

SSEI Research Task Summary – T26

Task Number: SSEI/T26

Lead Delivery Organisation : Civil Aviation Authority

Project Title : Assurance of Evolving Software: Open Systems and Legacy Components

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

Open Systems Architecture approaches appear to offer considerable benefits, in terms of reduced development costs and shorter timescales than traditional software development methods. The approach has been used successfully on defence-related systems, e.g. submarine sonar. However, there are unresolved issues concerning assurance and assessment of open systems themselves, and of legacy software and COTS products ported onto open systems. These issues threaten the wider adoption of Open Systems development in military and civil applications.

This task aims to provide a strategy and supporting guidance as to how legacy and COTS software can be safely integrated into modern software systems.

Nature of Work (what is it?)

Recent work on the assurance of highly-integrated software systems has identified several 'research challenges'. In terms of software design, these include the mechanics of component composition and the provision of architectural barriers to failure propagation. For safety assurance arguments, challenges include the ability to bound the impact of a change to argument and evidence, the separation of claims about infrastructure from those concerning applications, and the acceptability of using evidence from process to support claims about the safety of a product.

In terms of design, the task will provide practical guidance on the identification and classification of modules, dependencies and interfaces in existing software and infrastructure, It will also provide detailed guidance on the development of well-structured, assurance arguments for pre-existing software.

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

This task will have 4 main outputs:

- Guidance for software developers and system integrators on the identification and categorisation of architectural barriers within pre-existing software and the protections they afford
- Guidance on the use of process evidence in safety assurance arguments
- Guidance on the derivation of evidence concerning 'black-box' software components
- Guidance on the nature of confidence required of evidence in assurance arguments and the development of intelligible arguments

Timescales 24-month task, June 2010 to May 2012

Partners University of York, University of Bristol, MBDA

Related Work SSEI/T6, SSEI/T11, SSEI/T21, SSEI/T22

Task Lead Andrew Eaton
Andrew.Eaton@caa.co.uk
01293 573504