

SSEI Research Task Summary – T23

Task Number: SSEI/T23

Lead Delivery Organisation : Agent Oriented Software

Project Title : Certifiable Safety-Critical Software Systems that can be Incrementally Upgraded

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

The new generation of Unmanned Air Systems (UAS) have a high degree of autonomous capability, provided by decision-making software which replaces functions performed by the human crew of a manned or remotely-piloted vehicle. These extend beyond flight control functions to a range of other critical roles, e.g. sense-and-avoid, mission management and re-routing. If such UASs are to undertake missions beyond those for which they are initially designed, it must be possible for the on-board Autonomous Mission Management system to be upgraded with the necessary additional or revised behaviours. The challenge is to permit such upgrades without the need for large-scale recertification.

This task aims to produce guidance on the design and assessment of decision-making software, including a Standard of Best Practice on incremental certification for decision-making software.

Nature of Work (what is it?)

A major challenge for the adoption of embedded, autonomous software-based systems to replace mission and flight-critical functions is the cost and time required to assess changes to the software, once it has initially been certified. Modifications often incur re-certification costs approaching the cost of the original clearance. This task aims to produce a certification process for decision-making software which makes the re-certification effort more commensurate with the scale of the change introduced. Outputs from this task will extend earlier work on software-based systems which are subject to incremental upgrade.

This task will develop a safety-case architecture for incrementally-certified decision-making software, and guidance on the argument strategies and evidence artefacts required, specialising previous work on incremental and modular certification.

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

This task will have three outputs:

- Guidance on the design of embedded software-based systems to support an incremental certification approach
- Guidance on the development of safety case and assurance arguments for incrementally-upgradeable software
- Guidance on the nature of the process- and product-based evidence required to support such arguments

A substantial case study will be produced, based on the addition of autonomous behaviours to an autonomous decision-making system for UAS operation

Timescales 26-month task, January 2010 to February 2012

Partners University of York, CAA, Kestrel Technology LLC

Related Work T6, T11, and the ASTRAEA Programme

Task Lead Hasan Acar
hasan.acar@aosgrp.co.uk
01223 308000