

SSEI Research Task Summary – T22

Task Number: SSEI/T22

Lead Delivery Organisation : University of York

Project Title : Updating Guidance on the Application of Civil Software Standards to DS 00-56

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

MOD's policy with regard to software development standards is that they should be "as civil as possible, and only as military as necessary". It is therefore imperative that both industry and MOD understand how to demonstrate that use of the evolving civil standards for software development – DO-178 and IEC 61508 - meets the requirements of DS 00-56 Issue 4.

This task will evaluate the proposed changes in DO-178C and IEC 61508 against UK MOD standards. In particular, it will examine the variety of methods and processes available to COTS vendors to satisfy the certification objectives of the civil standards and the possibilities the civil standards afford for novel development techniques, and provide guidance as to what additional evidence might be required to satisfy the military standards.

Nature of Work (what is it?)

Some of the proposed changes in the civil standards have not yet been assessed against UK MOD standards. These are primarily in the areas of tool qualification, model-based design and verification, the use of object-oriented technology and the deployment of formal methods. The civil standards are also less prescriptive than their predecessors, which means that techniques other than testing can be used to demonstrate the satisfaction of safety objectives.

The task aims to assess the certification strategies suggested by the evolving civil standards to determine whether the kinds of evidence they describe for each integrity level is sufficient to support a compelling safety argument as required by DS 00-56 Issue 4. Where there is a 'gap' between civil and military requirements, the SSEI will identify where deficiencies are likely to occur and recommend solutions to bridge the gap.

Outcomes (what will it produce/has it produced ?)

This task will produce 3 outputs:

- Guidance for software developers and acquirers as to the principal changes in the second edition of IEC 61508 and DO-178C and their implications for satisfaction of DS 00-56
- A report identifying current and future trends in military and civil safety culture, such as a move to a less prescriptive approach and an increasing dependency on COTS products. Guidance as to likely effects of these cultural changes on future civil and military standards
- Updates to the Standard of Best Practice on Software in the Context of DS 00-56 Issue 4 to address non-MOD standards

Timescales 15-month task, July 2009 to September 2010

Partners

Related Work SSEI/T6, SSEI/T11, SSEI/T21

Task Lead Professor John McDermid
john.mcdermid@cs.york.ac.uk
01904 432726