

Consolidated Survey Responses

Id#	Survey Question	Question Category	Answers				
Part A - Demographic							
A1	Please provide your name, position and organisation.	Narrative	Respondents from the following organisation contributed to this survey. Australian Defence Organisation (Royal Australian Air Force, Defence Materiel Organisation, Defence Science and Technology Organisation) UK Ministry of Defence Defence Science and Technical Laboratories Defense Contract Management Agency USAF Aeronautical Systems Centre Engineering USG Software Verification Agency New Zealand Defence Force Beca Applied Technologies New Zealand Critical Systems Labs Canada BAE Systems Australia Ultra Electronics UK QinetiQ UK Raytheon Australia Nova Defence and Nova Systems Australia FAA DERs				
A2	How many years of experience do you have developing safety-related or safety-critical systems?	Choice	0-2 4	3-5 3	6-10 6	11-15 4	16+ 3
A3	How many years of experience do you have undertaking compliance assessments on safety-related or safety-critical systems?	Choice	0-2 2	3-5 5	6-10 7	11-15 3	16+ 3
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 10	3-5 3	6-10 2	11-15 3	16+ 2

A5	What domain do you presently work in?	Choice	Aviation 13	Maritime 1	Land 1	Information Systems 3	Other 2
A6	What type of organisation do you work for?	Choice	Military 5	Professional Service Provider 4	Commercial Developer 4	Government 4	Other 3
A7	What type of work do you undertake?	Choice	Development 4	Integration 4	V&V 5	Compliance Assessment 10	Other 2
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 2	1 5	2-5 8	5-10 4	11+ 1
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 2	1 7	2-5 8	5-10 1	11+ 2
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 7	1 4	2-5 4	5-10 2	11+ 3
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 5	1 4	2-5 5	5-10 4	11+ 2
A12	On how many programs have you developed SOR or SOW clauses pertaining software assurance or safety for acquisition or modification contracts?	Choice	0 5	1 3	2-5 7	5-10 3	11+ 2
A13	On how many programs have to been required to comply with a software assurance or safety standard due to contractual requirements?	Choice	0 2	1 4	2-5 10	5-10 2	11+ 2
A14	Do you agree to have your name and organisation published as a contributor to this survey in the survey results?	Choice					
A15	Do you agree to being contacted after the survey for follow up questions regarding your answers to the survey?	Choice	Yes 19	No 1			
A16	Are you willing to participate in a workshop to further evaluate the frameworks described by this body of work?	Choice	Yes – definitely 6	Maybe – time permitting 11	No 3		

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.				2	10	8
B1.1b	There is evidence of untreated sources of systematic faults preventing or disrupting the design certification and service release of systems.				2	11	7
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.				2	9	9
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.			1	2	8	9
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.			1	2	12	5
B1.2	Where specific examples supporting your answers to the above statements can be provided, please provide them.	Narrative	On an undisclosed project. B1.1.a some industries are doing a better job than others through the standards in use and how compliance with the standards is enforced. Therefore in the good industries, this statement will be less true than in the not as good type of industries. Aircraft industry would be in the “good” industry category. Sometimes some hazard sources have actually been overlooked or not identified during analysis. There are a number of situations where hazards have been overlooked during analysis and where incidents/accidents occurred. Even in the situation where hazards have been identified during analysis, mitigation may not be appropriate. Have seen a number of programs where software, LRU, system and procedural measures have been put in place to mitigate systematic faults. These have included designs that				

			<p>apply both fault avoidance & fault tolerance techniques.</p> <p>Experience suggests single layer of mitigation to single point failures only. Have seen large inconsistencies in approaches depending on project / team.</p> <p>The architectural design of the A380 APEX is also supported with ARINC data buses.</p> <p>Most platform fail safe is on the basis of functional failure. Consideration of systematic failure, if considered, will be addressed in the software development. However, compliance will deemed to have been addressed by a process defined by a safety objective, i.e. Software Level or Software Integrity level.</p> <p>Partitioning being used as a barrier between critical functions (i.e. OFP and mission-specific applications or GPWS)</p> <p>The answers entirely depend on the specific contractor. Where for instance a contractor has had considerable experience, especially in the civil world, then I could easily say all negative answers would all become strongly positive (e.g. B1.1a and b). The opposite tends to be true for new entrants and military only contractors, especially from the US because of the apparent low bar set by DoD and the general lack of knowledge of these issues and the apparent national defence (Read : ‘commercial’ or/and ‘litigation’) interests of these contractors to give access to evidence. This is because the customer community(s) – the market – in each case has different expectations. As you point out in your papers, the drivers are different and it essentially comes down to the market and how well it is regulated.</p>
--	--	--	---

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)			2	2	12	4
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.			2	1	13	4
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.				1	15	4
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.			4	1	10	5
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.			2	2	12	4
B2.2	Are there any additional factors that lead to inadequate treatment of systematic faults? What are they?	Narrative	Inadequate treatment due to a programme focus on system ‘features’ rather than protection mechanisms. Lack of education resources, training in this area Lack of uniform software approach available (but case by case approaches are usually adopted) Legacy approach to use redundant hardware Inexperience (supplier and buyer), complexity, cost and schedule impacts of applying comprehensive integrity/assurance programs. Isolating software development from system. Leads to incomplete understanding of system requirements. The passage of system requirements to the Hardware / Software development puts greater emphasis on the capability and performance requirements in relation to safety requirements. The number of System Safety				

			<p>Assessments that provide the safety objective as the mitigation is numerous. The question of how a safety related software function is protected is often left unanswered or mitigated by restatement of compliance to the safety objective (procedural).</p> <p>Safety requirements, rarely identified, need to be traceable to the functional failure or hazard. Mitigation i.e. software protection mechanisms need to aligned to the safety requirement.</p> <p>Lack of competency.</p> <p>I think your papers tend to conflate hardware architecture and software architecture as one idea and this should not be the case. Defence against systematic faults can be achieved through either approach (not necessarily an exclusive OR). Suggest that software architecture may help with systematic failures of hardware (e.g. defence against cascading faults) and vice versa. Maybe the characterisation and list of the faults we are trying to defend against would be useful. I will send you a list of the ‘things we are afraid of’ in software – i.e. a bug list which might help.</p> <p>Inadequate identification of sources of systematic faults.</p>
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	<p>There are weaknesses, which in my limited experience, are due to a focus on feature requirements rather than safety requirements.</p> <p>I don't.</p> <p>The link is weak and tenuous.</p> <p>System Safety and Software and Aircraft engineers may not connect enough direction development of a project. Huge projects can easily lead to faults slipping through the cracks.</p> <p>Don't believe.</p> <p>It is not necessarily the case that I believe that that they do or do not, it is that they can if used properly. For instance, I have ‘Strongly Disagreed’ with B2.1e. If SILs/DALs are used naively then I could agree with the statement. The problem is that there is no link between an activity in the</p>

			software development process and the mitigation of a hazard. This is unlike in mechanical design where, for example, a strut is designed with known properties of the metal (within a statistical bound), the expected load it will undergo enabling stress/strain/torsion/etc. calculations, add a safety factor (say x1.5) and therefore a claim that ‘systematically’ the strut will ensure safety within the design load constraints. Actually, we mean statistically, rather than ‘systematically’. So unless we can say something like ‘because the software is free from e.g. pointer errors, the wings will therefore never be subject to undue loads’ we would appear to be stuck.				
	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.		5	14	1		
B2.4b	Existing software assurance standards ensure the provision of sufficient evidence of architectural treatments to sources of systematic faults.		4	12	2	2	
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	Software Assurance Standards only focus on applying a commensurate level of rigour to the software lifecycle process, and does not explicitly direct developers to apply architectural mechanisms for fault avoidance and tolerance. Apart from the vague guidance surrounding the definition of a software architecture and achievement of partitioning integrity (in DO-178B), there is very little a developer can leverage upon with respect to employing architectural mechanisms for avoidance and tolerance of systematic faults. Software assurance standards tend to get applied at the software level, rather than at the system level. Lack of specific objective in the architecture area that relate to fault avoidance and fault tolerance				

			<p>My experience with any software assurance standard is DO-178B. With some exceptions, focus of DO-178B appears to be applying varying levels of rigor and independence in planning, development, testing & verification, config management, quality, etc., commensurate with criticality level. There is far less focus on the product architecture, the failure behaviour or level of evidence required.</p> <p>Whilst architecture is used, and provides a diagrammatic concept of the software, such architectural handling of faults does not bound error conditions to that section of code. For instance, a systematic buffer overrun may have impacts in architecturally unrelated code. I therefore do not agree that certainty can be had that architectural mechanisms can provide fault tolerance.</p> <p>Software assurance standards do not provide certainty hence assurance. They rely on the passage of safety attributes from the system design. Should the safety related function transferred from system to software be without its safety protection (requirement) then there is no direction for the architectural design to incorporate the appropriate protection.</p> <p>With multiple suppliers all making products with differing 'interpretations' of DO-178B (etc.), the prime integrator may not know all the ways that fault avoidance and tolerance are dealt with to ensure the system-level product is safe and effective.</p> <p>They provide a degree of confidence only.</p> <p>Having re-read 2.2.1 at least twice over, I am convinced that you are conflating hardware and software architecture, In which case, your argument is flawed. I believe that there is sufficient mechanism in CS2X.1309, ARP4754 and DO178 to provide the hooks for sufficient argument for safety from a system perspective. Whether it could be stronger, esp in 4754 is an interesting point (I have yet to get hold of ARP4754A). If you solely look at DO178 for architectural safety then you will never find it because DO178 is not a 'software safety standard' even though it</p>
--	--	--	---

			<p>often is thought of as being so and hence you will never get the safety mitigation you might be looking for out of it.</p> <p>That said, if someone set out to intelligently argue why what they have produced by meeting DO178 objectives meets system safety objectives, then I can see how that might and has been achieved.</p> <p>Very limited measures of architectural treatments to faults in software assurance standards.</p> <p>They don't really deal with architecture, more process focused.</p> <p>Safety standards tend to deal with architecture more so than software standards from a fault treatment perspective.</p> <p>The safety standards deal with fault treatment, software standard deal with fault / error removal or prevention.</p>
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	<p>Yes, this would be a useful idea, as it will provide developers with a set of guidance for producing evidence that the software architecture they have established adequately mitigates the risk of systematic failures, commensurate with the level of safety integrity that has been assigned to the software item.</p> <p>There would be benefit in providing a system level assurance framework to address fault tolerance at the system level when required.</p> <p>It would be nice. Certainly more should be done to produce evidence of architectural treatments of systematic faults. However issues may be in the details to be provided and in the level of granularity used. I suspect a significant amount of work would have to be done to describe the expectations in terms of artifacts in this area. I wonder if this topic was brought up in the SC-205 / DO-178C group and what was the outcome of any discussion.</p> <p>Yes. The resulting evidence would aid in the compliance assurance and certification process.</p> <p>Architectural treatments of faults in software should be evidenced. However, such a treatment is not sufficient to</p>

			catch all systematic faults. Yes it would be appropriate, if only it was know what the protection mechanism should be, derived from system analysis perhaps. Unless all functional software requirements are to be treated the same irrespective of safety objective. Yes – if cost effective for potential system failure. Again, are you talking about software or hardware? I don’t believe that this can adequately be achieved by software alone and hence cannot further answer the question. Yes. Assurance and safety need to be an integrated approach				
	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?			7	7	6	
B2.7b	The classes of systematic faults the system is tolerant against, under specific conditions?		4	5	7	4	
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?		3	6	8	3	
	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.			1	1	7	11
B2.8b	The AC25.1309 fail safe design criteria are an important consideration when architecting a system.				2	6	12
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,				2	5	13

	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.		4	4	9	3			
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.	2	5	5	5	3			
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.	3	11	4	2				
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.	6	8	3	3				
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.	4	10	3	3				
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.		1	1	2	13	4		
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).		1	1	2	14	3		
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.		1	1	3	11	4		
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.			3	1	12	4		
B2.10	Where possible, describe specific examples of confirmation or counter evidence to Table 3.	Narrative	Table follows the idea behind Reason's Swiss Cheese model for accident causation. Overall, a sound, though complicated set of 3 of 4 projects meet the criteria of the table. I am currently involved in an aircraft mission system						

			development that has fault tolerance requirements in the spec. It uses amongst other things distributed and dissimilar hardware/software, exception handlers, board and LRU level independent watchdog timers, and the ability to handover/reconfigure to operate in degraded modes. I am far from certain how to interpret Table 3. For instance, does one read L to R or the other way (bold is evaluated last). I think I am supposed to infer that something has failed at some level that leads to an accident? An example, or better still 2+, of how the table is supposed to be read might be helpful, but there are too many caveats to make sense. Perhaps you have tried to put what might be a series of flow diagrams into a table? Hence my strong disagreements and my lack of example to argue for or against your proposals. Not all solutions would comply with the table, but some of the solutions that doesn't comply may have a reduced level of safety or confidence in safety.				
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	The assertions regarding the effects of architecture bounding uncertainty within Section 6.1 of [ReM10] are valid. Specifically: <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			2	3	11	4
		Narrative	Some thoughts: It is rather difficult to determine the validity of these assertions, due to the uncertain nature of latent defects (or systematic faults). Certainly, the idea behind the layering of detection and handling mechanisms at different levels of abstraction is sound, and intuitively it makes sense that uncertainty in the occurrence systematic faults would decrease as the number of mechanisms for detecting and handling them (and at different levels of abstraction) increases. Ultimately however, doesn't this rely on an				

	<p>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.</p> <ul style="list-style-type: none"> • 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>	<p>assumption that the detection and handling mechanism is in itself perfect? Otherwise, wouldn't a level of design assurance commensurate with the failure category also apply to the development of those detection and handling mechanisms?</p> <p>The gap between two layers (finite value), and three layers (small finite value) offers room for argument of sufficiency of the two layer approach. No doubt three layers are 'better', however an applicant may see the additional layer as an unnecessary burden (cost).</p> <p>In general agreement with these assertions</p> <p>The assertions appear to be a reasonable attempt to block the propagation of the failure.</p> <p>2 or 3 layers is the best approach, with significant testing to back it all up. The onus should be on the prime integrator to test thoroughly to prove this, and to substantiate claims and s/w assurance and associated software levels.</p> <p>They appear to be valid, although the measurement of uncertainty remains a concern.</p> <p>They might be valid, but consider whether the lack of knowledge of how a failure manifests at the first level is the same lack of knowledge throughout all levels. Hence on this basis, we quickly get to the Rumsfeldian 'unknown unknowns'! Can we realistically say that because the software guys did not know how to trap and deal with errors within their software that the system and architecture can deal with it? Well perhaps, but then reverse the argument, if you knew you might have to deal with these errors at the system/architecture level, then perhaps the software guys should be told to sort them out at source.</p> <p>Do you mean by 'handling' that the fault is also correctly isolated? By this I mean that the system will know where (& when) the fault is and what to do about it. If not, detection merely tells you that something is wrong and the system may react incorrectly. For example, incorrectly ignoring one of 2 sources that is deemed to be drifting,</p>
--	--	--

			when the static one should be the source that is ignored. There would appear to be an implicit assumption here of diversity in the detection techniques (as well as the layer) and I am not sure that this is valid. I am also concerned that failure of software in some way can be detected by software and that this might not be considered ‘diverse’ in your scheme. Furthermore, it seems to me that the detection at any level can be implemented by software and hence could itself fail the diversity test. I refer you to the bug list I will send to you as this is a [probably incomplete] list of the ways in which software could fail.				
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		1	1	13	5
B3.1c	There will always be some uncertainty, no matter how much evidence there is.				2	8	10
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.				1	9	10
B3.2	It is plausible that architectural assurance could be based on measures of effectiveness of layers of defences against sources of systematic faults.				1	16	3
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.				1	14	5
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).				2	12	6
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				2	15	3

	avoidance/tolerance is consistent with the design philosophy of the AC25.1309 fail safe design criteria? If not, explain why?	Narrative	It is fair to say it is an interpretation but not necessarily the only interpretation, given my comments re detection above. Doesn't address the probabilistic aspects, but these aren't relevant to systematic faults anyway. Thus what is presented is a reasonable approximation to avoid probability issues.				
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		1	1	14	4
B4.2d	Prescribing ASAL levels (Table 4 of [ReM10]) based on the number of systematic faults the system must be resilient against is feasible.			1	1	15	3
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.			1	1	14	4
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.			1	1	13	5
B4.2g	The ASAL framework prescribes useful product benchmarks. Explain why or why not?					3	14
		Narrative	One can immediately gauge the layers of defences against systematic faults that a certain product possesses. In this way, it may be a suitable means to benchmark products against each other. For ASAL 3, it may be difficult to prove the system is tolerant to all possible combinations of two 'systemic faults' that can be imagined. 'testing for absence' is difficult. Ideally I am inclined to agree but It depends largely on what artifacts and type of documentation the applicants will be expected to provide and how it will be assessed. The ASAL framework shows much promise but may offer false confidence if poorly executed. These tables use keywords such as "independent components", "differing layers of abstraction", "independent of the initiating fault condition", "independent of the proceeding detection/handling mechanism". In today's complex systems do we always fully understand all of the failure paths, or if the design is truly void of common mode failures, and the true level of independence at different				

			<p>levels of abstraction? Is partitioned software a valid layer if it contains some of the same code (and hence exhibits potentially the same systematic faults)?</p> <p>Its conceptual simplicity is its major advantage. It would be relatively straightforward to show compliance with the levels.</p> <p>As I understand your methodology uses artifacts that are commonly produced.</p> <p>Independent levels of detection/handling is key.</p> <p>Accurate measurement of uncertainty.</p> <p>Use of words ‘Prescribing’ and ‘Requiring’ is very strong. As I suggest in the narrative to B4.2a it is perhaps one way of achieving your aim, but not necessarily the only one....hence inclined to disagree. However, there are some interesting concepts which perhaps need to be generalised and if possible simplified.</p> <p>Yes, it makes explicit the requirement for layers of defences.</p> <p>Requires contractors to demonstrate these outcomes, but gives them flexibility in doing so.</p>				
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		1	3	16	1
		Narrative	<p>Already follows a similar methodology prescribed in aviation system safety standards, in terms of integrity levels, and assurance requirements imposed by those levels.</p> <p>There will be many conversations between the regulator and applicant along the lines of : “what about this, what about that”, and “that combination is improbable” .</p> <p>Agree the ASAL framework is feasible, but design agencies and certification authorities need to be well trained in its use and must not apply it blindly. The ASAL should only be used by experienced individuals and is not a substitute for engineering judgment.</p> <p>The benchmarks are non ambiguous, and therefore compliance / design should be easier to provide evidence for.</p>				

			<p>It appears to put greater emphasis on functional protection. Protection methods need to be identified and analyzed for correctness.</p> <p>Puts onus on LRU suppliers and primes alike to document their products detection/handling and behaviours.</p> <p>Feasible or possible is not equal to cost effective.</p> <p>They are an approach, but have some limitations as already explained.</p>				
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		1	2	16	1
		Narrative	<p>Would immediately generate a set of safety requirements resulting from the determination of the ASAL.</p> <p>Agree generally. The comment at B4.2g and B4.2h applies. See above</p> <p>As I understand your concept safety related functions will have width protection at system level (redundancy) and depth protection at LRU and module level.</p> <p>Gives measurable criteria.</p> <p>May give a false impression of defence in depth.</p> <p>Practically speaking, when buying off the shelf – not. Possible for new developments.</p>				
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		1	5	13	1
		Narrative	<p>In theory, it shouldn't. However, there will definitely be some restriction to design flexibility as it requires for instance, the system to accommodate diverse systematic faults.</p> <p>Agree generally for new systems. However there are systems (hardware + software) that have had prior acceptance and have a long and successful service history (e.g., F-16 flight control system). In cases where an option involves re-use of an existing technology, ASAL requirements may be prohibitive and limit good options</p> <p>Agree, but showing independence of fault conditions is non-trivial</p> <p>It does not appear to greatly diverge from what the current</p>				

			<p>standards require.</p> <p>Does not seem unreasonable, but examples would be great.</p> <p>Evaluation of cost/benefit.</p> <p>The view of industry is likely to be yes! Perhaps 2 diverse systematic faults could be enough to achieve the required confidence at Catastrophic, or perhaps 3 is insufficient; what is enough in what context? From a military perspective there are benefits in demanding less because it will be cheaper and are prepared to accept a risk. Not sure that this is necessarily the case in civil aviation, especially where huge automation takes away decisions from the pilot.</p>				
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		1	6	12	1
		Narrative	<p>Agree generally. The comment at B4.2j applies.</p> <p>They do not impose a mechanism / implementation for fault detection, only a level of system abstraction</p> <p>The designer of the system should be considering protection mechanism for each development step, there interaction and independence.</p> <p>Does not seem unreasonable, but examples would be great.</p> <p>As per B4.2j</p>				
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			2	8	10
		Narrative	<p>Any additional evidence wrt assurance against systematic failures would be useful for any certification authority.</p> <p>Provides guidance to examine the entire systems protection mechanisms at all levels, and provides the regulator with visibility how each level contributes to protect against systemic faults.</p> <p>With competencies (and authorizations) of various regulators in specific and defined disciplines (i.e. software) there are possibly weaknesses at the boundaries of each discipline.</p> <p>It's a good start, however whilst application of the ASAL framework may provide increased confidence, it does not specify the level of evidence, or how it is to be achieved,</p>				

			<p>communicated and documented.</p> <p>As fault detection mechanisms are at different abstraction layers, they can be evaluated independently.</p> <p>It provides the confidence that should a systematic fault develop the designer has made provision for the event and verified the system under event conditions.</p> <p>Certifiers must know how fault avoidances/fault tolerance is used in the system.</p> <p>Aids completion requirements.</p> <p>Absolutely agree as it will be part of an argument as to why an aircraft should be allowed to go flying.</p>				
B4.2 m	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	2	4	8	6	
		Narrative	<p>It is feasible to believe that this would be sufficient, since no other standard currently calls out this much evidence. If not sufficient, then I don't know what would be. The question more is – is it feasible that this is a reasonable approach for a certification authority to evaluate architectural assurance of systematic faults?</p> <p>WRT Table 4: Testing, proving, or demonstrating the system is robust against all combinations of every possible two systemic faults may be challenging.</p> <p>What information would a component manufacture be required to provide a system integrator to assist compliance?</p> <p>Comment B4.2l applies.</p> <p>Agree. The tricky bit would be demonstrating the independence of fault conditions.</p> <p>This concept will need to be integrated in to a reliability base solution. Treatment of systematic faults will be undermined should the physical reliability be ignored.</p> <p>May need to expand on methods.</p> <p>This needs to be tested and I have outlined some concerns above.</p> <p>Evidence would be required on the confidence of each layer</p>				

			of defence also. Would also need to address the ‘goodness’ of the demonstration on how these were achieved.				
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		5	10	5	
		Narrative	<p>Depending on the user and unique circumstances, operators may accept different levels of risk (e.g., commercial versus military, peace versus war, the cost of a life – i.e, the many versus the few, etc.). There may be architectures where safety assurance constraints and their associated costs have been traded against other constraints such as time into service, available tools/technologies, availability of a skilled workforce, produceability, etc. For example the military may offset reduced assurance by applying procedural mitigations.</p> <p>Though an example is not at hand, it is possible that there are examples of safety of flight critical systems designed without ASAL like levels of abstraction/independence, that have proven to be acceptably safe. These systems are likely to be simple, well understood and to have evolved after consideration of field data. It would appear that ASAL is more important for new and complex systems where there is little or no precedence, and behavior under all possible circumstances cannot reasonably be determined by testing or analysis.</p> <p>Unsure, space systems which “must be perfect”.</p> <p>Some fault detection is done in software, so is this diverse? I think an Integrated Modular Avionics system would fail to meet this because it has the same hardware throughout with software providing all the functions including, fault detection/isolation and rescheduling of spare equipment to maintain functionality.</p>				
B4.2o	The benefits of the ASAL concept described in Section 7.3 of [ReM10] are valid. Specifically: <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 	Agreement		2	1	13	4
		Narrative	All of these statements appear to hold true. Demonstrating compliance, as outlined above in B4.2m may be difficult (or may be perceived to be ‘too’ difficult).				

	<p>absence and detection/handling of systematic faults commensurate with the worst credible failure condition.</p> <ul style="list-style-type: none"> • 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. <p>Explain why or why not? Are there any additional benefits?</p>		<p>Agree generally. Previous comments apply.</p> <p>Seems simple to prove and implement, but artifact generation is still an open item for designers/integrators.</p> <p>The logic is inescapable for fault types already experienced. What about faults we have yet to experience i.e. unique combination events'?</p> <ul style="list-style-type: none"> • It may be one approach • Agree • Disagree – it outlines a possible confidence mechanism but is not measurable (i.e. the 'degree') and hence is no different than that for, e.g. DO178. • It might be simplistic rather than simple as it ignores certain architectures that could comply with the framework, but fail to meet the required demonstrably safe systems (e.g. IMA) • It effectively prescribes at least part of the architecture. • Agree it forces some thought. • Don't know <p>Might cause both purchaser and developer to think about architecture, but likely to be in a prescriptive, non-flexible manner.</p>				
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</p>	Agreement	1	1	1	14	3
		Narrative	<p>Agree with these limitations, especially the last one regarding its reliance on bounding uncertainty. Ultimately, this framework relies on having the right detection and handling mechanism.</p> <p>These statements appear to hold true. In practice, there may be a requirement for component (LRU) vendors to provide additional guidance to the integrator to make sure system level protection mechanisms are correctly implemented (or vice-versa). This is not a bad thing, but may reduce the ability to take an 'off-the-shelf' approach to systems</p>				

	<p>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>	<p>integration – and therefore increase costs.</p> <p>I see the first two limitations as very important limitations if not major limitations. (If these limitations are not addressed, they may overturn many of the benefits above).</p> <p>If the second limitation is not addressed, it may undermine the whole concepts. Objective based software assurance standards are good up to a point, industry will ask for some guidance on what is expected and what they have to produce. In addition a fairly consistent way of assessing these ASAL should be described. Guidance documents will have to provided.</p> <p>The listed limitations appear valid generally.</p> <p>Previous comments/limitation in this section apply, particularly B4.2h, i.e., consideration is not given to the level of training/experience that would be needed in order for the ASAL framework to work. Also, consideration is not given to how such a framework may be perceived by those that will have it imposed upon them. I say this from experience as in Australia Defence Industry is still coming to grips with DO-178B and the associated costs. This paper does not provide a cost/benefit type argument. Contractors tend to have more of a short term rather than big picture view due to the nature of contracts.</p> <p>However, if the handling of safety requirements derived from the System safety assessment were not bundled into system requirements but given greater prominence would this negate the ASAL concept?</p> <p>Collusion of existing standards may be challenging but worthwhile. Evidence/artifacts still a large open topic.</p> <p>What level of confidence is sufficient?</p> <p>Does it address diversity in detection techniques? Not sure it covers fault isolation and hence could still lead to cascading faults.</p>
--	--	---

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?			1	2	7	5
		Narrative	Having done these audits, I can attest that provision of this type of evidence would be extremely useful in making a certification assessment. To date, much of the evidence provided is process based, and little explicit evidence linking the system architecture’s ability to tolerate faults is presented. Reduces the chance of focusing on ‘process’ compliance (or even feature compliance). It forces safety to be considered as an input to conceptual design/tradeoffs and throughout development/verification. It will command conversation at design reviews and incur safety directed testing/analysis. It will force collaboration and interaction with the certification authority. All of these things are positive. It is easier to demonstrate fault tolerance against faults rather than predict their likelihood. But is this not what is supposed to happen? The safety objective (RTCA/DO-178B Annex A) is defined by the Functional Hazard Analysis. The System Safety Assessment provides the analysis and mitigation for the safety related function. The mitigation is wrapped up as a safety requirement and bundled in with the System requirements thrown over the wall to the software development team. Having mandatory requirements lowers designs chance of missing specifications. Inclined to agree but I think it already is covered and don’t				

			support the ASAL framework Provides product focus. This visibility is usually hard to get by other means. Existing software assurance standards don't provide this information, and safety standards have a probability of failure focus.				
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				10	5
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.			5	4	5	1
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.		1	3	6	2	3
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	1. yes review of evidence would be improved if we start with the software requirements pertaining to architectural behaviours and fault tolerance. 2. The architectural basis to the ASAL framework would be sufficient means to achieving this. The trouble may be that it requires more evidence than what would be sufficient. Yes Yes and yes. Without specific architectural behaviour and fault tolerance requirements there are no grounds for asking for evidence. Without specific requirements, consideration will not be given in the conceptual design. As the conceptual architecture is formed pre-bid, it may not be possible to change the architecture or apply such considerations retrospectively. Yes, a strong, unambiguous framework is helpful in achieving this. I think it would provide a better link to understanding however hazards/critical functional failures have been				

			<p>mitigated in the software.</p> <p>The FAA/EASA may have more visibility than U.S. Military Certification Offices.</p> <p>Yes, starting from the beginning with explicit requirements would be helpful.</p> <p>Not sure it is not giving the engineer a false confidence.</p> <p>It is a starting point and a useful one. Whether ASAL helps is another matter.</p> <p>Yes, it is useful.</p> <p>Yes, it provides an initial product focus against which to relate all evidence.</p> <p>Potentially. Yes.</p> <p>Yes, absolutely.</p> <p>Yes, this is consistent with the FAA Job aid which uses a traceability structured review to examine the evidence.</p>
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	<p>Potential drawbacks to COTS systems since the contractor would be constrained by the existing architecture, and thus compliance to the ASAL framework would be difficult. In the case of developmental systems, one must be very careful that the right low level requirements are developed from the ASAL requirements. Failure to derive relevant architectural requirements from the ASAL framework will inevitably introduce contractual disputes.</p> <p>Testability</p> <p>The certification and acquisition agency may not have the experience and/or skillsets to manage such a program and perform compliance assessment. The ASAL framework could perceivably be used as a reason to keep on asking for more from the contractors. The framework will rely on access to pragmatic individuals who are able to make judgements/decisions on the basis of good experience and reasoned logic.</p> <p>None.</p> <p>An appreciation of the expected outcomes and as stated</p>

			<p>earlier the relationship with system reliability.</p> <p>Would need specific criteria for success.</p> <p>None I can identify.</p> <p>It is overly complex as per comments above.</p> <p>None, it appears useful.</p> <p>No significant drawbacks as a compliance assessment benchmark.</p> <p>Educating developers on what's required.</p> <p>None, the contractor should have costed and planned for the demonstration activities.</p> <p>How it relates to other safety or assurance requirements in the contract would need clarification.</p>
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	<p>The drawback would be related directly to the contractor's interpretation of compliance to the contracted standard, vs the potentially more onerous interpretation of the user, as a result of applying the ASAL framework as a guide to establishing assurance requirements. Hence, any requirements derived from ASAL must be identified up front.</p> <p>Testability</p> <p>How the ASAL framework is integrated with the DO-178B objectives is not clear.</p> <p>There is no defined order of precedence in either standard for potential conflict of requirements.</p> <p>Not currently full understanding the level of integration between the ASAL and Civil standards but my current concern is one of over engineering a solution.</p> <p>ASAL would have to have near-concrete cross-talk to the other standards.</p> <p>Confusion. A potential for lack of experience is a cause for concern.</p> <p>Integration with standards is not yet clear.</p> <p>The other standards may not drive a sufficient architectural focus, and as such the benchmark may not be achieved.</p>

			<p>Addressing compatibility issues between the approaches.</p> <p>The benchmark here may differ from the contractor's interpretation of the standard, and thus the differences may lead to dispute over the work required. If it is used only on the certification authority side to inform risk, then it will probably be useful.</p> <p>It isn't a requirement of the civil framework, so the developer would be working under existing standards. The ASAL framework might be useful as supporting guidance to the job aid reviews.</p>
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	<p>Yes it does. Essentially, the ASAL framework would immediately allow one to gauge the number of independent defences a system's architecture accommodates against systematic failures.</p> <p>Yes, to a high degree.</p> <p>The level of certification evidence is not defined, hence whilst the framework may result in a safer design, it may not automatically improve the level of knowledge.</p> <p>Potentially. All approaches are subject to a level of interpretation.</p> <p>The weakness of the Civil standards is the system/software interface with regards to the passage of safety requirements. The ASAL concept attempts to improve this interface through the imposition of detection and handling mechanisms and therefore as a default improves safety.</p> <p>It adds, by giving clarity.</p> <p>It confuses the situation with respect to what is required by which process to achieve which goal.</p> <p>Yes.</p> <p>Yes.</p> <p>Undecided.</p> <p>Yes – much more targeted at questions that always get asked.</p> <p>It really depends on how well ARP5754 is executed and the</p>

			evidence provided in standard fault trees and FMEAs.
B4.4e	What is your overall belief regarding the usability of the ASAL framework for addressing the motivating issues and limitations with the current state of practice identified earlier within these survey questions?	Narrative	<p>I go back to the importance of carefully defining any derived requirements resulting from the ASAL framework. Its usability is highly dependent on the linkage between it and the defined system/software level requirements.</p> <p>Very usable, but guidance required to clarify the limitations you've identified in Section 7.4</p> <p>It is definitely a positive step in the right direction. It needs to be sold to those that will employ it. It needs to be shown to work via some good and representative case studies. End users need to be appropriately trained. It needs to be integrated with current software assurance standards. The level of evidence required to achieve certification needs to be explicitly defined.</p> <p>Its simplicity leads to clear and unambiguous application. In the requirements, design and implementation stages of a project, as well as during V&V.</p> <p>It is a methodology worthy of further study however; if a robust system/software interface was implemented by good practice the benefit of ASALs would be reduced.</p> <p>ASAL could be useable with further integration with other standards/practices.</p> <p>Useable, but would the additional confidence claimed be real?</p> <p>In my opinion – no because it confuses the issue.</p> <p>It is useful.</p> <p>Based on the explanation in the paper it appears useable, but an example would provide better illustration.</p> <p>Might be useable, but wouldn't be favoured over the current approaches.</p> <p>Seems useable. An example application would be beneficial.</p> <p>It emphasizes architecture which is important. Properly integrated with existing practices, it may be useful.</p>

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	A great idea, that would definitely be worth proposing to technical regulatory authorities within Defence. Yes, subject to approval from senior management. This question is better directed at organisations making compliance findings (e.g., DGTA/Technical Airworthiness Regulator or SPO Project Offices/Design Acceptance Representative). Potentially. Not currently. No. No. No. Perhaps. No.					
	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?			1	3	7	4	
		Narrative	Helps to reduce ambiguity in the accreditation phase of a project, and reduce the risk of major design rework. Helps testing processes.					
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			2	8	5	
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.			3	5	5	2	
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		1	1	3	7	3	

	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	<p>It may be perceived as a cost and schedule burden. A lack of good experience in the subject area would drive up the costs in the bid as it would be seen as a risk area both in terms of development and also in terms of the likely handling by the certification authority. The lack of suitable experience may reduce the number of potential bidders, reduce competition, and hence limit options for the acquisition agency.</p> <p>Design under the proposed framework requires system knowledge at more levels of abstraction. It requires the system designers to be specialist in more fields.</p> <p>Mechanisms would have to be defined, but with deviation allowed by the cert/designer.</p> <p>Perception and reduced flexibility.</p> <p>It is overly complex.</p> <p>Learning curve, different to existing standards.</p> <p>Educating developers on what's required.</p> <p>How it relates to other safety or assurance requirements in the contract would need clarification.</p>					
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	<p>How the ASAL framework is integrated with the DO-178B objectives is not clear.</p> <p>None.</p> <p>Would probably need a clear application of cross-reference.</p> <p>Additional cost.</p> <p>It adds a layer of complexity and confuses the issues.</p> <p>Integration with other standards.</p> <p>Addressing compatibility issues between the approaches.</p> <p>It isn't a requirement of the civil framework, so the developer would be working under existing standards. The ASAL framework might be useful as supporting guidance to the job aid reviews.</p>					

B4.6c	What is your overall belief regarding the usability of the ASAL framework for addressing the motivating issues and limitations with the current state of practice identified earlier within these survey questions?	Narrative	<p>As per B4.4e.</p> <p>As a benchmark and guide the framework goes someway to an easily applicable standard on product development.</p> <p>Needs further investigation, but could be worthwhile.</p> <p>It is a step in the right direction.</p> <p>Already addressed.</p> <p>It may be useful for guiding the application of the fail safe design criteria.</p> <p>Might be useable, but wouldn't be favoured over the current approaches.</p> <p>It emphasizes architecture which is important. Properly integrated with existing practices, it may be useful.</p>
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	<p>I cannot talk on behalf of a global company, however I suggest it would be interested if funded appropriately as an R&D task.</p> <p>Potentially.</p> <p>No.</p> <p>No.</p> <p>No.</p> <p>No.</p>

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).		1	1	1	7	10
C1.1b	Safety assurance standards should set evidence provision requirements (i.e. benchmarks for the sufficiency of evidence provision).					8	12
C1.1c	Safety assurance standards should set process requirements (i.e. prescription of methods and techniques, development lifecycle and transition criteria).		2	4	3	7	3
C1.1d	Safety assurance standards should not limit process (i.e. application of methods and techniques)		2	5	3	7	3

	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.

2	6	7	5	
		2	16	2
3	13	2	2	
2	10	2	4	2
1			10	9
10	7	2	1	
		1	5	14
		1	10	9
	2	2	8	8
	1	3	8	8
		1	10	9
	1	1	13	5
			10	10
			13	7
3	12	4	1	

C1.1t	There is evidence in industrial practice of confusion over the role of assurance levels in safety assurance standards.		2	2	12	4
C1.1u	There is evidence in industrial practice of confusion over the application of assurance levels in safety assurance standards.		1	1	13	5
C1.1v	There is evidence in industrial practice of confusion over evidence requirements for demonstrating safety of systems.		1	1	13	5
C1.2	Where specific examples supporting your answers to the above statements can be provided, please provide them.	Narrative	<p>In my experience auditing Software Development Agencies for compliance against prescribed software assurance standards, there was ample evidence of confusion regarding the SDAs obligations in meeting the requirements of the assurance standard (in this case, DO-178B).</p> <p>The word ‘confusion’ confused me to some extent.</p> <p>I’ve seen evidence of acquisition agencies trying to apply higher levels of assurance to non safety critical systems, i.e, mission systems where failure consequence is a reduction in efficiency/capability only.</p> <p>The whole paper is predicated on software systems and hence there is an issue, especially in context of 2.1.1. I am unaware of any direct link between the fear of a software fault that we think we have defended against and system failure and aircraft accident when it subsequently manifests. Or in your words “what are the structured set of properties of the product and its evidence that permits a conclusion to be directly established that the behaviours are appropriate with respect to safety” (aka the \$64,000 question). I do not agree with much of 2.1.1 especially the implication that assurance standards were written by a collection of well-meaning individuals who did not understand what they were doing! You also say that ‘right conclusions’ are implicit – define ‘right’.</p> <p>The confusion results mostly from inexperience in application of the standards and the requirements of the certification authority.</p>			

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.		1	1	1	10	7
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.		1	1	6	7	5
C2.1c	The integrity levels used in other software assurance standards don't have any inherent product meaning. Provide examples where necessary?		1	1	6	7	5
		Narrative	In the ADF context, I definitely agree that all prescribed assurance standards relating to software development are process, rather than product focussed (including quality assurance methodologies such as CMMI). Only experience with software assurance standards is DO-178B. These standards are an agreed set of best practice and in the case of DO178B, aircraft are not crashing as a result of its use and hence one can conclude that the software product has some safety integrity. Def Stan 00-55 has been avoided so much, it is difficult if not impossible to say how good it is, but has a similar thrust to many other standards (mandating techniques apart). ISO26262 is perhaps the most recently issued new standard (DO178C being merely a revision – technology supplement notwithstanding, not that it is a ‘Standard’ anyway). It has severe weaknesses in that it is has no independent regime for product or evidence review, Highly Recommends techniques and expects then to be used even if others would be better. There’s a lot more wrong with it but these are just 2 of the low lights! IEC61508 and related standards.				
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.				1	11	7

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).				12	6	
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.	5	8	3	2		
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.			3	12	5	
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?			2	4	10	4
		Narrative	Definitely a plausible concept as this would provide some explicit and tangible measure of the product’s ability to meet safety objectives. Non-satisfaction and associated behavior may be difficult to measure / articulate. I am inclined to agree when you talk about product or for top-level systems. However for low-level components, this may be more difficult to achieve or may not even be possible. One of the important aspect of assurance level is the flow down to sub-systems / components / configuration items. If assurance levels have an inherent product meaning then that will force conversations and reviews of fail safe and fault tolerance nature of design and focus on credible failures that have significant consequences. Coverage is not guaranteed by assurance levels that focus on adherence to lifecycle processes. The ultimate goal of product development is to produce an assurable product, not to follow processes.				

			<p>Intangible artifacts/evidence without real meaning for the product is wasted.</p> <p>Should reflect the whole system, but just parts.</p> <p>Depends on whether you are talking about software...see previous answers. There is no physical property of software and hence is not measurable. It's behaviour is to a certain extent dictated by the hardware, so not possible in isolation to determine software behaviour.</p> <p>A product focus would be useful.</p> <p>Or be relatable to a product meaning...</p>				
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		2	2	11	5
		Narrative	<p>I am more inclined for it to focus on both outcomes and activities. Or at least link the outcomes to activities.</p> <p>Guidance to achieving outcomes can happen in two broad ways: Outlining an acceptable means (i.e. a process), or 'trial and error'. There is utility in providing an acceptable means (a process) to eliminate wasted effort.</p> <p>Same as above. I am inclined to agree when you talk about product or for top-level systems. However for low-level components, this may be more difficult to achieve or may not even be possible.</p> <p>One of the important aspect of assurance level is the flow down to sub-systems / components / configuration items.</p> <p>Agree within reason. I don't think an assurance framework can ignore use of a completely inappropriate technique, even if the claimed outcome is OK.</p> <p>Proscribing processing and development methodologies reduces design flexibility, in many cases adding to the cost of a project, with no benefit to the final product.</p> <p>Makes it clear for designers.</p> <p>Where achievable more numerical criteria should be provided.</p> <p>Again, to a certain extent depends on whether you are talking about software. However, I agree that because we may have tested something does not mean it has achieved</p>				

			<p>any particular safety objective. The approach by DO178 is flawed in one respect and that is it does focus on testing rather than assurance of absence of errors. If it was re-written to say that so long as EOC can be assured to be free from error (e.g. missing requirements, presence of all requirements, non-interference by non-executable code – e.g. dead code, etc...see bug list), then we would have a far more concrete measure of the goodness of the code. To a certain extent, this is what the technical supplements to DO178C were supposed to achieve. The closest to achieving this was the Formal Methods supplement. However, throughout the whole tortuous process, there was a red line and that was EOC had to be tested in the target hardware and hence all supplements insist on this. The only exception being the FM supplement - see section FM6.7 esp sub para f. Also see coverage at FM6.7.1 and then finally alternate methods in FM12.3.5.</p>				
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		1	2	13	4
		Narrative	<p>Agree. Such a framework would enable easier justification of activities to achieve the desired outcomes.</p> <p>Provides utility to the regulator in assessing compliance (or gaps), provides utility to the applicant in directing their focus on safety protection mechanisms (not just features / process), and useful for component vendors and system integrators for understanding the protection mechanism contributions they are required to contribute at each level.</p> <p>Understanding the relevance and degree to which a claim or evidence supports/fulfills an outcome is essential. Making it explicit reduces uncertainty and make compliance findings and subsequent certification easier.</p> <p>This simplifies the assurance bodies work in certifying the design, reducing time and expense.</p> <p>Effect on overall system</p> <p>There is a lot of misunderstanding that because a software something has achieved a certain DAL/SIL that there is a direct link between the level and safety – there isn't. For</p>				

			DAL at system level there is but it is statistically based. Therefore, directly in both cases it achieves a level of confidence and this is fine. So long as the statistical link for hardware and the collective agreement approach for software is clearly explained, I see no need for a further framework...hence the 'inclined to disagree'.				
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		1	4	10	5
		Narrative	<p>Yes. This relates to my comment against C3.1b above. I would prefer a framework that allows the relationship between the technique/method to the desired safety outcomes.</p> <p>As per C3.1c. Applies equally to techniques/methods and how they support the outcome.</p> <p>Think this will not achieve the aim.</p> <p>This is no different to the question above in many respects. However, I also refer you to the FM Supplement as this makes explicit properties that can be assured and errors detected using FM. In the general case, I am not so sure.</p>				
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		1	4	11	4
		Narrative	<p>There will be challenges here in determining exactly what is prescriptive enough.</p> <p>We do not want the framework to be too prescriptive as it will limit design flexibility, techniques, methods, etc.</p> <p>We are interested in system behaviours not software behaviours.</p> <p>This is too broad/general a question to answer. By goals do you mean: "the system will never overflow", "the system will always completely satisfy the stated requirements and nothing else"....?</p>				
C3.2	Are there any key principles or factors that the above principles don't include?	Narrative	<p>Making sure that assurance levels still work when they are flowed down to sub-systems / components / configuration items.</p> <p>I wonder if an assurance framework should also consider the competence, experience & authorisations of the</p>				

			<p>organisation and individuals that are applying the framework. Some organisations may not have the experience or maturity to cope with some of the concepts in the referenced papers. Higher assurance levels would imply a need for a higher level of competence in the design and certification organisations. The converse is true.</p> <p>Seems complete.</p> <p>Concentrate on system effects.</p> <p>There is a flow or path in your principles which has to be accepted before the complete argument can be accepted. If one of the stated principles is flawed/not accepted like I don't, the whole lot collapses. I think you could consider making them independent of each other, clearly relate them to either software or hardware rather than 'product' and decouple also from the previous paragraphs (false) conclusions.</p> <p>Can't think of any.</p> <p>Methods of assignment, and what they are assigned to is not directly covered here.</p>				
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
C3.3a	It is plausible that evidence assurance should not be independent of product assurance requirements.		1	1	1	15	2
C3.3b	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.				1	14	5
C3.3c	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?			1	4	10	5
		Narrative	Seems a reasonable designation for a framework that relies on layers of defences... therefore one would need to distinguish systems based on the number of defences that exist. One can argue that this 'constrains' the undesired behaviour, or 'enables' the desired behaviour. Can go				

			<p>either way.</p> <p>Not sure if the question is about the right choice of the term ‘constraint’ or whether the question deals with the fact that a ‘constraint’ can only either be an absence or a detection/handling mechanism</p> <p>Note 1: Absence has not been defined per say in the first paper. The first two instances of the use of ‘absence’ are actually in parenthesis.</p> <p>Note 2: The term ‘Constraint’ and later ‘Constrained’ under ESAL sound similar but are used in very different context. I wonder if the choice of words is the most judicious here.</p> <p>It allows detection/handling mechanisms, techniques, methods that may come from different discipline areas to be communicated and described in a common place using common language that is understood across disciplines.</p> <p>Agree, although it is likely not all constraints may be specified.</p> <p>Provided the constraint can be proven by test or demonstration.</p> <p>This is possible but needs to be reasoned about properly at the system/architecture/platform level. IN my UK based experience, this is what happens now and also in highly critical systems in civil aircraft (e.g. why Byzantine failures in 777 FCS have been adequately dealt with in the design)</p> <p>Useful term, but would benefit from better definition within the papers.</p> <p>Some example constraints would be useful to help better qualify the term.</p>				
C3.3d	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		1	5	13	1
C3.3e	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?			1	18	1	
		Narrative	<p>Needs additional to consider this question.</p> <p>I’m not aware of more plausible means.</p> <p>If I have understood your papers correctly (and I am not sure I do), then the approach is suggesting that you say</p>				

			what the system does do, what it should not do and then claim/describe/argue why it does that. This is effectively a safety argument and one should not re-invent the wheel.
C4	Our 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	<p>Yes. I am not sure whether there are any other factors, but the factors listed here seem reasonable.</p> <p>Gaining agreement between the regulator and applicant on the ‘any circumstances’ and ‘unexpected circumstances’ (CSAL 3 and 2) may be problematic. (i.e. multiple regulators consistency across multiple applicants, etc.)</p> <p>In theory and on paper this approach seems feasible. In reality I don’t know. This overall approach is certainly different than existing certification frameworks. It appears valuable but the feasibility can really only be assessed through real examples. Attempting to assess feasibility as a mental exercise where one applies the methodology described in theory on practical examples may have some value but likely be limited value.</p> <p>It may be feasible but it is difficult to make a determination without seeing a typical real world worked example.</p> <p>It’s not clear to me if this framework does anything to advance our ability to systematically account for intended or unintended behaviours, and hence how certainty (or conversely uncertainty) is to be quantified. Assume this is why the ESAL concept appearing later is fundamental to making CSAL work.</p> <p>Yes, it is a systematic and readily applicable approach.</p> <p>Seems feasible.</p> <p>Seems feasible, however the uncertainty definition adds little value e.g. define unlikely.</p> <p>If I have this right...the proposed approach is to have confidence that systematic failures cannot happen. I am choosing to relate this to a DAL A system and all that</p>

			<p>follows applies in this case. By ruling out 2 of the sources of systematic error for CSAL2 what claims for confidence can realistically be made? The situation is even worse for CSAL3. I don't understand the rationale behind the removal of principles in general, let alone the rationale for the removal of any specific principle over another – it all seems arbitrary. If there is a group consensus, with rationale, then I might be able to support the approach, but this seems to be mirroring the confidence approach to software DAL but at a higher level and ultimately claiming it solves the confidence issues wrt software but without a group buy-in to something that I think is flawed. For anything other than a DAL A system, I cannot see how it helps, other than to add another layer of complexity with no clear answer.</p> <p>Yes feasible.</p> <p>Feasible, yes.</p> <p>Yes, having systematic identification and assessment of behaviours is important to establishing confidence. External sources of violations are also important.</p> <p>Seems very subjective.</p> <p>Seems feasible. Coverage of internal and external factors. How does requirements validity versus satisfaction fit in here?</p> <p>The factors seem to have the right coverage, and thus provided they can be evaluated, it is feasible.</p>
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	<p>Yes. Seems to be compatible with other assurance levels defined in other standards.</p> <p>This seems feasible, though I feel this may be difficult to demonstrate satisfactorily, in practice. The matrix of every constraint in the system against each guiding principle possible behaviour may results in a large number of assessments.</p> <p>The approach to qualification appears feasible from a theoretical standpoint.</p> <p>Seems reasonable in principle, but what defines</p>

	<p>(CSAL1)</p> <p>Does this approach to qualification seem feasible? Explain why or why not?</p>		<p>credible/unlikely/expected/unexpected and who decides if that is good enough given the consequences of a particular systematic failure?</p> <p>I do agree, but there is a level of judgement in defining “expected” circumstances.</p> <p>Seems feasible. Levels appears consistent with logical arguments of operating circumstances in avionics / aviation.</p> <p>Apply with general rationale – interpretation of English terminology remains a concern. What more can reasonably be done?</p> <p>No – see above. Once you remove one principle, my confidence is zero.</p> <p>Yes feasible.</p> <p>Feasible, yes.</p> <p>Yes, feasible. Cannot think of a better way to qualify this.</p> <p>Seems very subjective.</p> <p>The levels seem to imply a degree to which the analysis has been systematic at finding sources of violations. These seems feasible, and seems to reflect a robustness/resilience like property of the constraint.</p> <p>I can see how the definitions will be useful, but they are somewhat subjective, as they rely on the adequacy of the identification of the circumstances.</p>
C4.2c	<p>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?</p>	Narrative	<p>Yes. Seems to be compatible with other assurance levels defined in other standards.</p> <p>The number of levels appears satisfactory.</p> <p>The approach appears to the number of CSAL levels appear right.</p> <p>Levels appear good – any more and it would be too complex to use. Glad to see recognition that absolute assurance can never be achieved and/or exist.</p> <p>Yes, each has a concise and logical meaning.</p> <p>More levels could yield more resolution, but could be overly complex.</p>

			<p>Repeats some of the problems of existing ACs.</p> <p>In my view it is either assured or it isn't. I believe that your definition of CSAL4 is possible and achievable (use of FM for instance) and then all we need to decide is what evidence we don't have on a case-by-case basis and make a judgement. I remain to be convinced that we can use CSAL as a framework and would rather see a reasoned argument based upon a DAL.</p> <p>Yes feasible.</p> <p>Feasible, yes. Levels ok.</p> <p>Yes, five levels seems about right.</p> <p>The number of levels appears ok, but the subjectivity might make it difficult to determine the differences.</p> <p>More levels would be excessive, fewer would be insufficient. Good to see absolute assurance is recognised as not achievable.</p> <p>The number of levels is workable.</p>
C4.2d	<p>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.</p> <p>Is it feasible that these guiding principles correlate to the CSAL level definitions?</p>	Narrative	<p>I am not sure. This would require more time to determine.</p> <p>Yes</p> <p>I agree that these guiding principles correlate to the CSAL definitions. Should the term partitioning be introduced for the last two guidelines ?</p> <p>I find myself wondering if there is a basis for the guiding principles at the respective CSAL levels and whether the set is derived from an established body of knowledge. I also wonder if there is a step missing to assess and/or tailor these principles based in the particular system and application. For example will a reuse system or a COTS based system require some different guiding principles?</p> <p>Yes</p> <p>Yes</p> <p>No</p> <p>Yes feasible.</p> <p>Feasible, yes.</p>

			<p>Yes.</p> <p>Perhaps some more description of the correlation could be provided.</p> <p>This may be improved if the relationships are more explicitly modelled in the explanation.</p> <p>These principles strongly mirror those already used in civil aviation software certification. The correlation to the CSAL definitions could use some additional explanation.</p>
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	<p>Possibly. Would require more time to think about this.</p> <p>TBA</p> <p>The list of guiding principles looks fine.</p> <p>We have all seen seemingly unrelated changes break code and/or change behaviours. Which one of the guiding principles addresses maturity of design/freedom from further change and immunity of detection and handling mechanism from being affected by change?</p> <p>I have also seen detection and handling mechanisms broken due to a human error or inadequate version control in a complex build. I have also seen working code broken by tweaks to configuration variables (that exist outside the code). Do any of the listed guiding principles address the human in the loop aspects?</p> <p>No.</p> <p>None identified.</p> <p>Given that 3 subsumes 1 and 2 and 2 subsumes 1, then all we need to review is CSAL 3. What is the practical difference between ‘refined behaviours and ‘implemented behaviours’. It seems that the last 2 bullets (‘Conditions...internal/external’) cover all the other 5 and given that this is the case, it covers everything that may or may not occur. Therefore useful in that they cover all cases but ultimately un-useful because they do not add any value!</p> <p>Undecided</p> <p>None identified.</p>

			<p>None identified, but a case study might help identify the adequacy.</p> <p>See above comments</p> <p>See comment above.</p> <p>None identified.</p>
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	<p>The proposed apportionment of guiding principles seems reasonable.</p> <p>They appear suitably apportioned / balanced</p> <p>Would require additional thinking. It is possible that I'd suggest slightly different apportioning</p> <p>I'm not aware of a better way to apportion the guiding principles to CSAL levels, but still wonder on what basis the proposed allocations have been made.</p> <p>No.</p> <p>None identified.</p> <p>Use a reasoned argument.</p> <p>Undecided.</p> <p>Apportionment ok.</p> <p>Apportionment appears ok.</p> <p>See above comments</p> <p>Yes, but they may be less valid. See comment above.</p> <p>Apportionment is consistent with civil practice in a general sense.</p>
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	<p>Not prepared to make the argument of completeness at this stage, however intuitively, I think there is a reasonable case to be made that the categorisation is sufficiently complete.</p> <p>is 'specified behaviour' a subset of 'refined behaviour' and a subset of 'implementation behaviour'?</p> <p>They appear sufficiently exclusive at first glance.</p> <p>This is a question for organisations that have extensive experience in the subject area.</p> <p>Yes. Each is clear, and the categories are unambiguous.</p> <p>Debate could be had about the definition of expected</p>

			conditions, which would be produce specific. OK No – see Answer to C4.2e Yes. Yes, that seems possible. Yes. See above comments They appear reasonably complete. Yes, an argument could be made.				
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?				2	13	5
		Narrative	Reads as a ‘well defined safety requirement’ Agree you need to start with evidence supporting the intended function of the constraint. Inclined to agree but need to bolster the definition with “defines the behaviours required and not required” I see validity has been emphasised here in addition to satisfaction.				
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		1	3	10	6
		Narrative	This may be onerous to provide evidence – does it require the applicant to articulate all known language vulnerabilities, target computer behaviours etc., and how they’re addressed for each constraint, or just once in an overarching document.? My understanding of this guiding principle changes each time I re-read this section. Don’t really care about this as I want to know what ‘the system’ is supposed to do and that it can do it.				

			Alternatively, if it is accepted that the level of refinement <u>is</u> the implementation, then fine, but seems like an unnecessary level of detail which will not help.				
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	1		3	9	7
		Narrative	I'm not entirely sure how the evidence would be articulated by the applicant to the regulator. Do 'model based developments' and other abstractions require some form of tool qualification? As per C4.3b. Now we are talking only about software? I thought this was about architecture and included hardware?				
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		1	2	9	8
		Narrative	Seems logical. Experience says implementing language and development environment can influence behaviours. The implementation level is often built on a large stack of tools. It may be that the actual implementation following the tool chain is different from the evidenced source code implementation. This is the important bit, but note comments at C4.3b				
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	1		3	11	5
		Narrative	Appears feasible, however I have no feeling for the depth/quality of evidence at each CSAL level, what form it will take, and how that equates to improved assurance. See comment at C4.3c				
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	1		3	11	5
		Narrative	This guiding principle may be used to address comments at C4.2e. The complexity of this may be too much for all implemented code. See also comment C4.3c. Is this a re-badging of derived requirements? Or/and of structural coverage? This is already covered in software guidance e.g. DO178B/C				
C4.3g	<i>Introduced or generated behaviours that may violate the 'constraint'</i> provides a feasible means	Agreement	1		3	11	5

	of integrating evidence relating to compiler translation, traceability into executable object code, and additional behaviours introduced during translation. Explain why or why not?	Narrative	Narrative as per C4.3e. The complexity of this may be too much for all implemented code.				
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	1		3	11	5
		Narrative	Experience has shown behavioural changes occur when code is deployed on target versus development computer.				
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	1		3	11	5
		Narrative	Narrative as per C4.3e. Initialisation may not be a repeatable process, so this may be unreliable as evidence.				
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	2	2	3	6	7
		Narrative	Defining all sources of unacceptable external interference might be arduous. My understanding of this guiding principle changes each time I re-read this section. Does 3.2.6. contradict itself re: internal versus external to the system? These conditions should be specified as part of a constraint. Otherwise how do you assure that all external factors relating to a constraint are accounted for? Complexity grows exponentially. I would rather see a reasoned argument. See also C4.2e				
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	2	2	3	7	6
		Narrative	Providing evidence that all sources of unacceptable external interference have been addressed, might be arduous As per C4.3j.				
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	2	2	3	6	7
		Narrative	Defining all sources of unacceptable external interference (and then providing evidence to show they've been addressed) might be arduous.				

			Seems logical. Experience says external environment can induce unexpected behaviours. Potentially infinite supply of external factors.				
C4.3 m	Conditions or behaviours external to the system that may violate the constraint 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	2	2	2	9	5
		Narrative	Defining all sources of unacceptable external interference (and then providing evidence to show they’ve been addressed) Narrative as per C4.3e.				
	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?		1	1	5	13	
		Narrative	It is feasible there is a linear relationship. Each level (except for CSAL4 which is not used) seems to line up reasonably with each ASAL. Not sure if there are some overlaps, but there may be potential for this. Why does the 3rd detection /handling mechanism for ASAL3 require CSAL3? It looks feasible but I’d rather not give a too quick answer here. Agree. A higher ASAL level should require more layers of independent absence/detection handling mechanisms, and should also require that a greater number of the CSAL guiding principles be applied in the analysis of each mechanism to drive down the uncertainty. Without greater levels of claims assurance, the ASAL levels give false confidence in the level of assurance provided. Concepts appear to support a linear relationship. Given my views above on CSALs I cannot answer in any other way. However, the principle of saying ‘I have				

			defence in depth from an architectural perspective therefore I am more confident' is accepted, so long as it is argued.				
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	1	1	1	10	7
		Narrative	<p>If you can argue that the ASAL – CSAL linear relationship exists, then it would only follow that there is also a direct relationship with the failure condition severity category.</p> <p>As per previous, it makes sense that higher failure severity should drive higher CSAL levels and hence consider more ways in which the constraint may be compromised.</p> <p>Argument fails as I don't accept CSAL</p> <p>More severe the fault, the more confidence in the evidence seems intuitive.</p>				
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	1	2	3	13	1
		Narrative	<p>Agree interference of the additional layers is a key consideration to make sure assurance is not diminished. It's not clear to me why in the CSAL framework additional layers would be entertained as the best you can hope to achieve for the extra burden is break even. Perhaps this becomes clearer in the ESAL section.</p> <p>This table is way too complicated and combines too many caveats/notes; similar to problems previously encountered and commented upon earlier. You need to consider flow diagrams.</p> <p>Probably requires some evaluation against common architecture types to ascertain validity.</p> <p>I can see how it may be possible to need less confidence.</p>				
C4.4d	Table 2 of [RMc10] provides a feasible means of linking ASAL and CSALs. Explain why or why not?	Agreement	1	1	4	11	3
		Narrative	<p>Could only really assess this by going through a more extensive analysis, which I don't have time to do right now. Intuitively, it makes sense however.</p> <p>ASAL level 3 allows the second and third detection/handling mechanism to both be at LRU level as long as they are independent. Is establishing independence problematical at the same level?</p>				

			See above comment.				
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	2	2	2	9	5
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	<p>Definitely feasible. If you can provide a strong enough claim that your constraint at one level is more than adequately assured, then depending on the whole system architecture, then this may indeed be enough to argue that there is no need for further protection at other layers. However this may represent a contradiction to the research.</p> <p>Could one detection /handling mechanism for ASAL3 be CSAL2 where the others are CSAL 3.</p> <p>Not sure I fully understand the question</p> <p>My first thoughts on reading this paper were that near absolute assurance at any one level could work to reduce the assurance required at other levels.</p> <p>Agreed, but assurance levels need to be very high for this to occur, and component needs to be relatively isolated from rest of system.</p> <p>Power supplies or other systems could make this happen.</p> <p>In theory Yes.</p> <p>Narrative to C4.4e: More important than what? I would rather have either a highly assured single layer (adequately argued) or a series of adequately assured layers providing the same assurance but, of course, argued differently.</p> <p>C4.4f. Not sure I understand the question, but here goes. Are you saying that one might argue that sufficient defence in depth is achieved and hence no further defences are required? If so, absolutely. Is CSALs the way to achieve this – nope – use an argument!</p> <p>Feasible, yes.</p> <p>Perhaps, but it would depend on the situation and severity of failure condition.</p> <p>Potentially.</p> <p>It depends. I've seen programs where the contractor made very strong claims that certain faults weren't present, and</p>				

			then these faults appeared in service. Fault treatment should address both prevention and tolerance in any design activity. One or the other may not be sufficient. This appears to be reflected in the tables. Potentially, it depends on coverage of faults from a detection/handling perspective, and confidence in the evidence.				
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	Not that I can think of at the moment. I can't think of any other factors at this point but this is the type of question where if I had days and weeks to think about it I may come up with a different answer. None that I'm aware of. No. None identified. Omission of rationale argument as the alternative. No. Seems ok. None identified.				
	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?			1	2	11	7
		Narrative	This is not too far from what we have now with DO-178B SOI outcomes. But the techniques may be important too. You can expect experienced organizations to use the right methods / techniques but it is not always the case. This approach accords nicely with SE methodologies and the way lifecycle products are specified in ASDEFCON contracts. Quality in => quality out.				

			<p>Agreed that this is better than mandating a set of techniques to be used (i.e. test). However, it has to be linked to some specific claim about what the used technique does to achieve the claimed result. Furthermore, this is also only good if there is coverage of the evidence categories in a complete manner. This has yet to be defined...more on this no doubt later....</p> <p>Provides a much more generic approach, and may be familiar in part to DO-178B users, as the attributes are similar to the objectives of that standard.</p> <p>While this differs to the DO-178B lifecycle objectives, the intent is consistent.</p>				
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		1	1	13	5
		Narrative	<p>Probably not within the set of attributes. I'd say at the evidence level</p> <p>Yes if " requirements satisfaction" involves a verification activity.</p> <p>Aligns with hardware thinking.</p> <p>Need to define the set of attributes, but as a starter for 10, this is OK. Needs to go further....argument for completeness/comprehensiveness?</p>				
C4.5c	Should configuration consistency 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	2	6	3	7	2
		Narrative	<p>Should be addressed within the set of attributes as it provides a means to distinguish the level at which configuration consistency is achieved for different Levels.</p> <p>There are benefits to each, however at the evidence level it may make compliance assessment easier.</p> <p>As per a previous comment, configuration inconsistency can break a build or worse invoke unexpected behaviour that is not easily detectable. I believe it should be considered as an attribute of each lifecycle product relevant to the claims in the CSAL.</p> <p>Configuration is an integral part of large scale software development</p> <p>As long as the code matches the entire requirements set and</p>				

			<p>testing proves no hazards.</p> <p>Question does not comply with the agreement categories. Answer is the latter IMO.</p> <p>It is important, but is more appropriate in the relationship between the evidence and the attribute. Of course, the configuration that the whole case relates to should be defined somewhere.</p> <p>Yes, but it needs to be inherent in each attribute.</p>				
C4.5d	The set of attributes for each software lifecycle product class is adequate (Annex A to [RMc10]). Explain why or why not?	Agreement		2	4	12	2
		Narrative	<p>Appears Adequate</p> <p>Generally yes, noting comment at C4.5c regarding potential for needing a configuration consistency attribute.</p> <p>The attributes may or may not be complete – covers all eventualities! Seems to resemble DO178 quite closely in terms of the categories as you suggest, but unhappy with the assignment of tolerability – more later....</p> <p>At least covers the DO-178B objective topics.</p>				
C4.6	What attributes have been missed, or what attributes are inappropriate?	Narrative	<p>Not sure for now.</p> <p>Nothing stands out.</p> <p>Configuration Data plays a key role in how a system behave. Perhaps it should be considered.</p> <p>More time would be required for a detailed review of the list of attributes.</p> <p>Narrative as per C4.5d.</p> <p>No opinion</p> <p>None identified.</p> <p>Planning and certification liaison don't feature, but since they don't relate to the product you're trying to emphasise, I can see why they have been left out.</p>				

	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.			1	1	12	5
C4.7b	The tolerability of limitations concept is useful because it prompts direct consideration of the limitations in an article or type of evidence.			1	1	9	9
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.			1	1	12	6
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	<p>Seems like a reasonable categorisation of evidence goodness</p> <p>I think this makes compliance assessment more straightforward and flexible for the regulator.</p> <p>The applicant will be after a ‘minimum level of effort’ and thus aiming to find the ‘sweet spot’ of limitations in terms of relevance, trustworthiness and results for the applicable ESAL.</p> <p>The approach looks sounds but more time would be required to make a definite judgement.</p> <p>I have no idea how this would work practically though.</p> <p>The approach seems feasible however there needs to be good training and guidance available to those trying to apply it. Determination of relevance, trustworthiness and level of goodness of results of evidence will often be subjective and may result in variability of usage between organisation, e.g., what your experience tells you is trustworthy, relevant, etc, may be different from what my experience tells me.</p> <p>Yes, although highly likely that ESAL 3 and 2 dominate in any requirement.</p> <p>Feasible; Yes!. Limitations would have to be fully defined and constrained.</p>				

			<p>Feasible, but will it aid understanding, or confuse those with language definition difficulties.</p> <p>Only if an argument was used and was directly linked to the specific project and a 'level' was not defined. The general principle of tolerability as you define it is OK, but trustworthiness, relevance and results all need to be independently judged (read: 'argued') in context. Trivial example, but I could trust a result which might not be relevant for a particular claim (e.g. result: there are no divide by zeros; context: there is no use of division in the program; outcome in question: still does not mean overflow is absolutely avoided).</p> <p>Yes plausible.</p> <p>Feasible, yes.</p> <p>Yes, feasible, but potentially prone to subjectivity</p> <p>Yes</p> <p>Addresses what I understand to be the main properties of evidence.</p> <p>The qualification seems feasible, and to some extent is what should already be being justified in a PSAC. However, many PSACs aren't this focussed and read much more like development plans.</p>
C4.8b	<p>It is plausible to consider tolerability of limitations as the extent to which:</p> <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 techniques non-treatment of a limitation should not introduce uncertainty disproportionate to the limitation such that it would likely lead to a violation of the constraint. <p>Is this concept plausible? Why or why not?</p>	Narrative	<p>My understanding is that the tolerability categories describe the extent to which one can tolerate limitations in evidence provided to substantiate "goodness" (for want of a better word) of a constraint. Not sure I understand the second dot point (too many double negatives)...</p> <p>'Tolerability' suits the regulators parlance – especially when assessing deficiency, however the applicant may prefer a more 'defined' benchmark to know exactly where the goal-posts lay.</p> <p>Concept is plausible. I wonder once more about the practical application of these concepts.</p> <p>Agree in principle. There may be inconsistent identification of limitations and application of complementary methods.</p>

			<p>The idea of assessing whether a limitation introduces uncertainty disproportionate to the limitation is scary as this is so open to interpretation. How do you measure these things and judge the degree of disproportionality? How are these quantified/compared?</p> <p>Yes, although time intensive.</p> <p>Plausible. Yes!. Examples of limitations and evidence of effect would need to be defined clearly in guidance for designers.</p> <p>Plausible, but should there be some limitation in complimentary methods.</p> <p>For the first bullet – I agree but again need to have the word argue. The second bullet is completely arbitrary and cause for huge debate because of the word ‘disproportionate’ and the fact this uncertainty is not measurable (even by your previous CSAL approach).</p> <p>Yes.</p> <p>Plausible, yes.</p> <p>Yes, feasible, but again subject to subjectivity. Is there an example?</p> <p>Yes, but it might be hard for contractors to know what limitations are important and what ones are not. This might make it a very subjective argument. Could a standard or typical list of limitations be documented somewhere as guidance?</p> <p>This is very feasible, but I worry that many of the practitioners in our contractors are process monkeys, and may not have the holistic understanding to make these arguments. A process needs to be agreed up front, perhaps based on this methodology and then followed by the practitioners.</p> <p>Sounds in principle. I’m not sure that most developers think this hard about it in practice, as they are used to their activities being dictated by industrial practice.</p>
--	--	--	---

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	Seems like a reasonable set of properties to determine the goodness of evidence. Yes It is feasible that these properties are adequate. The presentation of these properties is somewhat conceptual and may appear to others theoretical. How would these properties work when applied to a real-life project? I don't have the answer to that question Yes, if the subjectivity can be taken out of it, and a way found to ensure organizations apply it consistently. Yes, although there is no guard against selective evidence being presented, i.e. evidence detrimental to the a parties desired outcome be discarded by said party. Yes. Appears that they are adequate. Yes, but not in the framework suggested. Yes. Yes. Yes. Yes. Reasonable basis. Yes.				
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.			2	2	14	2
C4.9b	Trustworthiness of evidence is highly subjective and derivative of human involvement in the product of evidence.				3	8	9
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?				2	16	2
		Narrative	The concept appears sound; however the term trustworthiness tends to relate to honesty. Not meeting a				

			<p>‘trustworthiness’ requirement may be taken the wrong way by an applicant as an accusation of acting maliciously or dishonestly.</p> <p>This is generally true in my experience; however some individuals are very well qualified and trained but not very experienced. Competency takes a balance of the three.</p> <p>None of these processes preclude the possibility of deliberate biasing of evidence.</p> <p>The problem is egotistical experts, can get away with more.</p> <p>Over reliance on part performance.</p> <p>There is a bit more to it for example, the selection of techniques, the underpinning robustness of a programming language, complexity of the project, etc. IN so far as this is not included in the definition, then trustworthiness if a function or your list, plus a delta.</p> <p>It might also be a function of the configuration control of the evidence.</p>				
C4.9d	Qualifying human competencies is difficult, even with the aid of competency frameworks.	Agreement	1	8		8	3
C4.9e	Table 4 of [RMc10] provides a feasible approach to benchmarking trustworthiness of evidence. Explain why or why not?	Narrative		2	3	13	2
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		6	8	6	
		Narrative	depending on the definition of ‘expert’ and their expected involvement, it may introduce difficulties				

			<p>It is very prescriptive. Notes and definitions are very hard to interpret. What is intellectual, mechanistic, conceptual and applied independence? Why does ESAL 3/2 allow “None” for mechanistic and conceptual independence as does ESAL levels 0 and 1.</p> <p>Alternatively could adjust formality of reviews and inspections and ask for differing levels of authorized reviewers/inspectors commensurate with ESAL level.</p> <p>None of these requirements look out of line with standard (non safety critical) software practices.</p> <p>I can see this side of the coin too, but it is still a good table that is in line with CMMI.</p> <p>Seems straightforward, but remember bad day syndrome. One would need a PhD in its application.....and even then I’m not sure because I would have to be able to explain to others and this is where it falls down.</p> <p>Most work in real developments is done by practitioners, supervised by experts. It may be difficult to find enough experts to comply with the table.</p> <p>Many developers don’t have the experts you’re suggesting may be required. They often buy in the expertise through consultants and DERs.</p>				
C4.9g	<p>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:</p> <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	1	1	10	6	2

	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?			2	2	5	6
		Narrative	<p>The framework appears to make the regulators role more straightforward.</p> <p>Nothing beats concrete evidence.</p> <p>Adds a layer of complexity.</p>				
C4.10 b	It is beneficial to the compliance assessment/audit process to have evidence explicitly related (e.g. by traceability) to 'constraints'.	Agreement			2	10	3
C4.10 c	Current safety and software assurance standards employed already provide adequate benchmarks for evidence sufficiency that are explicit to the certification authority.			3	2	7	3
C4.10 d	Limitations in certification authority confidence of evidence sufficiency would not inhibit a successful certification assessment.		2	8	1	4	
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	<p>Yes, categorization of evidence in this way would assist in certification assessments.</p> <p>Yes, it appears to</p> <p>Yes. Despite the subjectivity and learning curve this framework is a big improvement over other current software assurance standards.</p> <p>Yes, this would aid auditors.</p> <p>Probably yes, but not using the framework</p> <p>Yes.</p> <p>Yes. Yes.</p> <p>Potentially, but it is not how assessments are currently done.</p> <p>Yes, provides a good place to target audits and compliance</p>				

			<p>assessments.</p> <p>Yes, this is consistent with the traceability used in the job aid reviews.</p>
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	<p>Challenges in actually assessing the evidence – I would imagine this level of auditing would require extensive specialist training.</p> <p>If not carefully managed, it may require the applicant to have to prove a negative (beyond robustness testing).</p> <p>As per C4.13a below.</p> <p>Evidence attributes and other compliance mechanisms would need to be defined.</p> <p>Too complex</p> <p>None I can think of.</p> <p>None.</p> <p>Unfamiliarity with the approach.</p> <p>None, the contractor should have costed and planned for the demonstration activities.</p> <p>Mostly that it would be something new, and both developers and evaluators would be new to it.</p>
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	<p>As above, but even more difficult since there would need to be mapping exercise done in this scenario.</p> <p>I’m not 100% sure it provides the applicant with a defined goal for them to understand completeness.</p> <p>As per C4.13b below.</p> <p>Needs correlation to the other standards.</p> <p>Adds an unnecessary layer of complexity.</p> <p>Integration with other standards needs some clarification.</p> <p>How do you handle the shortfalls in evidence that might arise contractually? However, at least the shortfalls would potentially have a product meaning.</p> <p>It wouldn’t be compatible with the contracted standards, at least not without some further clarification.</p> <p>The benchmark here may differ from the contractor’s</p>

			<p>interpretation of the standard, and thus the differences may lead to dispute over the work required. If it is used only on the certification authority side to inform risk, then it will probably be useful.</p> <p>While it has many similarities to DO-178B, the differences may be notable from an evidence perspective. This does not imply it is inferior to DO-178B, just differently focused. Which is better for safety would depend on if it drives designer in the right direction.</p>
C4.11d	Does the CSAL/ESAL framework improve the knowledge about sufficiency of evidence over existing assurance approaches? Why?	Narrative	<p>Yes, because it forces you to look more objectively at the right evidence. It does however pose challenges in executing the process correctly. If not done correctly, there would be risk of diminishing returns in expending this much effort in evidence review.</p> <p>Not sure, but the sufficiency of evidence appears better focused on safety objectives.</p> <p>Yes the proposed framework places emphasis on producing the right evidence, minimization of uncertainty and maximization of trustworthiness/relevance commensurate with impact of violation of each constraint.</p> <p>Yes.</p> <p>No because it is too complex to work out what needs to happen.</p> <p>Yes.</p> <p>Yes because it seems to have more product focus.</p> <p>Unsure</p> <p>Yes, because at least it tried to measure it and relate it to the product risk.</p> <p>Yes, because of what it targets. However the evidence sufficiency requirements of the existing approaches are benchmarked by the FAA.</p>
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	<p>Yes – if it's done as defined in this research. The concern is that it would be difficult to contract to such a framework and I would imagine that even if you attempted to, what you would get is a less stringent negotiated set of</p>

			<p>requirements.</p> <p>It should do, but the ASAL also appears to do this on its own.</p> <p>I would think so mainly due to the product and evidence focus.</p> <p>Yes.</p> <p>Makes things even worse.</p> <p>Yes.</p> <p>Yes – again product focus appears useful.</p> <p>Potentially, because it appears to have more product focus.</p> <p>Yes, as above.</p> <p>It aims to provide better traceability, and this may help. A good safety assessment would also do this.</p>
C4.10 f	What is your overall belief regarding the usability 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	<p>In an ideal world – this would be extremely useful. My concern is that it is extremely ambitious.</p> <p>My initial thoughts are that the CSAL/ESAL approach will not be any more usable than current practices. Perhaps seeing an example of implementation would change this perception.</p> <p>As per C4.13c below.</p> <p>Increases usability – but needs specific timeframes and evidence examples.</p> <p>Unuseable.</p> <p>Useable, needs an example, and trial.</p> <p>Seems useable, a case study would be useful.</p> <p>Unsure, requires further development and some examples.</p> <p>It seems to have enough merit to be worthy of further trial application. Perhaps also useful to draw the attention of standards committees to some of the ideas.</p> <p>An interesting new perspective versus the current approaches.</p>
C4.10 g	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	Narrative	<p>Possibly. With the approval of senior management and our client.</p>

	validation?		<p>This would be better directed at the ADO in the context of this section.</p> <p>No.</p> <p>No.</p> <p>No.</p> <p>Not within the current project.</p> <p>No.</p>				
	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
C4.12 a	Making explicit the categories of evidence and the attributes thereof, is beneficial to the system development process. Explain why or why not?		1	2	2	5	5
		Narrative	<p>Current software assurance standards are weak in this regard.</p> <p>Provides clear guidance on required deliverables, design constraints, and testing. Simplifies time planning, reduces budget risk.</p> <p>The more clear the definitions the better.</p> <p>Adds boundaries and provides certainty.</p>				
C4.12 b	It is beneficial to the system development process to have evidence explicitly related (e.g. by traceability) to 'constraints'.	Agreement	1	1	3	6	4
C4.12 c	Current safety and software assurance standards employed already provide adequate benchmarks for evidence sufficiency that are explicit to the certification authority.		1	2	3	5	4
C4.12 d	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.		1	1	3	5	5
C4.13	Provide answers to the following questions:	Narrative					
C4.13 a	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	<p>Has potential to significantly increases the workload and associated cost as well as place demands on skill profile and numbers required in project resources. A steep learning curve and some subjectivity makes it risky. Software safety is likely to be the winner so the customer needs to be</p>				

			<p>willing to pay for it.</p> <p>Moves onus to developer to put in place appropriate methods to provide levels of requirements, rather than following a predetermined process</p> <p>See C4.11b.</p> <p>Time for education and additional costs (see DefAust 5679)</p> <p>Too complex</p> <p>Learning curve for different mindset.</p> <p>None identified.</p> <p>Unfamiliarity with the approach.</p> <p>Mostly that it would be something new, and both developers and evaluators would be new to it.</p>
C4.13 b	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	<p>Framework is more complex than DO-178B and is applied to each constraint rather than whole of software. The workload could be quite high and incur significant costs. It would be interesting to see the cost/benefit of ASAL/CSAL/ESAL 3 versus DO-178B level A for the same product development.</p> <p>Potential conflict of standards. Additional overhead of work.</p> <p>See C4.11c.</p> <p>Cost and time increase for sector specific standards.</p> <p>Adds an unnecessary layer of complexity</p> <p>Integration with other standards needs some clarification.</p> <p>None identified.</p> <p>It wouldn't be compatible with the contracted standards, at least not without some further clarification.</p> <p>While it has many similarities to DO-178B, the differences may be notable from an evidence perspective. This does not imply it is inferior to DO-178B, just differently focused. Which is better for safety would depend on if it drives designer in the right direction.</p>
C4.13	What is your overall belief regarding the usability of the CSAL/ESAL framework for addressing the motivating issues and limitations with the current state of practice identified	Narrative	<p>There are challenges with the learning curve and subjectivity. This country is still coming to grips with DO-</p>

c	earlier within these survey questions?		<p>178B and may not have enough experts or the will to adopt such a framework. Given a high percentage of software developments in this country are arguably ASAL 0 or 1, the framework may not be seen as necessary.</p> <p>I would like to see such a framework in place, it is significantly more usable as it doesn't seem to generate paperwork for no benefit in system assurance.</p> <p>See C4.10f</p> <p>Improvement on DO-178B – drawback would be cost.</p> <p>Unusable</p> <p>Useable, but requires a trial.</p> <p>Potentially useable. Has a case study been done?</p> <p>Unsure, requires further development and some examples.</p> <p>An interesting new perspective versus the current approaches.</p>				
C4.13 d	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	<p>I can't say but there may be some interest if it was seen as a business opportunity. I suspect there are candidate project where it could be applied and that the company has individuals far better placed than I to make sense of what is being proposed.</p> <p>Potentially. Very interested in this idea, would require negotiation.</p> <p>See C4.10g</p> <p>No.</p> <p>No.</p> <p>No.</p> <p>No.</p>				
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.				1	8	11
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.				2	6	12
D1.1c	Goal-based standards permit substantial flexibility for designers, which give benefit in defining effective products.				2	11	7
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.			1	2	10	7
D1.1e	Prescriptive standards set clear benchmarks for evidence and activity completion.		1	1	1	6	11
D1.1f	Application of prescriptive standards may lead to limitations in relevance of the evidence to achievement of product safety objectives.		1	1	1	12	5
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.				1	6	13
D1.1h	Contracts which provide cost and schedule certainty are preferred by both suppliers and acquirers.		1	1	1	6	11
	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.			1	1	6	12
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).			1	1	9	9
D1.1k	Both acquirer and supplier will be seeking confidence that the contract will be successful prior to entering into the contract.					6	14
D1.1l	Should safety issues emerge during the contract, then timely and cost effective resolution will be a goal for both supplier and acquirer.					6	14
D1.1m	The contract and standard should support the resolution of safety issues, and not hinder it by contributing uncertainty to the dispute.					4	16

D1.1n	There is evidence in industrial practice of project slippages, overruns or cancellations due to issues concerning safety assurance and certification.			2	4	14
D1.1o	There is evidence is industrial practice that limitations in current approaches may be contributing to project slippages, overruns or cancellations			2	6	12
D1.2	Where specific examples supporting your answers to the above statements can be provided, please provide them.	Narrative	<p>Limitations in current approaches (D.1o) combined with a contracted focus on 'features and function' contribute to project slippages and failure. (features tend to be contracted ahead of safety).</p> <p>Not able to.</p> <p>Contractor processes that use standards as references for nothing more than lip service can confuse/dispute the contract and hinder certification.</p> <p>Certification needs to be on-going, not at end of phases.</p> <p>D1.1n: There are plenty, none of which but one will I talk about. The Chinook Mk 3 programme debacle was essentially caused by the then MoD(PE) team. They asked for assurance from Boscombe Down that their purchase off-the-shelf of the helicopter (i.e. the same as the Dutch?) could be certified. BD said they could see no reason why not so long as it was the same helicopter. MOD(PE) then said it was the same except for the avionics which would be new. BD said all bets were therefore 'off' but MOD(PE) went ahead and bought it anyway with the result that they sat in a hangar for most of their time. I got involved in 2002/3 on the 'get well programme' where the IPT was in severe danger of doing exactly the same thing again. I spotted it and stopped it. We have yet to have a replacement for these aircraft but we are getting close some 15 years or so after the original requirement was 'satisfied'.</p> <p>Numerous ADF projects have suffered slippages due to resolution of safety assurance issues.</p>			
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	Strongly Agree
D1.3a	Regulatory enforcement is enabled by the contract rather than via laws for the military circumstance.		1	2	3	8	6
	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.			1	2	10	7
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.			1	3	7	9
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.			2	2	8	7
D2.1b	ARP4754 and RTCA/DO-178B make no mention of integration with contracts as the means of evidence provision.			1	2	9	8
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.			1	2	15	2
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.			1	1	15	3
D2.1e	UK Defence Standard 00-56 Issue 4 doesn't address requirements on contracts for provision of arguments or evidence.			2	10	6	2
D2.1f	MIL-STD-882C and D contains guidance on contract integration throughout, including specific references to contract clauses, tender processes and data requirements.		1	1	5	6	7
D2.1g	Used in isolation to design requirements, MIL-STD-882C/D achieves safety regulation through contracts.		2	2	5	7	3

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:
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

	1	1	2	8	8
		1	3	7	9
		2	2	8	8
	Strongly Disagree	Inclined to Disagree	Undecided	Inclined to Agree	Strongly Agree
		1	1	13	5
		1	1	10	8
		1	1	10	8
		1	1	13	5
		1	2	9	8
		1	2	8	9
		1	2	11	6
		1	1	7	11
		1	2	7	10
1	1	4	10	4	

	the tender phase, it is plausible that the absence of this information in a tenderer's response may be overcome by adjusting the contractor's proposed costing by a risk figure based on the amount of uncertainty (or extent of suitability) in the tenderer's 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.

Agreement

			5	15
	1	1	4	14
	1	2	5	12
	1	2	10	7
	1	2	11	5
		2	10	8
		1	12	7
		1	7	12
	1	3	5	11
	1	2	10	7
	1	2	10	7

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.			1	2	7	10
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.			1	1	8	10
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.					2	18
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	<p>I would contend that it would decrease uncertainty. However, my concern would be that it would still come down to dollars, and that initial tender negotiations and subsequent contract negotiations would be greatly impacted by the obligation to produce this level of architectural detail. In essence, I would imagine that promises at the tender stage (and we would be limited at the amount of evidence they can actually produce, especially for developmental systems) will inevitably be broken at the contract stage. I would also imagine that there would be an enormous amount of caveats in submitted tenders, that would complicate the acquirer's tender evaluation process. Here, the developer would claim that that they are taking on too much risk (in schedule, financial, technical terms).</p> <p>Yes, the process should obtain greater architectural certainty over traditional methods (i.e. contracting a standard).</p> <p>Very suitable when a design is already established, but not as suitable when the contractor is tendering for a development based off functional requirements (where 'evaluation of architectural suitability' would traditionally be done at a Preliminary Design review.)</p> <p>I think this is a good solution and gives some early visibility into the architectural solution. Of course adding new requirements to an RFP will mean more work for the suppliers and some suppliers may argue against it</p>				

		<p>especially if a 4761 system safety assessment is performed along with DO-178B SW development.</p> <p>Their attitude could be “we are doing all safety based process in the civil world and you are asking us to perform additional safety work...”</p> <p>This goes back to the question how does this architectural certainty approach tie in with ARP4761/4754 and DO-178B.</p> <p>Agree in principle, however too much effort pre-contract may be prohibitively expensive, reducing the number of bidders and stifling competition. This is particularly true if candidate tenderers have to learn new technologies/techniques, recruit staff, prototype, perform modelling and simulation, invest in tools, test conceptual architectures, etc. Bidders may have to be compensated financially to attract their interest. Historically, and with some exceptions, large acquisition programs in this country already take several years worth of effort and heartache to get into contract.</p> <p>Also, should not underestimate what effect moving to COTS software elements will have with regard ability to access to data and determine architectural suitability.</p> <p>Architectural development is potentially non trivial and can incur significant cost to the developer. This process may have to provide funding for tender development.</p> <p>Feasible, yes. Needs to leave room for tradespace and technical advances during the conduct of the contract for long programs.</p> <p>Removes uncertainty in early phases, reduces risks and therefore lowers costs.</p> <p>If the right benchmarks can be agreed, the tender process is followed properly and the evaluation is undertaken by suitably qualified people, at the appropriate times during the contract, then yes. Actually – no chance.</p> <p>Yes feasible.</p> <p>Feasible, yes.</p>
--	--	--

			<p>Yes, feasible. Would require careful project management and education of tenderers.</p> <p>Feasible, but potentially difficult depending on solution maturity.</p> <p>Seems intuitive and feasible.</p> <p>Yes, seems feasible. But not directly relevant to current civil certification.</p>
	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	<p>Is it also worth including the definition of independent layers as discussed in the ASAL paper?</p> <p>Yes, I would use this, given the opportunity.</p> <p>Looks feasible</p> <p>Potentially yes though the requirement is a little simplistic and has a resulting number of challenges.</p> <p>The referenced table must have no ambiguity and guidance/training must be provided. This implies an education step.</p> <p>The tenderer/contractor needs to understand how to rate consequence/impact of failure so that they can assign a commensurate number layers of fault tolerance, avoidance/detection and handling mechanisms. This implies liaison with aircrew/operators and access to aircraft data.</p> <p>Need to make it clear this is for every credible failure path through the software having unacceptable/intolerable consequences (i.e., this is not for the single worst case failure of the whole software).</p> <p>This implies a full understanding of not only the architecture of the new software/LRU but also how it fits in the greater aircraft system, what failure may occur at the inputs and outputs, the full failure path through that system, and what impact those failures will have on aircrew and the aircraft.</p> <p>The severity rating scale needs to be defined and universally understood. Also what constitutes a “layer” must be defined.</p>

			<p>System and contract scope/responsibility boundaries will have to be defined.</p> <p>If specified pre-bid, any data provided to one tenderer needs to be provided to all to ensure a level playing field.</p> <p>It will need to be defined how the solution properties are to be communicated, documented and assessed.</p> <p>Also need to specify how the tenderer/contractor will verify compliance with this SOR clause. Every SOR requirement needs to be verifiable, and have a corresponding verification method defined in the associated VCRI.</p> <p>The acquirer will need to have a very good handle on how to assess claims against this requirement.</p> <p>Yes, outlining the required level of fault tolerance as part of the requirements gives greater certainty to the acquirer that the provided software will meet accreditation.</p> <p>Feasible, yes. The table references and evidence requirements would need to have consensus and to be comprehensive.</p> <p>Yes, but only with competent certification authorities.</p> <p>As per previous answers (B2.10), I am not convinced that the tabular approach is the right way. The words opposite up to the comma before “as specified {...” seem quite useable.</p> <p>Yes feasible.</p> <p>Feasible, yes.</p> <p>Yes.</p> <p>Feasible.</p> <p>Yes, seems straightforward articulation of the requirement.</p> <p>Yes, seems feasible. But not directly relevant to current civil certification.</p>				
	Informing Architectural Suitability						
D4.1b	[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	Narrative	In theory, it would be great to have such a clause, as it would definitely provide more information on the system’s architectural suitability to address systematic failures.				

	<p>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 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>	<p>Currently, tenderers would boast about how robust their processes are without actually providing credible evidence that they are capable of building systems can adequately deal with behaviours that are undesired. However, in this case, I would imagine that the CSSAS document would also be extremely limited in the level of architectural detail it can provide, given that they would not have even derived any software requirements at this stage. There is a risk that such a document would also result in just being a series of motherhood statements, with many caveats and few qualifications.</p> <p>Yes, however, it relies on the contractor having a fairly established design and also, understanding their system vendors (at component level) products and safety features. This is not a bad thing; it just raises the bar for the tender submission which adds cost to developing the submission and thus to the final price while reducing risk to the acquirer.</p> <p>Looks feasible but some may oppose to requesting new artefacts as part of a tender process which already requires a numerous number of documents to be provided.</p> <p>Again, yes agree generally. Comments at D4.1a apply equally.</p> <p>A DID would be required that defines the content of such a document.</p> <p>Can't emphasise enough the need for the acquisition/certification agency to be able to provide an example document that is not overly contrived or simplistic (in this country we still do not have a good example of a PSAC/SAS that is able to be made available to tenderers/contractors – mainly due to IP restrictions).</p> <p>Also need to emphasise the need for educating the tenderer with a training course and through provision of guidance.</p> <p>Yes, although again this is still potentially a large piece of work being done at risk by the tenderer.</p> <p>This would get primes to force their suppliers to live up to</p>
--	---	--

			<p>these tender docs, and not change the rotations of the earth later during contract execution.</p> <p>Yes, but only with competent certification authorities.</p> <p>As above, some of the italicised words seem useful but you have 2 statements and one document. I think these need to be merged in some way and the concepts (absence/detection handling mechanism) either removed or explained in a glossary description of the expected contents document.</p> <p>Yes feasible.</p> <p>Feasible, yes.</p> <p>Yes, although some tenderers may not have a solution maturity to enable them to write details. However, they should be able to document their approach.</p> <p>Feasible, but it would be good to see a DID of the documents to better understand how much work they would be.</p> <p>Feasible. May require some guidance to contractors on the level of effort required, to avoid grossly disproportionate levels of effort.</p> <p>Yes, seems feasible. But not directly relevant to current civil certification.</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	<p>It presents one way of determining the suitability of proposed solution. However, I would contend that the architectural description at the early stages (i.e. tender stage) would hardly be worth evaluating in detail, as it would unlikely be representative of the actual architecture.</p> <p>Yes. Although in the absence of a current framework, one can already request and achieve the same using current tender SORs.</p> <p>Generally agree</p> <p>Yes agree this should be feasible but wonder if we have enough good experienced and adequately skilled individuals in the acquirer organisations to make decisions with regard adequacy. My experience is that the required</p>				

			competency may not be there, and to compensate, acquisition agencies keep asking for more as they don't always know how much is good enough. Agreed. Yes. Feasible, but unlikely if certification authority is not involved. An approach like this might have benefits. Yes feasible. Feasible, yes. Yes. The benchmarks in these papers seem useful enough, and consistent with existing benchmarks. Feasible, yes. Yes. Yes, seems feasible. But not directly relevant to current civil certification.				
	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>My comments against D4.1, D4.1b apply here also.</p> <p>Yes this is entirely feasible, and would have saved a lot of work on 2 aircraft upgrade/acquisition projects I’ve been involved with.</p> <p>Simply it achieves this through the contractor having to clearly articulate it (and think about it up front). Applying the framework adds rigor and articulates expectations.</p> <p>Generally agree</p> <p>Yes appears feasible but may have initial teething problems.</p> <p>There needs to be good stakeholder engagement in establishing mutually agreeable SOR clauses.</p> <p>Suggest it is likely there will be inconsistent use and varied depth of information provided in contractor Software Architectural Assurance Document until such time that defence industry and acquisition agencies get up to speed and agree what constitutes acceptable content and detail.</p>				

	<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>		<p>This implies regular interaction, debate and feedback and even optimisation of DIDS/training through periodic symposiums and workshops.</p> <p>Yes, although evidence should be sort that development architecture is also tracking the CDRL architecture. It is my experience that these are regularity very disparate, and corrected in large steps late into a contract.</p> <p>Yes, feasible. The CDRL and DID will need to be vetted to ensure avionics/software is specifically addressed (not some boilerplate DID from 20+ years ago.).</p> <p>Feasible but unlikely that sufficient expertise exists in project teams of acquirer to make this a consistently viable approach.</p> <p>As per previous comments – possible.</p> <p>Yes feasible.</p> <p>Feasible, yes.</p> <p>Yes.</p> <p>Yes, this might potentially work, but there may be some solutions that it doesn't work well with because I architectural issues.</p> <p>Yes, this seems like a sensible document set to present this information in. As these will be new documents for many contractors, some examples would assist. For those using the safety argument paradigm, hopefully much of this information would already exist in a 'good' argument, but many arguments are just a rehash of the process mindset.</p> <p>Yes, seems feasible. But not directly relevant to current civil certification.</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> <p>1. Set benchmarks for argument and evidence suitability</p> <p>2. Proposal of argument and evidence using the tender process</p> <p>3. Evaluate argument and evidence suitability during the tender evaluation, and</p>	Narrative	<p>Similar comments to D4.1 would apply here.</p> <p>This would be nice but is-it really realistic to follow this approach during a tender process? Just wondering about additional effort involved,</p> <p>Agree feasible though again may not be without problems.</p>				

	4. Provide argument and evidence assurance during contract execution.		<p>GSN has been tried and rejected at BAE Systems, it is likely that analogous methods may suffer the same fate. Prescriptive approaches stifle design flexibility though provide better evidence. Getting the balance right is important.</p> <p>Biggest problem as you have mentioned in your paper will be if there is some disagreement on sufficiency of evidence during trials execution, particularly when the contractor believes what is being asked for is out of scope. This is an age old problem that plagues project every day. Having clauses that protect the acquisition agency in the SOW/SOR will be seen as an open chequebook by tenderers/contractors and will be untenable.</p> <p>Seems ok.</p> <p>Feasible, yes. Part of step 4 may be monitoring/surveillance by both acquirer and independent agencies.</p> <p>Looks good.</p> <p>Correct, it does.....</p> <p>Yes feasible.</p> <p>Feasible, yes.</p> <p>Yes, process feasible.</p> <p>Yes. Feasible process.</p> <p>Yes, feasible.</p> <p>Yes, seems feasible. But not directly relevant to current civil certification.</p>				
	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 an approach could set benchmarks for evidence suitability in a</p>	Narrative	<p>Yes it is feasible that it would set benchmarks for argument suitability in a contract. Getting agreement on both sides is less feasible however.</p> <p>Yes it is feasible that this approach could set benchmarks for evidence. The generic properties proposed already provide a good set of guiding principles for assessing the goodness of evidence.</p> <p>Yes, however one might need to include the relevant papers</p>				

	tender/contract? Explain why or why not?	<p>(‘assurance of claims and evidence’ etc) to aid the contractor in understanding.</p> <p>I don’t think that it is not feasible but I think that it will not be easy. In general I wonder about the general support that you will receive for this approach and the convincing argument you will have to make to change military procurement authorities.</p> <p>Yes I believe the proposed approach of setting benchmarks for evidence suitability is sufficiently feasible to make it worth giving it a trial on the right project.</p> <p>However, the process described is far more onerous than current approaches and will attract some resistance. It is likely to result in contractors and acquisition agencies requiring more educated and experienced staff, and contracts taking longer (hence being considerably more expensive).</p> <p>Though the whole of lifecycle cost/benefit is not discussed over traditional methods, it is possible that the proposed framework will result in smoother and more efficient certification and produce safer product. However design contractors generally do not participate throughout the whole lifecycle, and will seldom benefit from big picture savings.</p> <p>The framework needs to be far less intrusive for the majority of defence projects assessed as needing lower assurance levels such that it is almost business as usual. I believe this may be the case, though to use the DO-178B analogy, I have seen acquisition agencies try to apply inappropriately high assurance levels.</p> <p>Both of these approaches are feasible, but both require significant at risk work on behalf of the tenderer, which may reduce responses to a request to tender. A funded proposals round may be required for such a framework.</p> <p>Yes and Yes. So in addition to requirements tree, source and exec obj code is a great and complete set of evidence and products. The properties are very applicable to the above, especially any counter evidence that might exist or</p>
--	--	---

			<p>be found.</p> <p>Feasible and desirable if written and policed by regulatory authority and NOT acquirer project teams.</p> <p>6.1.1: You have previously used the word ‘architecture’ in what appears to be a mix of software and hardware architecture concepts. This section seems only to discuss software and hence you lose some of your argument. The strategy you outline does not seem to link attributes of DO178 to safety, but claims that this can be done. The example is you give is that an LLR is traceable to HLR – this is already an objective of DO178B and is further strengthened in DO178C (bi-directional traceability is required). Therefore it is difficult to see what this adds. The CSAL approach I have already commented upon and believe it adds an unnecessary layer of complexity and duplicates information for software that is already had to obtain.</p> <p>6.1.2: Examine your assumptions first. Just because you have not got limitless time/money does not necessarily limit the totality of evidence. In my world, $2+2=4$, how much time and money is required for this to be believed? Infinite? I recommend you remove this assumption. Second assumption is on the method and again is not always true. It might be limited because of the application upon which the method is being used. For instance, compliance with coding standards is relatively easy to do and demonstrate is completeness. Third bullet: If there are limitations in e.g. verification methodologies, this is a required declaration in the PSAC and the holes are expected to be filled by other techniques (possibly equally but differently flawed). I agree with [Wea03] on the properties of evidence.</p> <p>Yes feasible.</p> <p>Feasible, yes.</p> <p>Yes, Yes.</p> <p>Yes, Yes.</p> <p>Yes, these communicate the benchmarks in a generally</p>
--	--	--	--

			understandable manner. Some contractor education will be required. Yes, seems feasible. But not directly relevant to current civil certification.				
	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 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>	Narrative	<p>Yes it is feasible that this approach would inform the suitability of argument and evidence. However, to request such a level of detail with respect to evidence of assuring attributes for each constraint in a software item, at the tender phases seems extremely ambitious. At that stage, any information provided is always going to be optimistic.</p> <p>Yes it is feasible and such a document would aid in reducing project risk by increasing visibility of the required software assurance outcomes to the contract level. (rather than indirectly via a standard)</p> <p>Feasible but probably not easy.</p> <p>In addition the difficulty will be that evidence relevance, trustworthiness and results will likely be new concepts for the supplier. These concepts are quite novel and as such some organizations might resist these changes.</p> <p>Yes appears feasible but may have initial teething problems. Whilst having a product architecture rather than objective focus, this is familiar as it appears analogous to the DO-178B SDP & PSAC.</p> <p>Often contractors try to create SDPs and PSAC retrospectively and are faced with creating a document that describes what they have done rather than what they need to do. These documents should be gate/milestone through which a tenderer must pass before the contract is awarded (prior to detailed design/development)</p> <p>Good DIDS, templates, example document and training will be required.</p> <p>At this stage in the project, fine detail is not understood, therefore requiring a plan which will enforce methodology is premature. Better to request a software test plan, to ensure that whatever software is ultimately delivered, it is</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>	<p>well tested. This is in line with the principle of evidence collection, rather than the prescription of methodology.</p> <p>The software assurance plan idea as a sister to an SDP is great, but it depends on the constraints that are describe. Some developers may have the gall to believe they have no constraints. Too much internal process is relied on at certain developers/contractors where standards like DO-178B have not been applied – to where those contractors would likely refute having any/more constraints.</p> <p>Feasible, but expensive. Better approach is for the regulator to propose limits.</p> <p>It is unclear what the difference between the PSAC and the SAP would be. DO178 11.1.b Software overview “This section briefly describes the software functions with emphasis on the proposed safety and partitioning concepts...examples include resource sharing, redundancy, fault tolerance, mitigation of single event upset, and timing and scheduling strategies”. Also sub para c “summarizes the justification provided by the system safety assessment process, including potential software contributions to failure conditions”. It is accepted that perhaps it could be tightened up, but then in the verification section of DO178, it already describes the types of issues (bugs) that verification is expected to find and one should expect to see justification in the SVP why a certain technique is to be used. The purpose of the proposed SAP could therefore be seen as more a collection of already existing information, but this may have its merits. Another thought is that this is a re-badging of a safety argument.</p> <p>Yes feasible.</p> <p>Feasible, yes.</p> <p>Yes, the assurance plan provides a role similar to a PSAC, but is focussed on evidence sufficiency.</p> <p>Yes, feasible. To some extent extends current practices for SDPs and might improve PSAC like documents.</p> <p>I like the distinction between these plans, one saying what</p>
--	--	---

			<p>they do, the other justifying why it is sufficient. This later point is usually missed from the SDPs I normally see. It is even usually overlooked in some contractor PSACs.</p> <p>Yes, seems feasible. But not directly relevant to current civil certification.</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	<p>Yes, this approach would best rely on comparison against a defined benchmark. The whole idea behind the approach is after all to provide a more objective judgement of the goodness of evidence. Comparing against a benchmark decreases any tendencies for subjectivity in the assessment.</p> <p>Yes</p> <p>Likely feasible (previous comments apply)</p> <p>Agree feasible though general challenges described throughout responses to this section apply – particularly second part of response at D4.2.</p> <p>Yes</p> <p>Yes. True, if all the limitations and toolsets are known, as are the requirement sets. Provide a good academic examples, or real world anecdotes.</p> <p>Feasible but difficulties will arise due to a) requirement to involve regulator/certifier, b) bandwidth of regulator, c) experience of regulator.</p> <p>In principle – yes. However, there is also another problem and that is by having the information from multiple suppliers, it is often the case that MOD will cherry pick from all tenders and ask the winning bid to consider doing the extra bits from one of the losing bids. This is a persistent problem, especially where no bid meets or one only just meets the benchmark. It is human nature, esp within the military to have the ‘best’ and for civil servants to be seen to ‘add value’. Accordingly, at this stage industry is somewhat coy in providing too much information because competitive advantage leaks. The process you propose explicitly allows for extra negotiation and hence there is no credible defence against information</p>				

			(e.g. Intellectual Property) leakage. Yes feasible. Feasible, yes. Yes. Potentially, the project team would need specialists to do this. Yes. Yes, seems feasible. But not directly relevant to current civil certification.				
	Providing Argument and Evidence Assurance						
D4.2d	<p>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 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>	Narrative	<p>Agree that under this framework, a means for the supplier to summarise the compliance of claims against the prescribed benchmark.</p> <p>Yes,</p> <p>There may be (or appear to be by perception of the vendor) duplication with current activities (SOI #3 activities) or deliverables (00-56 Safety case), that may require resolution.</p> <p>Likely feasible (previous comments apply)</p> <p>Yes appears feasible. Whilst having a product architecture benchmark rather than objective focus, this is familiar as it is appears analogous to the DO-178B SAS.</p> <p>Challenges described throughout responses to this section apply – particularly D4.2.</p> <p>Yes. The required level of documentation is clearly and concisely described upfront.</p> <p>Many PM and Cert Authorities alike would love to see a summary document such as this. It often is lacking or is a piecemeal undertaking.</p> <p>Feasible but not cheap to product or certify.</p> <p>Cannot see the difference between this and a Software Accomplishment Summary or/and a re-badging of the safety case.</p>				

			<p>Yes feasible.</p> <p>Feasible, yes.</p> <p>Yes.</p> <p>Potentially, the project team would need specialists to do this.</p> <p>Summary documents conform to the normal model of plan, do, assess/review. These would be used for making compliance findings.</p> <p>Yes, seems feasible. But not directly relevant to current civil certification.</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.				2	9	9
D4.3b	The proposed framework will feasibly result in relative tender costs to acquirers versus current standards.			1	2	12	5
D4.3c	The proposed framework will feasibly result in relative contract costs to contractors versus current standards.		1	4	6	6	3
D4.3d	The proposed framework will feasibly result in relative contract costs to acquirers versus current standards.		1	4	7	5	3
D4.3e	Describe any cost implications with respect to the proposed framework?	Narrative	<p>The amount of risk that the contractor would take on as a result of such a framework is significantly higher than what they would take on under current prescribed standard. Although the framework aims to reduce or bound uncertainty is production of arguments, claims and evidence, there is also the element of uncertainty in the contractor's ability to meet the benchmark. This uncertainty will in turn materialise through increased cost.</p> <p>The contractor will be required to more tightly engage with their software team (or subcontractor) during the tender phase, thus increasing costs. (rather than the traditional method of putting the software team together after the</p>				

			<p>contract is won.</p> <p>Response above applies to higher assurance levels only, though it is hard to know how it would compare to DO-178B level A/B for example. Refer narrative at D4.2 & D4.2a. This country still has not come to grips with the cost of DO-178B.</p> <p>The pre contract work for both parties is greater, but the clarity in what is to be produced is greatly improved, which shroud lead to more accurate costing, and less likelihood of project slippage. The risk margins for both parties should therefore be lower.</p> <p>Most contractors might find creative ways to sell increased costs to customers.</p> <p>Training and maintenance of competency.</p> <p>More effort, defence against information/IP leakage. Cost increase by the contractor will be passed to the acquirer in some form.</p> <p>Although the tender will likely cost more, the implementation of the solution should avoid common issues that result in cost and schedule increases.</p> <p>In some cases, if major safety issues and redesigns are avoided then the real cost will be much lower. However it is impossible to ever prove this, because projects are almost never run twice.</p>					
	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.			1	1	12	6	
D4.4b	The proposed framework will feasibly result in relative tender schedule to acquirers versus current standards.			2	5	10	3	
D4.4c	The proposed framework will feasibly result in relative contract schedule to contractors versus current standards.			6	10	1	3	
D4.4d	The proposed framework will feasibly result in relative contract schedule to acquirers versus			8	8		4	

	current standards.						
D4.4e	Describe any schedule implications with respect to the proposed framework?	Narrative	<p>As above</p> <p>Reduces risk to the acquirer for the traditional ‘over-runs’ due to software assurance and protection mechanisms.</p> <p>Response above applies to higher assurance levels only, though it is hard to know how it would compare to DO-178B level A/B for example. Refer narrative at D4.2 & D4.2a. This country still has not come to grips with the cost of DO-178B.</p> <p>A product focused framework should reduce the assurance phase of the program significantly, at the cost of extra pre contract work for both parties.</p> <p>Agreement on correlation to existing standards may take time.</p> <p>The only schedule impact I can foresee is that there might be more certainty, but note the caveat of ‘might’.</p> <p>Although the tender will likely cost more, the implementation of the solution should avoid common issues that result in cost and schedule increases.</p> <p>As for cost.</p>				
	Systems Engineering Lifecycle Implications						
D4.5	Describe any systems engineering lifecycle implications to the proposed framework over and above contemporary practice?	Narrative	<p>Cost and schedule aside, the benefits to the systems engineering outputs will be enormous.</p> <p>Provides greater certainty and clarification and visibility of assurance (vs software features that the user is focused on)</p> <p>The evidence to be provided will have to be focused on the safety claims made. This will require a shift in the existing approach to software development for safety-critical systems where all the software within a single software component is treated in the same way with a DO-178B software level. Additional selective evidence will have to be provided and this will be new for SW engineer organizations.</p> <p>BAE Systems do have a defined Lifecycle Management (LCM) process, including defined Systems Engineering</p>				

			<p>system. This would have to be evaluated to see if it needed tweaking for the proposed framework. Potential problem areas are likely to be associated with in place processes for the bid and tender phases of the lifecycle.</p> <p>In this country, the proposed framework would have to be integrated with the AEO and Technical Airworthiness framework, including the TAMM. There are already big disconnects between ASDEFCON contracts and the TAMM, particularly with regard use of the word “approval” in different contexts.</p> <p>Any new framework needs to recognise the role an AEO, the SDE and his/her team of DEs provide, and how they satisfy the need for mechanistic/conceptual and intellectual independence and where the sponsor AEO, Project Office fits in with regard who does what with the various assessments of the framework outputs.</p> <p>It is also important that data originating from an AEO is recognised as being more “trustworthy” (due to the constraints, processes, competency assessments and measures that the AEO construct implies). Likewise, the framework needs to be integrated with Quality Systems and recognise what certifications such as ISO 9001/9100, etc, buy in terms of assurance confidence.</p> <p>It is not usual to provide more than a very abstract system architecture from the requirements before contract signing.</p> <p>May even reduce testing if contractor can prove robust processes and evidence up front.</p> <p>Additional things required earlier in the lifecycle.</p> <p>None that I know of.</p> <p>Might help enforce a better focus on requirements and architecture earlier in the lifecycle, which is consistent with systems engineering methodologies.</p> <p>More work in the front end. There is already such a great push regarding doing more with requirements in the front end of programs, that there may not be time.</p> <p>This is a new way of thinking for both projects and</p>
--	--	--	---

			<p>contractors, which will mean the lifecycle has to adapt to changes in expectations and activities.</p> <p>Not is a position to comment.</p>				
	Project Management Implications						
D4.6	Describe any project management implications to the proposed framework over and above contemporary practice?	Narrative	<p>Administrative burden associated with managing a framework that is much more complex would impose many challenges to project management (cost estimation, schedule management, compliance assurance effort).</p> <p>Intertwining the proposed framework with current internal practices to show compliance to all the required standards for all programs (IEEE 12207, ISO9001, DO-178B, etc), starts to increase the overheads and management burden.</p> <p>It is likely adopting a new framework will incur some risk initially, at least whilst it is new and remains an unknown quantity. Pressures to produce attractive bids and win contracts will remain. It is likely to take longer and be more costly getting into contract. Despite the framework attempts to make explicit what is required, it is likely that initially there will continue to be protracted disagreements over SOR requirements interpretation and scope, particularly with regard how much evidence is enough (mainly due to inexperience in both the supplier and buyer organisation). All of this implies a need for better project management and higher associated costs.</p> <p>Workload should be reduced, as uncertainty in non functional requirements is reduced (accreditation), which should reduce the burden on PM to resolve queries.</p> <p>PMs need to be versed in these standards, not just salesmen/businessmen, else software SMEs can fake compliance.</p> <p>Costs</p> <p>It may mean separate teams to do tender evaluation which implies a significant cost and management overhead to try to avoid accusations of IP leakage. However, it is just another thing to be managed, but how it might integrate is another aspect I cannot consider.</p>				

			<p>Education of contractors.</p> <p>Project managers have more to manage earlier in the program.</p> <p>As for D4.5</p> <p>Not is a position to comment.</p>				
	Contract Management Implications						
D4.7	Describe any contract management implications to the proposed framework over and above contemporary practice?	Narrative	<p>Administrative burden associated with managing a framework that is much more complex would impose many challenges to contract management.</p> <p>Increased program workload – at tender stage, demonstration of compliance. However the result is improved product (safety) assurance.</p> <p>Although not my area of expertise, it may be that contracts will be more complicated. It may also be that there is a greater need to have a mechanism for requirements once the preferred architecture and solution is known.</p> <p>Would be easier to enforce scope discussions and clear up evidence/artefact reviews.</p> <p>Intellectual property leakage is almost impossible to defend against accusation should any change be made to a winning bid – and they always are....it is the Law of the Sod!</p> <p>Education of contractors.</p> <p>As above.</p> <p>As for D4.5</p> <p>Not is a position to comment.</p>				
	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</i> </p>	Narrative	<p>It is feasible. However the contractor may see this as a risk to their delivery (over contemporary methods), and may pass on the costs of this risk in the acquisition price.</p> <p>Looks a bit optimistic to me.</p> <p>Narrative at D4.2 applies, i.e., this may be seen as an open chequebook by tenderers/contractors and hence will incur high risk dollars being included in costings or will be just seen as untenable.</p>				

<p><i>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> <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>	<p>There is a large risk in signing this if the requirements are not extremely transparent.</p> <p>Contractors may come up with some astronomical prices though and cite “moving targets” and “never ending requirements creep”. If the uncertainty is defined enough, the cost may be tolerable for an iron-clad SOW task.</p> <p>This is only feasible if the acquirer actually knows what he wants and sticks to it. Virtually unknown in ADF and BAE history.</p> <p>Too reliant on knowledge upfront and for DMO to free up sufficient funding.</p> <p>Whilst I like the words, the framework has flaws as per previous comments. It also assumes competence by both acquirer and contractor. This might be a gross assumption about at least one of the parties and hence the words are meaningless. Having just done a survey of software safety within DE&S, I can confirm that there are projects being managed by individuals who have no idea of the implications of software issues.</p> <p>Feasible, but few contractors would accept.</p> <p>Yes, but we wouldn’t accept this in contract negotiation. May be useful during tender phases.</p> <p>Feasible, but most contractors wouldn’t sign up to this.</p> <p>Interesting, but would result in large contingency risk costs in project estimates, irrespective of how confident the contractor was.</p> <p>Interesting, and I can see the intent. It would be interesting to run an evaluation on a real tender to ask for these costs, and see how much they vary.</p> <p>I suspect most contractors would deliberately try to make it expensive, so the tender chosen would need to be one where competition out ways risk aversion.</p> <p>May be challenging for developers to sign up to. This may increase contractual compliance risk, and thus increase cost.</p>
--	---

	Usability		
D4.9	What is your overall belief regarding the usability of the contracting framework for addressing the motivating issues and limitations with the current state of practice identified earlier within these survey questions?	Narrative	<p>The contracting framework looks good, specifically for large, high risk, fleet upgrades or new fleet acquisitions. Getting visibility of assurance requirements to the tender and tender evolution phases can only be positive.</p> <p>I anticipate that the application of the complete framework will be challenging because of its novel approach and because position vis a vis DO-178B is not clearly defined. I see the first part of the framework, obtaining architectural certainty as a very valuable approach that could likely be integrated by itself in new tenders Obtaining architectural certainty alone would likely reduce substantially the safety risk at contract signature time.</p> <p>Any evidence of moving these concepts from academia to the real world would constitute tangible assets for this framework.</p> <p>Previous comments apply throughout this session. Outcomes of this survey should be used to adjust your approach and address user community concerns. Updated approach should be broached with user community and including industry through engagement at the right levels. If there is enough interest, this may result in a trial if funding is able to be found.</p> <p>It is better than not specifying the requirements for certification as present.</p> <p>Good framework, but too dependent on certifier bandwidth and funding.</p> <p>It is not useable by MOD personnel as it is too complex, requires duplicate artefacts at architecture that are already somewhat difficult to define at software level, but does have some good words which may be useable in contracts.</p> <p>Useful. Requires further evaluation through example or trial.</p> <p>Potentially useable if a suitable case study backs it up.</p> <p>Potentially a usable framework which addresses some of the problems of the current approaches. Requires further</p>

			<p>case study and trial application.</p> <p>Interesting ideas. Would need to see an example or case study from practice.</p> <p>Overall, this seems to address many of the problems we already confront. It requires further evaluation and practice to see what real practical drawbacks it has.</p> <p>Overall, this seems useable in the military environment, which differs from the civil environment.</p>
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	