Abstract on DO178-B/ED-12C at The Ada Connection, June 2010, Edinburgh, UK

By Dewi Daniels

DO-178B, published in 1992, provides guidance for the development and verification of airborne software. It is in the process of being updated to DO-178C. Six years in the making, DO-178C is expected to be published by the end of 2011. This presentation provides a brief overview of what's new in DO-178C, how it will affect your software development and verification projects, and particularly its impact on Ada projects.

The changes to the DO-178C core text are evolutionary, rather than revolutionary. The terms of reference provided to the committee stated that DO-178C is to be backward-compatible with DO-178B. This should mean that if you have software processes that are compliant with DO-178B, then those software processes should also be compliant with DO-178C. However, one man's 'clarification' is another man's 'raising the bar'. This presentation will point out those changes that may affect your existing processes.

Two related documents, DO-248B (clarification of DO-178B) and DO-278 (air traffic management software) are being updated at the same time. In addition, there will be four new supplements, covering tool qualification, model-based design, object-oriented technology and formal methods. This presentation will give a very brief overview of these four supplements.

So what do these changes mean for the Ada community? The tool qualification supplement will provide better guidance on how to qualify software development and verification tools. The object-oriented technology supplement will provide better guidance on how to use the object-oriented features of Ada 95 (and Ada 2005) on DO-178C projects. The formal methods supplement will, at long last, allow certification credit to be taken for the use of technologies such as SPARK. DO-178C still doesn’t require the use of strongly typed languages; while it now allows certification credit for the use of formal methods (a term that covers a wide range of techniques, including formal specification, certain types of static analyses and program proof), it still does not mandate that they be used; and DO-178C still does not discuss the use of safety cases (though assurance cases do get a very brief mention). Nevertheless, on the whole, I believe DO-178C to be a step forward for the Ada community.

About the author

Dewi Daniels is managing director of Verocel Limited, a subsidiary of Verocel, Inc., the software verification company. Dewi has 30 years’ experience of safety-critical and high-integrity software development and verification. He was one of the original authors of the SPARK Examiner (he is pleased to see that his code is still present in the open source for SPARK GPL Edition!). Dewi is a member of SC-205/WG-71, the RTCA special committee/EUROCAE working group preparing DO-178C. He is an active member of SG-2 and of the DO-178C editorial team.