

SSEI Research Task Summary – T6

Task Number: SSEI/T6

Lead Delivery Organisation : University of York

Project Title : Software Safety Cases – Establishing a Systematic Approach

Research Theme : *Developing Dependable Systems*

Version : 3



Objective of Work (why are we doing it ?)

Conflicts about the adequacy of software safety cases can arise between developer and acquirer software authorities. This often occurs late in the project, once the majority of the safety case is developed, so results in significant project risk, leading to delays and cost overruns. The late identification of the requirement for additional software safety evidence is particularly problematic as it can significantly delay entry into service.

This task aims to provide guidance and 'standardisation' in the way that software safety arguments are presented and supported, giving improved transparency to all parties, earlier in the programme. It is expected that this will help all parties to reach agreement by significantly reducing subjectivity

Nature of Work (what is it?)

It is increasingly recognised that software safety cases should be hazard-focused and evidence based. However, there is insufficient guidance on how such safety arguments should be established, structured and presented, in the context of DS 00-56. In addition, many developers are unclear about how existing software assurance and software safety lifecycle activities relate to the problem of establishing a software safety case.

The aim of this task is to develop practical and accessible Standards of Best Practice (SoBP) that will address the concerns highlighted above and enable developers to construct software safety cases, acceptance authorities to review and accept these cases, and acquirers to guide and control safety-critical and safety-related software intensive projects.

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

This task will produce three outputs:

- SoBP for software developers and acquirers on establishing clearly structured, hazard-based arguments for software safety
- SoBP for software developers and acquirers on evidence selection for software safety cases, and determining the assurance offered by different forms of software safety evidence
- Case study examples of the application of the SoBPs

Timescales 36 months, March 2008 to February 2011

Partners

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

Task Lead Dr Tim Kelly
tim.kelly@cs.york.ac.uk
01904 432764