

You can save this page as HTML and then open it in Microsoft Word for further editing.

Title	Specific risk and standardised criteria for conducting aeroplane-level safety assessments of critical systems
NPA Number	NPA 2014-02

UK CAA (European.Affairs@caa.co.uk) has placed **13** unique comments on this NPA:

Cmt	Segment description	Pag	Comment	Attachm
44	3. Proposed amendments - CS-25 - Book 1 - CS 25.671	12 - 14	<p>Page No: Multiple, but commences on page 13</p> <p>Paragraph No: Multiple, but commences in CS25.671(c)(2); see also 25,671(c)(3)(iii) and 25.1309(b) para 6(ii) on page 41.</p> <p>Comment: The 1/1000 probability value associated with latent failures does not appear to be presented consistently and there is ambiguity in how this is to be applied, and variability in description which does not support a consistent approach to dealing with this.</p> <p>Justification: The value is not clearly explained; but it is implied as not the same as 1E-3 per flight hour. It is stated to be a probability (e.g. 25.671(c)(3)(iii) but the type of probability is not clear. When this is presented in the new text for 25.671(c)(2)(ii) on page 13 there is a suggestion that a latent failure of 1/1000 the probability of all other subsequent failures must be less than 1E-5. As presented, this implies that an overall rate of 1E-8 might be acceptable for a catastrophic failure and this is not thought to be the intent. In later examples, such as in the section covering compliance with 25.1309(b) para (6)(ii) at the top of page 41, the example used adds more clearly to an overall extremely improbable target of 1E-9, with reference to appendix 5 as examples. But overall the value remains ambiguous.</p> <p>Proposed Text: A clarification of the 1/1000 value is needed throughout the NPA.</p>	
45	3. Proposed amendments - CS-25 - Book 1 - CS 25.933	14	<p>Page No: Page 14 and page 33</p> <p>Paragraph No: Subpart E Powerplant – CS 25.933 Reversing Systems</p> <p>Comment:</p> <ol style="list-style-type: none"> CS25.933 has been changed to include the requirement to directly comply with 25.1309(b). The new wording in AMC 25.933 is contradictory. <p>Justification:</p> <ol style="list-style-type: none"> It is not apparent that the AMC 25.933 has been changed to be consistent with the proposed 25.933, in particular related to the latent failure requirements in 1309(b)(5). For example the 1/1000 value is not included in the AMC 25.933, yet the AMC provides guidance on addressing latent failures in thrust reverser systems. AMC 25.933 states that latent failures “should be 	

			<p>avoided whenever practical", but then further states that "neither failure may be pre-existing".</p> <p>Proposed Text: Amend AMC 25.933 to be consistent and match the intent of 25.1309.</p>	
46	3. Proposed amendments - CS-25 - Book 1 - CS 25.1309	14 - 15	<p>Page No: Multiple, but evident on page 15 and subsequent</p> <p>Paragraph No: CS25.1309(b)(4), (b)(5) and many subsequent paragraphs of CS and AMC.</p> <p>Comment: A new term has been introduced into the requirements and AMC by this NPA. The word encompassing this is "practical". The concept it embodies reaches beyond what should be applied. It is unclear whether the term should actually be Practicable rather than Practical to define the extent by which something can be done. However it is perceived that "Practical" and "Impractical" should be replaced with "Reasonably Practicable" and "Reasonably Impracticable".</p> <p>Justification: Many cases of usage now exist, an example is used to illustrate the issue:</p> <p>CS25.1309(b)(4) Any significant latent failure is minimised to the extent practical; and</p> <p>CS25.1309(b) (5)(i) it is impractical to provide additional fault tolerance.</p> <p>By requiring minimisation to the extent practical makes no allowance for technical complexity or cost in achieving this aim. The implication is that "if it is practicable", it must be done... regardless of cost or benefit. We do not believe this is economically viable for the majority of failure conditions to be considered.</p> <p>Consideration should possibly be given to the approach that considers the reasonableness of further safety mitigation so that risks/hazards are reduced So Far As Is Reasonably Practicable (SFAIRP), a term used in H&S legislation.</p> <p>A means of compliance with SFAIRP is the techniques used to reduce risks to a level that is As Low As Reasonably Practicable (ALARP), the important aspect being "Reasonably".</p> <p>In 1309(b)(1)(2)(3) we have qualitative limits set to define what we consider to be "good enough" in terms of safety objectives; these limits can be considered as reasonably practicable, but we do not embody the spirit of ALARP, because to do so would mean that the objectives are not really good enough and more should be done if it were reasonably practicable to do so.</p> <p>However, to minimise significant latent failures to the extent practical would essentially require a demonstration of their minimisation essentially to the point of zero unless it could be shown that this is not technologically possible. Cost and benefit in this minimisation are irrelevant.</p> <p>If the requirement was to minimise the significant latent failures to the extent reasonably practicable, then the</p>	

			<p>process would be to minimise the risks to the point whereby their continued minimisation is no longer beneficial, where continued effort expended would outweigh any additional benefit considering factors such as technological development and cost... and possibly complexity and weight too. Here, a more practical approach can be taken to minimisation, allowing engineering judgement and industry experience to be used; to maintain a requirement of "to the extent practical" could be harmful to the industry.</p> <p>In addition CS25.1309c.(2) introduces the terminology "technologically feasible" and "economically practical", which appear to head towards the concept of reasonably practicable, implying that the concept is plausible.</p> <p>Finally, the last statement on page 41 against 25.1309c.(6) refers to what can be feasible and practical changing with time and circumstances. This is one of the aspects of the ALARP principle used in many industries, whereby the developing organisation is responsible for maintaining the risks of or to their product as low as reasonably practicable for the life of the product, including the monitoring of new technologies that could improve safety. The logistics of this clearly requires a post-delivery-support contract, but it is a concept already in place.</p> <p>Proposed Text: Change "Practical" and "Impractical" to "Reasonably Practicable" and "Reasonably Impracticable".</p>	
47	3. Proposed amendments - CS-25 - Book 2 - AMC 25.671	18 - 32	<p>Page No: 22</p> <p>Paragraph No: 9 Evaluation of... - CS 25.671(c)</p> <p>Comment: 4th paragraph is ambiguous and requires revision.</p> <p>Justification: This states that "<i>CS 25.671(c)(2) requires the evaluation of any combination of failures not shown to be extremely improbable, excluding the types of jams...</i>" which is inaccurate as they should positively be shown to be extremely improbable</p> <p>Proposed Text: Change sentence to "<i>to CS 25.671(c)(2) requires the evaluation of any combination of failures to show that they are extremely improbable, excluding the types of jams...</i>"</p>	
48	3. Proposed amendments - CS-25 - Book 2 - AMC 25.671	18 - 32	<p>Page No: 24</p> <p>Paragraph No: (b) related to determination of control system jam positions - CS 25.671(c)(3)</p> <p>Comment: The AMC related to determination of control system jam positions - CS 25.671(c)(3) on page 24, uses an argument that a value for 15Kts can be used for crosswinds considering that a jam will more likely be encountered before the aircraft reaches V1 as opposed to between V1 and VLOF. Such an argument appears valid. However, the subsequent paragraph suggests that the same argument can be used for the approach and that a reasonable crosswind value during approach and landing of 15Kts can equally be used. But the justification seems less valid.</p>	

			<p>Justification: For takeoff, the likelihood of encountering a control jam before V1 will be due to the greater control input used at slower airspeed than at V1, so the likelihood of encountering a jam reduces; for the approach, the speed will be decaying as the approach continues, so the likelihood of encountering a jam increases as the approach and landing continue, and this implies the opposite logic for the take off case; so the justification for limiting the crosswind value for calculations at 15Kts does not seem justified.</p> <p>Proposed Text: "crosswind values for landing should not be limited to 15kts but should be as defined for the aircraft limitations."</p>	
50	3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309	33 - 47	<p>Page No: 35</p> <p>Paragraph No: 4h</p> <p>Comment: Throughout the document, a global find and replace of "airplane", with "aeroplane" would be appropriate. "Aircraft" is not the correct term either as this encompasses more than just fixed wing aeroplanes which CS25 focuses.</p> <p>Justification: As a NPA for CS 25, the terminology related to Large Aeroplanes should be used. Airplane is an American term used within the FARs.</p> <p>Proposed Text: Replace each instance of "Airplane" with "Aeroplane".</p>	
51	3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309	33 - 47	<p>Page No: 36</p> <p>Paragraph No: 5f</p> <p>Comment: AMC25.1309 Definitions on page 36 has seen the deletion of the definition for Complex with no identified alternative provided. A new definition for "Complexity" is added, but complexity is only a means of measuring how complex something is.</p> <p>Justification: Without the definition for when something's complexity has been assessed to be "complex" many other aspects of the NPA's AMC material lose their definition; complex is a frequently used term which now lacks a definition.</p> <p>"Complex" is not defined in related industry documents, e.g. ED-79A/ARP4754A because it is/was defined within the AMC. Its removal will be problematic, we do not believe that it should have been deleted. The addition of "complexity" seems a good idea but not at the expense of losing the definition for complex.</p> <p>Many entries are still made within the document to things that are "complex"; if the definition is lost, these lose their meaning.</p> <p>Proposed Text: Retain the definition for Complex; include the new definition for complexity as a measure of how complex a function, system or item is.</p>	
52	3. Proposed amendments - CS-25 -	33 - 47	<p>Page No: 37</p> <p>Paragraph No: 8 c. (3)</p>	

	Book 2 - AMC 25.1309		<p>Comment: The NPA introduces new text for para c. Item (3) deals with the latency aspect but is difficult to understand as written because in total it implies that the subject (each catastrophic failure condition) is remote... and clearly it needs to be extremely improbable.</p> <p>Justification: As presented, the text allows a catastrophic condition arising through two failures, one of which is latent, to only be remote rather than extremely improbable, and it does not specify that it is the non-latent failure that must be remote and the two together extremely improbable.</p> <p>Proposed Text: "When a catastrophic failure condition can result from two failures, either of which is latent for more than one flight, the remaining failure is remote when either one is pre-existing."</p>
53	3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309	33 - 47	<p>Page No: 40</p> <p>Paragraph No: (6) compliance with CS 25.1309(b)(4) and (5)</p> <p>Comment: The third paragraph that begins "There can be situations..." goes on to say that "... it may not be in the public interest to rigidly apply such criterion." This seems to imply that compliance is unnecessary and this does not seem to be valid AMC material.</p> <p>The fourth paragraph then states that a demonstration of compliance is not expected, but that if the Agency identifies a significant latent failure of concern the applicant will need to provide evidence of impracticality. This is difficult because it puts the responsibility of finding compliance on the Agency, whereas the applicant should normally demonstrate compliance for the Agency to accept.</p> <p>Noting the point raised in b above, where responsibility for determination of significant latent failures is put on the Agency, the paragraph that deals with CS 25.1309(b)(5) compliance states that significant latent failures of concern should be highlighted to the agency as early as possible. This would seem a valid statement, but does it not mean that the statement in the previous paragraphs dealing with 1309(b)(4) are now contradicted?</p> <p>Justification: The means by which latent failures are to be identified within the paragraphs addressing compliance with CS 25.1309(b)(4) and (5) are contradictory.</p> <p>Proposed Text: Revise text such that compliance is shown by the applicant</p>
54	3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309	33 - 47	<p>Page No: 41</p> <p>Paragraph No: c (2) Compliance with CS 25.1309(c)</p> <p>Comment: The paragraph suggests that the loss of annunciation should be considered a Major failure condition, whereas it should be assessed in its own right in accordance with 25.1309b but in recognition of the associated failure condition that it is responsible for annunciating.</p>

			<p>Justification: The failure of an indication system is similar to the failure of a protection system; whilst the loss of the system in conjunction with the failure that it is supposed to annunciate could be significant (or catastrophic in some cases for protection systems), the loss of the indication or indication system alone should be assessed in its own right in accordance with 1309b. To state categorically that it is major would be an unnecessary burden if the 1309b assessment showed that the loss of the indication was simply dealt with and resulted in a slight reduction in safety margins only ... or slight crew workload increase, when it would normally be Minor. In other cases, the loss of indication might be more than Major. This is not to be confused with the assignment of the FDAL per ED-79A Section 5.2.4 that might assign a minimum FDAL of C for a protection system associated with a catastrophic failure. Clarification of the desired intent in this approach is therefore requested.</p> <p>Proposed Text: "Loss of annunciation should be assessed in accordance with 25.1309b in its own right and in combination with the failure of the function that it is associated with."</p>	
55	3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309	33 - 47	<p>Page No: 42</p> <p>Paragraph No: c. (2)(ii)</p> <p>Comment: New text refers to considerations that could "affect the FHA outcome," It is considered that it is important if they affect the functional failure condition classification, to be more specific.</p> <p>Justification: Output of FHA here would be the FFCC</p> <p>Proposed Text: Change to: "... or diversion time can adversely affect the functional failure condition classification, ..."</p>	
56	3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309	33 - 47	<p>Page No: 44</p> <p>Paragraph No: 11 g</p> <p>Comment: The second paragraph, having stated that extremely remote operational or environmental conditions might be considered, it states that in such cases it is acceptable to classify the single failure as at least major to ensure adequate development assurance and reliability. It is not clear why this is suggested because the severity of the failure cannot be considered as "at least major", it has to be considered as catastrophic in combination with the operational or environmental conditions.</p> <p>Justification: Section 5.2.4 of ED-79A clearly identifies that this can then be used to ensure that adequate development assurance and reliability are assigned to the system. This deals with protection systems, but applies here equally. The text as presented would jeopardise that agreed methodology and we would like to understand the rationale for its suggested inclusion.</p> <p>The intent is to ensure adequate development assurance, and thus 5.2.4 of ED-79A addresses this by allowing nothing lower than FDAL C; this is not the same as a FFCC</p>	

			of Major. Proposed Text: "In these limited cases, it is acceptable to assign a development assurance level of B or C to ensure adequate development assurance and a commensurate reliability for the systems that provide protection against the events."	
57	3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309	33 - 47	Page No: 45 Paragraph No: 12 a Comment: Final sentence of paragraph at top of page 45 suggests that the AFM will contain all the expected crew actions. This is not practical. Justification: The AFM will contain all the necessary procedures that the crew should follow, but it cannot contain all expected crew actions which could be much higher... it should actually dictate what should be done. Proposed Text: "The applicant should provide a means to ensure the AFM will contain all the required crew actions."	