Tutorial Form

Title Practical Experiences of Safety and Security-Critical Technologies

Presenters Rod Chapman and Peter Amey
Contact name Peter Amey
Contact address Praxis Critical Systems, 20 Manvers Street, Bath, BA1 1PX, UK
Contact phone +44 (0)1225 466991
Contact fax +44 (0)1225 469006
Contact email sparkinfo@praxis-cs.co.uk

Requested level Intermediate

Abstract The tutorial identifies the special properties of systems intended for use in ultra-reliable domains and the qualitative shift in development methods that is required to achieve those properties. The advantages (and weaknesses) of Ada are introduced in the contexts of the ISO HRG report on High-Integrity Ada and of the SPARK sub-language. The demands of common, important development standards are described together with appropriate and cost-effective techniques for meeting them. Finally project experience illustrating successes in meeting the main standards is discussed.

Presenter summary

Peter Amey

Peter Amey is an aeronautical engineer by original professional training and achieved Chartered Engineer status through the Royal Aeronautical Society. He served as an engineering officer in the Royal Air Force and spent several years at the Boscombe Down test establishment working on the certification of aircraft armament systems. Peter joined Program Validation Limited to develop the high-integrity language SPARK and its support tool the SPARK Examiner and continues that work today with Praxis Critical Systems. As well as developing SPARK he has used it on major programmes including Tornado, Eurofighter and the Lockheed C130J.

Peter teaches SPARK and Ada on a regular basis and has lectured widely on the development of critical systems. Most recently this has included the keynote address "Logic versus Magic" at Ada Europe 2001, "Closing the Loop: the Influence of Code Analysis on Design" at Ada Europe 2002, "A Language for Systems not Just Software" at SIGAda 2001 and "High Integrity Ravenscar" at Ada Europe 2003. Peter has also had a well-received article published in Crosstalk Journal.

Rod Chapman

Roderick Chapman received MEng and DPhil degrees from the University of York, England in 1991 and 1995 respectively. He is currently products manager at Praxis Critical Systems, leading the design and development of the SPARK language and toolset. Before joining SPARK team, Rod was involved in the implementation high-integrity real-time and embedded systems, including SHOLIS (the first system implemented to the Def Stan 00-55 SIL4 standard), the Lockheed Martin C130J Mission Computer, and the MULTOS CA. Rod has presented tutorial, papers and panel sessions at many conferences, including SIGAda, Ada Europe, and STC, and remains a member of the Ada95 HRG.

Why you should participate in this tutorial? Because the presenters, and their company, Praxis Critical Systems, have an exceptional level of experience in the development of safety- and security-critical systems. Their experience spans aviation and rail in the safety domain as well as financial systems in the security domain; they have developed systems to meet all of the principal standards such DO-178B, Def Stan 00-55 and Common Criteria. The tutorial provides a unique opportunity to compare development approaches, their relationships with the various standards and to discover which approaches prove most cost-effective in practice