tutorial on C#, .NET, and Ada, and Ed Schonberg is presenting a paper on Ada 2012. AdaCore is a Platinum Sponsor for this conference. The company is exhibiting and also hosting a Birds-of-a-Feather session.
www.sigada.org/conf/sigada2010/

Certification Together International Conference 2010
October 26–28, 2010 / Toulouse, France
Cyrille Comar is presenting "OOT DO-178C Supplement", and Matteo Bordin is presenting "The challenges of agile certification". Dr. Comar is also co-presenting "DO178C/ED12C OOT, A User's Perspective" with Hugues Bonnin (Capgemini) and Fred Rivard (IS2T). AdaCore is a Platinum Sponsor of this event.
www.certification-together.com/index.php?option=com_content&view=article&id=73&Itemid=80

FOSDEM 2011
February 5–6, 2011 / Brussels, Belgium
Thomas Quinot is delivering a talk on the GNAT technology and Ada.
www.fosdem.org/2011/call_for_mainspeakers_devrooms

Safety-critical Systems Symposium
February 8–10, 2011 / Southampton, UK
Robert Dewar is presenting "A Pragmatic View of Formal Methods: The Hi-Lite Project". AdaCore is a major sponsor of this event.
www.scsc.org.uk/diary.html?opt=detail&id=126

newsflash

Ravenscar for LEGO MINDSTORMS NXT
The new release of the GNAT GPL edition for the LEGO MINDSTORMS NXT offers educators and students the opportunity to experiment with real-time embedded systems development in Ada using the Ada 2005 Ravenscar profile. The release includes Ada drivers to access the NXT brick and its connected sensors and actuators. This technology is community-based: users are encouraged to contribute additional drivers, teaching material and demos. The release can be downloaded from **www.libre.adacore.com**, or through GNAT Tracker for GAP members.

GNATbench 2.4.1
The latest GNATbench release supports three new Wind River platforms — VxWorks 653 v2.3, VxWorks Cert v6.6.2, and VxWorks MILS v2.1 — as well as VxWorks 6.8 and Workbench 3.2. It uses the Wind River default "flexible" managed build type for all new projects, allowing users to specify the folders containing sources. The deprecated "standard" managed builds are still supported for existing GNATbench projects, with a project conversion wizard supplying an option to convert them to the new build type. GNATbench 2.4.1 uses GPRbuild, the AdaCore multi-language builder, when building the Ada portion of a Workbench project, and can thus also compile code written in other languages.

Ada Web Server for Wind River's VxWorks
AdaCore's Ada Web Server (AWS) is available for Wind River's VxWorks RTOS, bringing web-based connectivity and control to embedded applications. When used in conjunction with GNAT Pro, AWS enables developers to embed an Ada-based web server within any application, making it accessible through web browsers. AWS for VxWorks allows users to connect through a direct TCP/IP link to board-level applications, for system management purposes such as control, configuration, and/or maintenance. The two-way interface is both lightweight and flexible. For more information please visit
www.adacore.com/home/products/gnatpro/add-on_technologies/web_technologies/.

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