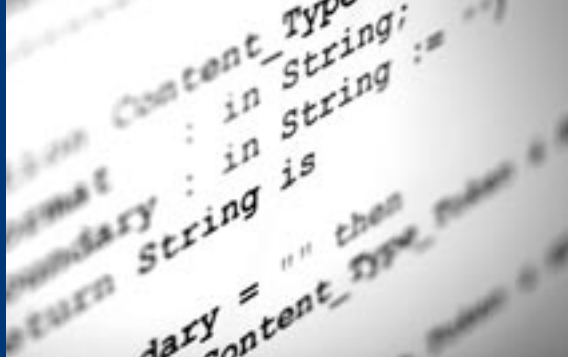
GNAT Pro insider

an AdaCore Publication
Spring 2009
www.adacore.com



newsflash

Contract Award from BAE Systems UK

BAE Systems UK has signed a corporate-wide, unlimited-usage licensing agreement with AdaCore, providing every BAE Systems developer in the UK with access to AdaCore's GNAT Pro Ada development environment. This contract potentially applies to all Ada projects at BAE Systems UK facilities. Existing projects can freely migrate to GNAT Pro, and new Ada projects can select GNAT Pro, with no additional costs to BAE Systems UK.

OPEES Project Participation

AdaCore has joined the European-funded OPEES (Open Platform for the Engineering of Embedded Systems) project. OPEES's mission is to foster innovative engineering technologies for dependable / critical software-intensive embedded systems, and to ensure that these technologies are available and viable over the long term. To achieve this goal, the OPEES partners are building an Open Source ecosystem based on relevant business models. AdaCore brings to this project its experience in developing Freely Licensed Open Source embedded systems toolsets.

contents

SPARK Pro Launched 1
Open-DO Initiative 1
Current Releases 2
In the Pipeline 2
Academia Corner: Vermont Technical College 2
Interview with Michaël Friess 3
Webinar Schedule 3
Ada Gem: Pragma No_Return 4
Conferences/Events 4

SPARK Pro Launched

SPARK Pro, an Integrated Development Environment combining AdaCore's GNAT Programming Studio with Praxis High Integrity Systems' SPARK language tools, is now available from AdaCore. Targeted especially for high-assurance applications, SPARK Pro can be used with AdaCore's GNAT Pro toolsuite to provide a complete development environment for systems that must be reliable, safe, and secure. A later release of SPARK Pro is planned to include support for AdaCore's GNATbench IDE.

Designed by Praxis, SPARK is an Ada subset extended with a contract language that allows a program's specification to be precisely expressed and verified. The SPARK tools perform static verification that combines soundness, low false-alarm rate, depth of analysis, and efficiency. The SPARK tools also generate evidence for correctness that can be used to build a constructive assurance case meeting the requirements of industry regulators and certification schemes. All SPARK features are part of standard Ada—either Ada 83, Ada 95, or Ada 2005.

SPARK Pro is available worldwide from AdaCore, with support delivered by both companies using AdaCore's web-based GNAT Tracker support system. Current SPARK users have the option to transition to the new environment, which is also available as a standalone product. The launch of SPARK Pro is the first available product following the technical and marketing partnership announced last year between Praxis and AdaCore.

Praxis and AdaCore have worked together previously on high-assurance systems. One example is the Tokeneer project implemented by Praxis for the US National Security Agency (NSA) using the SPARK language and toolset and AdaCore's GNAT technology.

Open-DO Initiative

Collaborative Framework for Developing Certifiable Software

AdaCore has launched a new initiative for the High-Assurance community, with the goal of producing a cooperative and open framework to reduce the effort in developing certifiable software. Its name, "Open-DO", reflects one of the intended application domains: safety-critical systems requiring certification against the highest levels of the DO-178B avionics safety standard.

Open-DO was established to exploit two of the most promising trends that have been taking hold in software engineering:

- **Effective collaboration through Open Source communities, and**
- **Innovative methodologies such as Agile, Lean and eXtreme programming.**

Its mission is to demonstrate that these techniques are practical for developing software that needs to meet high-assurance certfication standards.

Open-DO aims to reduce certification costs by making available a number of Freely Licensed Open Source Software (FLOSS) tools, by providing a framework in which these tools can be integrated, and by addressing a number of workflow support issues.

Key to the success of the Open-DO initiative is wide participation from a variety of communities including FLOSS developers, safety-critical programmers, tool providers, avionics industry leaders, researchers and professors from academia, and certification authorities.

Potential topics of interest include:

- **Open verification tools with qualification material**
- **Open qualification material for closed verification tools**
- **Open development tools with qualification / certification material**
- **Open life-cycle management tools**
- **Open certifiable components (with certification material)**
- **Open educational material on the certification process and standard evolution**

To learn more, please visit www.open-do.org or contact info@open-do.org.

< current releases >

GNAT Pro 6.2

GNAT Pro 6.2.1 was released during Q1 2009 on 18 native and 28 cross platforms, qualified for 146 different configurations. New supported plaforms include:

- x86_64 Mac OS X (64 bits)
- Java Virtual Machine on Windows
- x86 Elinos (hosted on GNU/Linux)
- AVR microcontroller Elf format (hosted on Windows)
- LEON Elf format (hosted on Windows)

For a full list of supported platforms, please visit **www.adacore.com/home/gnatpro/supported_platforms**.

GNAT Pro 6.2 includes two additional components on main native platforms:

- GNAT Ada-Java Interfacing Suite, a toolset that simplifies combining natively compiled Ada code with Java running on a JVM, and
- GNAT Component Collection (GNATcoll), a set of reusable packages and utilities that are derived from the GNAT tools themselves.

The 6.2 release also includes GPS 4.3, the latest version of the GNAT Programming Studio IDE. GPS 4.3 is compatible with GNAT Pro versions 3.16a1 through 6.2.

GNATbench 2.3

The latest GNATbench release introduces SPARK support into Eclipse. Specific new features include additional contextual menu entries, dedicated SPARK output windows, Marker/Problems view integration, and distinct color selections for SPARK annotations.

C and C++ Binding Generators

GNAT Pro 6.2 includes a binding generator that produces Ada package specifications corresponding to C and C++ header files. This automates what in the past has often been a tedious manual process, and makes it much easier to reuse large C or C++ APIs in an Ada context. Since the generated code exploits Ada 2005 features such as "limited with" clauses and anonymous access types, there is a more direct mapping between the original API and the generated binding than was possible in previous versions of Ada.

< in the pipeline >

CodePeer Error Detection Tool

AdaCore, in partnership with SofCheck, is working on an Ada code analysis tool that detects logic errors early and helps reduce system development effort.

Named CodePeer to suggest its role as an automated peer reviewer of a project's source code, the tool analyzes Ada programs for a wide range of flaws including pointer misuse, buffer overflows, numeric overflow or wraparound, division by zero, dead code, unused variables, and concurrency hazards (race conditions).

CodePeer finds logic flaws in software without executing the program. It works by analyzing every line of code, considering every possible input and every path through the program, in order to find any construct that might cause the program to terminate abnormally or produce a meaningless result.

CodePeer will be especially valuable in high-assurance applications that need to be certified against safety or security standards. It can be used both during system development, to prevent errors from being introduced, and retrospectively on existing code, to detect and remove latent bugs.

CodePeer is expected to be available during Q4 2009.

Support for VxWorks 6 Cert

A GNAT Pro release later this year will support Wind River Systems' VxWorks 6 Cert operating system for safety-critical applications. The product will feature full integration with Workbench, two run-time profiles suitable for DO-178B level A applications (Zero Footprint and Ravenscar), as well as a full Ada run-time profile to assist incremental porting of existing code to the operating system.

< academia corner >

Spotlighting a GAP Member

Vermont Technical College (Randolph Center, Vermont, US)

Students Using SPARK and GNAT for Arctic Sea Ice Buoy and CubeSat Projects

Under the direction of Professors Carl Brandon and Peter Chapin, students at Vermont Technical College are using AdaCore's GNAT development environment along with Praxis' SPARK tools on two NASA-sponsored programs with large software components. For the first project, the students are designing and building both the hardware and software for an Arctic Sea Ice Buoy that measures wind speed, direction, temperature and GPS position. Data from the buoy are sent back to the home base via the Iridium satellite network. The students are producing the prototype buoy for the study of sea/ice interaction in the Arctic Ocean, and a follow-on grant will fund placement of between 10 and 20 buoys on the Arctic Ocean ice.

The second project is a continuation of work on CubeSat, a space satellite 10 cm in diameter with a mass of 1 kg. The CubeSat software is considerably more complex than that of the Sea Ice Buoy, but the two projects share a common software methodology and some of the code.

"Vermont Tech was one of the first colleges to sign up for the GNAT Academic Program, and we are pleased that AdaCore has taken the initiative in promoting the use of Ada in undergraduate curricula," said Prof. Brandon. "The ocean and space projects require extremely high reliability: a bug in the deployed software is expensive to fix and may even cause damage to or loss of the equipment. Using the SPARK language with the GNAT compiler and tools has been an excellent experience for the students in how to build high-assurance software."

A paper by Professor Brandon, describing the software methodology used in the two projects, appeared in the September 2008 issue of *Ada Users Journal*.

Interview with Michaël Friess Technical Sales Manager, AdaCore EU

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

I learned Ada while a student at TELECOM ParisTech (formerly ENST) in France, in a course given by AdaCore EU's Managing Director, Franco Gasperoni. After graduation I took an internship at AdaCore's Paris and New York offices; since I had a special interest in embedded systems I worked on the GNAT cross-compiler technology. The internship led to a full-time position starting in 2001, which has been a mix of technical development work and pre-sales support.

You are in charge of sales and strategic partnerships for Europe, the Middle East, and Asia. What does this involve?

I interact directly with customers, partners, and the AdaCore development team. In addition to the non-technical work required, I have to understand the needs and expectations of the industry in order to find appropriate solutions. This regularly means "thinking outside the box", and I will frequently propose new features or directions for the GNAT Pro technology. A challenging and exciting job, especially considering the variety of cultures and technical practices in the parts of the world that I cover!

You work with customers who produce safety-critical systems. How do you see software technology evolving in this area?

Developing a safety- or security-critical application generally means making conservative decisions: a tool or programming language with a long and successful track record is maintained and reused, rather than being replaced by something more modern, because changes can introduce risk. Relying on 20-year old technology to implement new systems is the strange paradigm the industry often has to live with when it comes to high-integrity systems.

So stability is important, but that doesn't mean that recent advances are completely ignored. One new dynamic is the increasing usage of Lean Programming, a set of software development principles adapted from the manufacturing industry. Lean Programming techniques can definitely be used for avionics and other high-integrity applications: building a system more efficiently (quicker, cheaper) can also make it safer. Another example is the emergence of Object-Oriented Programming (OOP) in safety-critical software. Safe usage of OOP has been the subject of considerable study in recent years, and I know of some systems using Ada 2005 OOP features that have been certified to the highest levels of the DO-178B avionics safety standard.

Since AdaCore's products are based on the Freely Licensed Open Source Software (FLOSS) model, I should also note another trend: the growing interest in community-maintained FLOSS toolsets for safety-critical development. Several major aerospace companies are now actively involved in FLOSS activities, which give them a way to share costs and to gain higher assurance in the correctness and longevity of the systems they develop. One such initiative is Open-DO, which AdaCore launched earlier this year (it's described in an article on page 1 of this newsletter). I find the Open-DO concept especially exciting since its goal is to develop a FLOSS framework that covers the complete development cycle for safety- and security-critical applications. This project will involve the collaboration of a number of companies, each bringing its particular expertise on some part of the system. I can see the Open-DO initiative catching on in avionics, railway transportation, military, automotive, and many other industries.

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

Since I can no longer find time to write software as part of my professional activity, programming has turned into a kind of hobby for me. But during the winter you will more likely find me looking for fresh powder snow and moguls!

Webinar Schedule

Monday, 27 April / Introduction SPARK Pro

This webinar, conducted by Dr. Rod Chapman from Praxis, will present the concepts behind the Correctness-by-Construction methodology and will include a demo of the SPARK Pro toolset.

Tuesday, 12 May / GNAT Pro for OpenVMS on HP Integrity Servers

This webinar, presented jointly by AdaCore and HP, will describe the latest GNAT Pro development environment for HP Itanium OpenVMS, with a focus on porting Ada code from VAX and Alpha server platforms.

To register for these webinars, and for a full list of upcoming and past webinars, please visit **www.adacore.com/home/gnatpro/webinars**

Michaël Friess photo: Gary Matoso

Ada Gem: Pragma No_Return

The AdaCore website includes a series of helpful hints about the Ada language, called Ada Gems. Here is a sample from this series, Gem #16, written by Bob Duff from AdaCore. For the complete set, please visit **www.adacore.com/category/developers-center/gems/**

It is occasionally useful to have a procedure that never returns normally, where "normally" means reaching the "end" or executing a "return;". For example, a procedure might format an error message based on its parameters, send the message to a log file, and then unconditionally raise an exception. Other ways to avoid returning normally are to loop forever, and to wait upon an entry barrier that never becomes True.

Such procedures are unusual, and therefore deserve to be documented. A comment works, but pragma No_Return is better because the compiler makes sure that the procedure does not, in fact, return:

```
procedure Log_Error (...);
pragma No_Return (Log_Error);  --  Mark it as a non-returning
                               --  procedure
procedure Log_Error (...) is
begin
   Put_Line (...);
   raise Some_Error;
end Log_Error;
```

Pragma No_Return in Ada 2005 was inspired by the implementation-defined pragma No_Return that has existed in GNAT for some time. Now it's a standard feature of the Ada language.

According to the Ada RM, if a non-returning procedure reaches the "end", Program_Error is raised. But that's just a tripping hazard; what we really want is a compile-time check. In fact, if there is any control-flow path that can reach the "end" of a supposedly non-returning procedure, GNAT will give a warning. As always, you can tell GNAT to treat warnings as errors. These warnings are necessarily conservative, so you might sometimes need to use pragma Warnings(Off) to prevent the compiler from "crying wolf".

newsflash

GNAT-on-MINDSTORMS Release

GNAT-on-MINDSTORMS, the GNAT toolsuite for the LEGO MINDSTORMS NXT platform, is now available to members of the GNAT Academic Program as an educational aid to teach students how to construct high-integrity robotics systems in Ada. The GNAT-on-MINDSTORMS package includes a GNAT tool chain for the ARM7 processor, an Ada API to interface with the hardware, code samples, and teaching material.

Ada Support for Model-Based Design

AdaCore will be participating in the Eclipse Model Development Tools (MDT/Papyrus) project, with the goal of increasing the tool support for Ada in modeling technology. The company's contribution to the project will be UML2 and SysML code generators that produce Ada 2005 and SPARK. AdaCore is also investigating possible development of an Ada back end for Mathworks Simulink, based on the technology produced by the EU-funded Gene-Auto project.

Wind River Aerospace and Defense Regional Conferences

Theme: Meeting the Threats of the Next Decade

AdaCore is exhibiting at Wind River's series of regional conferences in the US: Dallas (Irving) TX, 14 April; Huntsville AL, 23 April; Manhattan Beach CA, 21 May; Philadephia PA, 4 June; Arlington VA, 17 June; Framingham MA, 17 September.
www.windriver.com/announces/ad_conference2009

Conferences / Events ■ April – November 2009

ESC Silicon Valley 2009
30 March–2 April / San Jose CA, US

AdaCore is exhibiting at this conference.
esc-sv09.techinsightsevents.com/

RoboBusiness 2009
15–16 April / Boston MA, US

Lars Asplund is giving a talk on High-Assurance software in robotics. **www.robobusiness.com/**

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

AdaCore is exhibiting at this conference, and Ben Brosgol is presenting a tutorial on safety-critical software technology. **www.sstc-online.org/**

DASIA 2009
26–29 May / Istanbul, Turkey

José Ruiz is presenting a paper on Open-DO, and Matteo Bordin is presenting a paper on model-driven engineering. AdaCore is an exhibitor at this event. **pagesperso-orange.fr/eurospace/dasia.html**

Avionics USA
1–2 June / San Diego CA, US

Robert Dewar is giving a talk on the Open-DO initiative, and AdaCore is exhibiting at this conference. **www.avionics-usa.com**

Safety-Critical Systems—the Tools and Culture for Optimum Return on Investment
4 June / Bristol, UK

AdaCore is a major sponsor of this event and Franco Gasperoni is giving a talk on Open-DO.
www.scsc.org.uk/diary.html?opt=detail&id=80

Ada-Europe 2009
8–12 June / Brest, France

AdaCore is a major sponsor of this event. Talks and/or tutorials are being delivered by José Ruiz (Ada 2005 task dispatching), Quentin Ochem (building cross-language applications using Ada), Pat Rogers (embedded systems programming, fault tolerance), and Matteo Bordin (coverage analysis of safety-critical applications).
conferences.telecom-bretagne.eu/rst2009/

SIGAda 2009
1–5 November / Tampa Bay FL, US

AdaCore is a Platinum sponsor of this conference, and Greg Gicca is a conference chair.
www.sigada.org /conf/sigada2009

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