

# Embedded Systems: Take a New Look at Ada

Robert Dewar, President and CEO, AdaCore

[Take a New Look at Ada](#)

*The Ada language offers an easy path to solid code.*

**by Robert Dewar, President and CEO, AdaCore**



The world of computer technology has two incompatible characteristics. First, many computer systems have long lives. Second, students and many engineers pay attention to only the latest technologies and they believe old technologies have died out. The "yesterday's-fashion" phenomenon has applied to the Ada programming language, too. If engineers have heard of Ada at all, they may assume it is an old US Department of Defense technology that disappeared long ago.

And yet, Ada appears alive and well as a language for large-scale critical systems. Almost all modern commercial aircraft, such as the new Boeing 787 Dreamliner aircraft rely on much software written in Ada.

Why do programmers continue to use Ada? First, software systems can operate for decades and undergo continual changes, so programmers choose a language that already has a long life and still meets modern requirements. Second, translating large software systems from one language to another requires a huge effort and usually makes the new software unstable. Software developers should almost never recode older programs solely to

## Embedded Systems: Take a New Look at Ada

Published on Electronic Component News (<http://www.ecnmag.com>)

---



"update" to a new language.

Engineers and programmers can make a strong argument that they prefer Ada for large critical systems, and that the use of other languages is a technical mistake. The basis for that claim lies in the growing importance of safety and security. Our lives and environments increasingly depend on complex software in systems that include aircraft and nuclear power plants, but more subtle examples exist. Moody's Investors Services, for example, recently acknowledged that a software error caused it to rate some complex financial investments as minimal risks rather than as more risky.

Ada is the only widely used language whose standard specifically addresses safety and security issues. Many of the potential security problems reported in today's systems relate directly to hacker and cyber-terror attacks based on buffer overflows. Ada provides run-time checks that do not allow buffers to overflow so that type of attack cannot continue.

In a presentation at a US National Security Agency conference, Microsoft described its approach of adding range assertions to C-language code to allow statistical detection of possible buffer overflows. (Assertions keep values within known bounds.) According to the presenter, Microsoft has added half a million assertions to the Vista code, which yielded tens of thousands of possible buffer overflows that needed investigation. A more secure language such as Ada would have prevented this problem at its source. Range information becomes a fundamental part of any Ada program.

More importantly, Ada lends itself better to formal reasoning and high levels of security that require the use of formal methods. These methods mathematically prove and ensure that divide-by-zero, off-by-one, and similar errors cannot occur in Ada code. The designers of Ada had this approach in mind from the start. The Praxis SPARK language, an advanced dialect of Ada, makes use of this type of formal

## Embedded Systems: Take a New Look at Ada

Published on Electronic Component News (<http://www.ecnmag.com>)

---

analysis to eliminate unexpected run-time errors. Ada compilers can compile SPARK code, which includes additional annotations. These annotations tell the compiler that specific sections of code can or cannot access and change certain variables, for example. Instead of "gluing" annotations onto C code after the fact, Praxis viewed them as a critical component of SPARK from the start. SPARK also includes a complete framework for formal proof of properties of programs.

The use of formal methods in conjunction with Ada is not science-fiction. Software for the United Kingdom's next air-traffic-control system--iFacts--will rely entirely on Ada code. The iFacts developers will use the SPARK approach that lets them apply full formal proof of correctness techniques. See also the paper by Amey and Chapman listed below.

We find many developers take a close second look at Ada when they face requirements for highly reliable safety- and security-critical software. To date, over 150 universities have enrolled in the AdaCore GNAT academic program (GAP) that provides free tools and support for computer-science curricula that include Ada. This alone shows a renewed interest in Ada but and in high-quality software development.

### About the author

Dr. Robert Dewar, co-founder, president and CEO of AdaCore has been involved with the Ada programming language since its inception in the early 1980s. As co-director of both the Ada-Ed and the GNAT projects, he led the NYU team that developed the first validated Ada compiler.

### For further reading

*"Ada & Next-Generation Air-Traffic Control," Dr Dobbs Portal, June 19, 2007.* [www.ddj.com/web-development/199905389](http://www.ddj.com/web-development/199905389) [1].

*Amey, Peter and Roderick Chapman, "Industrial Strength Exception Freedom," Praxis. 2002.* [www.praxis-his.com/pdfs/Industrial\\_strength.pdf](http://www.praxis-his.com/pdfs/Industrial_strength.pdf) [2].

*Barnes, John, "High Integrity Software: The SPARK Approach to Safety and Security," Addison Wesley. 2003.*

*Oates, John, "Moody's computer 'bug' caused over-optimistic credit ratings," The Register.* [www.theregister.co.uk/2008/05/21/moodys\\_investigates\\_ratings](http://www.theregister.co.uk/2008/05/21/moodys_investigates_ratings) [3].

*Williams, Chris, "Dept of Homeland Security tests cyberterrorism response," The Register.* [www.theregister.co.uk/2006/02/13/us\\_cyber\\_storm/](http://www.theregister.co.uk/2006/02/13/us_cyber_storm/) [4].

**Source URL (retrieved on 04/28/2015 - 5:01pm):**

<http://www.ecnmag.com/articles/2008/10/embedded-systems-take-new-look-ada>

**Links:**

## **Embedded Systems: Take a New Look at Ada**

Published on Electronic Component News (<http://www.ecnmag.com>)

---

[1] <http://www.ddj.com/web-development/199905389>

[2] [http://www.praxis-his.com/pdfs/Industrial\\_strength.pdf](http://www.praxis-his.com/pdfs/Industrial_strength.pdf)

[3] [http://www.theregister.co.uk/2008/05/21/moodys\\_investigates\\_ratings](http://www.theregister.co.uk/2008/05/21/moodys_investigates_ratings)

[4] [http://www.theregister.co.uk/2006/02/13/us\\_cyber\\_storm/](http://www.theregister.co.uk/2006/02/13/us_cyber_storm/)