GNAT Pro Safety-Critical for Railway Applications

The GNAT Pro Safety-Critical development environment supports rail applications that need to meet the highest levels of safety certification. It includes run-time libraries specialized for use in safety-critical systems, as well as several tools for static analysis and testing. GNAT Pro Safety-Critical can be used in conjunction with other AdaCore products such as the SPARK Pro formal verification environment or the CodePeer advanced static analysis tool, providing a unique development framework that supports a wide range of verification activities.

In addition to a fully customizable run-time library, GNAT Pro Safety-Critical supplies several predefined run-time profiles (libraries corresponding to restricted feature choices). The Zero Footprint (ZFP) profile reflects an Ada language subset that does not require any Ada run-time phases, thus reducing the memory footprint to a run-time profile implemented in the Ada compiler. The Ravenscar Extended profile implements the Ravenscar tasking subset on top of ZFP. These profiles are ideal for high-criticality applications, for example, those that need to be certified to Software Safety Integrity Level (SIL) 3/4. For lower levels of criticality, the Ravenscar Extended profile provides features such as exception handling and stack overflow checking. GNAT Pro Safety-Critical has been adapted to meet the needs of CENELEC standards for software development processes (EN 50128:2011, EN 50126:1999, and EN 50129:2003, for SIL 3/4), and a variety of certification-related material is available to supplement the product:

- Qualification material for several product components: the GNAT Pro compiler as a class T3 tool, the GNATcheck coding standard checker as a class T2 tool, the GNATMetrIC code metrics generator as a class T3 tool, and the GNATTest/Ada ITN testing framework as a class T2 tool.
- Qualification material is also available for several other tools that can be used in conjunction with GNAT Pro Safety-Critical:
  - SPARK Pro's GNATprove as a class T2 tool to show proof of absence of run-time errors,
  - The CodePeer static analysis tool as a class T2 tool and data for control flow analysis, and
  - The GNAtcoverage and GNATemulator dynamic analysis tools as class T2 tools for code coverage analysis.

GNAT Pro Safety-Critical has been used to develop rail systems certified to SIL 4 of EN 50128. The product is available for x86 Windows and SPARC Solaris host development platforms, targeting PowerPC. For more information, please visit www.adacore.com/gnat-pro-safety-critical/

**Conférences / Events ▶ April–October 2014**

Embedded Masterclass
April 8–10 / Birmingham, UK
Robert Dewar is giving a talk on freely-licensed software in critical applications and systems. AdaCore is a Silver Sponsor and exhibitor.

www.embedded-masterclass.com/

Tool Qualification Symposium
April 9 / Munich, Germany
Martin Bondi is giving a talk on the economics of tool qualification. AdaCore is a sponsor and exhibitor. www.tqs.de/de/2014/

Civil Avionics International Forum
April 22-23 / Shanghai, China
AdaCore is a sponsor and exhibitor. www.gallunecnevents.com/CIF2014/en/home.html

High Confidence Software and Systems Conference May 6–9 / Antwerp, Belgium
Yannick Moy is giving a talk on SPARK 2014: “Formal program verification for all.” Contact cpsn.org/group/hcss_conference

AVUS' Unscreened Systems
April 21–25 / Shanghai, China
AdaCore is a sponsor and exhibitor. www.avusShow.com/events/avus2014/2014/public/show.aspx

**CodePeer 2.3 Released**

Complete standalone package, usable with any Ada compiler

A new major version of the CodePeer static analysis tool is now available. CodePeer performs automated analysis and validation of Ada source code—including Ada 2012—identifying potential bugs before program execution to find errors. The tool also conducts impact and vulnerability analysis when existing code is modified, and, using control-flow, data-flow and other advanced static analysis techniques, it generates comprehensive reports logic errors that would otherwise only be found through labor-intensive debugging.

With CodePeer 2.3, customers will find improved usability, increased functionality, and better tools integration.

CodePeer 2.3 includes an independent Ada semantic analyzer and can thus operate as a standalone tool, simplifying the installation process. It supports most Ada compilers and allows users to specify target machine characteristics such as endianness and the range of numeric types, and so can now handle the majority of existing Ada 83 and 95 code bases.

- Enhancements to the analysis engine mean fewer “false positives”, and CodePeer’s diagnostic messages are more precise, for example warning when a formal parameter is declared with a mode that is more general than necessary.
- The tool’s support for reviewing messages has been re-engineered to offer additional ways to classify messages. There is also a new optional method for performing a review directly via a source code change (via pragma Annotate!), in addition to the existing separate database for dependency information.
- Among its new features CodePeer 2.3 can detect floating point overflows on unconstrained types.
- To simplify the development process, CodePeer 2.3 is more closely integrated into AdaCore’s GNAT Programming Studio (GPS) and GNATBench IDE.

CodePeer has always been a standalone tool connecting to the GNAT Pro technology—a coding standard verification tool (GNATcheck), a source code metric generator (GNATMetrIC), and a document generator.

For additional information, please visit www.adacore.com/codepeer/

**GNATCoverage 1.2 Supports Hardware Probes**

The latest release of AdaCore’s source and object code coverage analysis tool has greatly widened the product’s applicability, adding support for trace data generated by hardware probes. GNATCoverage’s innovative technology does not require instrumentation of the executable. To meet this goal, previous versions have relied on traces provided by the host-resident GNATemulator target emulator tool. GNATCoverage 1.2 can still use GNATemulator, but it also supports iSys hardware probes generating Nexus trace data, as well as Valgrind on Linux. By deriving source coverage results from a non-instrumented executed running test-suite, the technology can measure the tool’s effectiveness. GNATCoverage 1.2 can significantly simplify the coverage analysis effort in a certification context.

GNATCoverage 1.2 can handle Ada 95, Ada 2005, and many new features in Ada 2012. It can also be used for SPARK 2014 and provides Beta support for C. Other enhancements include generation of coverage information for generic on a per-instance basis, and improved HTML output.

GFNet has been qualified as a T2 tool for railway applications that need to comply With EN-50261:2011. Qualification material is also available for GNATCoverage as a verification tool (GNATcheck) for SPARK systems at TOLs-S-D0-TNCS for Ada and systems. GNATCoverage qualitative analysis up to Modified Condition/Decision Coverage (MC/DC) can thus be used as part of the verification process for systems that need to be certified up to Level A. GNATCoverage is the only non-instrumenting coverage technology available, but uses a modified version of the McDC analysis that is written to individual pins, thus ensuring results are unambiguously positional.

Please visit www.adacore.com/gnatcoverage/1.2.
New subscription option for GNAT Pro Safety-Critical

As an add on for service of GNAT Pro Safety-Critical, AdaCore is finalizing a new kind of subscription for customers who need to detect errors on defined release branches. This facility is especially useful in certification contexts where compiler failures are unacceptable, even when the failures are only detected after certification. A detailed report must be written to assess the potential impact or if the certificate is voided. Patchs to avoid hardware bugs may also be applied. Every corrective action comes with a corresponding impact analysis.

GPS to include new documentation generation tool

The next release of the GNAT Pro Programming Studio IDE will include GNALoc, a new command line tool for documentation generation. Among its features are support for JavaDoc/Doxygen style tags in documentation comments, support for comment placement detection, support for separating documentation comments from code comments, and a new extensible HTML back end.

SPARK Pro 14

SPARK Pro 14 is the first full release of the next-generation SPARK toolset, which implements the SPARK 2014 language. SPARK 2014 is a rich subset of the Ada programming language. Traditional means such as testing, and eases the transition from Ada to SPARK for applications that need the additional assurance gained from formal proofs of program properties.

The main features of the new language and toolset include:
- Concurrency with Ada 2012 syntax
- Larger Ada language subset
- Executable contracts
- Hybrid verification (the ability to combine unit test with proof)
- Formal Contract library
- Generative mode for data dependencies in Ada (the ability to perform data flow analysis without explicit global declarations)
- Improved diagnostics for information flow and verification errors.


Distributed GPBuild

The latest version of the GPBuild tool, included in GNAT Pro 7.2, supports distributed compilation and addresses the problem of long build times for very large applications. For users who wish to take advantage of distributed compilation, GPBuild’s innovative approach requires minimal or no changes to project files and does not impose restrictions on what can be built. A project that compiles normally with GPBuild will also compile in distributed mode.

With distributed GPBuild, a local machine can perform some compilations but also sends compilation requests to any number of remote server machines. Once the compilation phase is done, binding and linking are performed on the local machine. Distributed compilation can be used for Ada, C, C++, or any other language supported by GPBuild.

Speedup of system builds with distributed GPBuild can be significant. During the Beta test of the new capability, one user reported that a build previously taking 2.5 hours was reduced to 10 minutes. Ada is specifically targeted at large and complex applications, and GNAT Pro’s new support for distributed GPBuild helps users take full advantage of Ada’s “programming in the large” features while avoiding compile bottleneck.

GNAT Industrial User Day

This year’s GNAT Industrial User Day will be held on Thursday, September 25, in Paris. Attendees will hear news about the latest tools and features, product roadmaps, and practical tips from technology experts. Presentations will include updates on new technologies such as the upcoming qualifiable model compiler / code generator, and a selection of tutorials will help attendees understand and perfect programming techniques.

As always, AdaCore staff will be on hand to answer questions, together with other industrial users who will share their experiences in using GNAT and Ada. For registration details and further information, please contact events@adacore.com or visit www.adacore.com/gnatpro-day/.
SPARK 14 Pro

SPARK 14 Pro is the first full release of the next-generation SPARK toolset, which implements the SPARK 2014 language. SPARK 14 Pro is a rich subset of Ada 2012, excluding only those language features that would make program verification unduly burdensome. It enables a novel verification approach that allows combining previously verified code with code that has been verified through traditional means such as testing, and eases the transition from Ada to SPARK for those that have to take advantage of the additional assurance gained from formal proofs of program properties.

The main features of the new language and toolset include:

- Convergence with Ada 2012 syntax,
- Larger Ada language subset,
- Executable contracts,
- Hybrid verification (the ability to combine unit test with test code),
- Formal Container library,
- Generative mode for data dependencies (the ability to perform data flow analyses without explicit declaration).

Additional information on the SPARK 14 language—including a number of programming tips and techniques—may be found at www.spark-2014.org.

Distributed GPBuild

The latest version of the GPBuild tool, included in GNAT Pro 7.2, supports distributed compilation and addresses the problem of long build times for very large applications. For users who wish to take advantage of distributed compilation, GPBuild’s innovative approach requires minimal or no changes to project files and does not impose restrictions on what can be built. A project that compiles normally will also compile in distributed mode.

With distributed GPBuild, a local machine performs some compilations but also sends compilation requests to any number of remote server machines. Once the compilation phase is done, binding and linking are performed on the local machine. Distributed compilation can be used for Ada, C, C++, or any other language supported by GPBuild.

Speedup of system builds with distributed GPBuild can be significant. During the Beta test of the new capability, one user reported that a build previously taking 2.5 hours was reduced to 20 minutes. Another user reported a 10.10 minutes. Ada is specifically targeted at large and complex applications, and GNAT Pro’s new support for distributed GPBuild helps users take full advantage of Ada’s “programming in the large” features while avoiding compilation bottlenecks.

New subscription option for GNAT Pro Safety-Critical

As an add-on service for users of GNAT Pro Safety-Critical, AdaCore is finalizing a new kind of subscription for customers who need access to defect corrections on defined release branches. This facility is especially useful in verification contexts where compiler or library changes are needed to fix identified defect problems, even when the corresponding certificate must be analyzed to assess the potential impact or certified code. Patches to avoid hardware bugs may also be applied. Every corrective action comes with a corresponding impact analysis.

GPS to include new documentation generation tool

The release of the GNAT Programming Studio IDE will include GNAdaDoc, a new command-line tool for documentation generation. Among its features are support for JavaDoc/Doxygen style of tags in documentation comments, support for comment placement detection, support for separating documentation comments from code comments, and a new extensible HTML back-end.

Spotlighting a GAP Member

Vermont Tech’s CubeSat is in orbit and sending down photos and data

Vermont Tech’s Lunar CubeSat, launched into a low earth orbit in November 2013 to test the navigation systems that will be used for the eventual lunar mission, has been successfully transmitting photos and inertial measurement unit data since reaching its initial orbital position. The satellite works in sunlight, since the software-controlled battery protection system failed immediately and the batteries were overcharged and destroyed. Although SPARK Pro 7.2 includes several new tools, including GNAT2XML, which generates an XML version of a semantically analyzed Ada program and thus helps developers write Ada analysis tools in any language. Enhancements to existing tools include a new version of the GNAltp printer with improved Ada layout, and an enhanced GPBuild multipurpose builder that offers greater flexibility and support of both distributed and parallel builds.

This release adds support for Wind River’s VxWorks 6 and C for x86 and LynxOS/178 Real-Time Operating Systems (RTOS). It also extends GNAT Pro’s ARM support to now include Android, generic Linux on ARM, Boardcom ARM, and Wind River’s VxWorks 6 on ARM.

Of the twelve university CubeSats that were launched, Vermont Tech’s is the only one still fully functioning.

You have been involved with software verification from many perspectives, including debugging technology, formal methods, and coverage tools. Do you see any trends or developments offering hope that future systems can be less susceptible to the sorts of expensive “glitches” that are so common today?

Of the twelve university CubeSats that were launched, Vermont Tech’s is the only one still fully functioning.

You were involved with software verification from many perspectives, including debugging technology, formal methods, and coverage tools. Do you see any trends or developments offering hope that future systems can be less susceptible to the sorts of expensive “glitches” that are so common today?

A lot of these glitches come from a misuse of a component, that is, a misunderstanding of its interface: how to use it, what it does. To tackle this problem, something as simple as source code documentation—comments—has been basic software engineering practice for decades. Unfortunately, almost the entire documentation is informal and it is mostly hand written. It is difficult to keep the documentation current and to check that the code actually follows what is documented. More and more developers are exploring the use of static analysis and formal methods to establish a link between the code and the documentation. Formal methods are used to establish properties that must hold to ensure the reliability of software. Static analysis is used to verify that the code conforms to the properties. These methods can be applied to any programming language and can help in understanding how the code actually works.

This year’s GNAT Industrial User Day will be held on Thursday, September 25, in Paris. Attendees will hear news about the latest tools and toolset features, product roadmaps, and practical tips from technology experts. Presentations will include updates on new technologies such as the upcoming qualifiable model compiler / code generator, and a selection of tutorials will help attendees understand and perfect programming techniques.

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

I would ideally like to keep up with the many advances in human knowledge in this century, in many areas: contemporary art, music, literature, philosophy, and most especially mathematics. Modern algebra in particular is a fascinating field. Many ideas and results from this field will be of importance in the future and I have a particular interest in the history of mathematics and the relation between mathematics and physics.
For up-to-date information on conferences where AdaCore is participating, please visit www.adacore.com/gnatpro-safe-critical/

Embedded Masterclass
April 8–10 / Birmingham, UK
Robert Dewar is giving a talk on using freely-licensed software in critical systems. AdaCore is a Silver Sponsor and exhibitor.

www.embedded-masterclass.com

Tool Qualification Symposium
April 9–10 / Munich, Germany
Matthias Bonder is giving a talk on the economics of tool qualification. AdaCore is a sponsor and exhibitor.

www.tqs10.com

Civil Aviation International Forum
April 22–23 / Shanghai, China
AdaCore is a sponsor and exhibitor.


High Confidence Software and Systems Conference
May 6–9 / Antwerp, Belgium
Yannick Moy is giving a talk on SPARK 2014. "Formal program verification using Ada and SPARK: a success story". AdaCore is a sponsor and exhibitor.

www.cefcs05.org

AVVIS's Unnoticed Systems Announced
April 27 / Athens, Greece
AdaCore is an exhibitor.

www.avvis.org/gus14/conf2014

Australie System Safety Conference
May 28–30 / Melbourne, Australia
AdaCore is a major sponsor.


Ada-Europe 2014
June 23–27 / Paris, France
AdaCore is a major sponsor and exhibitor. Ban Brogol, Yannick Moy, and Toshi Take are presenting tutorials. For more information, please visit www.adata.org

www.ada-europe.org

TAP 2014
October 15–23, 2014 / Paris, France
AdaCore is a Platinum sponsor/exhibitor, and Tuckar Tu is a Program Chair. See www.tap2014.org

CodePeer 2.3 Released
For additional information, please visit www.adacore.com/codpeep

GNCoverage 1.2 Supports Hardware Probes
The latest release of AdaCore's source and object code coverage analysis tool has greatly widened the product's applicability, adding support for trace data generated by hardware probes. GNCoverage's innovative technology does not require instrumentation of the executable. To meet this goal, previous versions have relied on traces produced by the host-resident GNCoverage target emulator tool. GNCoverage 1.2 can still use GNCoverage, but it also supports iSystems hardware probes generating Nexus trace data, as well as Valgrind on Linux. By deriving source coverage results from a non-instrumented execution of running testcases, GNCoverage 1.2 can run with the highest possible safety assurance. GNCoverage 1.2 can significantly simplify the coverage analysis effort in a certification context.

GNCoverage 1.2 can handle Ada 95, Ada 2005, and many new features in Ada 2012. It can also be used for SPRK 2014 and provides Beta support for C. Other enhancements include generation of coverage information for generics on a per-instance basis, and improved HTML output.

GNCoverage has been qualified as a T2 tool for railway applications that need to comply with EN-50128:2011. Qualification material is also available for AdaCore's coverage analysis toolset GNCoverage 1.2. It can be used for railway systems that need to be certified up to Level A. GNATcoverage is the only non-instrumenting coverage analysis tool of its kind. Use of GNCoverage in combination with GNCoverage 1.2 will simplify the coverage analysis effort in a certification context.

Product Spotlight:
GNCoverage 1.2 Supports Hardware Probes
Conferences/Events
Adacore Conference in the Pipeline
Academia Comer: Vermont Technical College (US)
Interview with Jérôme Gauffin
GNCoverage Industrial User Day
For additional information, please visit www.adacore.com/gncoverae/