

SSEI Research Task Summary – T21

Task Number: SSEI/T21

Lead Delivery Organisation : University of York

Project Title : Managing System and Software Safety Case Interface Issues

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

Most defence systems involve a substantial supply chain, and problems arise due to the problems of managing safety across organisational boundaries, both in terms of impact on product safety, and on the safety case. Safety requirements for software are often missing, inadequately defined or assumed (incorrectly) to be derivable by a lower-tier supplier. Further sub-contracts are often finalised before software safety requirements are understood, with attendant risks of substantial change. Conversely, there may be cases in which full disclosure at an organisational boundary is not desirable.

This task aims to provide guidance to support the development and expression of adequate software safety requirements. It also aims to show how safety-case architectures can be used to manage requirements across system and contractual boundaries.

Nature of Work (what is it?)

Safety-related requirements flowed down to software developers from the system level often fail to consider the specific failure characteristics of software or the ways in which these can be analysed to provide information which can usefully be deployed in a system safety case. There is also a need for contracts to be sufficiently flexible to handle the evolution of software safety requirements over the lifecycle of a system.

This task will provide practical guidance on how software requirements can be derived by exploiting knowledge of other systems. The task will produce best-practice guidance on the expression of software safety requirements, on the management of contractual specifications to allow for evolving system and software safety cases and on the associated safety-case architectures.

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

This task will produce a Standard of Best Practice addressing three areas:

- Guidance for software developers and acquirers on the definition of software safety requirements
- Guidance on the expression of software safety requirements across organisational, technical and contractual boundaries
- Guidance for software acquirers on the exploitation of safety-case architectures to manage safety requirements throughout the system lifecycle

Timescales 15- month task, July 2009 to September 2010

Partners

Related Work SSEI/T2, SSEI/T3, SSEI/T6 and SSEI/T11

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