

Assurance of Evidence for Software System Safety Cases for Aviation Systems

Squadron Leader Derek W. Reinhardt



Research Evaluation Questionnaire Version 1.1

Department of Computer Science

THE UNIVERSITY *of York*

1 Introduction

Thank you for taking the time to participate in this research evaluation questionnaire. The time and expertise you can contribute will very much appreciated by the authors and really helpful to this research.

The following sections of this evaluation provide an overview of the research work for which a subsequent evaluation questionnaire is provided. Instructions are provided on how to complete the evaluation questionnaire. Furthermore, a strategy is suggested on how to minimise the impost on your very valuable time in completing the survey.

2 Research Overview

The failure circumstances of complex aviation systems involving technologies such as software are dominated by systematic faults. However, there is evidence in industrial practice that systematic faults are often poorly resolved by the coupling of software assurance (i.e. safety integrity levels and design assurance levels) with traditional system safety methodologies (i.e. hazard assessment, failure modes analysis, etc). This research effort is developing and examining a potential alternative evidence-based approach to the assurance of software against systematic faults in the context of aviation systems. The research is motivated by the author's previous and ongoing involvement in the certification of software acquired and modified by the Australia Defence Force for aircraft systems, and the substantial challenges and limitations presented in applying current assurance standards to these circumstances. The research hypothesis is as follows:

- It is feasible to develop a product behavioural evidence-based approach for demonstrating the safety of software for aircraft avionics systems;
- that it is possible to establish a framework to defensibly reason as the suitability and sufficiency of evidence produced with respect to product behaviours; and
- that minimises program certification and contracting risks by reducing or removing ambiguity of evidence requirements between the system supplier and the assessor or regulator.

The research has led to the development and proposal of a conceptual framework for:

- determining, expressing, and evaluating a software system product's architectural and fault avoidance and fault tolerance behaviours relevant to safety in both normal and failure modes of the system;
- expressing and evaluating the dependability of these behaviours based on a framework of claims relevant to potential evidence types;
- expressing and evaluating suitability and sufficiency of the evidence relevant to the framework of claims;
- ensuring that the framework is compatible with the certification environment of both the civil and military domains.

Several papers provide explanation of the conceptual framework, as follows:

- D.W. Reinhardt and J.A. McDermid, “Assuring Against Systematic Faults Using Architecture and Fault Tolerance in Aviation Systems” presented at the Improving Systems and Software Engineering Conference (ISSEC) 23-25 Aug 2010.
- D.W. Reinhardt and J.A. McDermid, “Assurance of Claims and Evidence in Aviation Systems” presented at the IET System Safety Conference 18-20 Oct 2010.
- D.W. Reinhardt and J.A. McDermid, “Contracting for Architectural, Claims and Evidence Assurance” for University of York Department of Computer Science technical report publication.
- D.W. Reinhardt and J.A. McDermid, “Contracting for Assurance of Military Aviation Software Systems”, proposed for publication at the Australian System Safety Conference 2012.

3 Evaluation

3.1 Purpose

The purpose of this research evaluation questionnaire is to establish via survey feedback on the plausibility, feasibility and usefulness of the conceptual framework and its motivations. This is necessary because it is rarely feasible to provide evaluation of the application of such research frameworks to entire projects, as is it usually not possible to run a project twice. Therefore, these survey results will be used to supplement targeted analytic and empirical evaluations activities being undertaken separately by the authors.

This evaluation is targeted at persons representing a cross section of regulators, technical specialists and practitioners from across government, regulatory and commercial organisations.

3.2 Estimated Completion Time

By comparison, this is a relatively onerous survey questionnaire to complete, and the authors do appreciate every effort made to complete this survey. The survey is comparatively long because it deals with a relatively large body of work, and numerous concepts within this work. Recognising that people’s time is valuable and that time may not be available to complete the whole survey in a single go, the survey is presented in three distinct sections. This also provides an option for those people that cannot complete the entire survey, to complete a section that most interests them.

The benefits to completing this survey are as follows:

- your input will contribute to the validation of this research,
- a complete summary of responses will be prepared for conference or journal publication to provide enduring record of your input,
- your input will form the basis of targeted workshops to further explore novel and constructive critique,
- this work is shaping a re-focus of thinking regarding assessment of risk of systematic faults,
- this work may influence future approaches employed by the Australia Defence Force and other Airworthiness Authorities.

The entire survey, including all reading and responding is estimated to take 5-7 hours to complete, although the authors recommend that respondents complete the survey in several blocks of time of no longer than 2 hours. The breakdown of times is as follows:

- Read and familiarise with the survey: 30 mins.
- Architectural Assurance: 1 hour to read the paper; 30-40 mins to complete the survey.
- Claims and Evidence Assurance: 1 hour to read the paper; 30-40 mins to complete the survey.
- Contracting for Assurance: 1 hour to read the short paper; optional 1.5 hours to read the extended paper; 30-40 mins to complete the survey.

These timings are based on several trial surveys conducting during development of this questionnaire. Timings may vary based on the level of effort applied to narrative response questions.

3.3 Instructions for Completing Evaluation

The evaluation should be conducted as follows:

1. Read and familiarise yourself with the layout and questions of the survey. Take specific note that, in each section of the survey, questions are grouped as follows:
 - Motivating Issues – examining plausibility of issues that motivate the research
 - State of the Practice – examining plausibility of limitations in the current practice
 - General Principles – examining the plausibility of the general approach to addressing the motivating issues (i.e. the principles on which our approach is developed)
 - Our Approach – examining the feasibility and usefulness of the proposed approach
2. Complete the section on Demographic information
3. Complete the section on Architectural Assurance
 - Read the paper “Assuring Against Systematic Faults Using Architecture and Fault Tolerance in Aviation Systems”
 - Complete the survey questions on architectural assurance
4. Complete the section on Claims and Evidence Assurance
 - Read the paper “Assurance of Claims and Evidence in Aviation Systems”
 - Complete the survey questions on claims and evidence assurance
5. Complete the section on Contracting for Assurance
 - Read the paper “Contracting for Assurance of Military Aviation Software Systems”
 - (Optional) Read the extended paper “Contracting for Architectural, Claims and Evidence Assurance”
 - Complete the survey questions on contracting for assurance.

3.4 Use of specified terms

Throughout the papers and survey, some nouns are afforded a meaning that may be more specific than the general English meaning of the words used. To ensure the appropriate meanings are afforded to nouns, survey respondents are requested to read the papers carefully, and to answer the survey questions in the context of the applied meaning within the applicable paper. The reader is encouraged to pay specific attention to the meaning of the following terms: software assurance standard, safety assurance standard, fault avoidance, fault tolerance, absence, detection and handling, constraint, and attribute. These words have specific meaning in the context of this research work.

4 Evaluation Questions

The evaluation questions are contained at Annex A. Please indicate your answer by either:

- circling the applicable answer for a choice type question,
- ticking the applicable column under an answer heading, or
- providing a written narrative where the question requests it.

5 Enclosures

The following papers are enclosed with this evaluation:

D.W. Reinhardt and J.A. McDermid, “Assuring Against Systematic Faults Using Architecture and Fault Tolerance in Aviation Systems” presented at the Improving Systems and Software Engineering Conference (ISSEC) 23-25 Aug 2010.

D.W. Reinhardt and J.A. McDermid, “Assurance of Claims and Evidence in Aviation Systems” presented at the IET System Safety Conference Oct 2010.

D.W. Reinhardt and J.A. McDermid, “Contracting for Architectural, Claims and Evidence Assurance” for University of York Department of Computer Science technical report publication.

D.W. Reinhardt and J.A. McDermid, “Contracting for Assurance of Military Aviation Software Systems”, proposed for publication at the Australian System Safety Conference 2012.

Annex A – Evaluation Questions

Id#	Survey Question	Question Category	Answers				
Part A - Demographic							
A1	Please provide your name, position and organisation.	Narrative					
A2	How many years of experience do you have developing safety-related or safety-critical systems?	Choice	0-2	3-5	6-10	11-15	16+
A3	How many years of experience do you have undertaking compliance assessments on safety-related or safety-critical systems?	Choice	0-2	3-5	6-10	11-15	16+
A4	How many years of experience do you have working for a certification authority (e.g. military airworthiness authority, national airworthiness authority, etc)?	Choice	0-2	3-5	6-10	11-15	16+
A5	What domain do you presently work in?	Choice	Aviation	Maritime	Land	Information Systems	Other
A6	What type of organisation do you work for?	Choice	Military	Professional Service Provider	Commercial Developer	Government	Other
A7	What type of work do you undertake?	Choice	Development	Integration	V&V	Compliance Assessment	Other
A8	How many developments do you have experience applying a software assurance standard such as RTCA/DO-178B or UK Defence Standard 00-55 to?	Choice	0	1	2-5	5-10	11+
A9	How many developments do you have experience applying a safety standard such as SAE ARP4754, MIL-STD-882C/D or UK Defence Standard 00-56 to?	Choice	0	1	2-5	5-10	11+
A10	How many compliance assessments do you have experience undertaking against a software assurance standard such as RTCA/DO-178B or UK Defence Standard 00-55?	Choice	0	1	2-5	5-10	11+
A11	How many compliance assessments do you have experience undertaking against a safety standard such as ARP4754, MIL-STD-882C/D or UK Defence Standard 00-56?	Choice	0	1	2-5	5-10	11+
A12	On how many programs have you developed SOR or SOW clauses pertaining software assurance or safety for acquisition or modification contracts?	Choice	0	1	2-5	5-10	11+
A13	On how many programs have to been required to comply with a software assurance or safety standard due to contractual requirements?	Choice	0	1	2-5	5-10	11+

A14	Do you agree to have your name and organisation published as a contributor to this survey in the survey results?	Choice	Yes	No			
A15	Do you agree to being contacted after the survey for follow up questions regarding your answers to the survey?	Choice	Yes	No			
A16	Are you willing to participate in a workshop to further evaluate the frameworks described by this body of work?	Choice	Yes – definitely	Maybe – time permitting	No		
Part B - Architectural Assurance							
B1	Motivating Issues						
B1.1	Considering your general experience with safety-related and safety-critical systems, to what extent do you agree or disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
B1.1a	There is evidence in contemporary industrial practice of potentially hazardous sources of systematic faults not being adequately treated or mitigated in systems.						
B1.1b	There is evidence of untreated sources of systematic faults preventing or disrupting the design certification and service release of systems.						
B1.1c	There is evidence in contemporary industrial practice of architectural design features being used to provide mitigations (including fault avoidance or fault tolerance) to sources of systematic faults in systems.						
B1.1d	There is evidence in contemporary industrial practice of architectural design features being used to provide layers of defences (i.e. greater than a single defence) against each source of systematic faults in systems.						
B1.1e	There is evidence in contemporary industrial practice of the fail safe design criteria being used as a design philosophy for the mitigation or treatment of sources of systematic faults in systems.						
B1.2	Where specific examples supporting your answers to the above statements can be provided, please provide them.	Narrative					

B2	State of the Practice						
	Treatment of Systematic Faults						
B2.1	Considering your general experience with the application of software assurance standards and safety standards, to what extent do you agree or disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
B2.1a	Sources of systematic faults in aviation systems may be inadequately treated by design practices prompted by the coupling of software assurance practices (e.g. RTCA/DO-178B, UK Defence Standard 00-55 Iss2), with traditional system safety methodologies (e.g. ARP4754/61, MIL-STD-882C/D, UK Defence Standard 00-56 Iss4)						
B2.1b	Inadequate treatment of systematic faults is due in part to limitations in the assessment of requirements validity across the interface between software assurance and safety standards.						
B2.1c	Inadequate treatment of systematic faults is due in part to limitations in evidence showing that the identified behaviours of the system and software are acceptable with respect to safety.						
B2.1d	Inadequate treatment is due in part to the emphasis by current software assurance standards on process adherence rather than critical evaluation of product properties and behaviours.						
B2.1e	Inadequate treatment is due in part to Safety Integrity Levels (SILs) and/or Design Assurance levels (DALs) not having any inherent product behavioural meaning; as they are a means of process mechanisation.						
B2.2	Are there any additional factors that lead to inadequate treatment of systematic faults? What are they?	Narrative					
B2.3	If you believe that the coupling between software assurance practices and traditional system safety methodologies provides robust resolution of sources of systematic faults in practice, explain why?	Narrative					
	Role of Architecture						
B2.4	Read Section 2.2.1 of [ReM10]. To what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
B2.4a	Existing software assurance standards provide certainty that architectural mechanisms will be used to provide fault avoidance and fault tolerance of systematic faults.						

B2.4b	Existing software assurance standards ensure the provision of sufficient evidence of architectural treatments to sources of systematic faults.						
B2.5	If you believe software assurance standards don't provide certainty that architectural mechanisms will be used to provide fault avoidance and fault tolerance, explain why? If you don't believe they do, explain why not?	Narrative					
B2.6	If software assurance standards don't adequately provide architectural certainty, should assurance frameworks explicitly integrate evidence requirements for architectural treatments to systematic faults? Explain why or why not?	Narrative					
Qualifying the Extent of Fault Avoidance and Tolerance							
B2.7	Read Section 2.2.2 of [ReM10]. To what extent do current software assurance standards, and the provision of evidence they require, assist certification authorities establish answers to the question about the following:	Extent	Grossly Insufficient	Insufficient	Minimally Sufficient	Sufficient	Excessive
B2.7a	The effectiveness of the system's tolerance against systematic faults?						
B2.7b	The classes of systematic faults the system is tolerant against, under specific conditions?						
B2.7c	The extent to which any redundancy or other documented fault avoidance or fault tolerance mechanisms may be violated by the occurrence of systematic faults?						
Fail Safe Design Criteria							
B2.8	Read Section 4.0 of [ReM10]. To what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
B2.8a	The Advisory Circular (AC)25.1309 fail safe design criteria are intended to apply to all sources of faults, including both random and systematic sources of faults.						
B2.8b	The AC25.1309 fail safe design criteria are an important consideration when architecting a system.						
B2.8c	The AC25.1309 fail safe design criteria prompt the application of one or more of the following fault avoidance or fault tolerance approaches for each source of fault or failure: redundancy, backup systems, monitors, isolation of systems, components and elements, designed failure effect limits, designed failure path, fault and error tolerance.						
B2.8d	The design philosophy of the AC25.1309 fail safe design criteria is encompassed within existing safety standards.						

B2.8e	Existing safety standards already require sufficient provision of evidence of the application of the design philosophy encompassed within the AC25.1309 fail safe design criteria.						
B2.8f	Existing software assurance standards are explicit regarding requirements for the application of the design philosophy encompassed within the AC25.1309 fail safe design criteria.						
B2.8g	Existing software assurance standards prompt the application of the design philosophy encompassed within the AC25.1309 fail safe design criteria to the software architectural design process.						
B2.8h	Existing software assurance standards require sufficient provision of evidence of the application of the design philosophy encompassed within the AC25.1309 fail safe design criteria.						
	Examination of Real Aviation Systems						
B2.9	[ReM10] presents the results of the examination of several real world aviation systems with respect to fault avoidance and fault tolerance. Table 3 of [ReM10] presents a set of generalised observations regarding the provision of fault avoidance and tolerance with respect to systematic faults. To what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
B2.9a	The layers categories (software, partitioned software, LRU level and system level) identified at Table 3 of [ReM10] are a suitable categorisation of the layers at which fault avoidance or fault tolerance mechanisms might be employed for aviation systems.						
B2.9b	For aviation systems developed/operated/evaluated by your organisation, the number of layers of fault avoidance/tolerance mechanisms inferred by Table 3 of [ReM10] is consistent with the design of your systems (i.e. 3 for catastrophic, 2 for major/hazardous, 1 for minor).						
B2.9c	For aviation systems developed/operated/evaluated by your organisation, the combinational rules for fault avoidance/tolerance mechanisms inferred by Table 3 of [ReM10] are consistent with those systems.						
B2.9d	The aviation systems developed/operated/evaluated by your organisation provide adequate fault tolerance with respect to the fail safe design criteria for sources of systematic faults.						
B2.10	Where possible, describe specific examples of confirmation or counter evidence to Table 3.	Narrative					

B3	General Principles						
	Layers of Defences and Bounding Uncertainty						
B3.1	Read Section 6 of [ReM10]. Section 6 of [ReM10] proposes that one effect of the application fail safe design criteria, and thus the application of layers of fault avoidance/fault tolerance mechanisms, is the degree to which layers bound the uncertainty in sources of faults of any single item/component/system or any single fault avoidance/tolerance mechanism. To what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
B3.1a	<p>The assertions regarding the effects of architecture bounding uncertainty within Section 6.1 of [ReM10] are valid. Specifically:</p> <ul style="list-style-type: none"> With no absence or detection/handling mechanisms, uncertainty is unbounded and will tend to infinity. Therefore this type of architecture should only ever be employed when there is no safety effect. With one (1) absence or detection/handling mechanism, uncertainty may still tend to be very large depending on the extent of the fault coverage. Therefore, a system with only one mechanism layer must not have severe failure modes. With two (2) layers of mechanisms, uncertainty may be very large, but it is likely much less and will often tend towards a finite value depending on the extent to which the classes of cascading faults resolve to the taxonomy at the second layer. Therefore a system with two mechanism layers is suitable for any system except for those with the most severe failure modes, provided the right mechanisms are employed at each layer of course. With three (3) layers of mechanisms, uncertainty may be large, but it is likely much less and will often tend towards a small finite value depending on the extent to which the cascading faults resolve to the taxonomy at the second and third layers. Therefore a system with three mechanism layers is suitable for any system, even those with severe failure modes, provided the right mechanisms are employed at each layer of course. Additional mechanisms may bound the uncertainty further, provided they continue to enforce the resolving of fault classes to those analysed and treatable at the subsequent mechanisms layer. <p>If you believe these assertions are invalid, please explain why?</p>	Narrative					
B3.1b	Even if the uncertainty cannot be quantitatively modelled, the qualitative reasoning provides sufficient motivation for employing one or more layers of fault avoidance/fault tolerance.	Agreement					
B3.1c	There will always be some uncertainty, no matter how much evidence there is.						
B3.1d	If there will always be some uncertainty, no matter how much evidence there is, a single fault avoidance or fault tolerance mechanism can never provide absolute confidence that a source of systematic fault will not violate the layer of defence.						

B3.2	It is plausible that architectural assurance could be based on measures of effectiveness of layers of defences against sources of systematic faults.						
B3.3	It is plausible that the more severe the consequences of a fault on the system’s behaviour, the more effective the layers of defences against sources of systematic faults should be.						
B3.4	It is plausible that the effectiveness of the layers of defences against source of systematic faults is based on one or more of the following factors: the number of layers, the extent to which layers may be violated by coincident fault effects, the independence of the layer from the initiating fault condition, the appropriateness of detecting and handling a fault class at the level of system abstraction (e.g. software, LRU, system level).						
B4	Our Approach						
	ASAL Definition						
B4.1	The ASAL concept is defined by Tables 4 and 5 of [ReM10]. To what extent do you agree or disagree with the following statements.	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
B4.2a	The ASAL framework’s implementation of the treatment of systemic faults through fault avoidance/tolerance is consistent with the design philosophy of the AC25.1309 fail safe design criteria? If not, explain why?						
		Narrative					
B4.2c	Prescribing ASAL levels (Tables 4 and 5 of [ReM10]) based on Failure Condition Severity (i.e Catastrophic, Hazardous/Major, Minor and No Safety Effect) is feasible.	Agreement					
B4.2d	Prescribing ASAL levels (Table 4 of [ReM10]) based on the number of systematic faults the system must be resilient against is feasible.						
B4.2e	Prescribing ASAL levels (Table 5 of [ReM10]) based on the layers at which fault avoidance or fault tolerance mechanisms should be provided is feasible.						
B4.2f	Requiring that evidence of coverage of classes of systematic faults (i.e. omission, commission, early, late, value) be required in showing compliance Table 4 of [ReM10] is a feasible way of ensuring classes of faults are not left untreated.						
B4.2g	The ASAL framework prescribes useful product benchmarks. Explain why or why not?						
		Narrative					
B4.2h	The layer benchmarks prescribed by the ASAL framework are feasible for the development of real aviation systems? Explain why or why not?	Agreement					
		Narrative					

B4.2i	The benchmarks prescribed by the ASAL framework are useful for design agencies as design requirements to be imposed on a design. Explain why or why not?	Agreement					
		Narrative					
B4.2j	The benchmarks prescribed by the ASAL framework (Table 4 of [ReM10]) do not overly restrict design flexibility. Explain why or why not?	Agreement					
		Narrative					
B4.2k	The benchmarks prescribed by the ASAL framework (Table 5 of [ReM10]) do not overly restrict design flexibility. Explain why or why not?	Agreement					
		Narrative					
B4.2l	The insight into the extent to which fault avoidance / fault tolerance has been employed in the software system architecture is useful for a certification authority conducting certification assessments. Explain why or why not?	Agreement					
		Narrative					
B4.2m	It is feasible that Tables 4 and 5 of [ReM10] would be sufficient to ensure the adequate provision of evidence for certification authority certification evaluation of architectural assurance of systematic faults. Explain why or why not?	Agreement					
		Narrative					
B4.2n	Architectures or their associated constraints can be identified from other real world examples of safety-related or safety-critical systems which are grossly inconsistent with the ASAL concept. What are they and why?	Agreement					
		Narrative					
B4.2o	<p>The benefits of the ASAL concept described in Section 7.3 of [ReM10] are valid. Specifically:</p> <ul style="list-style-type: none"> • The ASAL concept explicitly integrates requirements for architectural treatments to systematic faults into the traditional assurance approach, and is compatible with the existing safety analysis of [ARP4754] and other similar standards. • The ASAL concept provides a multidimensional (better than binary) perspective on the absence and detection/handling of systematic faults commensurate with the worst credible failure condition. • The ASAL concept quantifies (in the product context) the degree of fault tolerance within a system and its software for each system's contribution to aircraft level failure conditions. Therefore, the ASAL as a level inherently has a product meaning. • The ASAL concept is simple, and therefore doesn't burden assurance frameworks with complex, non-objective prescriptions. • The ASAL concept doesn't prescribe specific architectures, and is therefore, inherently flexible. It instead focuses on the treatment of systematic faults by the architecture. • The ASAL concept encourages fault tolerance architectures for the systems whose functions most need fault tolerance (i.e. those with the most severe hazards or failure conditions) • The ASAL concept is analytically compatible with observations of systematic fault tolerance management in actual aviation systems. 	Agreement					
		Narrative					

	Explain why or why not? Are there any additional benefits?						
B4.2p	<p>The limitations of the ASAL concept described in Section 7.4 of [ReM10] are valid. Specifically:</p> <p>The explicit integration of the ASALs with software assurance standard (e.g. RTCA/DO-178B) objectives hasn't yet been clarified.</p> <p>The ASAL concept sets no benchmarks for the level of evidence required to demonstrate that numbers of diverse systematic faults do not contribute to identified failure modes. The ASAL concept does not address 'how much is enough?' for software evidence.</p> <p>The ASAL concept relies on bounding uncertainty, of which a fundamental factor is the extent to which faults at one layer of abstraction resolve to a detectable set at the next layer of abstraction. However, the ASAL concept doesn't provide an explicit measure of the specific contextual claims about detecting and handling systematic faults as they propagate to high levels of system abstraction, and thus support inferences about the suitability of the proposed detection and handling capabilities of the system architecture.</p> <p>Explain why or why not? Are there any additional limitations?</p>	Agreement					
		Narrative					
ASAL Framework Application							
Certification Assessments/Audits by Certification Authority (complete only if you have certification authority experience)							
B4.3	Considering the ASAL framework concept from the perspective of a certification assessment or audit, to what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
B4.3a	Making explicit system and software requirements pertaining to fault avoidance and fault tolerance mechanisms providing defences against sources of systematic faults is beneficial to the certification assessment/audit process. Explain why or why not?						
		Narrative					
B4.3b	It is beneficial to the compliance assessment/audit process to have evidence explicitly related (e.g. by traceability) to fault avoidance and fault tolerance mechanisms, rather than the relationship being implicit.	Agreement					
B4.3c	Current safety and software assurance standards employed already provide evidence of fault avoidance and fault tolerance that makes the effectiveness of these mechanisms explicit to the certification authority.						

B4.3d	Limitations in certification authority visibility via evidence of system treatments (i.e. fault avoidance and fault tolerance mechanisms) such as those prompted by the ASAL framework concept would not inhibit a successful certification assessment.						
B4.4	Provide answers to the following questions:	Narrative					
B4.4a	During certification assessments, is review of evidence improved if the starting point for evidence traceability and assessment was system/software safety requirements pertaining to architectural behaviours and fault tolerance? Does the architectural basis to the ASAL framework provide useful means for achieving this?	Narrative					
B4.4b	Assuming a situation where the ASAL framework has been contracted for (i.e. contract SOR clauses specifically reference Tables 4 and 5 of [ReM10]), what drawbacks are there to the application of the ASAL framework as a compliance assessment/audit framework/benchmark?	Narrative					
B4.4c	Assuming a situation where other standards have been contracted for (i.e. contract SOR and SOW reference relevant sections of RTCA/DO-178B), what drawbacks are there to the application of the ASAL framework as a compliance assessment/audit tool?	Narrative					
B4.4d	Does the ASAL framework improve the knowledge about the level of safety of a software system over existing assurance approaches? Why or why not?	Narrative					
B4.4e	What is your overall belief regarding the useability of the ASAL framework for addressing the motivating issues and limitations with the current state of practice identified earlier within these survey questions?	Narrative					
B4.4f	Is your organisation willing to undertake trial application of the ASAL concept as a benchmark for one of your compliance assessment/audit activities for the purposes of further validation?	Narrative					
	Development by Design Agency (complete only if you have design agency experience)						
B4.5	Consider the ASAL framework concept from the perspective of application to a real system development by your organisation, to what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
B4.5a	Making explicit system and software requirements pertaining to fault avoidance and fault tolerance mechanisms providing defences against sources of systematic faults is beneficial to the design development process. Explain why or why not?	Narrative					
B4.5b	It is beneficial to the design development process to have evidence explicitly related (e.g. by traceability) to fault avoidance and fault tolerance mechanisms, rather than the relationship being implicit.	Agreement					

B4.5c	Current safety and software assurance standards employed already provide evidence of fault avoidance and fault tolerance that makes the effectiveness of these mechanisms explicit to the certification authority.						
B4.5c	Design agencies experience problems getting equipment certified because current standards do not provide a consistent means of satisfying the certification authority about the level of safety provided by a design. It is feasible that the ASAL framework may improve this situation.						
B4.6	Provide answers to the following questions:	Narrative					
B4.6a	Assuming a situation where the ASAL framework has been contracted for (i.e. contract SOR clauses specifically reference Tables 4 and 5 of [ReM10]), what drawbacks are there to the application of the ASAL framework as a design development benchmark by designers?	Narrative					
B4.6b	Assuming a situation where other standards have been contracted for (i.e. contract SOR and SOW reference relevant sections of RTCA/DO-178B), what drawbacks are there to the application of the ASAL framework as a design development benchmark by designers?	Narrative					
B4.6c	What is your overall belief regarding the useability of the ASAL framework for addressing the motivating issues and limitations with the current state of practice identified earlier within these survey questions?	Narrative					
B4.6d	Is your organisation willing to undertake trial application of the ASAL concept to one of your developments for the purposes of further validation of this research?	Narrative					
Part C - Claims and Evidence Assurance							
C1	Motivating Issues						
C1.1	Read Section 2.1.1 of [RMc10]. Considering your general experience with assurance standards applicable to safety-related and safety-critical systems, to what extent do you agree or disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C1.1a	Safety assurance standards should set product safety outcomes (i.e. product safety benchmarks).						
C1.1b	Safety assurance standards should set evidence provision requirements (i.e. benchmarks for the sufficiency of evidence provision).						
C1.1c	Safety assurance standards should set process requirements (i.e. prescription of methods and techniques, development lifecycle and transition criteria).						
C1.1d	Safety assurance standards should not limit process (i.e. application of methods and techniques) flexibility at all.						

C1.1e	Safety assurance standards should limit process flexibility directly by prescribing the techniques or methods acceptable to development.
C1.1f	Safety assurance standards should limit process flexibility indirectly by setting benchmarks for evidence provision from which limitations in evidence will implicitly identify limitations in process, methods and techniques.
C1.1g	Safety assurance standards should not set benchmarks for evidence provision (i.e. evidence provision will be entirely flexible).
C1.1h	Safety assurance standards should not limit design flexibility at all.
C1.1i	Safety assurance standards should only limit design flexibility in that unsafe designs would not comply with the standard.
C1.1j	Safety assurance standards should not concern themselves with product safety, and only focus on evidence provision.
C1.1k	Safety assurance standards should concern themselves with both product safety (i.e. by specification of product safety benchmarks), and evidence provision (i.e. by specification of evidence provision benchmarks).
C1.1l	Safety assurance standards should ensure that products that comply with the standard have a consistent product safety basis for complying.
C1.1m	Consistency in the outcomes of safety assurance standards should be established through the provision of product safety benchmarks.
C1.1n	Consistency in the outcomes of safety assurance standards should be established through the provision of evidence provision benchmarks.
C1.1o	Consistency in the outcomes of safety assurance standards should be established through both the provision of product safety and evidence provision benchmarks.
C1.1p	Consistency in the outcomes of safety assurance standards should be achieved through the certification authority's compliance assurance activities.
C1.1q	When a shortfall exists against a safety assurance standard, the standard should facilitate the product safety impact of the shortfall in product safety terms (i.e. explicit increase in risk).
C1.1r	The definition of objectives and outcomes of a safety assurance standard should ensure that the impact of any non-compliance has a specific product meaning.
C1.1s	It is sufficient for shortfalls against a safety assurance standard to have meaning only with respect to the software lifecycle, and have no inherent product safety meaning.

C1.1t	There is evidence in industrial practice of confusion over the role of assurance levels in safety assurance standards.						
C1.1u	There is evidence in industrial practice of confusion over the application of assurance levels in safety assurance standards.						
C1.1v	There is evidence in industrial practice of confusion over evidence requirements for demonstrating safety of systems.						
C1.2	Where specific examples supporting your answers to the above statements can be provided, please provide them.	Narrative					
C2	State of Practice						
C2.1	Read Section 2.1.1 of [RMc10]. To what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C2.1a	The assurance levels used in RTCA/DO-178B don't have any inherent system/software product meaning; they are prescriptions of objectives and software lifecycle activities.						
C2.1b	The integrity levels used in UK Defence Standard 00-55 Iss 2 don't have any inherent product meaning; they are prescriptions of software lifecycle activities and methods.						
C2.1c	The integrity levels used in other software assurance standards don't have any inherent product meaning. Provide examples where necessary?						
		Narrative					
C2.1d	In general, the objectives/criteria of current software assurance standards (e.g. RTCA/DO-178B, UK Defence Standard 00-55 Iss 2) are all expressed as outcomes/achievements of the development lifecycle, rather than in terms of their contribution to assuring behaviours of the software product with respect to safety.						
C2.1e	Assurance or integrity levels are a useful means of prescribing criteria tailored to specific circumstances (i.e. often based on failure condition severity).						
C2.1f	Assurance or integrity levels as a concept (broader than just those that exist in current standards) should not form part of assurance standards as their lack of system/software product focus cannot be overcome.						
C2.1g	Current assurance standards provide an adequate approach for the purposes of system safety certification until better evidence based with product meaning assurance standards can be developed.						

C3	General Principles						
	Key Principles of Assurance Level Definitions						
C3.1	Section 2.3 of [RMd10] describes five key principles of assurance level definitions. To what extent do you agree/disagree with them as follows:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C3.1a	It is plausible that assurance levels should have an inherent product meaning – i.e. they should be a measure of some physical property of the product and its behaviours, and non-satisfaction of the assurance level criteria should directly infer a product behavioural difference. Explain why or why not?						
		Narrative					
C3.1b	It is plausible that assurance levels should focus on outcomes rather than activities – i.e. they should not concern themselves with specific techniques or methods, but instead set objective benchmarks for properties of the product that should be established. Explain why or why not?	Agreement					
		Narrative					
C3.1c	It is plausible that an assurance framework should make explicit the relevance of the claims underpinning the assurance level definition – i.e. what does complying with the assurance level actually directly achieve. Explain why or why not?	Agreement					
		Narrative					
C3.1d	It is plausible that the assurance level framework should include a mechanism for inferring the relationship between any given technique and method, and the outcomes or objectives they satisfy by ensuring that the factors/properties underpinning each objective are explicit. Explain why or why not?	Agreement					
		Narrative					
C3.1e	It is plausible that an assurance framework should be goal setting in terms of outcomes and objectives of the framework, and only as prescriptive in premises as necessary to ensure explicit benchmarking for compliance with respect to the product related behaviours of the software. Explain why or why not?	Agreement					
		Narrative					
C3.2	Are there any key principles or factors that the above principles don’t include?	Narrative					
	Relationship to Architectural Definitions						
C3.3	Read Section 2.4 of [RMc10]. To what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C3.1a	It is plausible that evidence assurance should not be independent of product assurance requirements.						
C3.1b	Providing an explicit linkage between a product (and thus architectural) assurance paradigm and						

	an evidence assurance paradigm is plausible to ensure the evidence assurance paradigm maintains a product focus.								
C3.1c	The generic designation as a ‘constraint’ on the behaviour of the system and its software, for any absence or detection/handling mechanism used to provide a layer of defence against a source of systematic faults, is plausible. Explain why or why not?	Narrative							
C3.1d	Using the ‘constraint’ concept as a means of linking architectural assurance and claims/evidence assurance provides a plausible focus point for claims and evidence assurance.	Agreement							
C3.1e	There are more plausible means than providing a linkage between architectural assurance and claims/evidence assurance than using the concept of a ‘constraint’. Please describe?	Narrative							
C4	Out Approach								
	CSAL Definition								
C4.1	Read Sections 3 and 3.1 of [RMd10]. Please answer the following questions?	Narrative							
C4.1a	<p>The CSAL concept is intended to qualify the assurance of the ‘constraint’ based on taxonomy of factors that might transpire to violate the ‘constraint’. The factors are:</p> <ul style="list-style-type: none"> certainty in sources of violations internal to the constraint implementation, which include: <ul style="list-style-type: none"> intended and unintended behaviours of the implementation of the ‘constraint, the degree to which the behaviours are systematically accounted for, and the certainty in sources of violations related to and external to the constraint implementation (e.g. relationships to other functions, environment, context, etc). <p>Does this approach seem feasible? Explain why or why not?</p>	Narrative							
C4.1b	<p>The CSAL levels are defined based upon distinct qualification of certainty/uncertainty in sources of violation of the ‘constraint’. The core idea being to set evidence benchmarks (in claim groups, and evidence sufficiency rules) to bound uncertainty. The qualifications are as follows:</p> <ul style="list-style-type: none"> the remaining uncertainty would unlikely lead to a violation of the ‘constraint’ under any credible circumstances (CSAL3) the remaining uncertainty would only lead to a violation of the ‘constraint’ under unexpected circumstances (CSAL 2) the remaining uncertainty could lead to a violation of the ‘constraint’, but this would not be expected under normal operating conditions that would exercise the ‘constraint’ 	Narrative							

	(CSAL1) Does this approach to qualification seem feasible? Explain why or why not?						
C4.2c	Five CSAL levels (of which the upper bound CSAL 4 is for definition purposes only and is not used) are defined: No Assurance, Limited Assurance, Nominal Assurance, Near Absolute Assurance, Absolute Assured (not used). Is the number of levels feasible? Explain why or why not? Are more or fewer levels feasible?	Narrative					
C4.2d	Table 1 of [RMc10] sets guiding principles for the substantiation of claims and provision of evidence with respect to satisfaction of attributes of the software lifecycle products. These guiding principles are intended to provide general categories for claims and evidence grouping on which more specific claims/evidence can be based. Is it feasible that these guiding principles correlate to the CSAL level definitions?	Narrative					
C4.2e	In terms of completeness, are there any guiding principles that have been omitted in the list presented for CSAL 3, CSAL2, or CSAL 1?	Narrative					
C4.2f	In terms of apportionment, are there alternative ways of apportioning the set of guiding principles between CSAL levels that provides better alignment to the level definitions? What are they?	Narrative					
C4.2g	While some non-exclusivity is unavoidable, are these guiding principles categories sufficient mutually exclusive such that an argument could be made about their completeness of categorisation? Explain why or why not?	Narrative					
	Systematically Accounting for Intended and Unintended Behaviours						
C4.3	Read Section 3.2 of [RMc10] to examine in more detail the general evidence categories defined in Table 1 of [RMc10]. To what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C4.3a	<i>Specified behaviours with respect to the ‘constraint’</i> provides a feasible category of evidence against which evidence can be provided of validity and satisfaction of the specification of requirements of the ‘constraint’. Explain why or why not?						
		Narrative					
C4.3b	<i>Refined behaviours with respect to the ‘constraint’</i> provides a feasible category of evidence against which evidence can be provided of the validity and satisfaction of any refined behaviours of the ‘constraint’ at a chosen level of abstraction. Explain why or why not?	Agreement					
		Narrative					
C4.3c	<i>Refined behaviours with respect to the ‘constraint’</i> provides a feasible means of integrating evidence from software design, software architecture, and model based developments and other modelling activities that are abstracted from the implementation. Explain why or why not?	Agreement					
		Narrative					

C4.3d	<i>Implementation behaviours with respect to the 'constraint'</i> provides a feasible category of evidence against which evidence can be provided regarding potential sources of violation at the implementation level. Explain why or why not?	Agreement					
		Narrative					
C4.3e	<i>Implementation behaviours with respect to the 'constraint'</i> provides a feasible means of integrating evidence relating to implementation language properties (constructs, vulnerabilities), and other properties pertaining to source code. Explain why or why not?	Agreement					
		Narrative					
C4.3f	<i>Introduced or generated behaviours that may violate the 'constraint'</i> provides a feasible category of evidence against which evidence can be provided regarding translations of source code into executable object code. Explain why or why not?	Agreement					
		Narrative					
C4.3g	<i>Introduced or generated behaviours that may violate the 'constraint'</i> provides a feasible means of integrating evidence relating to compiler translation, traceability into executable object code, and additional behaviours introduced during translation. Explain why or why not?	Agreement					
		Narrative					
C4.3h	<i>Target computer behaviours that may violate the 'constraint'</i> provides a feasible category of evidence against which evidence can be provided regarding the behaviour of the implementation on the target computer. Explain why or why not?	Agreement					
		Narrative					
C4.3i	<i>Target computer behaviours that may violate the 'constraint'</i> provides a feasible a means of integrating evidence relating to target computer initialisation properties, memory management, arithmetic handling behaviours, target computer failure modes, I/O failures, etc. Explain why or why not?	Agreement					
		Narrative					
C4.3j	<i>Conditions or behaviours external to the 'constraint', but internal to the system, that may violate the 'constraint'</i> provides a feasible category of evidence against which evidence can be provided to show that other behaviours of the system don't violate the constraint. Explain why or why not?	Agreement					
		Narrative					
C4.3k	<i>Conditions or behaviours external to the 'constraint', but internal to the system, that may violate the 'constraint'</i> provides a feasible means of presenting non-interference evidence of containment or mediation between the 'constraint' and other behaviours, functions and dependencies of the software system. Explain why or why not?	Agreement					
		Narrative					
C4.3l	<i>Conditions or behaviours external to the system that may violate the constraint</i> provides a feasible category of evidence against which evidence can be provided to show that other conditions or behaviours initiated from factors external to the system don't violate the 'constraint'. Explain why or why not?	Agreement					
		Narrative					
C4.3m	<i>Conditions or behaviours external to the system that may violate the constraint</i> provides a feasible means of presenting non-interference evidence of containment or mediation between the 'constraint' and environmental and contextual factors. Explain why or why not?	Agreement					
		Narrative					

	ASAL to CSAL Relationship						
C4.4	Read Section 4 of [RMc10]. To what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C4.4a	It is feasible that there is a linear/proportional relationship between architectural assurance ASAL levels (resilience in terms of layers of defence against systematic faults) and claims assurance CSAL levels (the degree of uncertainty in key properties relating the 'constraint' to potential sources of violation of the 'constraint'). Explain why or why not?						
		Narrative					
C4.4b	It is feasible that claims assurance is also related to failure condition severity, as is achieved by inference through linear/proportional relationships to architectural assurance. Explain why or why not?	Agreement					
		Narrative					
C4.4c	The mechanism for specifying CSAL levels for Additional Detection and Handling Mechanism in Table 2 of [RMc10] is feasible. Explain why or why not?	Agreement					
		Narrative					
C4.4d	Table 2 of [RMc10] provides a feasible means of linking ASAL and CSALs. Explain why or why not?	Agreement					
		Narrative					
C4.4e	It is feasible that defence in depth provided by layers of adequately assured 'constraints' is more important to achieving safety than reliance on single highly assured 'constraints'.	Agreement					
C4.4f	Although not strictly part of the CSAL framework, is it feasible that for claims assurance to be used to provide additional strength for one layer to mitigate the need for one or more requisite layer? Explain why or why not?	Narrative					
C4.4g	Are there any factors which have been missed that effect the proposed ASAL to CSAL relationship in Table 2 of [RMc10]? Please explain?	Narrative					
	Attributes of Software Lifecycle Products						
C4.5	Read Section 6 and Annex A to [Rmc10]. To what extent do you agree/disagree with the following:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C4.5a	It is feasible that attributes based on outcomes/results of a set of generic software lifecycle products (i.e. evidence categories/types) (rather than the techniques or methods that produced the results) can be defined as the basis of an assurance framework. Explain why or why not?						
		Narrative					

C4.5b	Basing a set of attributes based on coverage of: requirements validity, requirements satisfaction and requirements traceability for each software lifecycle product (i.e. evidence) category provide confidence the set of attributes is comprehensive. Explain why or why not?	Agreement					
		Narrative					
C4.5c	Should configuration consistency should also be addressed within the set of attributes, or should it be addressed at the evidence level, as it is more a property pertaining directly to a piece of evidence?	Agreement					
		Narrative					
C4.5d	The set of attributes for each software lifecycle product class is adequate (Annex A to [RMc10]). Explain why or why not?	Agreement					
		Narrative					
C4.6	What attributes have been missed, or what attributes are inappropriate?	Narrative					
ESAL Definition							
C4.7	The ESAL concept is defined by Table 3 of [RMc10]. To what extent do you agree/disagree with the following:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C4.7a	Basing evidence assurance on the tolerability of limitations in evidence provision is feasible because the set of evidence will never be infinite/absolute.						
C4.7b	The tolerability of limitations concept is useful because it prompts direct consideration of the limitations in an article or type of evidence.						
C4.7c	The tolerability of limitations concept is useful because it prompts direct consideration of how one article or type of evidence may be combined with other evidence to resolve limitations.						
C4.8a	<p>The ESAL levels are defined based upon distinct qualification of tolerability of limitations with respect to assuring an attribute of a software lifecycle product with respect to the ‘constraint’. The core idea being to set evidence benchmarks (in terms of permissible gaps in evidence) to bound uncertainty. The qualifications are as follows:</p> <ul style="list-style-type: none"> • limitations (in relevance, trustworthiness or results) in evidence would be intolerable (ESAL 3) • limitations (in relevance, trustworthiness or results) in evidence would be tolerable provided those limitations are constrained (ESAL 2) • limitations (in relevance, trustworthiness or results) in evidence would be tolerable (ESAL 1) <p>Does this approach to qualification seem feasible? Explain why or why not?</p>	Narrative					

C4.8b	It is plausible to consider tolerability of limitations as the extent to which: <ul style="list-style-type: none">the limitations of each method or technique are systematically identified and treated where practicable by the application of complementary methods and techniquesnon-treatment of a limitation should not introduce uncertainty disproportionate to the limitation such that it would likely lead to a violation of the constraint. Is this concept plausible? Why or why not?	Narrative					
C4.8c	Relevance (implying both directness and coverage) of evidence, trustworthiness of evidence and result of evidence are properties of evidence and are used as the basis for the ESAL framework. It is feasible that they are adequate?	Narrative					
	Trustworthiness of Evidence						
C4.9	An alternative approach to the general limitations approach described by Table 3 of [RMc10] is specified in Table 4 of [RMc10] for benchmarking the trustworthiness of evidence. To what extent do you agree/disagree with the following statements with respect to Table 4:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C4.9a	Trustworthiness of evidence is characterised by the extent to which the results of the evidence might be misrepresented in their correctness.						
C4.9b	Trustworthiness of evidence is highly subjective and derivative of human involvement in the product of evidence.						
C4.9c	Trustworthiness is a function of developer competency, reviews and inspection effectiveness (approach, competency, independence), and the application of mechanistic or conceptual independence. Why or why not are these sufficient?						
		Narrative					
C4.9d	Qualifying human competencies is difficult, even with the aid of competency frameworks.	Agreement					
C4.9e	Table 4 of [RMc10] provides a feasible approach to benchmarking trustworthiness of evidence. Explain why or why not?						
		Narrative					
C4.9f	Table 4 of [RMc10] is overly prescriptive, and thus could not be feasibly be complied with for real developments. Explain why or why not, and provide examples if possible?	Agreement					
		Narrative					

C4.9g	A different approach that instead relies on identification and treatment of the following factors would be more feasible than that specified by Table 4 of [RMc10]. Factors would include: <ul style="list-style-type: none"> • limitations with developer competency, • limitations in review and inspections: approaches, competencies, and independence • limitations in mechanistic and conceptual independence 	Agreement					
	Framework Application						
	Certification Assessments/Audits by Certification Authority (complete only if you have certification authority experience)						
C4.10	Considering the CSAL/ESAL framework concept from the perspective of a certification assessment or audit, to what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C4.10 a	Making explicit the categories of evidence and the attributes thereof, is beneficial to the certification assessment/audit process. Explain why or why not?	Narrative					
C4.10 b	It is beneficial to the compliance assessment/audit process to have evidence explicitly related (e.g. by traceability) to ‘constraints’.	Agreement					
C4.10 c	Current safety and software assurance standards employed already provide adequate benchmarks for evidence sufficiency that are explicit to the certification authority.						
C4.10 d	Limitations in certification authority confidence of evidence sufficiency would not inhibit a successful certification assessment.						
C4.11	Provide answers to the following questions:	Narrative					
C4.11 a	During certification assessments, is review of evidence improved if the evidence is categorised based on software lifecycle product attributes that generically apply to any ‘constraint’? Does the evidence basis to the CSAL/ESAL framework provide useful means for achieving this?	Narrative					
C4.11 b	Assuming a situation where the CSAL/ESAL framework has been contracted for (i.e. contract SOR clauses specifically reference Tables 1 to 3 and Annex A of [RMc10]), what drawbacks are there to the application of the CSAL/ESAL framework as a compliance assessment/audit?	Narrative					
C4.11 c	Assuming a situation where other standards have been contracted for (i.e. contract SOR and SOW reference relevant sections of RTCA/DO-178B), what drawbacks are there to the application of the CSAL/ESAL framework as a compliance assessment/audit tool?	Narrative					

C4.11d	Does the CSAL/ESAL framework improve the knowledge about sufficiency of evidence over existing assurance approaches? Why?	Narrative					
C4.10e	Does the CSAL/ESAL framework when combined with the ASAL framework improve the knowledge about the level of safety of a software system over existing assurance approaches? Why?	Narrative					
C4.10f	What is your overall belief regarding the useability of the CSAL/ESAL framework for addressing the motivating issues and limitations with the current state of practice identified earlier within these survey questions?	Narrative					
C4.10g	Is your organisation willing to undertake trial application of the CSAL/ESAL concept as a benchmark for one of your compliance assessment/audit activities for the purposes of further validation?	Narrative					
	Development by Design Agency (complete only if you have design agency experience)						
C4.12	Consider the CSAL/ESAL framework concept from the perspective of application to a real system development by your organisation, to what extent do you agree/disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
C4.12a	Making explicit the categories of evidence and the attributes thereof, is beneficial to the system development process. Explain why or why not?						
		Narrative					
C4.12b	It is beneficial to the system development process to have evidence explicitly related (e.g. by traceability) to ‘constraints’.	Agreement					
C4.12c	Current safety and software assurance standards employed already provide adequate benchmarks for evidence sufficiency that are explicit to the certification authority.						
C4.12d	Design agencies experience problems getting equipment certified because current standards do not provide a consistent means of satisfying the certification authority about the level of safety provided by a design. It is feasible that the CSAL/ESAL framework may improve this situation.						
C4.13	Provide answers to the following questions:	Narrative					
C4.13a	Assuming a situation where the CSAL/ESAL framework has been contracted for (i.e. contract SOR clauses specifically reference Tables 1 to 3 and Annex A of [RMc10]), what drawbacks are there to the application of the CSAL/ESAL framework as a design development benchmark by designers?	Narrative					
C4.13b	Assuming a situation where other standards have been contracted for (i.e. contract SOR and SOW reference relevant sections of RTCA/DO-178B), what drawbacks are there to the application of the CSAL/ESAL framework as a design development benchmark by designers?	Narrative					

C4.13c	What is your overall belief regarding the useability of the CSAL/ESAL framework for addressing the motivating issues and limitations with the current state of practice identified earlier within these survey questions?	Narrative					
C4.13d	Is your organisation willing to undertake trial application of the CSAL/ESAL concept to one of your developments for the purposes of further validation of this research?	Narrative					
Part D - Contracting for Assurance of Military Aviation Software Systems							
D1	Motivating Issues						
D1.1	Read Section 1 of [ReM12]. Considering your general experience with assurance standards applicable to safety-related and safety-critical systems, to what extent do you agree or disagree with the following statements:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
	Standards Paradigm: Goal-based or Prescriptive?						
D1.1a	It is plausible that the paradigm of the safety assurance standard (i.e. goal-based or prescriptive) is a crucial factor for achieving effective regulation through contracts.						
D1.1b	It is plausible that the paradigm of the safety assurance standard (i.e. goal-based or prescriptive) is a crucial factor for achieving adequate provision of evidence to the regulatory authority from the supplier.						
D1.1c	Goal-based standards permit substantial flexibility for designers, which give benefit in defining effective products.						
D1.1d	Application of goal-based standards may lead to limitations with respect to establishing contractually enforceable benchmarks for evidence and argument sufficiency and suitability.						
D1.1e	Prescriptive standards set clear benchmarks for evidence and activity completion.						
D1.1f	Application of prescriptive standards may lead to limitations in relevance of the evidence to achievement of product safety objectives.						
D1.1g	The regulatory and safety assurance paradigm used should be compatible with the contracts used, without impairing or detracting from the achievement of system safety.						
D1.1h	Contracts which provide cost and schedule certainty are preferred by both suppliers and acquirers.						
	Integrating the Standard's Lifecycle with the Tender/Contract Lifecycle						
D1.1i	The integration of the safety assurance standard with the contractual lifecycle is a crucial factor in the achievement of safety regulation via the contract.						

D1.1j	The safety assurance standard should assist in reducing uncertainty about the delivered product, argument and evidence prior to the establishment of a contract (i.e. through tender processes).					
D1.1k	Both acquirer and supplier will be seeking confidence that the contract will be successful prior to entering into the contract.					
D1.1l	Should safety issues emerge during the contract, then timely and cost effective resolution will be a goal for both supplier and acquirer.					
D1.1m	The contract and standard should support the resolution of safety issues, and not hinder it by contributing uncertainty to the dispute.					
D1.1n	There is evidence in industrial practice of project slippages, overruns or cancellations due to issues concerning safety assurance and certification.					
D1.1o	There is evidence in industrial practice that limitations in current approaches may be contributing to project slippages, overruns or cancellations					
D1.2	Where specific examples supporting your answers to the above statements can be provided, please provide them.	Narrative				
	Differences with Military System Acquisition Contracts					
D1.3	Read Sections 2 and 3 of [ReM12]. To what extent do you agree or disagree with the following:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree
D1.3a	Regulatory enforcement is enabled by the contract rather than via laws for the military circumstance.					
	Impact of Uncertainty at Contract Signature					
D1.3b	It is plausible that uncertainty in the specification of design requirements and provision of assurance evidence through the contract may increase the risk of the contract being unsuccessful.					
D1.3c	It is plausible that information regarding design solution, safety argument and evidence, if sought and used effectively during tender processes, can reduce uncertainty, and thus reduce potential contract success risks.					

D2	State of Practice						
D2.1	To what extent do you agree or disagree with the following:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
D2.1a	Information on integration between the safety assurance standard lifecycle and contract lifecycle varies significantly between standards.						
D2.1b	ARP4754 and RTCA/DO-178B make no mention of integration with contracts as the means of evidence provision.						
D2.1c	It is plausible that the certification authority liaison and artefact requirements within ARP4754 and RTCA/DO-178B could be used to achieve potential contract integration, and safety regulation via contract.						
D2.1d	It is plausible that the certification authority liaison and artefact requirements within ARP4754 and RTCA/DO-178B could be used to achieve safety regulation via a contract.						
D2.1e	UK Defence Standard 00-56 Issue 4 doesn't address requirements on contracts for provision of arguments or evidence.						
D2.1f	MIL-STD-882C and D contains guidance on contract integration throughout, including specific references to contract clauses, tender processes and data requirements.						
D2.1g	Used in isolation to design requirements, MIL-STD-882C/D achieves safety regulation through contracts.						
D2.1h	How to seek the right information and effectively evaluate it with respect to safety for military aviation software systems is still very much a challenge.						
D2.1i	Existing standards and contracting approaches offer limited guidance on how safety assurance standard and contract integration might be achieved effectively.						
D2.1j	Existing standards and contracting approaches offer limited guidance on how safety regulation may be achieved through contractual mechanisms.						

D3	General Principles						
D3.1	To what extent do you agree or disagree with the following:	Agreement	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
D3.1a	It is plausible that a trade-off between the benefits of limitations of goal-based and prescriptive standards may achieve effective safety regulation via contracts.						
D3.1b	It is plausible that obtaining architectural certainty from the tender phases and prior to entering into a contract enables early insight into potential architectural shortfalls that may impact safety.						
D3.1c	It is plausible that obtaining architectural certainty from the tender phases and prior to entering into a contract enables supplier consideration of architectural suitability including the application of fault avoidance and fault tolerance mechanisms.						
D3.1d	It is plausible that architectural certainty may in part be achieved by the setting of benchmarks for solution architectural suitability.						
D3.1e	Benchmarks should not be specifying solutions so they do not stifle novelty or limit flexibility; they should instead set measurable criteria against which different solutions can be evaluated.						
D3.1f	It is plausible that reducing architectural uncertainty at the time of contract signature can be achieved through a tender phase mechanism that informs the acquirer of the proposed architecture.						
D3.1g	It is plausible that architectural suitability information requested through the tender processes permits evaluation of the extent to which the holistic safety and software architecture requirements are costed into the tender response.						
D3.1h	The retrospective incorporation of constraints to treat systematic failure modes is rarely straightforward, particularly when architectural change is required.						
D3.1i	It is in the acquirer's interests to establish the extent to which the contractor has determined an architecture based on the types of constraints required to meet safety objectives.						
D3.1j	Although many sub-system architectures may not be well defined for large system acquisitions the tender phase, it is plausible that the absence of this information in a tenderer's response may be overcome by adjusting the contractors proposed costing by a risk figure based on the amount of uncertainty (or extent of suitability) in the tenderers proposed architecture.						
D3.1k	Monitoring throughout the contract is important because it allows the acquirer to measure the progression of the architecture throughout the contract lifecycle, and to respond early if there are divergences to acquirer understanding and assumptions from the tender evaluation.						

D3.2	To what extent do you agree or disagree with the following:
D3.2a	The set of evidence supplied is never infinite (because we don't have infinite time or money), thus the assurance it provides is never absolute; so there will always be limitations in the totality of evidence.
D3.2b	The evidence produced from each method or technique will always have some limitation with it, and complementary evidence from one or more methods or techniques will usually be required to resolve the limitation.
D3.2c	As there will always be limitations in the evidence; it is plausible to determine if the limitations in argument and evidence are tolerable in the specific context?
D3.2d	It is plausible that obtaining argument and evidence certainty from the tender phases and prior to entering into a contract enables early insight into potential argument and evidence shortfalls.
D3.2e	It is plausible that forcing explicit context agreement between acquirer and supplier on the measures of argument and evidence sufficiency as part of the contract requirements removes uncertainty post contract signature regarding argument and evidence sufficiency.
D3.2f	It is plausible that argument and evidence certainty may in part be achieved by the setting of benchmarks for argument and evidence suitability.
D3.2g	Benchmarks should not be specifying specific techniques or methods such that they stifle novelty or limit flexibility; they should instead set measurable criteria against which argument and evidence can be evaluated.
D3.2h	It is plausible that reducing argument and evidence uncertainty at the time of contract signature can be achieved through a tender phase mechanism that informs the acquirer of the proposed argument and evidence.
D3.2i	It is plausible that argument and evidence suitability information requested through the tender processes permits evaluation of the extent to which the provisioning of argument and evidence are costed into the tender response.
D3.2j	By requiring each tenderer to explicitly justify the adequacy of their software development against a predefined set of criteria, then it is plausible that suppliers are provided a consistent set of expectations for costing their software development programs and understanding adequacy.
D3.2k	The retrospective supplementation of argument and evidence to treat argument and evidence shortfalls is rarely straightforward, particularly when argument change is required, or evidence is require from additional techniques and methods.
D3.2l	It is in the acquirer's interests to establish the extent to which the contractor has determined the sufficiency of their argument and evidence against acquirer expectations/benchmarks.

Agreement

D3.2m	Monitoring throughout the contract is important because it allows the acquirer to measure the suitability of argument and evidence throughout the contract lifecycle, and to respond early if there are divergences.						
D4	Our Approach						
	Obtaining Architectural Certainty						
D4.1	<p>[ReM12] proposes a four step process is proposed for obtaining solution architectural certainty, as follows:</p> <ol style="list-style-type: none"> 1. Set measurable benchmarks for architectural suitability 2. Inform architectural suitability using the tender process 3. Evaluate architectural suitability during the tender evaluation, and 4. Provide architectural assurance during contract execution. <p>It is feasible that the following process could obtain architectural certainty? Explain why or why not?</p>	Narrative					
	Setting Benchmarks for Architectural Suitability						
D4.1a	<p>[ReM12] proposes that SOR clauses could communicate the solution properties regarding the requisite number of layers of fault tolerance and avoidance/detection and handling requirements. The following is an example of a generic SOR clause to achieve this:</p> <p><i>The [System Name] architecture and mechanisms for achieving fault avoidance and fault tolerance, against each type of credible systematic fault, shall meet the requirements for layers of fault avoidance and fault tolerance, where the number of layers is commensurate with the worst credible failure condition, as specified at {reference a Table in the SOR detailing the benchmark numbers of layers for each failure condition severity}</i></p> <p>Is it feasible that such an approach could set benchmarks for architectural suitability? Explain why or why not?</p>	Narrative					
	Informing Architectural Suitability						
D4.1b	<p>[ReM12] proposes that one possible approach would be to require the tenderer, through the tender SOW, to provide a Conceptual System and Software Architecture Suitability Document. The document would describe how the system's architecture and mechanisms for achieving fault tolerance against systematic faults would meet the benchmarks established above. The intent is to provide a description of the architecture at a level of fidelity that the acquirer can evaluate against the benchmark, without forcing the supplier to completely design and implement the system before contract signature. For a largely mature design, the document can focus on what already exists, and whether or not it requires supplementation; for a</p>	Narrative					

	<p>developmental design it provides a framework for the supplier to cost the architectural elements of their system with improved accuracy. The following is an example of the generic Tender SOW clauses to achieve this:</p> <p><i>The [Tenderer] shall prepare a [Conceptual System and Software Architecture Suitability Document] per TDRL XX to describe how the [System Name] architecture and mechanisms for achieving fault avoidance and fault tolerance, against each type of credible systematic fault, is proposed to meet the {reference to SOR's requirements for layered fault avoidance and fault tolerance of systematic faults}.</i></p> <p><i>The [Tenderer] shall prepare a [Conceptual System and Software Architecture Suitability Document] per TDRL XX to describe how each proposed constraint (i.e. absence/detection and handling mechanism) is proposed to achieve the architecturally layered fault tolerance requirements as defined by the SOR {reference the SOR requirement}.</i></p> <p>Is it feasible that such an approach could inform architectural suitability through the tender process. Explain why or why not?</p>						
	Evaluating Architectural Suitability						
D4.1c	Section 5.3 of [ReM12] proposes that architectural suitability can be evaluated by assessing the architectural description against the specific architectural benchmarks. It is feasible that such an approach could evaluate the suitability of proposed architectural solutions.	Narrative					
	Providing Architectural Assurance						
D4.1d	<p>Section 5.4 of [ReM12] proposes that under the contract, the acquirer will need to achieve two things. The first is that they will need to maintain the benchmarks for product suitability by inclusion of SOR, clauses similar to those defined in Section 5.1, but for the contract. Further the acquirer will require means to establish if the final 'as-delivered' architecture meets the prescribed benchmarks. This can be achieved by requiring the contractor to deliver (via appropriate SOW contract clause) a System and Software Architectural Assurance Document. The document would describe how the system's architecture and mechanisms for achieving fault tolerance against systematic faults actually achieves the benchmarks established above. The following is an example of the generic Contract SOW clauses to achieve this:</p> <p><i>The [Contractor] shall prepare a [System and Software Architectural Assurance Document] per CDRL XX to describe how the [System Name] architecture and mechanisms for achieving fault avoidance and fault tolerance, against each type of credible systematic fault, meets the {reference to SOR's requirements for layered fault avoidance and fault tolerance of systematic faults}.</i></p> <p><i>The [Contractor] shall prepare a [System and Software Architectural Assurance Document] per CDRL XX to describe how each proposed constraint (i.e. absence/detection and handling mechanism) achieves the architecturally layered fault tolerance requirements as defined by the</i></p>	Narrative					

	<p><i>SOR {reference the SOR requirement}.</i></p> <p>The Contract Data Requirements List (CDRL) should require that various iterations of the document be delivered at relevant system engineering milestones to permit the acquirer to monitor the evolution of the architecture under the contract.</p> <p>Is it feasible that such an approach could provide architectural assurance? Explain why or why not?</p>						
	Obtaining Argument and Evidence Certainty						
D4.2	<p>[ReM12] proposes a four step process is proposed for obtaining argument and evidence certainty, as follows:</p> <ol style="list-style-type: none"> 1. Set benchmarks for argument and evidence suitability 2. Proposal of argument and evidence using the tender process 3. Evaluate argument and evidence suitability during the tender evaluation, and 4. Provide argument and evidence assurance during contract execution. 	Narrative					
	Setting Benchmarks for Argument and Evidence						
D4.2a	<p>Section 6.1.1 provides one possible approach to setting benchmarks for arguments. The approach is based on a set of generic sub-claims with respect to a generic categorisation of software lifecycle products which can be related to specific product focused ‘constraints’.</p> <p>Is it feasible that such an approach could set benchmarks for argument/claims suitability in a tender/contract? Explain why or why not?</p> <p>Section 6.1.2 provides one possible approach to setting benchmarks for evidence. The approach is based on the generic properties of evidence including relevance, trustworthiness and results.</p> <p>Is it feasible that such as approach could set benchmarks for evidence suitability in a tender/contract? Explain why or why not?</p>	Narrative					
	Proposal of Argument and Evidence						
D4.2b	<p>Section 6.2 of [ReM12] proposes that one possible approach would be to require the tenderer, through the tender SOW, to provide a Software Assurance Plan to describe which set of claims are going to be demonstrated for each ‘constraint’. To ensure consistency in tenderer responses it is advantageous to align where possible the claims to the generic software lifecycle products and the generic attributes of each. The following is an example of a generic Tender SOW to achieve this:</p> <p><i>The [Tenderer] shall prepare a [Software Assurance Plan] per TDRL XX to propose the attributes that will be assured, for each software lifecycle product, for each constraint</i></p>	Narrative					

	<p><i>described in the [Conceptual System and Software Architecture Suitability Document].</i></p> <p>To reduce uncertainty about the intended limitations in evidence for each of the aforementioned attributes at the time of contract signature, the tender phase also requires a mechanism to provide information on the likely scope of the body of evidence and its potential limitations. One possible approach would be to require the tenderer, through the tender SOW, to provide two things:</p> <ol style="list-style-type: none"> 1) a Software Development Plan to describe which methods and techniques are going to be applied across the development, and 2) a Software Assurance Plan to describe how any limitations in the evidence produced from the methods and techniques described in the software development plan are tolerable with respect to relevance, trustworthiness and results. <p>The following is an example of a generic Tender SOW clause to achieve this:</p> <p><i>The [Tenderer] shall prepare a [Software Development Plan] per TDRL XX to describe the methods and techniques proposed to be used throughout the software development lifecycle, including description of techniques or methods used prior to this development but for which evidence is relevant.</i></p> <p><i>The [Tenderer] shall prepare a [Software Assurance Plan] per TDRL XX to describe how the evidence produced from the application of the [Tenderer] proposed methods and techniques is proposed to assure tolerability of limitations in evidence with respect to relevance, trustworthiness and results, for each attribute of each software lifecycle product, for each constraint described in the [Conceptual System and Software Architecture Suitability Document].</i></p> <p>Is it feasible that such an approach could inform argument and evidence suitability through the tender process? Explain why or why not?</p>						
	Evaluation of Argument and Evidence						
D4.2c	Section 6.3 of [ReM12] proposes that argument and evidence suitability can be evaluated by assessing the proposed argument and evidence against the specific argument and evidence benchmarks. Is it feasible that such an approach could evaluate the suitability of proposed argument and evidence assurance?	Narrative					
	Providing Argument and Evidence Assurance						
D4.2d	Section 6.4 of [ReM12] proposes that under the contract, the acquirer will require a means to establish if the final ‘as-delivered’ claims and evidence meets the prescribed benchmarks. This can be achieved by requiring the contractor to deliver (via appropriate SOW contract clause) a Software Assurance Summary Document. The document would describe how the assurance of the ‘attributes’ of software lifecycle products actually achieves the benchmarks established	Narrative					

	<p>during tender processes. The following is an example of the generic Contract SOW clauses to achieve this:</p> <p><i>The [Contractor] shall prepare a [Software Assurance Summary] per CDRL XX to describe the attributes that have been assured, for each software lifecycle product, for each constraint described in the [System and Software Architecture Document].</i></p> <p><i>The [Contractor] shall prepare a [Software Assurance Summary] per CDRL XX to describe how the evidence produced from the application of the [Contractor] proposed methods and techniques has assured the tolerability of limitations in evidence with respect to relevance, trustworthiness and results, for each attribute of each software lifecycle product, for each constraint described in the [System and Software Architecture Document].</i></p> <p>Is it feasible that such an approach could provide argument and evidence assurance? Explain why or why not?</p>						
	Contracting Framework Application						
	Cost Implications						
D4.3	To what extent are costs impacted by the framework:	Cost (Relative)	Much Lower	Lower	About the Same	Higher	Much Higher
D4.3a	The proposed framework will feasibly result in relative tender costs to contractors versus current standards.						
D4.3b	The proposed framework will feasibly result in relative tender costs to acquirers versus current standards.						
D4.3c	The proposed framework will feasibly result in relative contract costs to contractors versus current standards.						
D4.3d	The proposed framework will feasibly result in relative contract costs to acquirers versus current standards.						
D4.3e	Describe any cost implications with respect to the proposed framework?	Narrative					
	Schedule Implications						
D4.4	To what extent is schedule impacted by the framework:	Schedule (Relative)	Much Shorter	Shorter	About the Same	Longer	Much Longer
D4.4a	The proposed framework will feasibly result in relative tender schedule to contractors versus current standards.						

D4.4b	The proposed framework will feasibly result in relative tender schedule to acquirers versus current standards.					
D4.4c	The proposed framework will feasibly result in relative contract schedule to contractors versus current standards.					
D4.4d	The proposed framework will feasibly result in relative contract schedule to acquirers versus current standards.					
D4.4e	Describe any schedule implications with respect to the proposed framework?	Narrative				
	Systems Engineering Lifecycle Implications					
D4.5	Describe any systems engineering lifecycle implications to the proposed framework over and above contemporary practice?	Narrative				
	Project Management Implications					
D4.6	Describe any project management implications to the proposed framework over and above contemporary practice?	Narrative				
	Contract Management Implications					
D4.7	Describe any contract management implications to the proposed framework over and above contemporary practice?	Narrative				
	Resolution within Contract Scope					
D4.8	<p>Section 7 of [ReM12] proposed that one way to provide resolution within the contract scope is to make absolutely explicit this requirement for limitations to be resolved to the satisfaction of the acquirer through a statement of work line item. This line item can then be costed and suppliers will be empowered to resolve such issues. An example of how this might be achieved is as follows:</p> <p><i>Intolerable Limitations in Evidence, Claims or Architecture Where the [Acquirer]'s certification evaluation establishes that the [Contractor] has not achieved the requirements of the {reference applicable SOR and SOW clauses relevant to architecture, argument and evidence}, or there are shortfalls in the 'Tolerability of Limitations' of evidence, then the [Contractor] shall undertake one or more of the following remediation actions to resolve the shortfalls to the satisfaction of the certification authority: engineering change to architectural constraints, engineering change to implementation of architectural constraints, or additional analysis, verification and validation by further or supplementary application of methods or techniques. The [Contractor] shall amend all relevant deliverables per the CDRL to incorporate the engineering changes and additional evidence.</i></p> <p><i>Note to Contractors</i></p>	Narrative				

	<p><i>The above clause provides the means for the certification authority to address shortfalls against architecture, argument and evidence expectations. While this clause may be interpreted to result in unbounded programmatic risk for the contractor, the intent is to focus both acquirer and contractor efforts at establishing unambiguous consensus during the tender process and contract negotiations.</i></p> <p><i>The contractor should not sign the contract if they believe there remains substantial uncertainty regarding the provision of evidence against the framework, and instead request further clarification during contract negotiations.</i></p> <p>It is feasible to achieve resolution within the scope of the existing contract in this way? Clearly this approach is very dependent on the extent to which the framework reduces uncertainty. Is the uncertainty sufficiently reduced that this approach is feasible?</p>		
	Useability		
D4.9	What is your overall belief regarding the useability of the contracting framework for addressing the motivating issues and limitations with the current state of practice identified earlier within these survey questions?	Narrative	
D4.10	Is your organisation willing to undertake trial application of the contracting concept to one of your developments for the purposes of further validation of this research?	Narrative	