



Comment-Response Document 2014-02

Specific risk and standardised criteria for conducting aeroplane-level safety assessments of critical systems

Specifications for flight control systems and aeroelastic stability

CRD to NPA 2014-02 — RMT.0049 (25.029)

EXECUTIVE SUMMARY

This Comment-Response Document (CRD) contains the comments received on Notice of Proposed Amendment (NPA) 2014-02 (published on 27 January 2014) and the responses provided to them by the European Aviation Safety Agency (EASA).

It also contains the draft resulting CS-25 text.

Compared to the NPA 2014-02 proposal, several changes have been made to the proposed CS/AMC 25.1309 (system safety assessment) and CS/AMC 25.671 (flight control systems) to clarify various elements based on the comments received while keeping the main elements of the NPA proposal. Some provisions have also been added to address controllability during ditching with no engine power. Concerning the changes to the domain of structure, the proposed amendments to CS 25.629(b), AMC 25.629 and Appendix K are withdrawn; however, the proposed amendments to CS 25.629(d) are maintained. Finally, the proposed amendments concerning reversing systems in CS/AMC 25.933 are maintained.

Stakeholders are invited to review the draft resulting text (Appendix B) and provide their reactions, if any.

EASA will then prepare the next amendment of CS-25, taking into account the reactions received, if any.

Action area:	Design and maintenance improvements		
Affected rules:	CS-25 Large Aeroplanes		
Affected stakeholders:	Manufacturers of large aeroplanes and related airborne equipment		
Driver:	Safety; level playing field	Rulemaking group:	No
Impact assessment:	Light	Rulemaking Procedure:	Standard

EASA rulemaking process milestones

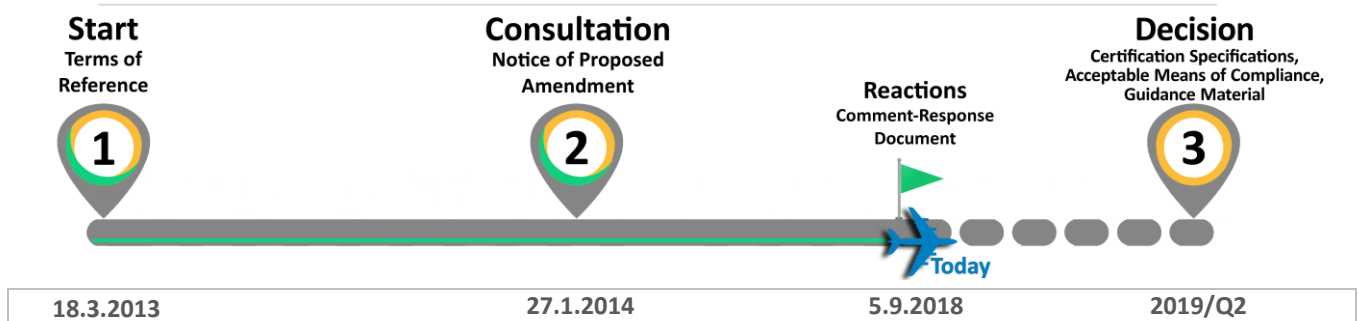


Table of contents

1. Procedural information	3
1.1. The rule development procedure	3
1.2. The structure of this CRD and related documents	3
1.3. The next steps in the procedure	3
2. Summary of the outcome of the consultation	4
3. Individual comments and responses	7
4. Appendix A — Attachments	175
5. Appendix B — Resulting text	176



1. Procedural information

1.1. The rule development procedure

EASA developed this CRD in line with Regulation (EC) No 216/2008¹ (hereinafter referred to as the 'Basic Regulation') and the Rulemaking Procedure².

This rulemaking activity is included in the EASA 5-year Rulemaking Programme³, which is part of the European Plan for Aviation Safety (EPAS) for 2018–2022, under rulemaking task RMT.0049. The scope and timescales of the task were defined in the related Terms of Reference (see cover page).

This draft amendment of CS-25 has been developed by EASA. All interested parties were consulted through NPA 2014-02⁴, which was published on 27 January 2014.

The text of this CRD has been developed by EASA.

Please refer to the cover page for the major milestones of this rulemaking activity.

1.2. The structure of this CRD and related documents

This CRD provides a summary of the comments and responses as well as the full set of individual comments (and the responses to them) received on NPA 2014-02. The draft resulting text is provided in Appendix B to this CRD.

1.3. The next steps in the procedure

The ED Decision amending Decision 2003/002/RM (CS-25) will be issued at the earliest 2 months after the publication of this CRD to allow for any reactions of stakeholders regarding possible misunderstandings of the comments received and the answers provided to them by EASA. This exceptional reaction period was decided by EASA because of the long delay since the publication of NPA 2014-02, the substantial nature of the proposed amendments to CS-25, and the nature of the comments received showing a need to improve various elements of the proposal.

Stakeholders are requested to submit their reactions, if any, not later than **5 November 2018** using the automated **Comment Response Tool (CRT)**, which is available at <http://hub.easa.europa.eu/crt>⁵.

¹ Regulation (EC) No 216/2008 of the European Parliament and the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC (OJ L 79, 19.3.2008, p. 1) (<http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1467719701894&uri=CELEX:32008R0216>).

² The Agency is bound to follow a structured rulemaking process as required by Article 52(1) of the Basic Regulation. Such a process has been adopted by the EASA Management Board (MB) and is referred to as the 'Rulemaking Procedure'. See MB Decision No 18-2015 of 15 December 2015 replacing Decision 01/2012 concerning the procedure to be applied by EASA for the issuing of opinions, certification specifications and guidance material (<http://www.easa.europa.eu/the-agency/management-board/decisions/easa-mb-decision-18-2015-rulemaking-procedure>).

³ <https://www.easa.europa.eu/document-library/rulemaking-programmes>

⁴ <https://www.easa.europa.eu/document-library/notices-of-proposed-amendments/npa-2014-02>

⁵ In case of technical problems, please contact the CRT webmaster (crt@easa.europa.eu).



2. Summary of the outcome of the consultation

EASA received 323 comments from 24 stakeholders, distributed as indicated below.

S	Page	Description	Comments
0	-	(General Comments)	12
1	1	Executive Summary	1
2	5-6	2. Explanatory Note (Paragraph 2.2, 2.2, 2.3)	2
3	6-11	2. Explanatory Note (Paragraph 2.4)	2
4	12	3. Proposed amendments	1
5	12	3. Proposed amendments - CS-25 - Book 1 - CS 25.629	10
6	12-14	3. Proposed amendments - CS-25 - Book 1 - CS 25.671	36
7	14	3. Proposed amendments - CS-25 - Book 1 - CS 25.933	1
8	14-15	3. Proposed amendments - CS-25 - Book 1 - CS 25.1309	26
9	15-16	3. Proposed amendments - CS-25 - Book 1 - APPENDIX K	7
10	17	3. Proposed amendments - CS-25 - Book 2	2
11	17	3. Proposed amendments - CS-25 - Book 2 - AMC 25.629	9
12	18	3. Proposed amendments - CS-25 - Book 2 - AMC 25.671(c)(1)	1
13	18-32	3. Proposed amendments - CS-25 - Book 2 - AMC 25.671	81
14	33	3. Proposed amendments - CS-25 - Book 2 - AMC 25.933(a)(1)	3
15	33-47	3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309	115
16	47-50	3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309 - new Appendix 5	9
17	51-58	4. Regulatory Impact Assessment (RIA) - 4.1 - 4.5	6

2.1. Commentators

Stakeholders who commented on NPA 2014-02 comprised:

- large aeroplane manufacturers (Airbus, Boeing, Bombardier, Dassault, Embraer, Gulfstream, Textron);
- aircraft systems or equipment manufacturers (Garmin International, Lockheed Martin Aeronautics, Rockwell Collins, Thales Avionics, Universal Avionics Systems Corporation);
- engine manufacturers (GE Aviation, Safran, Rolls-Royce);
- national aviation authorities (CAA Netherlands, CAA United Kingdom, DGAC France, FAA United States, LBA Germany, TCCA Canada);
- INTA (National Institute of Aerospace Technology, Spain);
- and two individuals.

2.2. General

Some comments reflected former dissenting opinions stated within the reports issued by the Flight Controls Harmonisation Working Group (FCHWG) and the Airplane-level Safety Analysis Working Group (ASAWG); various comments showed a need to improve the text to avoid confusion and provide clarification.

2.3. Ditching with no engine power

After the NPA consultation, EASA decided to make changes to the proposed amendments to CS 25.671(d) and the new AMC 25.671, in order to address the scenario of ditching with no engine power. Investigations or studies related to ditching accidents revealed that the most frequent factor



requiring a ditching is engine power loss, and in the majority of the cases a total engine power loss. Refer, for instance, to:

- NTSB accident investigation report NTSB/AAR-10/03, adopted on 4 May 2010, Loss of Thrust in Both Engines After Encountering a Flock of Birds and Subsequent Ditching on the Hudson River - US Airways Flight 1549 - Airbus A320-214, N106US - Weehawken, New Jersey on 15 January 2009, and
- DOT/FAA/TC-14/8 Review and Assessment of Transport Category Airplane Ditching Standards and Requirements, Final report dated May 2015.

Such scenario should therefore be considered for the certification of large aeroplanes in order to ensure that they are controllable and that the ditching configuration and parameters can be attained in the event of a total power loss.

After the Hudson River accident, the NTSB addressed the following safety recommendation to EASA:

UNST-2010-091: 'Require applicants for aircraft certification to demonstrate that their ditching parameters can be attained without engine power by pilots without the use of exceptional skill or strength. (A-10-91)'

In NPA 2014-06 'Regular update of CS-25'⁶, the proposed amendment of CS 25.671(d) and the corresponding material in the proposed new AMC 25.671 addressed the scenario of emergency landing following the loss of all engine power.

Because of the similarities in terms of design requirements and operational procedures required to ensure the controllability of the aeroplane after the failure of all engines to perform an emergency landing on ground and on water, EASA has amended CS 25.671(d) and AMC 25.671 to include the ditching scenario. This should not create new system design constraints compared to the NPA proposal, because the flight control system power requirements are considered to be similar for the ditching case compared to the landing case. However, this will ensure that adequate aeroplane flight manual (AFM) procedures are provided and evaluated to ensure that they are adapted to the 'no engine power' case.

2.4. Harmonisation with the FAA and TCCA

A wish to ensure harmonisation with the Federal Aviation Administration of the United States (FAA) and Transport Canada Civil Aviation (TCCA) has been expressed. EASA agrees with this goal — this is the reason why the publication of this CRD has been delayed since 2014. EASA has indeed been waiting for the publication of an equivalent FAA Notice of Proposed Rulemaking (NPRM) and draft Advisory Circulars in view of harmonising the certification specifications and acceptable means of compliance. Because of the recurrent postponement of the publication of the equivalent NPRM, EASA decided to proceed with the rulemaking task and publish this CRD. Should the FAA publish an NPRM in the coming months, EASA will take it into account when preparing the related ED Decision that will amend CS-25 and will seek harmonisation as far as possible.

⁶ <https://www.easa.europa.eu/document-library/notices-of-proposed-amendments/npa-2014-06>

2.5. Summary of the main changes made to the proposed amendments to CS-25

The main changes made compared to the proposal contained in NPA 2014-02 are summarised as follows:

a) CS/AMC 25.629 and Appendix K (Structure)

The proposed change to CS 25.629(b) was mainly driven by examples of changes in aerodynamic coefficients and redistribution of air loads due to structural and control deflections at higher load factors, which caused aeroelastic stability issues that were not predicted analytically but were discovered by flight test. However, it is recognised that this proposed change is not directly related to the main issues addressed by NPA 2014-02 and hence both this proposal as well as the proposed change to AMC 25.629 are withdrawn. The proposed change to Appendix K is also withdrawn as according to the comments received it goes beyond the initial scope of interaction of systems and structure, and further discussions between authorities and the industry are suitable before making such change. Finally, the proposed change to CS 25.629(d) has been maintained.

b) CS/AMC 25.671 (Flight control systems)

The text of the rule has been clarified while maintaining its intent. In CS 25.671(d), the ditching case has been added.

The AMC has been clarified, and new definitions have been added. In Chapter 8, changes have been made to reflect the introduction of the ditching case in CS 25.671(d).

Chapter 12 has been added at the end of the AMC to address the specificities of fly-by-wire flight control systems. The text has been derived from two generic Certification Review Items (CRIs), entitled 'Control Signal Integrity' and 'Formalisation of Compliance Demonstration', providing acceptable means of compliance and interpretative material that support compliance with CS 25.671 for fly-by-wire flight control systems in large aeroplanes.

c) CS/AMC 25.933 (Reversing systems)

The proposed amendments have been maintained.

d) CS/AMC 25.1309 (System safety assessment)

The text of the rule has been clarified while maintaining its intent; in particular, the specifications related to catastrophic failure conditions involving latent failures have been improved based on the comments received. In the AMC, various improvements of the wording have been made, new definitions have been added, and more notably, the 1/1000 criterion associated to the compliance with CS 25.1309(b)(4) has been withdrawn; the new text reflects the objective of 1) eliminate significant latent failures to the extent practicable, and 2) limit the latency of the remaining significant latent failures.

e) General

Other changes have been made to reflect the evolution of CS-25 that took place since the publication of NPA 2014-02. The changes show the status relative to CS-25 Amendment 21.

3. Individual comments and responses

In responding to comments, a standard terminology has been applied to attest EASA's position. This terminology is as follows:

- (a) **Accepted** — EASA agrees with the comment and any proposed amendment is wholly transferred to the revised text.
- (b) **Partially accepted** — EASA either agrees partially with the comment, or agrees with it but the proposed amendment is only partially transferred to the revised text.
- (c) **Noted** — EASA acknowledges the comment but no change to the existing text is considered necessary.
- (d) **Not accepted** — The comment or proposed amendment is not shared by EASA.

(General comments)

-

comment 6 comment by: *Luftfahrt-Bundesamt*

The LBA has no comments on NPA 2014-02.

response Noted.

comment 7 comment by: *CAA-NL*

We have no specific comments to this NPA, the proposals seems to be quite wel harmonised with the FAA.

response Noted.

comment 8 comment by: *DGAC France*

DGAC France has no specific comments on this NPA.

response Noted.

comment 183 comment by: *AIRBUS*

PROPOSED TEXT / COMMENT:

Airbus note that the changes proposed to the Structures paragraphs in this NPA have not been discussed with the appropriate Structure Regulatory and Industry representatives, more specifically the L&DHWG. Therefore, Airbus strongly recommends to involve the appropriate Industry and Regulatory representatives from the Structure community before expanding appendix K and CS25.629.

In this respect, Airbus does not choose to make many detailed comments to the proposals made in Appendix K and CS25.629, although many comments exist and need to be made on the changes. Airbus proposes to discuss these comments and recommendations in the appropriate context of the above mentioned Industry and Regulatory representatives from the Structure community.



	<p>RATIONALE / REASON / JUSTIFICATION: Appendix K and CS25.629 have been created/ revised during a harmonization activity by the ARAC Loads and Dynamics Harmonisation Working Group (L&DHWG) in the 90's. Structure representatives both from Industry and Authorities need to be consulted and review any proposed changes to Appendix K and CS25.629 in the correct context. The proposal also leads to a dis- harmonisation with the FAR25, and therefore need to be well evaluated and coordinated with the relevant appropriate Industry and Regulatory representatives from the Structure community before accepting such a dis-harmonisation. Therefore, Airbus proposes to involve the L&DHWG to consider any update to the Appendix K and CS25.629 coming from CS25.671 changes.</p>
response	<p>Noted. Please refer to the responses to comments #188 and #92.</p>
comment	<p>184 comment by: AIRBUS</p> <p>Airbus consider that on this flight control topic, EASA/FAA harmonised requirement and AMC is of the utmost importance. As such, Airbus kindly request EASA to set a representative panel from the authorities and the industry to review and finalise the comments during a specific comment review meeting</p>
response	<p>Partially accepted. EASA has been seeking harmonisation with the FAA and TCCA. This is why this rulemaking task has been delayed after the publication of the NPA: awaiting the publication of an equivalent FAA NPRM. Due to significant delays experienced by the FAA, it has been decided to proceed with the EASA rulemaking task. Should the FAA publish an NPRM in 2018, EASA will take it into account when preparing the related ED Decision that will amend CS-25 and will seek harmonisation as far as possible. It is not planned to establish a working group with the industry.</p>
comment	<p>198 comment by: Boeing</p> <p>GENERAL COMMENT Page: 1, 3, 5</p> <p>The term “critical systems” is used several times in the NPA title, executive summary, procedural information, and explanatory note. What is the definition of “critical systems” to which systems must comply with this rule/guidance? Regulation and guidance describe that the “latent failure” portion will apply to critical or hazardous failure conditions. Is this defined clearly enough? What about an FHA item that involves multiple systems, neither of which by themselves could not cause the top level event? Would this new requirement apply to these systems?</p> <p>REQUESTED CHANGE: Review and make sure intended scope is properly reflected in the explanatory and guidance material.</p> <p>JUSTIFICATION: Clarification is needed on this important issue to ensure consistent interpretation and application.</p>
response	<p>Noted. The term ‘critical systems’ as used in the title, in the explanatory note and in the RIA is not</p>

defined. We agree there is a potential lack of clarity about which systems are concerned. The certification specifications and acceptable means of compliance are, however, considered clear enough.

CS 25.1309(b)(4) applies to any significant latent failure. Significant latent failure is defined in AMC 25.1309 as a latent failure that would, in combination with one or more specific failures or events, result in a hazardous or catastrophic failure condition.

CS 25.1309(b)(5) applies to any catastrophic failure condition resulting from two failures, either of which is latent for more than one flight.

comment	269	comment by: <i>Transport Canada Standards Branch</i>
	General Note: TCCA has been engaged in harmonization discussions with EASA and the FAA regarding CS25.671, subsequent to this NPA being posted for public comments. Proposed changes as a result of these discussions are not reflected in the comments below.	
response	Noted.	

comment	289	comment by: <i>Poonam Richardet</i>
	Attachment #1 Dear EASA: Please find attached Textron Aviation's collective (Cessna and Beechcraft) response to the proposed, "EASA NPA- 2014-02: 'Specific risk and standardised criteria for conducting aeroplane-level safety assessments of critical systems'" Please contact us in case of any questions- Thank you for giving us the opportunity to respond to this NPA. <u>Poonam Richardet</u> Analyst Engrg Procedures, International Certification Regulatory Affairs Textron Aviation 316.517.5395 (Office) 316.218.8638 (Cell) <u>PRichardet@txtav.com</u>	
response	Noted. The comments of the attached letter have been extracted and inserted in the relevant sections of Chapter 3 of the CRD. Please refer to the relevant sections which contain the EASA responses.	

comment	290	comment by: <i>Rockwell Collins, Inc.</i>
	The concept of 'Specific Risk' being applied to all avionic designs has the potential to drive architecture decisions. Will EASA include criteria by which the avionics industry will know 'when and when not' existing avionics architectures will be allowed to be placed into new airframes without a Specific Risk Assessment? In other words, will EASA publish criteria that	



	<p>describe when existing certificated avionic architectures/designs will be allowed to be “grandfathered onto” a new airframe design? Please provide text regarding timeline for cut-in dates of this specific risk assessment requirement.</p>
response	<p>Noted. The type certification basis provides the applicable amendment of the certification specifications (refer to Part 21). The specific risk assessment will therefore be required for certification projects that include the corresponding amendment of CS-25 in their certification basis.</p>
comment	<p>309 comment by: <i>Thales Avionics- JD Chauvet</i></p> <p>THALES Avionics is concerned by the amendment of CS-25 and associated AMC regarding specific risk and standardized criteria for conducting safety assessments of critical systems. In particular, the proposed amendment introduces :</p> <ul style="list-style-type: none"> - new requirements into §25.1309 about System Design and Analysis ((b)(4) and (b)(5)) whereas there is no equivalent ones into CFR PART 25. - new Mean of Compliances for existing requirements such as §25.1309(c) or new ones such as §25.1309(b)(4), whereas FAA AC 25.1309-1 is not released since 1988. <p>Due to the potential negative impact on industry that could have any additional differences between the EASA rules and FAA ones, THALES Avionics is very keen that EASA and FAA succeed in achieving a full harmonization on such question before proceeding to CRD and final rules.</p>
response	<p>Noted.</p>
comment	<p>311 comment by: <i>Gulfstream Aerospace Corporation</i></p> <p>Attachment #2</p> <p>Gulfstream appreciates the opportunity to review this Notice of Proposed Amendment concerning certification specifications of large aircraft. EASA has encouraged comments to improve and support this NPA. Gulfstream is pleased to support EASA in this effort and offers the following specific comments and recommendations attached in the summary letter Individual comment responses will also be included throughout the CRT for each paragraph.</p>
response	<p>Noted. Individual comments are addressed in Chapter 3 of the CRD.</p>
comment	<p>341 comment by: <i>GE Aviation</i></p> <p>GE Aviation supports the objective of standardization so that an applicant can understand compliance requirements in advance. However, the proposed rule and advisory material introduces significant new ambiguities, and has limited success in achieving the objective. The NPA expresses concern over increased complexity of aircraft systems, and new requirements and policy are introduced to address this However, the accident data does not support the fear of increased complexity; more recent (and complex) aircraft have better safety records than older products. New interpretations are introduced by this NPA which could not be met by many or all of the existing fleet, without any safety benefit. For example, the new requirement to limit latency</p>

to 1/1000 effectively drives twin-engine airplanes out of service. (Engines are composed mostly of mechanical systems without monitoring, an overall engine failure rate may be typically 2/million hours, this implies a maximum time-on-wing of 500 hours to meet the new requirement. The customer expectation is at least 10x that time on wing.)

response Noted.
The 1/1000 criterion is withdrawn from AMC 25.1309 with regard to compliance with CS 25.1309(b)(4), but maintained for compliance with CS 25.1309(b)(5).

Executive Summary

p. 1

comment 80 comment by: FAA

We thank EASA for stating in the Explanatory Note section that *“Although mainly based on the recommendations from both FCHWG and ASAWG reports, harmonisation with FAA has also been considered of paramount importance when drafting the proposed Decision.”* As the FAA is considering similar rulemaking, we look forward to working with EASA to harmonize our respective regulations and guidance materials.

response Noted.
Support by the FAA is noted with appreciation.

2. Explanatory Note (Paragraph 2.2, 2.2, 2.3)

p. 5-6

comment 264 comment by: AIRBUS

This objective is partially achieved as some specific control systems remain with their more stringent criteria for double failures.

Rational:

- Thrust reverser specific regulation prohibit latent failure

response Noted.
Design configurations in paragraph 8.b.(2) and 8.b.(3) of AMC 25.933(a)(1) have traditionally been considered practical and deemed to be acceptable to EASA, hence the wording ‘it is impractical to provide additional fault tolerance’ in CS 25.1309(b)(5)(i).

comment 343 comment by: GE Aviation

The term “Critical aeroplane systems” is not defined. The Certification Process Study attempted to discriminate between “critical systems” and others, without reaching consensus; on close review, it was evident that very few airplane systems could be confidently agreed to not be Critical. The NPA greatly underestimates the increase in scope of safety assessment that the proposed rule /AMC will introduce.

response Noted.
Please refer to the response to comment #198.

2. Explanatory Note (Paragraph 2.4)

p. 6-11



comment	<p>199</p> <p>Page:7 Paragraph: 2.4.1.</p> <p>The proposed text states: “...harmonization with FAA has also been considered of paramount importance when drafting the proposed Decision. ...bi-lateral coordination with FAA (from which the corresponding NPRM is expected in the first half of 2014) ...”</p> <p>COMMENT: Some important details in this NPA disagree with currently stated FAA positions [e.g., acceptance (and in fact, codification) of 150% of §25.143 force levels for jams]. We are anxious to see the yet-to-be-released corresponding FAA NPRM to see if this is indeed harmonized.</p> <p>We ask that EASA be cognizant of the fact that if these requirements are, in fact, NOT harmonized with the FAA’s, then the cost, disruption, and potential for errors will be much higher and those risks need to be considered in the overall evaluation of this NPA.</p>	comment by: <i>Boeing</i>
response	<p>Noted.</p> <p>EASA intends to liaise with the FAA once the NPRM is published, and seek harmonisation as far as possible.</p>	
comment	<p>318</p> <p>Page: 7 Paragraph: 2.4. Overview of the proposed amendments 2.4.2. Control systems 2.4.2.(f)</p> <p>The proposed text states: “(f) CS 25.671(d) is proposed to be changed by clarifying that the all engine-out flight has to be considered at any point in the flight. It also should require the approach, flare to a landing and stopping capability of the aeroplane. Hereby it should be assumed that a suitable runway is available.”</p> <p>REQUESTED CHANGE: “(f) CS 25.671(d) is proposed to be changed by clarifying that the all engine-out flight has to be considered at any point in the flight. It also should require <u>aeroplane controllability while inflight, and during</u> the approach, flare to a landing and <u>while decelerating to a stop</u> stopping capability of the aeroplane. Hereby it should be assumed that a suitable runway, <u>defined as a hard surface runway or equivalent for which the distance available following touchdown is consistent with the available aeroplane ground deceleration capability to a stop with all engines failed</u>, is available.”</p> <p>JUSTIFICATION: The primary intent of draft CS 25.671(d) is to ensure that adequate aeroplane controllability is available following failure of all engines. To avoid an implied open-ended requirement on stopping performance, the term “suitable runway” should be defined as one having a hard surface, and for which the landing distance available following touchdown is consistent with the available aeroplane deceleration capability with all engines failed.</p>	comment by: <i>Boeing</i>
response	<p>Partially accepted.</p>	



The definition of 'suitable runway' has been added in AMC 25.671, Chapter 10. However, EASA does not wish to define a stopping performance requirement.

3. Proposed amendments

p. 12

comment

267

comment by: *Transport Canada Standards Branch*

p.12, CS25.629(b)

TCCA questions the inclusion/addition of CS 25.333 to CS 25.629(b) without any previous reference or explanation in the NPA. If redistribution of airloads is the impetus for this change, TCCA strongly recommends that wording similar to that of 25.301(c) be incorporated instead. This would directly address the re-distribution of loads (both airloads and internal loads) due to structural and control deflections and would limit the analytic workload to the specific areas of concern. The advisory material (AMC 25.629) and practice by certification authorities already provides for a wide range of variables to be considered for analysis.

p.12, CS25.629(d)(10)

TCCA have no objection to include the proposed dual system failure combinations in 25.629(d). TCCA prefers that determinate failure cases take priority in 25.629(d), and suggests these preferably should be introduced as CS25.629(d)(9); and existing CS25.629(d)(9) be re-titled as CS25.629(d)(10).

CS25.629(d)(9)

The existing CS25.629(d)(9) addresses the probabilistic failure states, which for structures would involve 25.302. Currently, there is no obvious link between 25.629 and 25.302 except through Appendix K. Therefore, TCCA preference would be to provide a direct reference in CS25.629, would be wording of the following nature:

“ Any damage, failure or malfunction arising from CS 25.631, 25.671, 25.672, and 25.1309 must be considered under 25.302 in accordance with Appendix K.”

response

First paragraph: Accepted.

The proposed change to paragraph (b) of CS 25.629 was mainly driven by examples of changes in aerodynamic coefficients and redistribution of air loads due to structural and control deflections at higher load factors, which caused aeroelastic stability issues that were not predicted analytically but were discovered by flight test. However, this proposed change is not directly related to the main issues addressed by the NPA, and hence this proposal is withdrawn. It may be reinstated as part of a more general update of CS 25.629.

Second paragraph: Accepted.

The existing CS 25.629(d)(9) becomes CS 25.629(d)(10), and the existing CS 25.629(d)(10) becomes CS 25.629(d)(11). The proposed CS 25.629(d)(10) becomes CS 25.629(d)(9), as follows:

(d) Failures, malfunctions, and adverse conditions. The failures, malfunctions, and adverse conditions which must be considered in showing compliance with this paragraph are:

(...)

(9) Any of the following failure combinations:

(i) any dual hydraulic system failure;

(ii) any dual electrical system failure; and

(iii) any single failure in combination with any probable hydraulic or electrical



system failure.

(9)(10) Any damage, failure or malfunction, considered under CS 25.631, CS 25.671, CS 25.672, and CS 25.1309.

(10)(11) Any other combination of failures, malfunctions, or adverse conditions not shown to be extremely improbable.

Third paragraph: Not accepted.

CS 25.629(b)(2) and (3) already refer to CS 25.302 and Appendix K.

3. Proposed amendments - CS-25 - Book 1 - CS 25.629 p. 12

comment 81 comment by: FAA

In general, we believe the proposed changes to CS 25.629, 25.933, 25.1309, and associated guidance materials are consistent with the ASAWG recommendations and the positions that we expressed to the WG.
We will consider EASA’s proposals in the development of our NPRM.

response Noted.
Support by the FAA is noted with appreciation.

comment 83 comment by: Dassault Aviation

Dassault-Aviation comment page #12
Extract:
CS 25.629(b)
Aeroelastic stability envelopes. The aeroplane must be designed to be free from aeroelastic instability for all configurations and design conditions within the aeroelastic stability envelopes as follows described below, for all configurations and design conditions, and for the load factors specified in CS 25.333

Comment:
Load factors being defined in 25.337, the reference should be 25.337 instead of 25.333. Furthermore, the combined probability of system failure and limit load factor application is extremely improbable. So Dassault-Aviation think that the load factors of 25.337 apply to nominal conditions only without system failure.

Requested Change:
The following redaction is suggested:
“Aeroelastic stability envelopes. The aeroplane must be designed to be free from aeroelastic instability within the aeroelastic stability envelopes described below, for all configurations and design conditions, and for the load factors specified in CS 25.337 in nominal conditions.”

response Please refer to the first part of the response to comment #267.

comment 84 comment by: Dassault Aviation

Dassault-Aviation comment page #12
Extract:



CS 25.629(d)

(10) Any of the following failure combinations:

(i) Any dual hydraulic system failure;

(ii) Any dual electrical system failure; and

(iii) Any single failure in combination with any probable hydraulic or electrical failure.

~~(10)~~(11) Any other combination of failures (...)

Comment:

Dassault-Aviation thinks that only foreseeable (e.g. not shown to be extremely improbable) dual hydraulic or dual electrical system failures need to be addressed. Suppression of paragraphs (i) and (ii) is suggested.

About the requirement (iii), Dassault-Aviation interpretation is that only probable system hydraulic (or electrical) furnishing loss has to be considered but not all elementary hydraulic (or electrical) item failures. Dassault-Aviation propose to modify "hydraulic or electrical failure" by "hydraulic or electrical furnishing loss".

Requested Change:

Dassault-Aviation suggest that CS 25.629(d)(10) only addresses single failures in combination with probable power furnishing loss: "(10) Any single failure in combination with any probable hydraulic or electrical furnishing loss.". Other combination of failures being covered by CS 25.629(d)(11).

response

First part of the comment: Not accepted.

As reflected in AMC 25.629, certain combinations of failures are not normally considered extremely improbable regardless of probability calculations. Due to the proposed changes to CS 25.671, this approach needs to be elevated to the level of a requirement.

Second part of the comment: Not accepted.

Not only furnishing loss, but also other failure cases need to be considered.

comment

116

comment by: *Garmin International*

Section 3.1. CS 25.629 (d) (10)

The proposed new CS 25.629 (d) (10) rule is redundant to the renumbered rule CS 25.629 (d) (11). Additionally, requirements CS 25.629 (d) (10) (i) & (ii) are redundant to the NPA AMC material stated in section 3.2 page 17. There is no obvious benefit or need for stating the requirements more than once in the regulations and in the associated advisory material. Remove CS 25.629 (d) (10) and retain the AMC guidance.

response

Please refer to the first part of the response to comment #84.

comment

117

comment by: *Garmin International*

Section 3.1. CS 25.629 (d) (10) (iii)

The ARAC ASAWG recommended to delete an identical statement now proposed as a rule in CS 25.629 (d) (10) (iii) from the applicable AMC. It is not consistent with the 10-9 numerical criterion associated with the term Extremely Improbable as stated in the AMC text included as part of this NPA (AMC 25.629 4.3, page 17). As written, CS 25.629 (d) (10) (iii) covers dual failures with joint probabilities of less than 1E-9. A more appropriate statement would be any single latent failure in combination with any probable hydraulic or electrical failure.

response

Please refer to the first part of the response to comment #84.



comment	<p>170</p> <p style="text-align: right;">comment by: AIRBUS</p> <p>PARAGRAPH / SECTION THE COMMENT IS RELATED TO: CS25.629b.</p> <p>PROPOSED TEXT / COMMENT: Delete the proposed text changes in CS25.629b.</p> <p>RATIONALE / REASON / JUSTIFICATION: It is difficult to understand the link with the NPA2014-02 subject of change and this particular change to CS25.629b. Airbus opinion is that the 2 are completely not related to each other. It is difficult to understand the reason for addition of the structural requirement CS25.333 to CS25.629 in the context of an update to a system requirement 25.671. Current form of CS25.629b has been introduced with FAR25 am 77 in 1992 and CS25 am 1, if there is a need for change to CS25.629b this needs to be prepared, discussed and agreed by the appropriate Industry and Regulatory representatives from the Structure community before proposing incorporating in CS25. The proposal also leads to a dis- harmonisation with the FAR25.629b, and therefore need to be well evaluated and coordinated with the relevant appropriate Industry and Regulatory representatives from the Structure community before accepting such a dis-harmonisation.</p>
response	<p>Please refer to the first part of the response to comment #267.</p>

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: CS 25.629

Comment: The proposed amendment is adding a new requirement, “and for the load factors specified in CS 25.333”. The rationale for this additional requirement is not addressed in section 2.4, “Overview of the proposed amendments”

Suggested change: Propose deletion of , “and for the load factors specified in CS 25.333”:

EASA response: Please refer to the first part of the response to comment #267.

comment	<p>171</p> <p style="text-align: right;">comment by: AIRBUS</p> <p>PARAGRAPH / SECTION THE COMMENT IS RELATED TO: CS25.629 (d)10/AMC25.629 §4.3</p> <p>PROPOSED TEXT / COMMENT: Delete the proposed text changes in CS25.629(d)10, restore the original AMC25.629§4.3 text, and discuss first in Group of appropriate Industry and Regulatory representatives from the Structure community .</p> <p>RATIONALE / REASON / JUSTIFICATION: It is difficult to understand what the system community really need. Today there are 3 more or less conflicting requirements proposed in CS25.629(d)10, AMC25.629 §4.3, and AMC25.671§9, which need to be streamlined to understand what the structure demonstration need to provide w.r.t flutter aspects. The conditions proposed in CS25.629(d)10 seem already included in the existing AMC25.629 §4.3 as acceptable MoC, so Airbus do not see the need to transfer this MoC into the requirement CS25.629(d)10. If there is a need for change to CS25.629(d)10 or AMC25.629§4.3 this needs to be prepared, discussed and agreed by the appropriate Industry and Regulatory representatives from the Structure community before proposing incorporating in CS25. The proposal also leads to a dis- harmonisation with the FAR25.629b, and therefore need to be well evaluated and coordinated with the relevant appropriate Industry and Regulatory representatives from the</p>
---------	--



	Structure community before accepting such a dis-harmonisation.
response	Please refer to the first part of the response to comment #84.
comment	185 comment by: <i>Embraer - Indústria Brasileira de Aeronáutica - S.A.</i>
	<p>CS 25.629(d)(10): The proposed CS 25.629(d)(10) calls out specific failure combinations to be considered in addition to the combinations not shown to be extremely improbable that are required by (d)(11). The justification for this is that has been the standard practice to consider these failure combinations regardless of probability. However, the ARAC ASAWG Report recommends the removal of the condition: any single failure in combination with any probable electric or hydraulic system failure from the AC/AMC 25.629-1A; and also recommends no changes to FAR/CS 25.629, with the justification that “The ASAWG believes that the guidance for validating failure rates and other assumptions in the AC/AMC 25.1309 is sufficient for ensuring adequate redundancy in these situations”. Embraer believes that is is not necessary to include the specific failure combinations of CS 25.629(d)(10).</p>
response	Please refer to the first part of the response to comment #84.
comment	200 comment by: <i>Boeing</i>
	<p>Page:12 Paragraph: CS 25.629 (d) (10) - Aeroelastic stability requirements</p> <p>The proposed text states: “(10) Any of the following failure combinations: (i) Any dual hydraulic system failure; (ii) Any dual electrical system failure; and (iii) Any single failure in combination with any probable hydraulic or electrical failure.”</p> <p>REQUESTED CHANGE: “(10) Any of the following failure combinations <u>unless shown to be extremely improbable:</u> (i) Any dual hydraulic system failure; (ii) Any dual electrical system failure; and (iii) Any single failure in combination with any probable hydraulic or electrical failure.”</p> <p>JUSTIFICATION: Requiring substantiation for any dual failure regardless of probability is not justified, as is consistent with AMC 25.629 guidance.</p>
response	Please refer to the first part of the response to comment #84.
comment	283 comment by: <i>Bombardier Aerospace</i>
	Bombardier does not agree with the changes proposed for CS-25.629(b), specifically the new requirement to use the load factors from CS-25.333. EASA has not offered any justification as to why the current practice of performing flutter analysis in 1-g level flight conditions is no longer acceptable, nor why the load factors of CS-25.333 would be more suitable.
response	Please refer to the first part of the response to comment #267.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: CS 25.629 (d)(10)(iii)

Comment: This NPA makes changes to replace “single + probable” in CS 25.671 & 25.1309, so why does it add “single+probable” into CS 25.629? This amounts to introducing a methodology to replace “single + probable” that would impose a significant burden on the small transport aircraft manufacturer without a commensurate safety/benefit while retaining “single + probable” in related regulations.

Suggested change: Propose deleting CS 25.629 (d) (10) (iii). The average risk implementation of 25.1309 should be sufficient, unless the aircraft falls under the umbrella of 14 CFR 26.11.

EASA response: Please refer to the first part of the response to comment #84.

3. Proposed amendments - CS-25 - Book 1 - CS 25.671

p. 12-14

comment

44

comment by: UK CAA

Page No: Multiple, but commences on page 13

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.

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.

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.

Proposed Text: A clarification of the 1/1000 value is needed throughout the NPA.

response

Accepted.

It is understood that confusion arose between probability and probability per FH.

Please note that CS 25.671(c)(2)(ii) does not replace CS 25.1309, which must be applied as well.

Nevertheless, CS 25.671(c)(2)(ii) has been reviewed and clarified.

comment

85

comment by: Dassault Aviation

Dassault-Aviation comment pages #12 and #13

Extract:**CS 25.671(b)**

Each element of each flight control system must be designed, ~~or distinctively and permanently marked~~, to minimise the probability of incorrect assembly that could result in the ~~failure of the system to perform its intended function~~ malfunctioning of the system.

Distinctive and permanent marking may be used only where design means are impractical.

{See AMC 25.671 (b).}

Comment:

Associated AMC 25.671(b) seems to alleviate the CS 25.671(b) requirement. Indeed it is stated that "For minor failure or No Safety Effect: Marking alone is generally considered sufficient to prevent incorrect assembly." To be consistent and to give full credit to this AMC deemed acceptable by Dassault-Aviation, the text of CS 25.671(b) should be adapted to confirm the possibility of distinctive and permanent marking alone on elements leading only to minor or no safety effects.

Requested Change:

The following redaction is proposed: "Each element of each flight control system must be designed to minimise the probability of incorrect assembly that could result in the malfunctioning of the system. Distinctive and permanent marking may be used: (i) Where design means are impractical; or (ii) For elements whose failure occurrence can only lead to minor or no safety effects."

response

Partially accepted.

The proposal is accepted in principle, but with some changes to the wording.

Comment from Textron Aviation (extracted from the letter attached to comment# 289):

Page/Paragraph: CS 25.671(c)

Comment: Change removes the language about "exceptional piloting skill and strength," however that phrase appears in other regulations. "Exceptional piloting skill and strength" is also struck from NPA AMC 25.671 Section 9 2nd paragraphs. However, NPA AMC 25.671 Section 9e1i 1st paragraph does state that CSFL procedures should not require exceptional piloting skill or strength.

Suggested change: Propose that the words "exceptional piloting skill and strength" should be retained.

EASA response: Not accepted. This is considered redundant as it is included in the definition of CSFL.

comment

86

comment by: Dassault Aviation

Dassault-Aviation comment page #13

Extract:

CS 25.671(c)(2)

For combinations of failures, excluding failures of the type defined in (c)(3):

(i) Any combination of failures not shown to be extremely improbable.

(ii) Given any single latent failure has occurred, the average probability per flight hour of any failure condition preventing continued safe flight and landing, due to the sum of all subsequent single failures, must be less than 1E-5, and the combined probability of the latent failures must be 1/1000 or less.

Comment:

25.671(c)(2)(ii) proposal is not consistent with the criteria defined in 25.1309(b)(5). If the rules towards the specific risks are not homogenized between 25.671 and 25.1309, it may be source of errors and complications when processing the analyses due to different computation rules.

Moreover the term "combined probability" is misleading. Does it refer to an average probability? It would be more suitable to adopt one unique set of criteria common to 25.671 and 25.1309. Thus DA suggest 25.671(c)(2)(ii) to refer directly to 25.1309(b)(5) criteria.

Requested Change:

The following redaction is proposed accordingly: "For combinations of failures, excluding failures of the type defined in (c)(3): (i) Any combination of failures not shown to be extremely improbable. (ii) Compliance with CS 25.1309(b)(5) should be considered for any combination of failures preventing continued safe flight and landing should comply."



response	<p>Not accepted.</p> <p>EASA considers it necessary to have the requirements of CS 25.671 in addition to CS 25.1309. CS 25.671(c)(2)(ii) has been clarified.</p>
comment	<p>87 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment pages #13</p> <p>Extract: CS 25.671(c)(3)(ii)</p> <p>The causal failure or failures must be assumed to occur anywhere within the normal flight envelope.</p> <p>Comment:</p> <p>This paragraph is not consistent with the results of ARAC FCHWG. Indeed, it was concluded that jams that occur just prior to landing have not to be addressed by 25.671(c)(3). The rationale for such a position is reminded below (issued from ARAC FCHWG report). <i>"25.671(c)(3) requires that the airplane be capable of landing with a flight control jam and that the airplane be evaluated for jams in the landing configuration. However, for the evaluation of jams which occur just prior to landing, proximity to the ground need not be considered for the transient condition. Given that some amount of time and altitude is necessary in order to recover from any significant flight control jam, there is no practical means by which such a recovery could be demonstrated all the way to touchdown. The potential delay in accomplishing a recovery could be on the order of 5 seconds as described in section 9.e. For a jam at a control deflection corresponding to .8g, a recovery may not be possible below approximately 200' even with a state of the art control system. While it is recognized that this means that a specific hazard is not addressed (a control jam that occurs, or is recognized, just before landing), this hazard is mitigated for the following reasons. First, the landing phase represents a limited exposure window in which a jam could occur. Second, successful operation of the controls throughout the flight minimizes the likelihood of a jam suddenly appearing during the landing phase. Third, a certain level of recovery capability will be ensured through compliance with this AC such that if a jam does occur during landing, the crew will have a reasonable chance of landing safely."</i></p> <p>Requested Change:</p> <p>Dassault-Aviation suggests to take credit from the ARAC FCHWG results and change this paragraph as follows: <i>"The causal failure or failures must be assumed to occur anywhere within the normal flight envelope except during the time immediately before landing where recovery may not be achievable when considering time delays in initiating recovery."</i> (also consistent with F7X CRI D-05).</p>
response	<p>Not accepted.</p> <p>Since the end of the ARAC activity mentioned, experience from in-service aeroplanes has shown the need to consider the case of jamming before landing.</p>
comment	<p>88 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment page #13</p> <p>Extract: CS 25.671(c)(3)(iii)</p> <p>In the presence of a jam considered under this subparagraph, any additional failure states that could prevent continued safe flight and landing shall have a combined probability of</p>

1/1000.

Comment:

In term of probability, this requirement should specify a maximum value not to exceed, and not a probability to reach.

Requested Change:

Specify "probability of less than 1/1000" instead of "probability of 1/1000".

response

Accepted.

Comment from Textron Aviation (extracted from the letter attached to comment# 289):

Page/Paragraph: CS 25.671(c)(2)(ii), CS 25.671(c)(3)(iii), CS 25.1309(b)(5), AMC 25.671 Section 9a, 3rd, paragraph, AMC 25.671 Section 9d, 1st paragraph, AMC 25.1309 Section 9b6i, AMC 25.1309 Section 9b6ii, AMC 25.1309 Appendix 5

Comment: NPA's implementation of "1/1000" would place a significant and disproportionate burden/cost on small transport category aircraft manufacturers, without a commensurate safety/benefit, in order to show compliance. Cessna/Beech's dissenting opinion to ASAWG provided those details, which could be a significant percentage of the overall development costs for small transport category aircraft.

Suggested change: In lieu of the "1/1000 specific risk" of the NPA being applicable to all aircraft, recommend that aircraft which do not meet the criteria of 14 CFR 26.11 (i.e., passenger capacity of 30 or more, or maximum payload capacity of 7500 lb or more) would be exempted from the "1/1000 specific-risk" aspects of NPA 2014-02. For aircraft which do not meet the criteria of 14 CFR 26.11, the average-risk methods of present 14 CFR 25.1309 (which would also apply to CS 25.671(c) (2) "combinations of failures not shown to be extremely improbable") would be sufficient for compliance.

EASA response: Not accepted.

CS 25.671 is applicable to all CS-25 large aeroplanes.

comment

89

comment by: Dassault Aviation

Dassault-Aviation comment page #13

Extract:**CS 25.671(c)(4)**

Any runway of a flight control to an adverse position that is caused by an external source.

Comment:

For a better comprehension, Dassault-Aviation suggest to replace "that is caused" by "if it is caused".

Requested Change:

Change as follows: "Any runway of a flight control to an adverse position ~~that~~ if it is caused by an external source."

response

Not accepted.

The original wording is deemed to be clear enough.

comment

90

comment by: Dassault Aviation

Dassault-Aviation comment page #14

Extract:**CS 25.671(e)**

The flight control system must be designed to ensure that the flight crew is aware whenever



the primary control means is approaching the limit of control authority.

Comment:

Annunciating that primary control means is approaching the limit of control authority is only profitable when it requires a specific crew action. The other cases requiring no specific crew action should be out of the scope of this requirement, particularly when approaching the limit of control authority is a normal response consecutive to a commanded crew action. This consideration is well translated through the CRI B-02 (F7X/F5X) whose redaction for this topic could be reused. It is also consistent with the ARAC FCHWG report.

Requested Change:

The following redaction issued from CRI B-02 (F7X/F5X) is proposed: "When a flight case exists where, without being commanded by the crew, control surfaces are coming so close to their limits that return to normal flight condition and (or) continuing of safe flight needs a specific crew action, a suitable flight control position annunciation shall be provided to the crew, unless other existing indications are found adequate or sufficient to prompt that action."

response

Not accepted.

The aim of the specification is to ensure the awareness of the flight crew the limit of control authority is being approached. Then it is the flight crew's decision to take any action based on this awareness. EASA considers that in some cases it may be difficult to decide whether or not flight crew action is required and, therefore, whether or not a means of indication must be provided, based on the proposed conditional specification.

Experience gained from in-service aeroplane occurrences has shown the benefit of the proposed specification.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: § 3.1 CS25.671(e)

Comment: The added requirement that "The flight control system must be designed to ensure that the flight crew is aware whenever the primary control means is approaching the limit of control authority." is overly restrictive for a purely mechanical system where the limit of control authority is defined by 25.143

Suggested change: change 25.671(e) to "A powered flight control system must be designed to ensure that the flight crew is aware whenever the primary control means is approaching the limit of control authority."

EASA response: Partially accepted.

EASA agrees in principle with the comment. We prefer to cover this point in AMC 25.671 rather than changing the rule. A new subparagraph has been created in paragraph 11 of the AMC.

comment

119

comment by: *Garmin International*

Section 3.1. CS 25.671(c)(2)(ii)

It was the objective of the ASAWG to have a consistent criteria and methodology for specific risk evaluations. The current CS 25.671 (c) (2) (ii) rule recommendation deviates from this objective since the definition of the term continued safe flight and landing in AMC 25.671 section 5 item c of this NPA does not correlate to the CS 25.1309 definition of Catastrophic. This is evident since AMC 25.671 section 5 item b of this NPA references AMC 25.1309 for the definition of a Catastrophic failure condition. Thus there is potential for change in the scope and application of specific risk beyond what the ASAWG deemed as warranted. The history of FAA CFR 25.671 (c) (2) resulted in many different compliance methodologies and this lesson learned should be applied when considering this new regulation. It is



response	<p>recommended that CS 25.671 (c) (2) (ii) be deleted since CS 25.1309 will apply.</p> <p>Noted.</p> <p>'Continued safe flight and landing' (CSFL) is deliberately defined differently from 'Catastrophic' (defined in AMC 25.1309) as there are failure conditions other than catastrophic that can prevent CSFL.</p> <p>We have defined specific criteria for CSFL, whereas catastrophic is more simply defined as loss of the aeroplane (see AMC 25.1309).</p> <p>A catastrophic failure would not be considered as meeting 'CSFL'. However, a failure preventing CSFL is not automatically catastrophic.</p>
comment	<p>120 comment by: <i>Garmin International</i></p> <p>Section 3.1. CS 25.671(c)(2)(ii)</p> <p>The current CS 25.671 (c) (2) (ii) rule recommendation deviates from the ASAWG proposal. It is unclear what is meant by "...and the combined probability of the latent failures must be 1/1000 or less." The quoted phrase is different from the CS 25.1309 (b) (5) (iii) criteria. According to this NPA's new AMC 25.1309 Appendix 5 item 2): "The dual order cut sets that contain a primary event that is latent for more than one flight are then identified from the list in Table A5-2. The probability of each of these latent events should be less than 1 x 10⁻³." There is an implication of two different methods of calculation between the two rules. It is thought that the ASAWG objective was to provide one standard method for addressing latent failures. This illustrates the ASAWG concern for the potential for discrepancies to occur if multiple specific risk criteria are present in multiple different rules. It is recommended that the NPA resolve this difference.</p>
response	<p>Please refer to the response to comment #86.</p>
comment	<p>121 comment by: <i>Garmin International</i></p> <p>Section 3.1. CS 25.671(c)(3)</p> <p>The existing CS 25.671 (c) (3) rule allows applicants to address Part 25 airplanes that have flight controls that cannot be split. For example, the Beechjet Model 400A is a part 25 airplane does not have the ability to split flight controls allowing independent operation. Under the current rule the applicant can show that a mechanical servo jam is Extremely Improbable. It is not clear how an avionics manufacturer wishing to perform an autopilot STC that interfaces with the 400A flight controls would be able to address the inability to split flight controls under the new rule since the premise of the rule implies the ability to split controls allowing independent pilot/copilot control. Please provide NPA guidance for legacy airplanes without the ability to split flight controls.</p>
response	<p>Not accepted.</p> <p>The proposed specification will be applicable to new designs. Modern design architectures are generally 'split' and would need to be designed to meet this specification.</p> <p>The Part 21 Changed Product Rule applies to legacy aeroplanes.</p>

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: CS25.671(c)(3), AMC 25.671 Section 9b 2nd paragraph, AMC 25.671 Section 9c

Comment: With regard to a single mechanical disconnect failures or jam, it should be acknowledged that there is some point in the approach, past which if the failure were introduced with the other criteria established in the AMC, recovery may not be able to be demonstrated within the time delays stated. Currently CS25.671(c) (3) allows an applicant to consider a jam is Extremely Improbable during any flight phase. The proposed CS25.671 (c) (3) removes this allowance, but specifically includes it in the jam evaluation for just before landing. However, it states that the use of a risk time in determining Extremely Improbable is not acceptable. "NPA AMC 25.671 Section 9c's opening paragraph attempts to describe the difficulty in dealing with jams in the landing phase without giving much additional information on what makes jams in the landing phase problematic from a compliance standpoint (namely, the time delays imposed by the AMC). Given a finite time (hence altitude) to recover from a jam (esp. given the delay times stated in the AMC), there is no practical means by which recovery could be demonstrated for compliance all the way to touchdown, for a jam occurring just prior to touchdown. There is some point in the approach past which a compliance demonstration of recovery could not be assured when delays are considered. AMC 25.671 Section 9c does state two conditions where jams in the landing phase may be shown to be Extremely Improbable, however one will be impossible to comply with, and the other will become a source of inconsistency between certification agencies and ACO's. In the first condition in AMC 25.671 Section 9c, states jams in the landing phase should be shown to be extremely improbably using relevant reliability data from in-service experience, without considering "risk time" in this determination; the jam itself must be $10e-9$, without considering "risk time". Such a standard will be impossible to comply with. Even during the FCHWG deliberation, in-service data showed a jam probability of approximately $10e-7$ (FCHWG Section 9 paragraph 6). Furthermore, no OEM has sufficient service history to justify a $10e-9$ jam probability. In the second condition in AMC 25.671 Section 9c2, jams in the landing phase should be shown to be extremely improbably by a qualitative assessment covering the design features intended to prevent jams, and a description of the means by which a jam could be alleviated. Unfortunately, the AMC provides no guidance on what types of design features would be considered adequate. Further, how does this qualitative assessment and description differ from that already required for compliance with the "prevention of jams" language of CS 25.685(a)? Lacking objective guidance this will become a source of inconsistency between certification agencies and ACOs. It is believed that the failure rate of a single mechanical disconnect in a primary flight control system is similar to that of a flight control jam. Consistency would require that both be excluded from showing CSFL in this small exposure time. Yet, the proposed AMC25.671(c) (I) does not allow a probability assessment to exclude this disconnect condition or a specific exclusion as in proposed FAR 25.671 (c) (3) (ii) for jams. Applicants have historically not been required to evaluate this type of disconnect failure just before touchdown for FAA certification. Current JAA 25.671(c)(I) would allow an applicant to consider a mechanical disconnect in this small time exposure Extremely Improbable.

Suggested change: Propose that the single mechanical disconnects and jams should be re-evaluated and allowance given for the small time exposure immediately before landing. There is sufficient experience to allow single mechanical disconnects and jams occurring immediately before landing to be allowed to be considered extremely Improbable based on the small exposure time immediately before landing.

Adopt the FCHWG 25.671(c) (ii) language which excluded jams "during the time immediately before landing where recovery may not be achievable when considering time delays in initiating recovery. In addition, adopt the language of FCHWG AC 25.671 Section 9b 2nd paragraph, which provides the rationale for the exclusion in the regulation.

Remove the language of AMC 25.671 Section 9c which excludes consideration for a jam on landing only if it can be shown to be extremely improbable without considering the limited risk time of the landing phase. Alternately, any such extremely improbable determination should inherently include the limited risk time of the landing phase.



Remove the language of AMC 25.671 Section 9c2 which excludes consideration for a jam on landing following a qualitative assessment of the design features intended to prevent jams as it is redundant with CS 25.685(a). Alternately, provide objective guidance on what types of features are considered adequate to exercise this exclusion.

EASA response: Not accepted.

The consideration not to allow risk time has been addressed in other comments, due to the possibility of a single event leading to a jam, for which EASA has evidence from service experience. The adequacy of a design will depend on the design selected by the applicant.

Typical features could include low-friction materials, dual rotation bearings, clearance, jack catchers.

A quantitative assessment is a check of a good design, not the starting point.

comment	<p data-bbox="359 750 406 772">122</p> <p data-bbox="1061 750 1476 772" style="text-align: right;">comment by: <i>Garmin International</i></p> <p data-bbox="359 806 694 840">Section 3.1. CS 25.671(d)(5)</p> <p data-bbox="359 840 1476 1052">The function to decelerate an airplane to rest does not seem to be a flight control function. The scope of this rule seems to expand into non-flight control functions, e.g. on ground deceleration devices. The safety criterion (defined by AMC 25.1309 via the FHA) for evaluating the ability to stop the airplane has traditionally been addressed under CS 25.1309 not CS 25.671. It is recommended that CS 25.671 (d) (5) be deleted or modified to characterize more clearly what flight control aspect is being addressed.</p>
response	<p data-bbox="359 1075 534 1108">Not accepted.</p> <p data-bbox="359 1108 1476 1220">The scope of the current CS 25.671(d) specification is already not limited to the flight control system. It is appropriate to have this bespoke specification covering all system aspects of engine-off landing.</p> <p data-bbox="359 1220 1452 1254">Note that the proposed amendment does not require a stopping performance assessment.</p>
comment	<p data-bbox="359 1321 406 1355">173</p> <p data-bbox="1220 1321 1476 1355" style="text-align: right;">comment by: <i>AIRBUS</i></p> <p data-bbox="359 1377 1037 1411">PARAGRAPH / SECTION THE COMMENT IS RELATED TO:</p> <p data-bbox="359 1411 614 1444">CS 25.671(d) page 13</p> <p data-bbox="359 1444 734 1478">PROPOSED TEXT / COMMENT:</p> <p data-bbox="359 1478 965 1512">Airbus propose to keep the current applicable text</p> <p data-bbox="359 1512 845 1545">RATIONALE / REASON / JUSTIFICATION:</p> <p data-bbox="359 1545 1380 1579">Airbus consider that the new requirement goes beyond the ARAC recommendations.</p> <p data-bbox="359 1579 375 1612">-</p>
response	<p data-bbox="359 1646 446 1680">Noted.</p> <p data-bbox="359 1680 1476 1747">The requirement is considered to be appropriate, even if it goes beyond the ARAC recommendations.</p>

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: 25.671d

Comment: The aircraft brake and nose wheel steering systems are designed to meet the specific certification requirements under CS25.735 and CS25.745, respectively. CS25.671 is a control system specific paragraph and should not be expanded to include aircraft level safety requirements. The aircraft level safety requirements are already adequately defined under CS25.1309.



EASA response: Not accepted.

The existing CS 25.671 already makes references beyond the flight control system. It is appropriate to consider all systems for an engine-off landing in this paragraph.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: 25.671d

Comment: Items d (1) thru d (5) do not include use of the word “landing” in reference to ground operations. As such it is understood that the specific definition of “landing” in section 5d is not invoked to add requirements above the system specific requirements of CS25.735 and CS25.745 and aircraft level safety requirements of CS25.1309.

Suggested change: Confirmation in discussion published with this rule that it is not the intent to levy additional requirements in place of system specific rules, but to require that dual engine failure does not disable both primary and emergency means of aircraft directional control.

EASA response: Partially accepted.

This rule does not replace CS 25.735 or CS 25.745. Please note that CS 25.735 and CS 25.745 do not deal with engine-off landings.

comment	186	comment by: <i>Embraer - Indústria Brasileira de Aeronáutica - S.A.</i>
	<p>CS 25.671(c)(1): It is not clear what the meaning or value is of the “For single failures” phrase, since the next phrase starts “Any single failure. . .” Embraer suggests that the first phrase be deleted and start subparagraph (c)(1) with “Any single failure, . . .”</p>	
response	Accepted.	

comment	196	comment by: <i>Embraer - Indústria Brasileira de Aeronáutica - S.A.</i>
	<p>CS 25.671(c)(2): It is not clear what the meaning or value is of the initial “For combinations of failures,” phrase, since the next phrase in (c)(2)(i) starts “Any combination of failures. . .” Embraer suggests that the first phrase be deleted and start subparagraph (c)(2) with “Any combination of failures not shown to be extremely improbable, excluding failures of the type defined in (c)(3), . . .” To make the residual risk requirement of 25.671(c)(2) more clear, Embraer suggests that it be revised to say “. . . due to the sum of the probability of all subsequent single failures, must be less than 1E-5, . . .”</p>	
response	<p>Partially accepted. The first proposed change is not accepted because it would change the applicability of the second specification (ii) to combinations of failures that are not shown to be improbable only, although the intent is to encompass all combinations of failures. The second proposed change is accepted.</p>	

comment	197	comment by: <i>Embraer - Indústria Brasileira de Aeronáutica - S.A.</i>
---------	-----	---



response	<p>CS 25.671(d): Since the existence of a suitable runway is relevant only for the requirement for flare, control during the ground phase, and the capability to stop, the proposed paragraph 25.671(d) would more logically be presented as: (d) The airplane must be designed so that, if all engines fail at any point of the flight it must be controllable in flight, on approach and if a suitable runway is available, it must be controllable during flare to a landing, during the ground phase and the airplane must be stopped.</p> <p>In addition, it would be helpful if EASA would add AMC to make clear that it is not necessary to consider adverse environmental conditions such as wet runway or tailwind conditions in showing compliance with the ground and braking phase.</p> <p>Partially accepted. The comment is agreed in principle. Detailed wording may vary in line with other similar comments received.</p>
comment	<p>201 comment by: Boeing</p> <p>Page:12 Paragraph: CS25.671(b) – Control Systems - GENERAL</p> <p>The proposed text states: “(b) Each element of each flight control system must be designed, or distinctively and permanently marked, to minimise the probability of incorrect assembly that could result in the failure of the system to perform its intended function malfunctioning of the system. Distinctive and permanent marking may be used only where design means are impractical.”</p> <p>REQUESTED CHANGE: “(b) Each element of each flight control system must be designed, <u>or distinctively and permanently marked</u>, to minimise the probability of incorrect assembly that could result in the failure of the system to perform its intended function malfunctioning of the system. Distinctive and permanent marking may be used only where design means are impractical.”</p> <p>JUSTIFICATION: Retain the phrase “or distinctively and permanently marked” and delete the last sentence, “Distinctive and permanent marking may be used only where design means are impractical.” The term “impractical” is subjective. Further, proposed AMC 25.671(b) phrasing defines when marking is acceptable.</p>
response	<p>Partially accepted. The specification has been rewritten taking into account this and other similar comments received.</p>
comment	<p>202 comment by: Boeing</p> <p>Page:13 Paragraph: 25.671(c)(2)(ii) – Control Systems - GENERAL</p> <p>The proposed text states: “(2) Given any single latent failure has occurred, the average probability per flight hour of any failure condition preventing continued safe flight and landing, due to the sum of all</p>

subsequent single failures, must be less than 1E-5, and the combined probability of the latent failures must be 1/1000 or less.

REQUESTED CHANGE:

~~“(2) Given any single latent failure has occurred, the average probability per flight hour of any failure condition preventing continued safe flight and landing, due to the sum of all subsequent single failures, must be less than 1E-5, and the combined probability of the latent failures must be 1/1000 or less. Single latent failure combinations that do not meet the criteria of CS25.1309(b)(5).”~~

JUSTIFICATION: First, CS 25.671(c) is for those failures that the airplane must be shown to be capable of continued safe flight and landing. Second, proposed paragraph 25.671(c)(2)(ii) is for failure combinations preventing continued safe flight and landing. CS 25.1309(b)(5) should be the single location for significant latent criteria.

response Please refer to the response to comment #86.

comment

203

comment by: Boeing

Page:13

Paragraph: 25.671(c)(3) – Control Systems - GENERAL

The proposed text states:

“(3) Any failure or event that results in a jam of a flight control surface or pilot control that is fixed in position due to a physical interference. ...”

REQUESTED CHANGE:

“(3) Any failure or event that results in a jam of a flight control system or surface ~~or pilot control~~ that is fixed in position due to a physical interference. ...”

JUSTIFICATION: The proposed wording only specifically identifies the surface and pilot controls for jamming, when (we believe) the intent is that jamming anywhere in the flight control system must be considered.

response Not accepted.

The proposed wording comes from the ARAC proposals and there is no adverse experience that would require a change.

comment

204

comment by: Boeing

Page:13

Paragraph: 25.671(c)(3)(ii) – Control Systems - GENERAL

The proposed text states:

“(ii) The causal failure or failures must be assumed to occur anywhere within the normal flight envelope.”

REQUESTED CHANGE: The term “normal flight envelope” should to be defined. Therefore, we suggest adding: “The material in AC 25-7, Appendix 7, should be used as the definition of “normal flight envelope.”



	<p>JUSTIFICATION: Without this definition clearly articulated, finding compliance will be impossible, as would be defining the benefit to safety.</p>
response	<p>Not accepted. Appendix 7 of AC 25-7 is not related to the flight envelope. Comment not understood.</p>
comment	<p>205 comment by: <i>Boeing</i></p> <p>Page:13 Paragraph: 25.671(c)(3)(iii) – Control Systems - GENERAL</p>
	<p>The proposed text states: “(iii) In the presence of a jam considered under this subparagraph, any additional failure states that could prevent continued safe flight and landing shall have a combined probability of 1/1000.”</p> <p>REQUESTED CHANGE: Delete this entire sub-paragraph.</p> <p>JUSTIFICATION: To ensure consistent probabilistic criteria, this should be covered and revised in CS 25.1309(b)(5). CS 25.671(c) is for those failures that the airplane must be shown to be capable of continued safe flight and landing. The proposed paragraph (c) is for failure combinations preventing continued safe flight and landing. The proposed text is in the wrong regulation and the intent is covered in CS 25.1309(b)(5). A jam plus an additional failure state should not be treated any differently than any other two-failure catastrophic condition.</p>
response	<p>Not accepted. A jam is considered to be an event, not a failure. Thus, it is treated in its own dedicated subparagraph. However, the same rule is applied to jam-alleviation means. EASA intends to keep CS 25.671 independent from CS 25.1309, in case of any future changes to either specification.</p>
comment	<p>206 comment by: <i>Boeing</i></p> <p>Page:13 Paragraph: 25.671(c)(4) – Control Systems - GENERAL</p> <p>The proposed text states: “(4) Any runaway of a flight control to an adverse position that is caused by an external source.”</p> <p>REQUESTED CHANGE: “(4) Any runaway of a flight control system or surface to an adverse position that is caused by an external source.”</p> <p>JUSTIFICATION: Clarifies the proposed wording.</p>
response	<p>Accepted.</p>
comment	<p>262 comment by: <i>Embraer - Indústria Brasileira de Aeronáutica - S.A.</i></p> <p>CS 25.671(c)(2)(ii): The proposed CS 25.671(c)(2)(ii) establishes another non-standardised criterion to limit latency by stating that “combined probability of the latent failures must be 1/1000 or less”. It</p>

	<p>does really differ from that one proposed for the CS 25.1309(b)(5)(iii), which presumably applies across all critical systems. Similar to thrust reverser, it looks that 25.1309(b) would not be good enough to regulate the safety of the flight control system yet each can be applicable to different systems with the same criticality.</p>
response	Noted.
comment	<p>270 comment by: <i>Transport Canada Standards Branch</i></p> <p>p.13, CS25.671(c)(3)(iii) Proposed rule currently reads: “In the presence of a jam considered under this subparagraph, any additional failure states that could prevent continued safe flight and landing shall have a combined probability of 1/1000.” It is recommended that wording be changed to “... combined probability of 1/1000 <u>or less.</u>” to better reflect the intent. This wording is already reflected in the corresponding AMC paragraph.</p>
response	Accepted.
comment	<p>297 comment by: <i>Rockwell Collins, Inc.</i></p> <p>(c).(2).(ii) For the statement, “... and the combined probability of the latent failures must be 1/1000 or less.”, the aspect of “combined probability” seems to conflict with CS 25.1309 (b).(5) where latent failures are considered one latent failure at a time, not as a “combined” set of latent failures. Please consider deleting this CS 25.671 paragraph, since CS 25.1309 will now cover this regulation.</p>
response	Please refer to the response to comment #86.
comment	<p>305 comment by: <i>Hélio A. Loureiro</i></p> <p>My proposed changes convention: · deletion in ; · insertion in blue; · reallocation by deletion and insertion there. =====</p> <p>Change 1: Delete the text “<i>For single failures:</i>”.</p> <p>(1) Any single failure, excluding failures of the type defined in (c)(3). Comment 1: No content change, just a writing suggestion to improve clarity. Rationale: The requirement in paragraph (c) applies to “any of the following failures ...”; so, it must be followed by a list of failures! The first failure in the list is just: “<i>any single failure ...</i>”. The text “<i>For single failures</i>” is meaningless and should be removed. =====</p> <p>Change 2: Delete the text “<i>For combinations of failures:</i>” and reallocate the text “<i>,excluding failures of the type defined in (c)(3)</i>”.</p> <p>(2) (i)Any combination of failures not shown to be extremely improbable, excluding failures of the type defined in (c)(3).</p>

Comment 2: No content change, just a writing suggestion to improve clarity. Rationale: The requirement in paragraph (c) applies to **“any of the following failures”**; so, **it must be followed by a list of failures!** The second failure in the list is just: *“any combination of failures”*. The text *“For combinations of failures”* is meaningless and should be removed.

=====

Change 3: Reallocate paragraph (c)(3)(ii) to new dedicated paragraph (g), and implement the following changes:

- a) insert *“Excluding failures of the type defined in (c)(3).”* at to replicate the context applicable to (c)(3)(ii);
 - b) replace the text *“the sum of all”* by the word *“any”*; and
 - c) delete the word *“combined”*.
- (g) Excluding failures of the type defined in (c)(3):

Given any single latent failure has occurred, the average probability per flight hour of any failure condition preventing continued safe flight and landing, due to any subsequent single failure, must be less than 1E-5, and the probability of the latent failure must be 1/1000 or less.

Comment 3: Reallocation plus content change. Rationale:

- i) Reallocation: The sub-paragraph (ii) is a requirement (“must be”) and **not a definition of a type of failures** (“not shown ...”). It is confusing to have a requirement in the middle of the list of failures to which the requirement in paragraph (c) applies. For clarity it is proposed to reallocate this requirement in a new dedicated paragraph (g);
- ii) Context replication: The original context is *“For combination of failures, excluding failures of the defined in (c)(3)”*. The condition *“combination of failures”* is already included in the requirement; so remains to be imposed the exclusion of *“failures of the type defined in (c)(3)”*.
- iii) Writing: the text *“the sum of all subsequent single failures”* may be read as *“the combination of all subsequent single failures”* while it intends to refer, I presume, to the occurrence of the failure condition as a result of the occurrence of the given latent failure combined with the subsequent occurrence of *“any”* single failure. So it is proposed to replace the text *“the sum of all”* by the word *“any”*;
- iv) Content change: The word *“combined”*, as used in the ARAC 25.671, refers to *“the sum of the probabilities”*, which is not harmonized with, and much more restrictive than, the NPA’s addition to 25.1309, paragraph (b)(5)(iii). It is proposed to remove the word *“combined”*. Note that the other possible meaning of *“combined”* is *“the product of the probabilities”*, but this is meaningless, and in practice, not restrictive at all.

=====

Change 4: Reallocate the jam evaluation criteria to the AMC.

(3) Any failure or event that results in a jam of a flight control surface or pilot control that is fixed in position due to a physical interference.

Comment 4: It is suggested that this text (deleted above) be reallocated to the AMC, since it is more a guidance for compliance than a requirement.

=====

Change 5: Reallocate the paragraph (c)(3)(iii) to a new dedicated paragraph (h).

(h) In the presence of a jam considered under this subparagraph, any additional failure states that could prevent continued safe flight and landing shall have a combined probability of 1/1000.

Comment 5: No content change, just a reallocation suggestion to improve clarity. Rationale:

The sub-paragraph (iii) (deleted above) is a requirement (“shall have”) and **not a definition of a type of failures** (“that results ...”). It is confusing to have a requirement in the middle of the list of failures to which the requirement in paragraph (c) applies. For clarity it is proposed to reallocate this requirement in a new dedicated paragraph (h).

=====

Change 6: *Reallocate the paragraph (c)(5) to a new dedicated paragraph (i).*

(i) Probable failures must be capable of being readily counteracted by the pilot.

Comment 6: *No content change, just a reallocation suggestion to improve clarity.*

Rationale:

The sub-paragraph (5) (deleted above) is a requirement (“must be”) and **not a definition of a type of failures** (“any runaway ...”). It is confusing to have a requirement in the middle of the list of failures to which the requirement in paragraph (c) applies. For clarity it is proposed to reallocate this requirement in a new dedicated paragraph (i).

response Partially accepted.
Comments 1 and 2 are accepted.
The other comments are not fully understood by EASA. No change has been made following these comments, but please note that the text of CS 25.671(c)(ii) has been further clarified.

comment 312 comment by: *Gulfstream Aerospace Corporation*

CS 25.671 (a)

“Each control and control system must operate with the ease, smoothness, and positiveness appropriate to its function. ~~(See AMC 25.671 (a).)~~ The flight control system shall be designed to continue to operate in any attitude and must not hinder aircraft recovery from any attitude.”

- GAC Response:

The added text constitutes a new and unrelated requirement.

The current wording may lead some to interpret the rule as a compound requirement for the flight control system, where smoothness and positiveness must be shown in any attitude. This would be difficult to demonstrate in unusual attitudes.

Recommended:

Good requirement management practice would indicate the new text should be added as a separate lettered item and not within 25.671(a).

response Accepted.
The second sentence has been clearly separated from the first sentence.

comment 313 comment by: *Gulfstream Aerospace Corporation*

CS 25.671 (b)

“Each element of each flight control system must be designed, ~~or distinctively and permanently marked,~~ to minimise the probability of incorrect assembly that could result in the failure of the system to perform its intended function malfunctioning of the...”

- GAC Response:

Common usage of the term "malfunction" in the industry is related to unintended function operation, not loss of function.

With the elimination of the word "failure", it can be interpreted that a potential mis-assembly resulting in a loss of function is not subject to this rule.

A potential mis-assembly resulting in a latent loss of function would, therefore, likely be considered acceptable under some interpretations of this proposed rule.

response	Accepted. The principle of this comment is accepted. CS 25.671(b) has been rewritten in the light of all the comments received.
comment	314 comment by: Gulfstream Aerospace Corporation CS 25.671 (c) "The aeroplane must be shown by analysis, test, or both, to be capable of continued safe flight and landing after any of the following failures or, including jamming, in the.." <ul style="list-style-type: none"> GAC Response: The wording "including jamming" is superfluous, recommend deletion.
response	Not accepted. As a 'jam' may result from an event that may not be considered to be a 'failure', it is deemed better to maintain this reference in the introductory sentence.
comment	315 comment by: Gulfstream Aerospace Corporation CS 25.671 (c)(2)(ii) "Given any single latent failure has occurred, the average probability per flight hour of any failure condition preventing continued safe flight and landing, due to the sum of all subsequent single failures, must be less than 1E-5, and the combined probability of the latent failures must be 1/1000 or less. Any combination of failures not shown to be extremely improbable, excluding jamming (for example, dual electrical or hydraulic system failures, or any single failure in combination with any probable hydraulic or electrical failure)." <ul style="list-style-type: none"> GAC Response: The wording of this item does not fit the paragraph. Also, the text does not make sense. The 1/1000 condition does not relate to "given any single latent failure has occurred".
response	Noted. This subparagraph has been rewritten.
comment	316 comment by: Gulfstream Aerospace Corporation CS 25.671 (c)(4) "Any runaway of a flight control to an adverse position that is caused by an external source." <ul style="list-style-type: none"> GAC Response: "Adverse position" and "external source" are vague. Recommended: <i>"(c)(4) Any flight control system condition resulting from a single particular risk occurrence, maintenance error, or other foreseeable external event."</i>
response	Partially accepted. The first part of the sentence is maintained with a change to clarify it; the second part is changed as proposed.
comment	317 comment by: Gulfstream Aerospace Corporation

CS 25.671 (c)(5)

"Probable failures must be capable of being readily counteracted by the pilot."

- GAC Response:

The wording of this item does not fit the paragraph.

response

Accepted.

The sentence has been rewritten.

comment

319

comment by: Boeing

Page:13

Paragraph: CONTROL SYSTEMS

CS 25.671 General

25.671(d)

The proposed text states:

"The aeroplane must be designed so that, if all engines fail at any point of the flight and a suitable runway is available, then it is controllable: if all engines fail.

- (1) In flight;
- (2) On approach;
- (3) During the flare to a landing;
- (4) During the ground phase; and
- (5) The aeroplane can be stopped."

REQUESTED CHANGE:

"(d) The aeroplane must be designed so that, if all engines fail at any point of the flight and a suitable hard surface runway or equivalent is available for which the distance available following the flare to landing is consistent with the available aeroplane deceleration capability with all engines failed, then it is controllable: if all engines fail.

- (1) In flight;
- (2) On approach;
- (3) During the flare to a landing, and
- (4) During ~~the ground phase; and~~ ground deceleration to a stop.
- ~~(5) The aeroplane can be stopped."~~

JUSTIFICATION:

Draft CS 25.671(d) requires controllability of the airplane after failure of all engines. It is reasonable to identify flight phases where this should be possible, so subparagraphs (1) "In flight," (2) "On approach"; and (3) "During the flare to a landing" appear to be consistent with past practice and appropriate to include in this requirement.

Specifying subparagraph (4) "During the ground phase" is less realistic since there is no definition provided for a "suitable runway," and, in fact, the safety record shows that a "suitable runway" with all engines inoperative could even be a river.

However, of particular concern, subparagraph 25.671(d)(5) ("The aeroplane can be stopped") does not refer to controllability or control systems. This subparagraph would appear to introduce a new implied airplane performance requirement related to stopping performance with all engines inoperative. The calculated stopping distance for an all-engines-out landing at an unplanned destination that might not even resemble a hard-surface runway would involve too many factors to drive a meaningful design criterion. Conversely, over-simplification of the situation would provide no benefit, or could drive system design changes that actually make the airplane less safe.

Boeing suggests that our concerns with subparagraphs (4) and (5) can be rectified by first



	<p>defining a “suitable runway” to have a hard surface as well as a distance available following flare to landing that is consistent with the available airplane deceleration capability on the ground with all engines failed. Additionally, we recommend revising subparagraph 25.671(d)(4) to refer to “ground deceleration to a stop,” and then subparagraph 25.671(d)(5), which has nothing to do with controllability, would become redundant and could be eliminated.</p> <p>Additionally, the proposed requirement (as stated in the NPA) could create a significant disharmonization with the U.S. FAA’s regulations. Our preference would be that a change of this magnitude should only be undertaken as part of a regulatory harmonization activity that includes participation by all the affected disciplines – airplane performance and handling qualities specialists, as well as systems and flight control specialists.</p>
response	<p>Partially accepted.</p> <p>Some aspects of this comment have been accepted. The proposed specification has been discussed with the FAA.</p> <p>Both EASA and the FAA prefer to keep some deceleration function as part of this paragraph.</p>
comment	<p>320 comment by: <i>Gulfstream Aerospace Corporation</i></p> <p>CS 25.671 (c)</p> <p>To make 25.671(c) clear and to resolve all the individual issues noted, Gulfstream proposes the following wording:</p> <p>“CS 25.671</p> <p>(c) The aeroplane must be shown by analysis, test, or both, to meet the following conditions:</p> <p>(1) To be capable of continued safe flight and landing after any of the following failures in the flight control system within the normal flight envelope:</p> <p>(i) Any single failure, excluding failures of the type defined in (c)(1)(iii).</p> <p>(ii) Any combination of failures not shown to be extremely improbable, excluding failures of the type defined in (c)(1)(iii).</p> <p>(iii) Any failure or event that results in a jam of a flight control surface or pilot control that is fixed in position due to a physical interference.</p> <p>(iv) Any flight control system condition resulting from a single particular risk occurrence, maintenance error, or other foreseeable external event.</p> <p>(2) Given any single failure, including failures of the type defined in (c)(1)(iii), the combined probability of all the subsequent failure states that could prevent continued safe flight and landing must be less than 1/1000.</p> <p>(3) Given any single latent failure has occurred, the combined average probability of all the subsequent single failures preventing continued safe flight and landing must be less than 1E-5 per flight hour.</p> <p>(4) The jam defined in (c)(1)(iii) must be evaluated as follows:</p> <p>(i) The jam must be considered at any normally encountered position of the control surface, or pilot controls.</p> <p>(ii) The causal failure or failures must be assumed to occur anywhere within the normal flight envelope.</p> <p>(5) Probable failures must be capable of being readily counteracted by the pilot.”</p>
response	<p>Not accepted.</p> <p>The proposed wording missed some points (e.g. jam) and does not seem to be clearer than the proposed wording in the NPA. An event leading to a jam is not necessarily a failure.</p>

comment	<p data-bbox="359 235 406 280">321</p> <p data-bbox="901 235 1498 280" style="text-align: right;">comment by: Gulfstream Aerospace Corporation</p> <p data-bbox="359 291 526 324">CS 25.671 (d)</p> <p data-bbox="359 324 1498 403"><i>"The aeroplane must be designed so that, if all engines fail at any point of the flight and a suitable runway is available, then it is controllable: if all engines fail.</i></p> <p data-bbox="359 403 782 582"> <i>(1) In flight; (2) On approach; (3) During the flare to a landing; (4) During the ground phase; and (5) The aeroplane can be stopped."</i> </p> <ul data-bbox="406 582 638 616" style="list-style-type: none"> • GAC Response: <p data-bbox="359 616 845 649">The last item does not fit the paragraph.</p> <p data-bbox="359 649 558 683">Recommended:</p> <p data-bbox="359 683 1498 761"><i>"(d) The aeroplane must be designed so that, if all engines fail at any point of the flight and a suitable runway is available, then:</i></p> <p data-bbox="359 761 782 974"> <i>(1) It is controllable: (i) In flight; (ii) On approach; (iii) During the flare to a landing; (iv) During the ground phase (2) The aeroplane can be stopped."</i> </p>
response	<p data-bbox="359 985 446 1019">Noted.</p> <p data-bbox="359 1019 1498 1108">The comment is agreed in principle, but CS 25.671(d) has been changed in a way that the recommended change does not apply anymore.</p>
comment	<p data-bbox="359 1153 406 1198">346</p> <p data-bbox="845 1153 1498 1198" style="text-align: right;">comment by: Universal Avionics Systems Corporation</p> <p data-bbox="359 1209 1498 1299">Page 13, section (c)(2)(ii). Meaning is unclear for "sum of single failures". Clarify intended method of analysis.</p>
response	<p data-bbox="359 1299 478 1332">Accepted.</p> <p data-bbox="359 1332 1498 1433">The text has been revised to refer to the sum of probabilities of all subsequent single failures.</p>
comment	<p data-bbox="359 1478 406 1523">362</p> <p data-bbox="1117 1478 1498 1523" style="text-align: right;">comment by: Hélio A. Loureiro</p> <p data-bbox="359 1534 861 1579">Alternative Proposal to 25.671(c)(2) & (3)</p> <p data-bbox="359 1579 1498 1646">1) The NPA's proposal for CS-25.671(c)(2)(ii) and for CS-25.1309(b)(5)(ii) and (iii) seems to follow the ASAWG ARAC "Specific Risk" proposal to harmonize 25.671 and 25.1309.</p> <p data-bbox="359 1646 1498 1713">2) But this harmonization proposal is not followed in the NPA's proposal for CS-25.671(c)(3)(iii), which maintains the FCHWG ARAC "25.671" proposal .</p> <p data-bbox="359 1713 1037 1758">3) My comments #305 and #342 follows the NPA closely.</p> <p data-bbox="359 1758 1498 1870">4) Nevertheless, I would like also to present my preferred alternative bold proposals to the 25.671(c)(2) and 25.671(c)(3), which resembles the FCHWG ARAC proposals, but which are slightly different:</p> <p data-bbox="359 1870 558 1904">For 25.671(c)(2):</p> <p data-bbox="359 1904 1498 2004"><i>"Given any single failure has occurred, the conditional probability of occurrence of any failure condition during any flight which could prevent continued safe flight and landing shall be less than 1/1000."</i></p> <p data-bbox="359 2004 558 2045">For 25.671(c)(3):</p>

“Given a jam of the type defined in (c)(3) has occurred, the conditional probability of occurrence of any failure condition during any flight which could prevent continued safe flight and landing shall be less than 1/1000.”

5) The comparison between these proposals vs. the FCHWG ARAC proposals must consider two cases:

a) the “given single failure” is *latent*: they are equivalent; and
 b) the “given single failure” is *evident*: they are different, since these proposals requires at least one failure to occur **after** the “given single failure” has occurred, while the FCHWG ARAC text does not require this.

6) These alternative proposals have the following advantages:

a) they do not distinguish between evident or latent failures when imposing the same “residual risk” limit for both;

b) they do not exclude any cutsets;

It seems to me that, for each catastrophic failure condition, what matters is, at first, its probability of occurrence during a flight, any flight!

And at second, it is its *conditional* probability of occurrence, given any single failure has occurred. Latent or evident, it does not matter; the result is a catastrophe!

This conditional probability is the sum of probabilities of occurrence, *during the flight*, of each single failure, or combination of failures, which combines with the “given single failure” to result in the occurrence of the failure condition *during the flight*.

Note that the “combination of failures” mentioned above may be, for instance, a combination of two latent failures, if the “given single failure” is evident!

In this case, for the combination to occur during the flight considered, at least one of the two latent failures must occur during such flight (supposing the worst case where the given single failure has occurred just at the start of the flight).

Note that the FCHWG ARAC text does not impose this restriction.

So these alternative proposals do **not** treat the same way failures which do **not** contribute the same way to the occurrence of the failure condition, given a single failure has occurred.

For instance: a failure condition has two (minimum) cutsets only:

$(F_1; F_2)$

$(F_1; F_3; F_4)$

Per our proposal, given F_1 has occurred:

$p(F_2) + p(F_3; F_4) < 1/1000$, or

$p(F_2) + p(F_3) * p(F_4) < 1/1000$, assuming F_3 and F_4 are independent.

That is, the restriction applied on F_2 is tighter than the restriction applied to F_3 or F_4 .

Concerning cutsets with order greater than 2, one may say that they are less significant than dual cutsets, but that’s not always true. If they are irrelevant, there is no burden from including them under the limit; on the other hand, if they are relevant, then they should be included.

response

Not accepted.

The proposal for CS 25.671(c)(2) is not accepted as it would be less stringent than CS 25.1309 (which will also apply).

The proposal for CS 25.671(c)(3) does not clarify the initial wording, and defining a ‘conditional probability’ does not provide a benefit in our opinion.

Evident-Evident failures are not considered to be a specific risk of concern. *Evident-Evident* cutsets may be excluded from specific risk.

EASA wishes to distinguish between evident and latent failures.

The greatest concern is with failures where the aircraft is one failure away from a catastrophic event.



3. Proposed amendments - CS-25 - Book 1 - CS 25.933

p. 14

comment

45

comment by: UK CAA

Page No: Page 14 and page 33**Paragraph No:** Subpart E Powerplant – CS 25.933 Reversing Systems**Comment:**

1. CS25.933 has been changed to include the requirement to directly comply with 25.1309(b).
2. The new wording in AMC 25.933 is contradictory.

Justification:

1. 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.
2. AMC 25.933 states that latent failures “should be avoided whenever practical”, but then further states that “neither failure may be pre-existing”.

Proposed Text: Amend AMC 25.933 to be consistent and match the intent of 25.1309.

response

Not accepted.

AMC 25.933 is considered consistent and matches the intent of CS 25.1309. AMC 25.933 has been changed as follows: ‘Latent failures involved in unwanted in-flight thrust reversal should be avoided whenever practicable. The design configurations in paragraphs 8.b.(2) and 8.b.(3) have traditionally been considered practicable and deemed to be acceptable to EASA.’ This change supports compliance with CS 25.1309(b).

Indeed, configurations described in 8.b.(2) have traditionally been considered to be practicable, and as such ensure compliance with CS 25.1309(b)(4). No dual failure combination, either of which is latent for more than one flight, leading to a catastrophic unwanted in-flight thrust reversal, should then remain in the thrust reverser system design. As such, CS 25.1309(b)(5) is not applicable. Therefore, the 1/1000 value introduced in CS 25.1309(b)(5)(iii) is not included in AMC 25.933 section 8.b.(2).

Comment from Textron Aviation (extracted from the letter attached to comment #289):Page/Paragraph: CS 25.933

Comment: This NPA seems to be codifying into the EASA CS 25.933 regulation the same requirements that the FAA has been enforcing through issue papers and that EASA was providing guidance through the AMC for thrust reversers certified by reliability. As the regulation still allows for compliance by controllability as an alternate means, those aspects do not seem to be affected by this NPA.

Suggested change: None.EASA response: Noted.

It is confirmed that the regulation still allows for compliance by controllability.

3. Proposed amendments - CS-25 - Book 1 - CS 25.1309

p. 14-15



comment

46

comment by: UK CAA

Page No: Multiple, but evident on page 15 and subsequent

Paragraph No: CS25.1309(b)(4), (b)(5) and many subsequent paragraphs of CS and AMC.

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”.

Justification: Many cases of usage now exist, an example is used to illustrate the issue:

CS25.1309(b)(4) Any significant latent failure is minimised to the extent practical; and

CS25.1309(b) (5)(i) it is impractical to provide additional fault tolerance.

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.

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.

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”.

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.

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.

If the requirement was to minimise the significant latent failures to the extent reasonably practicable, then the 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.

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.

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.

Proposed Text: Change “Practical” and “Impractical” to “Reasonably Practicable” and “Reasonably Impracticable”.



response	Partially accepted. The resulting text has been amended to read 'Practicable' and 'Impracticable' instead of 'Practical' and 'Impractical', ensuring consistency with other CS-25 requirements. In order to address the concept of technologically feasible and economically practicable, the resulting text refers to AMC 25-19 paragraph 8 'Design considerations related to significant latent failures' (and indirectly to Appendix 1 'Supplemental guidance for the use of CMRs').
comment	59 comment by: <i>Thales Avionics- JD Chauvet</i> CS 25.1309 section (4): the applicability of the "significant latent failure" in regard to failure condition severity class is unclear comparing to the definition made in AMC25.1309 5.v. and detailed made in 9b.(6) which associate it to hazardous and catastrophic FCs ==> directly clarify in (4) that it applies to hazardous and catastrophic FCs
response	Not accepted. CS 25.1304(b)(4) is applicable to any significant latent failure. The term 'significant latent failure' is defined in AMC 25.1309 section 5 'Definitions' as 'a latent failure that would, in combination with one or more specific failures or events, result in a Hazardous or Catastrophic Failure Condition'. It is then considered that there is no ambiguity about the failure condition classification related to significant latent failures.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: CS 25.1309 Additional requirement (b) (4).

Comment: Difficult to show compliance to "minimized to the extent practical". Even the AMC wording is vague with references to past experience and sound engineering judgment etc. The AMC states "There can be situations where it is not practical to meet the 1/1000 criterion. For example, if meeting this criterion would result in performing complex or invasive maintenance tasks on the flight line, thereby increasing the risk of incorrect maintenance."

The AMC states that it is not expected to see a demonstration of compliance but that the minimization of significant latent failures is rather expected to be an integral part of each applicant's normal design practices. It is not clear how compliance can be shown with regards to "minimization" and "sound engineering judgment".

Suggested change: Propose deleting this requirement because it would put an extra burden on the applicant when it only amounts to being a verification of the applicants normal design practices.

EASA response: Not accepted.

The approach proposed by EASA in the NPA (introducing CS 25.1309(b)(4) and CS 25.1309(b)(5)(i)) addresses the EASA dissenting opinion and the FAA dissenting opinion #2, submitted to the ASAWG and recorded in the report.

comment	61 comment by: <i>Thales Avionics- JD Chauvet</i> CS25.1309 (5)(iii): use of "maximum time" is inconsistent with average probability computation detailed in AMC25.1309 11.e. and Appendix3 ==> replace "maximum time" per "average time"
---------	--



response	<p>Partially accepted.</p> <p>The term ‘maximum exposure time’ should not prevent an average probability computation at the top event level (failure condition) for demonstrating compliance with the safety objectives.</p> <p>Distinct formulas for latent failures may be used to compute the worst-case flight probability or the average probability per flight. While the results are different, the ‘maximum exposure time’ for the latent failures is used in both computations.</p> <p>EASA recognises, however, that the NPA text for CS 25.1309(b)(5)(iii) may force the applicant to compute the worst-case flight probability. This text has been revised to read: ‘(iii) the occurrence probability of the latent failure does not exceed 1/1000.’</p> <p>The NPA text for AMC 25.1309 section 9.b.(6)(iii) is modified in accordance with the updated CS 25.1309(b)(5)(iii). The following text is added at the end of this subparagraph: ‘The occurrence probability of the significant latent failure for the 1/1000 criterion may be computed as either the worst-case flight probability or the average probability per flight. The applicant is not expected to run two different types of computation for compliance with CS 25.1309(b). [...]’</p> <p>The NPA text for AMC 25.1309 section 9.b.(6)(ii) is also modified in accordance with the updated CS 25.1309(b)(5)(iii). The resulting text reads: ‘[...] This is achieved by requiring that the occurrence probability of the latent failure does not exceed 1/1000. [...]’</p> <p>Following the same rationale, the NPA text for AMC 25.1309 section 11.e.(1)(v) is modified. The term ‘average’ is, however, not reintroduced as it is considered to be equally misleading. The resulting text reads: ‘(v) the average exposure time if the failure can persist for multiple flights.’</p>
comment	<p>91 comment by: <i>Dassault Aviation</i></p> <p>Dassault-Aviation comment page #15</p> <p>Extract: CS 25.1309(b)(5)(iii) the product of the maximum time the latent failure is expected to be present and its failure rate does not exceed 1/1000.</p> <p>Comment: Dassault-Aviation position for computing the occurrence probabilities of latent failures is to use the average probability, that is to say the product of the average time (and not the maximum time) the latent failure is expected and its failure rate.</p> <p>A different approach would be not consistent with ARP 4761, ARAC ASAWG and more particularly with the 25.1309 probability criteria that are defined as average probabilities per flight hour. It may also lead to unjustified constraints on maintenance (economic impact).</p> <p>Requested Change: Modify “maximum time” by “average time”.</p>
response	<p>Please refer to the response to comment #61.</p>
comment	<p>123 comment by: <i>Garmin International</i></p> <p>Section 3.1. CS 25.1309(b)(4)</p> <p>CS 25.1309 (b) (4) was not an ASAWG recommendation. Additionally, as written, the proposed rule is a qualitative requirement, which is cause for concern because minimization of “Any significant failure ... to the extent practical” is open-ended without a well-defined criterion for knowing when such a process is complete. It is recommended that CS 25.1309</p>

response	<p>(b) (4) be deleted.</p> <p>Not accepted.</p> <p>It is agreed the CS 25.1309(b)(4) provides a qualitative objective. How to meet this objective is then detailed in AMC 25.1309 section 9.b.(6)(1).</p>
comment	<p>124 comment by: <i>Garmin International</i></p> <p>Section 3.1. CS 25.1309(b)(4)</p> <p>The scope of CS 25.1309 (b) (4) goes beyond what was considered warranted by the ASAWG. The proposed AMC 25.1309 section 5 item v definition of the term “significant latent failure” encompasses Hazardous failure conditions. It is acceptable for Hazardous conditions to be caused by single failures (the current CS 25.1309 (b) (1) rule specifies a Catastrophic failure can “not result from a single failure” but there is no similar requirement in CS 25.1309 (b) (2) for Hazardous failures; the proposed CS 25.1309 is unchanged in this regard). It was therefore considered acceptable for the existing average probability calculation to determine exposure time (maintenance intervals) associated with failure combinations. Worst case deviation associated with latency still leaves the airplane one or more failures away from a Hazardous condition. It is recommended that CS 25.1309 (b) (4) be deleted.</p>
response	<p>Not accepted.</p> <p>Addressing by the term ‘significant latent failure’ the latent failures involved in hazardous failure conditions is not a new concept created with this NPA. It is also not new that the use of periodic maintenance or flight crew checks, to detect significant latent failures, is undesirable and should not be used in lieu of practical and reliable failure monitoring and indications.</p> <p>The aim of the NPA was to reinforce the above concept, thereby the proposed CS 25.1309(b)(4) and the associated acceptable means of compliance detailed in AMC 25.1309 section 9.b.(6)(1). Reinforcing this concept at the level of the specification was considered to be a prerequisite for introducing the specific risk quantitative criteria proposed by the ASAWG report.</p>
comment	<p>125 comment by: <i>Garmin International</i></p> <p>Section 3.1. CS 25.1309(b)(5)(i)</p> <p>CS 25.1309 (b) (5) (i) was not an ASAWG recommendation. The associated AMC 25.1309 does not define “fault tolerance”; therefore, it is not clear what is meant by this term. Fault tolerance can be defined as a system that continues its intended operation, rather than failing completely when some part of the system fails. This can apply to failures that contribute to a loss of function. However it may not be an appropriate term to use when addressing failures that contribute to a malfunction. In such situations it may be expected that the system is shutdown.</p> <p>The ASAWG proposed AC/AMC recommended that latent failures were to be avoided by monitoring or that dual failure combinations were to consider the addition of redundancy to reduce the effect of latency. If this is the intent it should be made clear to the reader. Please define the term “fault tolerance”. If the term is used in a broader sense than envisioned by ASAWG proposed AC/AMC guidance then it is recommended that CS 25.1309 (b) (5) (i) be deleted.</p>
response	<p>Partially accepted.</p> <p>The intention was to propose a text for CS 25.1309(b)(5)(i) in accordance with the ASAWG</p>

recommendation.

The text has been revised to state that 'it is impracticable to provide additional redundancy'.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: CS 25.1309 Additional requirement (b) (5).

Comment: Difficult to see how it can be shown that additional fault tolerance is impractical. Given that other proposed changes to CS 25.1309 are attempting to remove ambiguity, this change seems to be adding ambiguity.

Suggested change: Propose that this section be re-written to remove the ambiguity.

EASA response: Noted.

CS 25.1309(b)(5) and the related AMC material have been revised based on the detailed changes suggested by other comments. The resulting text should contribute to remove ambiguity.

comment	126	comment by: <i>Garmin International</i>
	<p>CS 25.1309 (b) (5) (ii) is a deviation from ASAWG recommended text. The proposed rule can be more clearly stated. Recommend the following text. "For failure combinations that contain the same latent failure, the sum of all subsequent single failures is remote."</p>	
response	<p>Partially accepted. The ASAWG recommended text was not considered clear enough, therefore the proposed deviation. EASA recognises, however, that the NPA verbiage could be improved. The resulting text reads: '(ii) given that a single latent failure has occurred on a given flight, the catastrophic failure condition is remote; and...'</p>	
comment	127	comment by: <i>Garmin International</i>
	<p>CS 25.1309 (b) (5) (iii) is a deviation from the ASAWG recommendation. The ASAWG recommendation for calculating probabilities of latent failures was consistent with the calculation methodology used in determining average probability. To make use of fault tree analyses, the applicant will have to change from an average probability calculation used in meeting the 10-9/FH objective. There is no rationale for why the average probability calculation that has been the standard calculation methodology used in showing compliance to CS 25.1309 is no longer acceptable to calculate the probability of latent failures. It is recommended that the ASAWG CS 25.1309 (b) (5) (iii) rule recommendation be incorporated instead of the NPA rule.</p>	
response	<p>Please refer to the response to comment #61.</p>	
comment	187	comment by: <i>Embraer - Indústria Brasileira de Aeronáutica - S.A.</i>
	<p>CS 25.1309(b): The NPA proposal was substantially changed from the ASAWG recommendation, most importantly in subparagraph (b)(5)(ii) that addresses residual risk for a catastrophic failure condition after a single latent failure. The ASAWG recommendation called for the combined</p>	

probability due to any subsequent single failure to be remote, while the NPA requires that the sum of all subsequent single failures be remote. It is not clear whether the NPA proposal is intended to be the same as the ASAWG recommendation. Embraer recommends that the recommendation of ASAWG be maintained. In addition, similar to our comment about CS 25.629, the residual risk requirement in CS 25.1309(b)(5)(ii) would be more clearly written as “. . . due to the sum of the probability of all subsequent single failures, . . .”

response Please refer to the response to comment #126.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: CS 25.1309(b)(5), AMC 25.1309 Section 8c3

Comment: NPA AMC 25.1309 Section 8c3 (and NPA CS 25.1309(b) (5)) adds that for catastrophic failure conditions, resulting from two failures, either of which is latent for more than one flight, “is remote when either one is pre-existing.” Since the existing AMC 25.1309 Section 7c1ii defines “remote” as a failure rate less than $10e-5$ but greater than $10e-7$, the addition is more severe than the former “single + probable” interpretation, which only required failure rates less than $10e-5$. The FCHWG sought to remove “per flight hour” and “failure rate” terms and rather focus on probabilities (which include inspection intervals, failure rates, and flight durations) by introducing the concept of “1 in 1000” – which the proposed NPA language seeks to undo. While the initial impetus for “1 in 1000” was for just such conditions where two failures (either of which could be latent) could lead to a CAT event, the “1 in 1000” concept was broad enough that it would and did apply to any combination of failures.

Furthermore, NPA CS 25.1309(b) (5) (iii) states that in addition to the “remote” criteria, the probability should be less than $1/1000$ for the latent’s only. The FCHWG’s $1/1000$ applied to all additional failures, latent or active.

Suggested change: Propose striking the NPA language in favor of a broad “1 in 1000” criteria, (per the FCHWG) which would cover the underlying reason for the NPA addition, in a more straightforward manner. There appears to be nothing gained by a “remote” as well as a “ $1/1000$ ” criteria.

EASA response: Not accepted.

Two criteria are implemented in the CS: limit latency and limit residual probability. Limit latency is intended to limit the time of operating with an existing latent failure. This is achieved by requiring that the occurrence probability of the latent failure does not exceed $1/1000$. Limit residual probability is intended to limit the average probability per flight hour of the failure condition given the presence of a single latent failure. This is achieved by defining the residual probability to be remote. Residual probability is the combined average probability per flight hour of all the single active failures that result in the catastrophic failure condition assuming one single latent failure has occurred.

comment 207

comment by: Boeing

Page:15

Paragraph: CS 25.1309 (b)(4) and (5) -- Equipment, systems and installations

The proposed text states:

“(4) Any significant latent failure is minimised to the extent practical; and

(5) For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, it must be shown that:

(i) it is impractical to provide additional fault tolerance; and



(ii) given any single latent failure has occurred, the catastrophic failure condition due to the sum of all subsequent single failures is remote; and
 (iii) the product of the maximum time the latent failure is expected to be present and its failure rate does not exceed 1/1000."

REQUESTED CHANGE:

~~"(4) Any significant latent failure is minimized to the extent practical; and~~

(4.5) For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, it must be shown that:

~~(i) it is impractical to provide additional fault tolerance; and~~

(i.ii) given any single latent failure has occurred, the catastrophic failure condition due to the sum of all subsequent single failures is remote; and

(ii.iii) the product of the maximum time the latent failure is expected to be present and its failure rate does not exceed 1/1000."

JUSTIFICATION: The Airplane-Level Safety Analysis Working Group (ASAWG) specifically recommended wording that was less subjective than "minimize" and "extent practical," as manufacturers (OEM) had experienced these words resulting in unbalanced application of regulations, subject to widely differing interpretations of Agency specialists. This seems to have led to the AMC paragraph that states, "The Agency does not expect a dedicated demonstration of compliance with CS 25.1309(b)(4)."

Impracticality has an economic component; an OEM may conclude that eliminating a significant latent is too costly to be practical. This is a highly subjective area that would likely result in the arbitrary application of this rule that the OEMs were concerned with in the ASAWG.

The same concern applies to the showing of impracticality in CS 25.1309(b)(5)(i), which amounts to the same requirement as in proposed (b)(4).

Based on the above concerns, and since compliance will not be shown to it; it is not appropriate to include proposed subparagraphs 25.1309(b)(4) and (b)(5)(i) in the rule.

response

Not accepted.

The approach proposed by EASA in the NPA (introducing CS 25.1309(b)(4) and CS 25.1309(b)(5)(i)) addresses the EASA dissenting opinion and the FAA dissenting opinion #2, submitted to the ASAWG and recorded in the report.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: CS 25.1309

Comment: Object to "(4) Any significant latent failure is minimized to the extent practical; and" because the requirement for meeting the rule is not clear and unambiguous. As a result, it is open for interpretation by the authorities and will create an unlevel level of safety across different aircraft OEMs.

Suggested change: Recommends that this be struck or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Not accepted.

The approach proposed by EASA in the NPA (introducing CS 25.1309(b)(4) and CS 25.1309(b)(5)(i)) addresses the EASA dissenting opinion and the FAA dissenting opinion #2, submitted to the ASAWG and recorded in the report. The acceptable means of compliance to CS 25.1309(b)(4) and CS 25.1309(b)(5)(i) are provided in AMC 25.1309 section 9.b.(6).



comment	<p>208</p> <p>Page:15 Paragraph: 25.1309(b)(5) -- <i>Equipment, systems and installations</i></p> <p>The proposed text states: “(5) For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, it must be shown that:”</p> <p>REQUESTED CHANGE: “(5) For each catastrophic failure condition that results from two failures, either <u>one</u> of which is latent for more than one flight, it must be shown that:”</p> <p>JUSTIFICATION: The current proposed wording is overly restrictive. It disallows the use of effective frequent periodic tests with an interval greater than one flight.</p>	comment by: <i>Boeing</i>
response	<p>Not accepted.</p> <p>A failure is latent until it is made known to the flight crew or maintenance personnel. The purpose of CS 25.1309(b)(5) is to apply additional safety objectives to the combination of two failures, where one failure is latent for more than one flight. The combination of two failures, where one failure is latent for less than one flight, was not considered to be a specific risk of concern. As such, the current proposed wording is considered to be less restrictive than the change requested by Boeing. The current proposed wording limits indeed the application of the additional safety objectives to a subset of latent failures.</p>	
comment	<p>209</p> <p>Page:15 Paragraph: 25.1309(b)(5)(ii) -- <i>Equipment, systems and installations</i></p> <p>The proposed text states: “(ii) given any single latent failure has occurred, the catastrophic failure condition due to the sum of all subsequent single failures is remote; and ...”</p> <p>REQUESTED CHANGE: “(ii) given any single that a latent failure has occurred, the catastrophic failure condition due to the sum probability of all subsequent single failures that could create a catastrophic failure condition on a given flight is remote; and ...”</p> <p>JUSTIFICATION: The proposed language is unclear and could be interpreted to be inconsistent with the parent paragraph. The guidance that this should be calculated in probability-per-flight-hour would be included in the AMC.</p>	comment by: <i>Boeing</i>
response	<p>Please refer to the response to comment #126.</p>	
comment	<p>210</p> <p>Page:15 Paragraph: CS 25.1309(b)(5)(iii) -- <i>Equipment, systems and installations</i></p> <p>The proposed text states: “(iii) the product of the maximum time the latent failure is expected to be present and its</p>	comment by: <i>Boeing</i>

failure rate does not exceed 1/1000.”

REQUESTED CHANGE:

“(iii) the ~~product of the maximum time~~ probability of occurrence of the latent failure ~~could be expected to be present (per occurrence) and its failure rate does not exceed~~ is on the order of 1/1000 or less.”

JUSTIFICATION: The proposed text refers to “the *maximum* time the latent fault is *expected* to be present.” This is potentially confusing, since the maximum time and the expected time are two different things. Assuming the intent is to apply the maximum time, the wording about expected time should be deleted. Also, clarify that this refers to the exposure time *per occurrence* of the fault, rather than, say, the maximum amount of time it could be present for the life of the airplane. Further, the proposed rule does not accommodate the way the probability is calculated by most fault tree programs which uses $P=1-e^{-\lambda t}$ (and is more accurate versus $P=\lambda t$).

NOTE: The proposal assumes a uniform failure rate, so it would not be suitable for components with an aging or wear-out characteristic. The discussion on page 10 does not seem to address the issue. If the regulator’s intent is to cover all possible failure distributions, then a better way of expressing the requirement would be simply to say that the probability of the latent fault being present on any flight shall not exceed 1/1000.

response

Partially accepted.

The text has been revised to read: ‘(iii) the occurrence probability of the latent failure does not exceed 1/1000.’

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: CS 25.1309

Comment: Object to (5)(iii) because it violates one of the constraints imposed by TAEIG on the ASAWG tasking, that average risk would not be changed as a result of this tasking(!). This is a re-occurring theme in this proposal, and Cessna finds this an over reach by EASA and very troubling. The proposed (5) (iii) changes the use of average risk in the calculations to the risk on the last flight before the inspection to check against the latent failure. This approach is not supported by SAE ARP 4761, the Arsenal Draft of AC 25.1309-1B or by AC 23.1309-1E.

Suggested change: Recommends that this be struck or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Please refer to the response to comment #61.

comment

211

comment by: Boeing

Page:15

Paragraph: Paragraph: CS 25.1309(c) -- *Equipment, systems and installations*

The proposed text states:

“(c) ... Crew alerting must be provided in accordance with CS 25.1322. Systems and controls, including indications and annunciations must be designed to minimise crew errors, which could create additional hazards, consistent with CS 25.1302.”

REQUESTED CHANGE:



“(c) ... Crew alerting must be provided in accordance with CS 25.1322. Systems and controls, including indications and annunciations must be designed to minimise crew errors, which could create additional hazards, ~~consistent with CS 25.1302.~~”

JUSTIFICATION: CS 25.1302 was written to apply to “flight deck equipment” that the flight crew interacts with. Adding a reference to CS 25.1302 into CS 25.1309(c) would make CS 25.1302 applicable to all systems, which is beyond the original intent of CS 25.1302.

response

Partially accepted.

The change was not meant to extend the application of CS 25.1302 to all systems installed on the aeroplane, but to direct the applicant to CS 25.1302 when addressing minimisation of the crew errors within the frame of CS 25.1309(c). The resulting text reads: ‘Installed systems and equipment for use by the flight crew, including flight deck controls and information, must be designed in accordance with CS 25.1302 to minimise crew errors which could create additional hazards.’

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: CS 25.1309(c) Reworded requirement

Comment: Deletion of “warning indication” and replacing with the crew alerting specific with CS 25.1322 deprives the analysis the ability to take credit for other means of indicating problems to the flight crew. It is possible some unsafe system operating conditions may result in, for instance, severe vibration. Or another example would be an abrupt departure from flight attitude (sudden roll or pitch). By requiring a specific crew alerting means (visual and/or aural) for each unsafe system operating condition, additional sensors and CAS (crew alerting) messages within the avionics system are required. These additional CAS messages for failure events that are obvious to the flight crew by tactile or other means would result in issues such as

- More CAS messages to clutter the display
- Increase weight to accommodate sensors
- Increase complexity to accommodate sensors
- Additional testing to show the CAS message works as intended, and is set at a point to allow flight crew response before the failure condition severity would increase.
- Additional analysis to support the CAS message.
- Additional analysis to ensure the new sensors does not have adverse effects on the airplane.

Suggested change: Propose that the phrase “warning indication” be retained.

EASA response: Partially accepted.

The concern is acknowledged. The suggested change ‘warning indication’ is, however, not considered to be adequate to address this concern. Clarification has been made in AMC 25.1309 section 9(c).

comment 265

comment by: AIRBUS

PARAGRAPH / SECTION YOUR COMMENT IS RELATED TO:

CS 25.1309 b 4 Equipment, systems and installations

PROPOSED TEXT / COMMENT:

Replace NPA

(4) Any significant latent failure is minimised to the extent practical; and



(5) For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, it must be shown that:

- (i) it is impractical to provide additional fault tolerance; and
- (ii) given any single latent failure has occurred, the catastrophic failure condition due to the sum of all subsequent single failures is remote; and
- (iii) the product of the maximum time the latent failure is expected to be present and its failure rate does not exceed 1/1000.

by ASAWG recommendation

“25.1309(b)(4) For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, it must be shown that -

(i) Given any single latent failure has occurred, the combined probability due to any subsequent single failure is remote; and

(ii) The probability of occurrence of the latent failure is on the order of 1/1000 or less.”

RATIONALE / REASON / JUSTIFICATION:

To be consistent with ASAWG recommendations.

Industry was concerned about the proliferation and use of the qualitative statements . Therefore ASAWG did not provide any qualitative recommendation for CS 25.1309 and recommended to put further qualitative criteria into the AMC by adding AMC 25.1309, Section 9.b.(6).

ASAWG recommended “The probability of occurrence of the latent failure is on the order of 1/1000 or less.”, but NPA quotes “the product of the maximum time the latent failure is expected to be present and its failure rate does not exceed 1/1000”. Herewith the calculation of the average probability per flight hour is excluded. Calculations to be performed in accordance with draft NPA EASA decisions are too constraining.

response

Partially accepted.

The qualitative criteria contained in the AMC for the significant latent failures minimisation need to be introduced by the CS. This is the purpose of CS 25.1309(b)(4), as proposed in the NPA.

The approach proposed by EASA in the NPA (introducing CS 25.1309(b)(4) and CS 25.1309(b)(5)(i)) addresses the EASA dissenting opinion and the FAA dissenting opinion #2, submitted to the ASAWG and recorded in the report.

Concerning the probability computation, please refer to the response to comment #61.

comment

284

comment by: *Bombardier Aerospace*

The proposed new requirement in CS 25.1309 (b)(5) for additional analysis where failures are latent for more than one flight should not be used in the specification. Duration of a flight and the number of flights in a day can vary greatly, depending on both the aircraft mission and the operator. While some failures may be dependent on number of cycles, many others depend purely on number of flight hours operated. As such it is not a suitable standard threshold for latency detection.

Bombardier recommends retaining the more general sub-paragraph (b)(4) and removing (b)(5) to the AMC, with additional guidance added to limit its applicability only to systems where failure probability is dependent on number of cycles. Appropriate latency thresholds could then be used for each system in the aircraft.

response

Not accepted.

The aim of CS 25.1309(b)(5) is to apply additional safety objectives to the combination of failures presenting a specific risk of concern. Concerning the specific risk related to latent failures, the issue related to a given flight is the condition where the latent failure is re-



conducted from one flight to the other. This condition could leave the aeroplane one failure away from a catastrophic failure condition. This is the reason why CS 25.1309(b)(5) is applicable to the combination of two failures, where one failure is latent for more than one flight.

comment	293	comment by: <i>Rockwell Collins, Inc.</i>
	(b).(4) For the statement, “(4) Any significant latent failure is minimised to the extent practical”. Isn't this requirement very ambiguous? What does “extent practical” mean? Will EASA include a definition of “practical”? The ASAWG at one point during the 4 year effort tried to make a distinction between “practical” = can it be done <u>and</u> “practicable” = can it be done under reasonable economic constraints and considerations. Please provide text that clarifies EASA’s position on this aspect.	
response	Please refer to the response to comment #46.	
comment	294	comment by: <i>Rockwell Collins, Inc.</i>
	(b).(5).(ii) For the statement, “(5) (ii) given any single latent failure has occurred, the catastrophic failure condition due to the sum of all subsequent single failures is remote;”. This paragraph is not specifically dealing with or mentioning IDALs, but wouldn't this paragraph be implying that every latent failure must be a level A so that the subsequent can be considered remote or level C? Please provide additional clarification, especially with regard to any implications for IDAL assignment	
response	Noted. CS 25.1309(b)(5)(ii) does not have any implication on the assignment of development assurance levels (FDAL/IDAL). Assigning a ‘remote’ qualitative probability objective to the sum of all subsequent single failures does not imply assigning an IDAL C. There is no link between occurrence probability objectives and development assurance levels. The assignment of FDAL/IDAL is based on the classification of the sizing failure conditions and the aeroplane/system architecture considerations.	
comment	298	comment by: <i>Rockwell Collins, Inc.</i>
	(b).(5).(iii) For the statement, “(iii) the product of the maximum time the latent failure is expected to be present” does not match what the ASAWG discussed and concluded. Please consider incorporating verbiage from the ASAWG recommendation (to allow for the average risk FTAs to be used for the Specific Risk calculations, or provide additional commentary as to why the “maximum time” is required.	
response	Please refer to the response to comment #61.	
comment	310	comment by: <i>AIRBUS</i>
	PARAGRAPH / SECTION the COMMENT IS RELATED TO: CS 25.1309 (b) (5) (iii)	

PROPOSED TEXT / COMMENT:

Replace:

CS 25.1309 (b) (5) (iii)

the product of the maximum time the latent failure is expected to be present and its failure rate does not exceed 1/1000

by

“the product of the maximum time the latent failure is expected to be present by its instantaneous failure rate does not exceed 1/1000.”

3. RATIONALE / REASON / JUSTIFICATION:

The NPA proposition works only with exponential law (constant failure rate). It would be better and universal to use instantaneous failure rate.

Alaternative proposal could be:

CS 25.1309 (b) (5) (iii) “the maximum probability to have an hidden failure present does not exceed 1/1000.”

response Please refer to the response to comment #210.

comment 323

comment by: *Gulfstream Aerospace Corporation*

CS 25.1309 (b)(5)(i) & (ii)

“(5) For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, it must be shown that:

(i) it is impractical to provide additional fault tolerance; and

(ii) given any single latent failure has occurred, the catastrophic failure condition due to the sum of all subsequent single failures is remote; and

(iii) the product of the maximum time the latent failure is expected to be present and its failure rate does not exceed 1/1000.”

- GAC Response:

Recommended:

“(i) it is impractical to provide fault detection eliminating the latency; and

(ii) it is impractical to provide additional fault tolerance; and (...)”

response Not accepted.

The CS 25.1309(b)(5)(i) that is proposed by this comment is considered to be addressed by the NPA proposal for CS 25.1309(b)(4) and the related guidance in the respective AMC.

comment 342

comment by: *Hélio A. Loureiro*

My proposed changes convention:

· deletion in ;

· insertion in blue;

· reallocation by deletion and insertion there.

=====

Change 1: Insert the text “*the occurrence of*”, and replace the text “*the sum of all*” by the word “*any*”.

(5) For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, it must be shown that:

(i) ...

(ii) given any single latent failure has occurred, the occurrence of the catastrophic failure condition due to any subsequent single failure is remote; and

(iii) ...



Comment 1: No content change, just a writing suggestion to improve clarity. Rationale:

a) Writing: The insertion of text "the occurrence of" makes it clear that "the catastrophic failure condition" is the one selected at the paragraph (5); without that text, this catastrophic failure condition is the one due to "the sum of all subsequent single failures", that is, the "combination of all subsequent failures", which is not the one selected at paragraph (5).

b) Writing: the text "the sum of all subsequent single failures" may be read as "the combination of all subsequent single failures" while it intends to refer, I presume, to the occurrence of the failure condition as a result of the occurrence of the given latent failure combined with the subsequent occurrence of *any* single failure. So it is proposed to replace the text "the sum of all" by the word "any";

=====

Change 2: Replace the text "the product of the maximum time the latent failure is expected to be present and its failure rate" by "the probability of occurrence, or presence, of the latent failure during any flight";

(5) For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, it must be shown that:

(i) ...

(ii) ...

(iii) the probability of occurrence, or presence, of the latent failure during any flight does not exceed 1/1000.

Comment 2: No content change, just a writing suggestion to improve clarity. Rationale:

The probability maybe calculate by other formulas than $\lambda * T$, where λ : failure rate, and T: the latent failure check interval. The text "any flight" includes also the flight just prior to next latent failure check. The exposure time for occurrence, or presence, of the latent failure during this flight is the check interval, which is the maximum exposure possible for that latent failure.

response

Comment 1: Please refer to the response to comment #126.

Comment 2: Please refer to the response to comment #210.

3. Proposed amendments - CS-25 - Book 1 - APPENDIX K

p. 15-16

comment

92

comment by: Dassault Aviation

Dassault-Aviation comment; page #16

Extract:

Appendix K - K25.2 (c)

System in the failure condition. For any system failure condition that results from a single failure or is not shown to be extremely improbable, the following apply:

Comment:

If a failure even single is extremely improbable ($<10^{-9}/FH$), it results that the combined probability of this failure with a limit maneuver or gust (of a probability of $10^{-5}/FH$) is far more improbable (less than $10^{-14}/FH$). So Dassault-Aviation do not understand this additional request and ask to suppress it for load computations.

Requested Change:

Rewrite this paragraph as: "System in the failure condition. For any system failure condition not shown to be improbable or that results from a single failure for aeroelastic stability requirements, the following apply: ..."



response	Accepted. The proposal is withdrawn, as single failures that are shown to be extremely improbable ($<10^{-9}/FH$) are not addressed in the graphs included in Appendix K.
comment	168 comment by: AIRBUS PROPOSED TEXT / COMMENT: Airbus note that the changes proposed to the Appendix K in this NPA have not been discussed with the appropriate Structure Regulatory and Industry representatives, more specifically the L&DHWG. Therefore, Airbus strongly recommends to involve the appropriate Industry and Regulatory representatives from the Structure community before expanding appendix K to other systems as the usual ones intended by the current Appendix K. In this respect, Airbus does not choose to make detailed comments to the proposals made in Appendix K, although many comments exist and need to be made on the changes. Airbus proposes to discuss these comments and recommendations in the appropriate context of the above mentioned Industry and Regulatory representatives from the Structure community. RATIONALE / REASON / JUSTIFICATION: Appendix K has been created during a harmonization activity by the ARAC Loads and Dynamics Harmonisation Working Group (L&DHWG) in the 90's. The appendix K method had a specific intent linked to certain dedicated systems that interact actively with structural loads. The appendix K followed several Special Conditions issued on programs with advanced flight control systems. Structure representatives both from Industry and Authorities need to be consulted and review any proposed changes to Appendix K in the correct context. The proposal also leads to a dis-harmonisation with the FAR25 Appendix K, and therefore need to be well evaluated and coordinated with the relevant appropriate Industry and Regulatory representatives from the Structure community before accepting such a dis-harmonisation. Therefore, Airbus proposes to involve the L&DHWG to consider any update to the Appendix K coming from CS25.671 changes.
response	Please refer to the responses to comments #188 and #92.
comment	188 comment by: Embraer - Indústria Brasileira de Aeronáutica - S.A. Appendix K25.1: The ARAC proposal for interaction of system and structure limited the applicability of the proposed appendix to airplanes equipped with flight control systems, autopilots, stability augmentation systems, load alleviation systems, flutter control systems, and fuel management systems, yet this NPA cites these as some examples and then further extends the applicability to conventional systems like hydraulic systems, electrical systems, and mechanical systems. Extending the applicability of this rule to conventional systems is clearly beyond the intended scope of the regulation and adds an unreasonable burden, since failures of these systems are already adequately covered by existing requirements. As proposed the rule would even be applicable to conventional airplanes, not equipped with active flight control systems.
response	Accepted. The proposal is withdrawn. However, please note that AMC 25.671 specifies that for failure conditions per CS 25.671(c)(1)(2), compliance should be shown with CS 25.302, unless otherwise agreed

with EASA.

comment	<p>189</p> <p style="text-align: right;">comment by: <i>Embraer - Indústria Brasileira de Aeronáutica - S.A.</i></p> <p>Appendix K25.2(d)(1) and K25.2(d)(2): The ARAC proposal specified that the system monitoring must check for failure conditions, not extremely improbable, that degrade structural capability, yet the NPA also requires consideration for any single failure. Adding single failure extremely improbable was not justified by events or any foreseen adverse trend in safety. Conditions of appendix K are too severe to be combined to extremely improbable failures. If these failures are to be considered, milder conditions should be adopted, like those used for jamming (continuation of flight or even definition of normally encountered positions) and, according to CS K25.2(c)(3), this fits better under AMC 25.1309(10)(c). In addition, there is currently no safety factor associated to extremely improbable failures.</p>
response	<p>Please refer to the response to comment #92.</p>

comment	<p>212</p> <p style="text-align: right;">comment by: <i>Boeing</i></p> <p>Page:15 Paragraph: <i>APPENDIX K Interactions of Systems and Structure K25.1 -- General</i></p> <p><u>The proposed text states:</u> “... These criteria also apply to hydraulic systems, electrical systems and mechanical systems. ...”</p> <p><u>REQUESTED CHANGE:</u> “... These criteria also apply may also extend to hydraulic systems, electrical systems and mechanical systems to the extent that they are used by the above systems. ...”</p> <p><u>JUSTIFICATION:</u> This appendix does not describe how to address hydraulic, electrical, and mechanical systems, as it is written to address the types previously listed. The text change accommodates this relationship while still addressing the presumed intent of the new text, and avoids the unclear case of how to address such systems directly that are not sufficiently described in the appendix.</p>
response	<p>Please refer to the response to comment #188.</p>

comment	<p>213</p> <p style="text-align: right;">comment by: <i>Boeing</i></p> <p>Page:16 Paragraph: <i>K25.2(c) -- Effects of Systems on Structures.</i></p> <p><u>The proposed text states:</u> “(c) <u>System in the failure condition</u>. For any system failure condition that results from a single failure or is not shown to be extremely improbable, the following apply: ...”</p> <p><u>REQUESTED CHANGE:</u> “(c) <u>System in the failure condition</u>. For any system failure condition that results from a single failure or is not shown to be extremely improbable, the following apply: ...”</p>
---------	--

JUSTIFICATION: With regard to the consideration of single failures in Appendix K, unlike the material for CS 25.671 and CS 25.1309, the proposed alignment of CS 25 Appendix K and CS 25.671 and CS 25.1309 has not been coordinated with the appropriate (government-industry) working groups. The proposed changes are not accompanied by any explanatory material on how to apply the single failure consideration to a rule that is inherently probabilistic in nature. For example, how are the relationships between failure rates and failure probabilities and safety factors to be applied to single failures with probabilities $<1E-9$?

Note that the October 1993 meeting of the Loads and Dynamics Harmonization Working Group included K25.2(c)(3) to address the particular criteria of CS 25.671(c). Airplane level structural loads requirements for single failures with CS 25.671(c) are already well-defined.

While the proposal ostensibly is aimed at reducing variability and confusion in the certification approaches for various system failures, it doesn't seem to achieve that goal. Harmonization and alignment of airplane level safety criteria should be reconsidered in the appropriate working group forums and thoroughly examined, including consistency with existing guidance material and certification practices.

response Please refer to the response to comment #92.

comment 344

comment by: GE Aviation

GE Aviation is concerned that the new expectations on system failures affecting structure will drive introduction of many new and complex monitoring systems, with associated unreliability and complexity, and without a concomittent safety benefit. The level of monitoring demanded by appendix K is far beyond that resulting from the MSG-3 process, and lacks a good connection to the severity of failure consequences.

response Please refer to the response to comment #188.

3. Proposed amendments - CS-25 - Book 2

p. 17

comment 93

comment by: Dassault Aviation

Dassault-Aviation comment page #17

Extract:

AMC 25.629(4.3)(iii)

A qualitative assessment should be conducted in addition to the quantitative assessment. The latent failure criteria of CS 25.1309 (b)(4) and (b)(5) must also be considered. However, Certain combinations of failures, such as dual electric or dual hydraulic system failures (including loss of hydraulic fluid), or any single failure in combination with any probable electric or hydraulic system failure (including loss of hydraulic fluid), are assumed to occur regardless of probability calculations and must be evaluated.

Comment:

The proposed amendment refers to a qualitative assessment. What are the expected requirements associated to it? Also Dassault-Aviation noticed that focus is made on hydraulic fluid loss although it is considered as already part of hydraulic system failure. Is there a specific reason for that?

Requested Change:

No requested change. Information request only.



response	Noted. EASA has reviewed the proposed changes to AMC 25.629 contained in the NPA, and has concluded that changes to the AMC are not needed at this stage, as the current text is deemed to be sufficient.
comment	268 comment by: <i>Transport Canada Standards Branch</i> p.17, AMC 25.629 paragraph 4.3(iii) TCCA questions the rationale for including a qualitative assessment of failures in AMC 25.629: "A qualitative assessment should be conducted in addition to the quantitative assessment." It is unclear what this qualitative assessment refers to.
response	Please refer to the response to comment #93.

3. Proposed amendments - CS-25 - Book 2 - AMC 25.629

p. 17

comment	118 comment by: <i>Garmin International</i> Section 3.2 AMC 25.629 section 4.3 The statement "...any single failure in combination with any probable electric or hydraulic system failure (including loss of hydraulic fluid), are assumed to occur regardless of probability calculations and must be evaluated" was considered by the ASAWG to be the same criterion as that contained in CS 25.671 (c) (2). This statement was interpreted by regulators as a specific risk requirement for CS 25.671 (c) (2) and over the years resulted in multiple different methods of specific risk compliance such as limit latent and residual risk, etc. It was the objective of the ASAWG to propose a consistent methodology for addressing specific risk. The retention of this AMC text and the incorporation of this criterion as rule undermines this objective. It is recommended to remove the quoted AMC 25.629 section 4.3 statement.
response	Please refer to the response to comment #93.
comment	190 comment by: <i>Embraer - Indústria Brasileira de Aeronáutica - S.A.</i> AMC 25.629 - (4)(4.3): As we commented about CS 25.629(d)(10) and its requirement for consideration of specific failure combinations regardless of probability, Embraer recommends that the ASAWG recommendation for consideration of only combinations not shown to be extremely improbable is sufficient. In this AMC, the sentence "Certain combinations of failures, such as dual electric or dual hydraulic system failures (including loss of hydraulic fluid), or any single failure in combination with any probable electric or hydraulic system failure (including loss of hydraulic fluid), are assumed to occur regardless of probability calculations and must be evaluated" should be removed.
response	Please refer to the response to comment #93.
comment	214 comment by: <i>Boeing</i>



Page:17

Paragraph: AMC 25.629 -- Aeroelastic stability requirements

4.3 -- Detail Design Requirements.

Unnumbered paragraph after 4.3.(iii)

The proposed text states:

"The actuation system minimum requirements should also be continuously met after any combination of failures not shown to be extremely improbable (occurrence less than 10^{-9} per flight hour). A qualitative assessment should be conducted in addition to the quantitative assessment. The latent failure criteria of CS 25.1309 (b)(4) and (b)(5) must also be considered. ..."

REQUESTED CHANGE:

"The actuation system minimum requirements should also be continuously met after any combination of failures not shown to be extremely improbable ~~(i.e., any combination not shown to have probability less than than 10^{-9} per flight hour)~~. A qualitative assessment should be conducted in addition to the quantitative assessment. ~~The latent failure criteria of CS 25.1309 (b)(4) and (b)(5) must also be considered.~~ ..."

JUSTIFICATION: Combinations of failures not shown to be extremely improbable have a probability greater than $1E-9$. The definition of extremely improbable in numerical terms is covered elsewhere in AMC and is not needed here. Our suggested strikethrough sentence above is not necessary here as it will be addressed under CS 25.1309 and does not add to the guidance under this AMC. The term "considered" used in this context is vague and does not provide any useful guidance.

response Please refer to the response to comment #93.

comment 215

comment by: Boeing

Page: 17

Paragraph: AMC 25.629 -- Aeroelastic stability requirements

4.3 -- Detail Design Requirements.

Unnumbered paragraph after 4.3.(iii)

The proposed text states:

"... A qualitative assessment should be conducted in addition to the quantitative assessment. ..."

REQUESTED CHANGE: Delete or clarify this sentence.

JUSTIFICATION: It is unclear what is meant by "a qualitative assessment."

response Please refer to the response to comment #93.

comment 216

comment by: Boeing

Page: 17

Paragraph: AMC 25.629 -- Aeroelastic stability requirements

4.3 -- Detail Design Requirements.

Unnumbered paragraph after 4.3.(iii)

The proposed text states:



"... The latent failure criteria of CS 25.1309 (b)(4) and (b)(5) must also be considered. ..."

REQUESTED CHANGE: Delete this sentence.

JUSTIFICATION: This proposed sentence is redundant to the statement in AMC 25.629 4.3.(iii), "...any damage or failure conditions considered under CS 25.571, CS 25.631, and CS 25.671, and CS 25.1309." The emphasis on CS 25.1309(b)(4) and CS 25.1309(b)(5) is either redundant or unclear.

response Please refer to the response to comment #93.

comment 324 comment by: Gulfstream Aerospace Corporation

AMC 25.629 (4.3)(iii)

"any damage or failure conditions considered under CS 25.571, CS 25.631, ~~and CS 25.671, and CS 25.1309.~~"

- GAC Response:

As written, the system is required to provide minimum stiffness or damping without regard to probability for all CS 25.1309 conditions, including those that are Catastrophic and extremely improbable.

Since any additional feature added to the system will also be subject to failure, and thus considered under CS 25.1309, this requirement is impossible to meet.

Recommended:

Delete highlighted text from (iii) and add:

"(iv) any failure conditions considered under CS 25.1309 that are not shown to be extremely improbable."

response Please refer to the response to comment #93.

comment 325 comment by: Gulfstream Aerospace Corporation

AMC 25.629 (4.3)(iii)

"The actuation system minimum requirements should also be continuously met after any combination of failures not shown to be extremely improbable (occurrence less than 10⁻⁹ per flight hour)."

- GAC Response:

Redundant with the Gulfstream proposed 4.3(iv). Recommend deletion.

response Please refer to the response to comment #93.

comment 326 comment by: Gulfstream Aerospace Corporation

AMC 25.629 (4.3)(iii)

A qualitative assessment should be conducted in addition to the quantitative assessment. The latent failure criteria of CS 25.1309 (b)(4) and (b)(5) must also be considered.

- GAC Response:

It is not clear what the application of a "qualitative assessment" can add to compliance with this rule, nor how CS 25.1309(b)(4)(5) have any bearing whatsoever on the issue. All the latent conditions covered by those requirements are already addressed by the "single failure" and "not extremely improbable failure" provisions of this rule. Recommend deletion.

response Please refer to the response to comment #93.



comment	327	comment by: Gulfstream Aerospace Corporation
	<p>AMC 25.629 (4.3)(iii) <i>"...probable electric or hydraulic system failure (including loss of hydraulic fluid), are assumed to occur regardless of probability calculations and must be evaluated.(CS 25.671), are not normally considered extremely improbable regardless of probability calculations. The reliability... "</i></p> <ul style="list-style-type: none"> GAC Response: Dual failures such as the ones mentioned here are not assumed to occur regardless of probability in complying with any other regulations. Since this is not a general practice, this text should be reworded accordingly. <p>Recommended: <i>"When complying with CS 25.629, the conditions described in (d)(10) should be assumed to occur regardless of probability."</i></p>	
response	Please refer to the response to comment #93.	

3. Proposed amendments - CS-25 - Book 2 - AMC 25.671(c)(1)

p. 18

comment	82	comment by: FAA
	<p>The proposed CS 25.671(c)(2) differs from ASAWG's recommendation. The ASAWG was tasked to recommend "specific risk" criteria that would harmonize the various proposals from the FCHWG, PPIHWG, and SDAHWG. We are concerned that the proposed CS 25.671(c)(2) would set a higher safety standard than for other systems, including propulsion system.</p> <p>Unless there is more background and rationale on the proposed changes in general we believe that there should be one level of safety for flight controls, systems and propulsion installations. Please provide the reasons for why the latent failure criteria for the flight control systems should be at a higher standard than for other systems and propulsion installations, or we propose that the standard developed in the ASAWG be used.</p>	
response	<p>Noted.</p> <p>System architectures could be developed with a high number of failures leading to the same consequence. Using the CS 25.1309(b) criteria will not lead to latency times with adequate check intervals.</p>	

3. Proposed amendments - CS-25 - Book 2 - AMC 25.671

p. 18-32

comment	47	comment by: UK CAA
	<p>Page No: 22 Paragraph No: 9 Evaluation of... - CS 25.671(c) Comment: 4th paragraph is ambiguous and requires revision. Justification: This states that "CS 25.671(c)(2) requires the evaluation of any combination of failures not shown to be extremely improbable, excluding the types of jams..." which is inaccurate as they should positively be shown to be extremely improbable Proposed Text: Change sentence to "to CS 25.671(c)(2) requires the evaluation of any</p>	



	<p>combination of failures to show that they are extremely improbable, excluding the types of jams...”</p>
response	<p>Not accepted. This is not correct. The purpose is to show continued safe flight and landing under these failure conditions. There is a secondary task to show that other combinations of failures are extremely improbable.</p>
comment	<p>48 comment by: UK CAA</p> <p>Page No: 24 Paragraph No: (b) related to determination of control system jam positions - CS 25.671(c)(3) 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. 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. Proposed Text: “crosswind values for landing should not be limited to 15kts but should be as defined for the aircraft limitations.”</p>
response	<p>Not accepted. It is agreed that the evolution of the likelihood is not the same during approach and landing compared to take-off. The probability of jamming is in the order of magnitude $1.10^{-6}/1.10^{-7}$. Considering the short time at risk, and the rate of encounter of crosswinds with speeds beyond 15 kt, leads us to conclude that 15 kt is a reasonable value. For instance, the rate of encounter of crosswinds of 18 kt is 1 every 100 flights.</p>
comment	<p>94 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment page #18 Extract: AMC 25.671(3) The following guidance and advisory materials are referenced herein: (...) Comment: AC 25-7B was cancelled by AC 25-7C (released on October 2012). If DO-178 is referenced, maybe DO-254 and DO-200 should be too. Requested Change: Update related documents as suggested.</p>
response	<p>Partially accepted. Agreed for AC 25-7C. DO-254 and DO-200 are not referenced in the AMC, so they do not need to appear in the list</p>

of standards.

comment	95	comment by: Dassault Aviation
	Dassault-Aviation comment page #19	
	Extract:	
	AMC 25.671(4)	
	Some parts of CS 25.671 (and the associated AMC) also apply to all control systems.	
	Comment:	
	Relevant parts of CS 25.671 (and the associated AMC) that apply to all control systems may be not identified if their applicability is not suitably highlighted.	
	Requested Change:	
	To avoid any omission, Dassault-Aviation suggest to identify explicitly the relevant parts that apply to all control systems (in addition of the use of “control systems” versus “flight control systems”).	
response	Accepted.	

comment	96	comment by: Dassault Aviation
	Dassault-Aviation comment page #19	
	Extract:	
	AMC 25.671(5)(c)	
	c. <i>Continued Safe Flight and Landing</i> . The capability for continued controlled flight and landing at an airport without requiring exceptional pilot skill or strength.	
	Comment:	
	A definition of “Continued Safe Flight and Landing” is already provided by AMC 25.933(a)(1): “ Continued Safe Flight and Landing : The capability for continued controlled flight and safe landing at an airport, possibly using emergency procedures, but without requiring exceptional pilot skill or strength. Some aeroplane damage may be associated with a failure condition, during flight or upon landing.”	
	Requested Change:	
	Dassault-Aviation suggest to use the same definition as given by AMC 25.933(a)(1). Reference to this AMC may be done so as to prevent from repetitions.	
response	Not accepted. The proposed definition comes from the ARAC working group, and EASA sees no reason to change it. AMC 25.671 provides more guidance on the definition of continued safe flight and landing.	

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: §3.1 C25.671(d) §3.2 AMC25.671 section 5

Comment: The definition of a “suitable runway” should be established in AMC25.671. It should be noted that with loss of all engines, and thus thrust reversers, the landing distance can be expected to be increased.

Suggested change: Add a definition to AMC25.671:

Suitable runway - a runway with the lateral dimensions, length and load bearing capability which meets the requirements defined in the Emergency procedures of the Airplane Flight Manual.



EASA response: Accepted.

However, please note that the assumption of availability of a 'suitable runway' intends only to clarify that continuation of flight to the destination or diversion runway is not required with all engines failed.

comment	<p>97</p> <p>Dassault-Aviation comment page #19</p> <p>Extract: AMC 25.671(5)(f) f. <i>Latency Period</i>. The duration between actions necessary to check for the existence of a failure – the action may be a pre-flight flight crew check, periodic maintenance check, or periodic maintenance inspection (including component overhaul). See also “Exposure Time”.</p> <p>Comment: This definition (not supported by the ARAC results) is not representative of all practical cases. Indeed, when calculating a fault tree, a latent failure may potentially be associated to an exposure time equivalent to the airplane life duration. In such cases, latency period is not defined as an interval delimited by check actions and thus proposed definition is not applicable. According ARP4761, a latency period may be defined as being a “time interval defined as the time between when an item was last known to be operating properly and when it will be known to be operating properly again. Proper operation may be verified during acceptance tests, maintenance checks, monitor cycle times, power-up tests, etc.”.</p> <p>Requested Change: Remove this definition or revise it in accordance with ARP4761.</p>	comment by: <i>Dassault Aviation</i>
response	Accepted. This definition has been removed.	
comment	<p>98</p> <p>Dassault-Aviation comment page #20</p> <p>Extract: AMC 25.671(5)(f) l. <i>Failure States</i>. As used in CS 25.671(c), this item refers to the sum of all failures and failure combinations contributing to a hazard, apart from the single failure (flight control system jam) being considered.</p> <p>Comment: This definition may involve an excessive effort in demonstration because the amount of failures and failure combinations may be in some cases very important. Thus, in numerical terms, sorting them so as to be able to consider their cumulative probabilities and assess the whole residual risk due to a given jam may become a very expensive task with a non-negligible economic impact on studies.</p> <p>Requested Change: Dassault-Aviation suggests the revision of this definition and of the relevant AMC on the basis of a minimal cutset by minimal cutset analysis for each failure condition considered individually.</p>	comment by: <i>Dassault Aviation</i>
response	Not accepted.	

The sum of ALL failure states must achieve 1/1000. It is not only to be considered for each minimal cutset.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.671 Section 5k5

Comment: NPA AMC 25.671 Section 5k5 breaks runaways and handovers into two different types. The 1st paragraph talks about failures internal to the airplane, and states that they are handled addressed under CS 25.671(c) (1) and (c) (2). The 2nd paragraph talks about external events which may cause a runway and that they are dealt with under CS 25.671(c) (4).

How a runaway/hardcover happens should not be cause to treat them under different paragraphs. Whether caused internally or externally, the end effect on the airplane is the same. Hence they should be handled under the same regulation. Splitting runaways/handovers into two different classes adds unnecessarily complications and adds needless work to the OEM and certification authorities.

FCHWG's proposed FAR 25.671(c)(4), proposed AC 25.671 Section 5k5, and proposed AC 25.671 Section 9d treated all runaways/handovers, whether internal or external, the same.

Suggested change: Propose eliminating the two classes (internal/external) of runaways from the NPA and treat all runaways/handovers the same.

Propose deleting "...that is caused by an external source" from CS 25.671(c) (4).

Propose changing "...under CS 25.671(c) (1) and (c) (2)" in AMC 25.671 Section 5k5's 1st paragraph to "under CS 25.671(c) (4)."

Propose deleting the 2nd paragraph of AMC 25.671 Section 5k5.

Propose adding FCHWG's AC 25.671 Section 9d titled "Runaway to an Adverse Position – FAR/JAR 25.671(c) (4)."

EASA response: Not accepted.

It is agreed that the end effect may be the same. However, it is quite usual to treat the internal and external causes differently.

comment 99

comment by: Dassault Aviation

Dassault-Aviation comment pages #20 and #21

Extract:

AMC 25.671(5)(m)

m. Flight Control System. (...) Examples of elements to be evaluated under CS 25.671 include (but are not limited to): (...).

Comment:

Dassault-Aviation think that, among the examples given, some are not to be considered as system part (even if belonging to the system function) but as structure elements. It is the case of control surfaces, attachment fittings and movable tracks. Such structure elements are submitted to structure requirements as Damage Tolerance under CS 25.571(b). Inspections are put in place to avoid their complete failure and even if cracks occur they remain below their critical length, they are detected before complete failure and the element is repaired or replaced. So it is the opinion of DA that primary structural elements followed in service have not to be submitted to the 25.671 single failure requirement, except pins or axles to cover



	<p>any mistake in mounting during aeroplane life.</p> <p>Requested Change:</p> <p>Dassault-Aviation suggest to revise the list of examples and to add an explanatory nota as proposed below:</p> <p>m. Flight Control System. (...) Examples of elements to be evaluated under CS 25.671 include (but are not limited to):</p> <ul style="list-style-type: none"> - Linkages - Cables - Pulleys - Quadrants - Valves - Actuators (including actuator components) - Track rollers and movable tracks - Bearings / Axles and Pins <p>NOTA: Those elements correspond to elements that may be removed in service within the scope of maintenance actions. They are not covered by 25.571(b) or could be mounted not correctly.</p>
response	<p>Partially accepted.</p> <p>The list of examples which constitute elements of a flight control system was reviewed extensively and has been updated. Please note that these are examples and are not intended to be definitive.</p>
comment	<p>100 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment page #21</p> <p>Extract:</p> <p>AMC 25.671(5)(n)</p> <p>n. <i>Probability vs. Failure Rate.</i> Failure rate is typically expressed in terms of average probability of occurrence per flight hour. In cases where the failure condition is associated with (...).</p> <p>Comment:</p> <p>AMC 25.671 does not seem to be the most appropriated location to host such a definition which may have a large application out of 25.671.</p> <p>Requested Change:</p> <p>This definition is considered as ARP4761 scope. Dassault-Aviation suggests its removing from AMC 25.671.</p>
response	<p>Not accepted.</p> <p>This definition is considered to be useful within AMC 25.671.</p>
comment	<p>101 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment page #22</p> <p>Extract:</p> <p>AMC 25.671(8)(b)</p> <p>The applicant should:</p> <p>(i) Analyze the assembly and maintenance of the system to assess the classification of potential failures.</p> <p>(ii) For Cat/Haz/Maj failures: Introduce Physical Prevention against mis-assembly or discuss with the Authority if Physical Prevention is not possible.</p>

(iii) For Minor Failure or No Safety Effect: Marking alone is generally considered sufficient to prevent incorrect assembly

Comment:

The term “failure” usually refers to a system malfunctioning whereas this AMC deals with the effects of an incorrect installation, connection or adjustment of parts of the control system. Dassault-Aviation suggest to replace “failures” by “incorrect assembly effects” which is consistent with (iii).

The abbreviations Cat/Haz/Maj are not defined in CS 25 (and the associated AMC).

According Dassault-Aviation, demonstrating that marking alone is only associated to parts of the control system whose incorrect assembly cannot have consequences worst than minor is an acceptable means of compliance towards 25.671(b). According this logic, paragraphs (ii) and (iii) may be inverted.

Requested Change:

Dassault-Aviation suggest the following wording instead of the proposed amendment:

“The applicant should:

(i) Analyze the assembly and maintenance of the system to assess the severity of potential incorrect assembly effects.

(ii) For parts of control system whose potential incorrect assembly cannot have effects worst than Major: Marking alone is generally considered sufficient to prevent incorrect assembly

For other parts (whose incorrect assembly may have effects worst than Major): Introduce Physical Prevention against mis-assembly or discuss with the Authority if Physical Prevention is not possible.”

response Accepted.

comment 102

comment by: Dassault Aviation

Dassault-Aviation comment page #23

Extract:

AMC 25.671(9)

a. Compliance with CS 25.671(c)(2).

(...)

b. Determination of Control System Jam Positions – CS 25.671(c)(3).

(...)

Comment:

No dedicated paragraph is provided for 25.671(c)(1). Dassault-Aviation wonder if it is an omission?

Requested Change:

Dassault-Aviation suggest to address 25.671(c)(1) through a dedicated paragraph.

response Not accepted.

It has been considered that CS 25.671(c)(1) is self-explanatory, especially as continued safe flight and landing is already defined elsewhere.

comment 103

comment by: Dassault Aviation

Dassault-Aviation comment pages #23 and #24

Extract:

AMC 25.671(9)(a)

The following failure combinations should be assumed to occur and should be addressed, within the scope of CS 25.629:



(1) Any dual power system failure (e.g. hydraulic, electrical)
 (2) Any single failure in combination with any probable failure.
 (3) Any single failure in combination with any power system failure.
 The aeroelastic stability (flutter) requirements of CS 25.629 should also be considered.

Comment:

This extract is essentially CS 25.629 oriented. If confirmed, it should be preferentially included in AMC 25.629. Also Dassault-Aviation thinks that only foreseeable (e.g. not shown to be extremely improbable) dual power system failures need to be addressed. Finally the item (3) is not consistent with CS 25.629(d) which refers to “Any single failure in combination with any probable hydraulic or electrical failure”. Especially the term ‘probable’ is missing in this AMC. See also comment on CS 25.629(d).

Requested Change:

Some clarification is requested on this extract. Inconsistency should be corrected too.

response

Accepted.

The list of failure combinations has been deleted. Only the reference to the CS 25.629 aeroelastic stability requirements has been maintained.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.671 Section 9a

Comment: NPA AMC 25.671 Section 9a 3rd paragraph indicates that “single probable” remains, as it states “...following should be assumed to occur and be addressed within the scope of CS 25.629: any dual power system failure, any single failure in combination with any probable failure, any single failure in combination with any power system failure.” However, with the words “within the scope of CS 25.629.”, does this mean that those “single probable” combinations only need to be shown flutter-free under 25.629, but need not be held to the CSFL standard of 25.671?

Suggested change: Propose clarification be provided that those “single probable” combinations only need to be shown flutter-free under 25.629, but need not be held to the CSFL standard of 25.671?

EASA response: Partially accepted.

The list of failure combinations has been deleted. Only the reference to the CS 25.629 aeroelastic stability requirements has been maintained.

comment

104

comment by: Dassault Aviation

Dassault-Aviation comment pages #23 to #27

Extract:**AMC 25.671(9)**

(b)(1)(iii) Flare/landing: (...).

(b)(2)(iii) Flare/landing: (...).

(c) Considerations for jams just before landing – CS 25.671(c)(3)(i)/(ii)

Comment:

The addition of these paragraphs is not consistent with the results of ARAC FCHWG. Indeed, it was concluded that jams that occur just prior to landing have not to be addressed by 25.671(c)(3). The rationale for such a position is reminded below (issued from ARAC FCHWG report).

“25.671(c)(3) requires that the airplane be capable of landing with a flight control jam and that the airplane be evaluated for jams in the landing configuration. However, for the



evaluation of jams which occur just prior to landing, proximity to the ground need not be considered for the transient condition. Given that some amount of time and altitude is necessary in order to recover from any significant flight control jam, there is no practical means by which such a recovery could be demonstrated all the way to touchdown. The potential delay in accomplishing a recovery could be on the order of 5 seconds as described in section 9.e. For a jam at a control deflection corresponding to .8g, a recovery may not be possible below approximately 200' even with a state of the art control system. While it is recognized that this means that a specific hazard is not addressed (a control jam that occurs, or is recognized, just before landing), this hazard is mitigated for the following reasons. First, the landing phase represents a limited exposure window in which a jam could occur. Second, successful operation of the controls throughout the flight minimizes the likelihood of a jam suddenly appearing during the landing phase. Third, a certain level of recovery capability will be ensured through compliance with this AC such that if a jam does occur during landing, the crew will have a reasonable chance of landing safely."

Especially Dassault-Aviation do not understand why this AMC states that "The use of a risk time for this analysis is not accepted" whereas ARAC FCHWG concludes that the limited exposure window is an acceptable mitigation factor when considering jams that occur just prior landing.

Requested Change:

Dassault-Aviation do not concur with the several paragraphs dealing with jams occurring prior to landing and ask to suppress them. The report of ARAC FCHWG provides the rationale to support this position.

Taking credit from the limited exposure time should be accepted to show that jams that occur just prior landing are extremely improbable.

response

Not accepted.

Jams can result from single events and it is not usual to consider a probability approach.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.671 Section 9b 6th paragraph, AMC 25.671 Section 9b1iii

Comment: NPA AMC 25.671 Section 9b1iii (and the 6th paragraph of Section 9b) adds consideration for jammed lateral control during the landing flare during a 15knot crosswind, but states that it's to maintain wings level. Pilot's using a "kick out" crosswind landing technique may not even input much, if any, of a lateral control input as the wings are generally level in the crabbed approach anyway. A pilot using the "wing-low" crosswind technique would not be maintaining wings-level as that would cause the airplane to drift across the runway. Hence, the proposed criteria is pilot-technique dependent (at best). Furthermore, the deflection will be based on the airspeed (i.e., as airspeed decreases, deflection would need to increase). Compared with the other, objective/performance-based criteria of the AMC, this particular criterion is open-ended, vague, and subject to pilot technique, which will lead to differing interpretations by OEMs and certification authorities.

(Compare the proposed criteria to Section 9b1i, which also is the deflection for wings-level in a cross-wind, but specifies a speed of V1. In that case, the stated airspeed eliminates the variation of deflection with different airspeeds. Furthermore, at V1 the aircraft is still on the ground, hence pilot technique is not as relevant as the landing flare.)

Suggested change: Propose removing AMC 25.671 Section 9b1iii.

EASA response: Not accepted.

The piloting technique is separate from the criteria used to define the sizing case.



Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.671 Section 9b2iii

Comment: NPA AMC 25.671 Section 9b2iii adds consideration for jammed longitudinal control during the landing flare, without providing guidance for pilot technique. (Compare this to Section 9b2i, where an objective pitch rate is provided, these minimizing differences due to pilot technique.) Pilot's using an aggressive flare for minimal sink rate will have a significantly different longitudinal control position than one performing a minimal flare with subsequent firmer touchdown. Compared with the other, objective/performance-based criteria of the AMC, this particular criteria is open-ended, vague, and subject to pilot technique, which will lead to differing interpretations by OEMs and certification authorities

Suggested change: Propose removing AMC 25.671 Section 9b2iii.

EASA response: Not accepted.

The standard is based on the procedure recommended by the manufacturers in order to remove the pilot technique variability from the discussion.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.671 Section 9b3iii

Comment: NPA AMC 25.671 Section 9b3iii adds consideration for jammed directional control during the landing flare during a 15knot crosswind, yet does not give allowance nor guidance on how the landing is to be conducted, which will result in the surface deflection being highly pilot-technique dependent. Pilot's using the "wing-low" crosswind technique may have a significantly different directional control position than a pilot using a "kick out" crosswind landing technique. (Furthermore, the deflection will be dependent on airspeed: slower airspeed, until NWS becomes effective, would result in larger deflections once on the ground.) Compared with the other, objective/performance-based criteria of the AMC, this particular criterion is open-ended, vague, and subject to pilot technique, which will lead to differing interpretations by OEMs and certification authorities.

Suggested change: Propose removing AMC 25.671 Section 9b3iii.

EASA response: Not accepted.

The piloting technique is separate from the criteria used to define the sizing case.

comment 105

comment by: Dassault Aviation

Dassault-Aviation comment page #25

Extract:**AMC 25.671(9)(b)(2)(i)**

Take-off: Three longitudinal flight control positions should be considered:

(A) Any flight control position from that which (...)

(B) Note: (...)

(C) The longitudinal flight control position (...).

(D) Using the manufacturer's recommended procedures, (...).

Comment:

Only a minor remark on form. This paragraph states that "Three longitudinal flight control positions should be considered" and it is subdivided into 4 subparts. Subparts (A) and (B) may be merged as they are linked one to the other and deal with the same topic.

Requested Change:

	Dassault-Aviation suggest to revise the subpart numbering into (A) to (C).
response	Accepted.

comment	106		comment by: <i>Dassault Aviation</i>
		<p>Dassault-Aviation comment page #27</p> <p>Extract:</p> <p>AMC 25.671(9)(d)</p> <p>In addition to demonstration of jams at “normally encountered position”, compliance with CS 25.671(c)(3) should include an analysis that shows that a minimum level of safety exists should the jam occur. This additional analysis should show that in the presence of a jam considered under CS 25.671(c)(3), the failure states that could prevent continued safe flight and landing must have a combined probability of less than 1/1000.</p> <p>Comment:</p> <p>No interpretation of CS 25.671(c)(3)(iii) is provided in this paragraph. It provides only a reminder of the requirement.</p> <p>Requested Change:</p> <p>Dassault-Aviation suggest to suppress this paragraph which is not helpful for the CS 25.671 interpretation.</p>	
response		<p>Not accepted.</p> <p>The text provides some additional guidance about why a minimum level of safety is requested as well as considering the jam itself.</p>	

comment	107		comment by: <i>Dassault Aviation</i>								
		<p>Dassault-Aviation comment page #28</p> <p>Extract:</p> <p>AMC 25.671(9)(e)(1)(iii)</p> <p>The following reaction times should be used:</p> <div style="border: 1px solid black; width: 100px; height: 50px; margin: 5px 0;"></div> <p>Comment:</p> <p>The pilot reaction time is considered to be dependent upon the pilot attentiveness based upon the phase of flight and associated duties. Especially:</p> <ul style="list-style-type: none"> · AMC 25.1329 (§ 14.2.1.3) states that “For the final phase and landing (e.g. below 25 m (80 ft)), the pilot can be assumed to react upon recognition without delay”. · AMC 25.101(h)(3) specifies a 2 second time reaction if a command to another crew member to take the action is required on ground. <p>Requested Change:</p> <p>Dassault-Aviation suggests the following reaction time revision based upon AMC 25.1329 and 25.101:</p>									
		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Flight Condition</th> <th style="text-align: center;">Reaction Time</th> </tr> </thead> <tbody> <tr> <td>On ground</td> <td>1 second*</td> </tr> <tr> <td>Final Phase and Landing (< 80 feet AGL)</td> <td>Immediate</td> </tr> <tr> <td>In air (< 1,000 feet AGL)</td> <td>1 second**</td> </tr> </tbody> </table>	Flight Condition	Reaction Time	On ground	1 second*	Final Phase and Landing (< 80 feet AGL)	Immediate	In air (< 1,000 feet AGL)	1 second**	
Flight Condition	Reaction Time										
On ground	1 second*										
Final Phase and Landing (< 80 feet AGL)	Immediate										
In air (< 1,000 feet AGL)	1 second**										

Manual flight (> 1,000 feet AGL)	1 second**
Automatic flight (> 1,000 feet AGL)	3 seconds
* 2 seconds / ** 3 seconds if control must be transferred between pilots.	

response

Not accepted.

The NPA proposed 'reaction times' table originates from the ARAC WG and is well-established.

The change proposed in this comment for the 'final phase and landing' comes from an AMC chapter dealing with failure conditions of the flight guidance system, such as an autopilot. The time needed to react to an autopilot disconnection may probably be considered to be lower than the reaction times expected following failure conditions considered within CS 25.671.

Furthermore, the proposed 'immediate' case does not consider the time needed to transfer the control to the other pilot.

comment

108

comment by: Dassault Aviation

Dassault-Aviation comment page #29

Extract:**AMC 25.671(9)(e)(1)(iv)**

If, using the manufacturer's recommended procedures, the following manoeuvres can be performed following the failure, it will generally be considered that continued safe flight and landing has been shown.

(A) A steady 30° banked turn to the left or right;

(B) A roll from a steady 30° bank turn through an angle of 60° (...)

(C) A push-over manoeuvre to 0.8 g, and a pull-up manoeuvre to 1.3 g;

(D) A wings level landing flare in a 90° crosswind of up to 10 knots (...)

(E) The aircraft remains on the paved runway surface during the landing roll (...)

Comment:

Meeting all these criteria ensures that the continued flight and landing is shown. However if one of them is not met, Dassault-Aviation underlines that it will not systematically mean that the continued safe flight and landing is compromised. For example, if a runway excursion occurs, criterion (E) is not met, but it does not mean that the continued safe flight and landing is compromised in any cases. To avoid any misinterpretation, Dassault-Aviation suggests adding a note stating this below the given list.

Requested Change:

Below the given list of criteria, Dassault-Aviation suggests to add this note: "If all these criteria are not met, the continued safe flight and landing may be shown on a case-by-case basis."

response

Partially accepted.

As with any AMC, applicants may consider alternative means of compliance and make proposals to EASA. It is not required to specifically state this here.

Please note that some authorities consider runway excursion to be 'catastrophic'.

comment

109

comment by: Dassault Aviation



	<p>Dassault-Aviation comment page #29</p> <p>Extract: AMC 25.671(9)(e)(2)(ii) Local structural failure (e.g. via a mechanical fuse or shear out) that could lead to a surface departure from the aircraft should not be used as a means of jam alleviation.</p> <p>Comment: The term “surface departure” is not well understood. Can some explanations be provided to Dassault-Aviation. Does it refer to jettisonable surfaces?</p> <p>Requested Change: No requested change. Information request only.</p>
response	<p>Noted.</p> <p>Surface departure means parts departing the aircraft as a result of failure and not of design or intent.</p>

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.671 Section 9e2ii 4th paragraph

Comment: NPA AMC 25.671 Section 9e2ii 4th paragraph states “Local structural failure (e.g., via mechanical fuse or shear out) that could lead to a surface departure from the aircraft should not be used as a means of jam alleviation.” While in principle this seems a reasonable addition, it seems buried in the text as it is under a section covering “structural strength for flight control system failures.” A better place for such language would be where the jams, procedures following a jam, and controllability following a jam is discussed (earlier in Section 9).

Suggested change: Propose moving to earlier in Section 9 where jams, procedures following a jam, and controllability following a jam is discussed (i.e., not buried in a section dealing with structural strength).

EASA response: Accepted.

comment	<p>110</p> <p style="text-align: right;">comment by: <i>Dassault Aviation</i></p> <p>Dassault-Aviation comment page #30</p> <p>Extract: AMC 25.671(9)(e)(2)(iii)(B) (B) Vertical and lateral discrete gusts corresponding to 40% of the limit gust velocity specified at V_c in CS 25.341(a) with high-lift devices fully retracted, and a 17 fps vertical and 17 fps head-on gust with high-lift devices extended.</p> <p>Comment: Vertical and lateral gust conditions are assumed as separate conditions.</p> <p>Requested Change: Dassault-Aviation propose to precise that vertical and lateral gust conditions are separate conditions: (B) Vertical and lateral discrete gusts corresponding (...), vertical and lateral gust being considered as separate conditions.</p>
response	<p>Accepted.</p>
comment	<p>111</p> <p style="text-align: right;">comment by: <i>Dassault Aviation</i></p> <p>Dassault-Aviation comment page #30</p>

Extract:**AMC 25.671(9)(e)(2)(iii)(B)**

A flexible aircraft model should be used for load calculations.

Comment:

According Dassault-Aviation, the use of a flexible aircraft model for load calculations is part of the current state of the art. No interest is seen to precise it here. The normal way of calculating the loads shall be used. Moreover rigid aircraft model leads generally to conservative loads.

Requested Change:

Dassault-Aviation suggest to suppress this sentence or to modify it as follows:

“The load computation methodology should be the one used for corresponding normal load cases or a conservative approach instead.”

response

Partially accepted.

A sentence has been added to the effect that a flexible aircraft model should be used where the use of a flexible aircraft model is significant to the loads being assessed.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.671 Section 9e2iii

Comment: NPA AMC 25.671 Section 9e2iii adds “a flexible aircraft model should be used for loads calculations.” Depending on the aircraft, fully-flexible loads models may not always be used, on all axes. Some OEMs may use a flexible model on some axes (pitch and roll) where aeroelastic effects may be more pronounced, but rigid models on other axes (yaw) where aeroelastics are not significant. Requiring a flexible loads model on all axes would increase the analysis burden on the OEM, likely with no increase in loads fidelity or safety.

Suggested change: Propose removing the sentence “A flexible aircraft model should be used for loads calculations.”

EASA response: Partially accepted.

A sentence has been added to the effect that a flexible aircraft model should be used where the use of a flexible aircraft model is significant to the loads being assessed.

comment

112

comment by: *Dassault Aviation*

Dassault-Aviation comment page #31

Extract:**AMC 25.671(11)(a)**

a. CS 25.671(e) requires suitable annunciation to be provided to the flight crew when a flight condition exists in which near-full flight control authority (whether or not it is pilot-commanded) is being used. Suitability of such an annunciation (...)

Comment:

Annunciating that primary control means is approaching the limit of control authority is only profitable when it requires a specific crew action. The other cases requiring no specific crew action should be out of the scope of this requirement, particularly when approaching the limit of control authority is a normal response consecutive to a commanded crew action. This is consistent with the CRI B-02 released in the scope of F7X and F5X and with the ARAC FCHWG report.

Requested Change:

	In accordance with the ARAC FCHWG results, Dassault-Aviation suggest to revise this paragraph so that it deals only with not pilot-commanded cases: CS 25.671(e) requires suitable annunciation to be provided to the flight crew when a flight condition exists in which near-full flight control authority (not pilot-commanded) is being used. Suitability of such an annunciation (...)
response	Not accepted. Occurrences are known where the pilot commanded at the limit of authority without being aware of this situation.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.671 Section 11a

Comment: NPA AMC 25.671 Section 11a adds “whether or not it is pilot-commanded.” FCHWG was “not pilot-commanded.” NPA language would require near-full-authority annunciation even in cases when it was pilot-commanded. Wouldn’t an annunciation of near-full-authority, while the pilot is commanding that authority, be distracting?

Suggested change: Propose replacing “whether or not it is pilot-commanded” with “not pilot-commanded” per the FCHWG draft AC.

EASA response: Not accepted.

There is already guidance on avoiding nuisance warnings in the same part of the AMC.

comment	113	comment by: <i>Dassault Aviation</i>
	Dassault-Aviation comment page #32	
	Extract:	
	AMC 25.671(13)	
	(...). Simulation methods should include an accurate representation of the aircraft characteristics and of the pilot response, including time delays as specified in Section 9.e.1.(iii).	
	Comment:	
	Only a minor remark on wording. The term “accurate” may be difficult quantifiable. The intent of this sentence is to remind that simulation methods should be representative of the expected A/C behavior so as to ensure an acceptable level of confidence in the value obtained.	
	Requested Change:	
	Dassault-Aviation suggests to replace “accurate” by “reliable”.	
response	Partially accepted. The principle of the comment is accepted, and is also applicable when using the term ‘reliable’. The term ‘accurate’ is considered to be appropriate.	
comment	114	comment by: <i>Dassault Aviation</i>
	Dassault-Aviation comment page #32	
	Extract:	
	AMC 25.671(13)(a)(2)	
	Simulation may be an acceptable alternative to flight demonstrations, especially when: (...)	



	<p>Comment: According Dassault-Aviation, simulation may also be an acceptable alternative to flight demonstrations for failure conditions whose probability is shown as extremely remote.</p> <p>Requested Change: Among cases where simulation may be an acceptable alternative to flight demonstrations, Dassault-Aviation suggests the consideration of the following additional item: “(v) The simulation is used to evaluate failure conditions whose probability is shown as extremely remote.”</p>
response	<p>Not accepted.</p> <p>The acceptability is based on considerations related to the severity of the failure case (from the Functional Hazard Assessment (FHA) process), not on the probability.</p>
comment	<p>128 comment by: <i>Garmin International</i></p> <p>AMC 25.671, Section 9.a The phrase “within the scope of CS 25.629” includes an incorrect reference to “CS 25.629” because the title of AMC 25.671 Section 9.a is “Compliance with CS 25.671(c)(2)”.</p>
response	<p>Partially accepted.</p> <p>It was correctly intended to refer to CS 25.629. The list of failure combinations, being inconsistent with CS 25.629(d), has been deleted. Only the reference to the CS 25.629 aeroelastic stability requirements has been maintained.</p>
comment	<p>129 comment by: <i>Garmin International</i></p> <p>AMC 25.671, Section 9.a, items (2) and (3) The assumption that these failure conditions should be assumed to exist is not consistent with the preceding paragraph that states “To satisfy these requirements, a safety analysis/assessment according to the techniques of AMC 25.1309 should be used.” These criteria assume dual detectable failure combinations that are extremely improbable (less than 1E-9) have to be assumed to exist. For example, item (2) assumes any single engine failure (probable failure of the order 2E-5) in combination with any single mechanical failure (probability in the order of 10-6 to 10-7) has to be assumed to exist even though such a combination would typically be considered Extremely Improbable. The inclusion of this AMC material is in conflict with proposed CS 25.672 (c) (2) (i) shown on page 13. Using AMC 25.671 section 9.a item (1) as an example, the dual detectable failures of concern seem to be any single probable failure in combination with any other single probable failure. This would include combinations such as dual generator failure, dual hydraulic failure, and dual engine failure. Loss of all thrust is addressed by proposed CS 25.671 (d). In addition it would include any single latent failure in combination with any single probable failure. This is addressed by CS 25.1309 (b) (5) specific risk criteria and the related AMC 25.1309 guidance. It is recommended that proposed AMC 25.671, section 9.a, items (2) and (3) be deleted.</p>
response	<p>Not accepted.</p> <p>The guidance in items 2 and 3 is additional to the probability assessment and is more a qualitative view of the aircraft architecture.</p>
comment	<p>130 comment by: <i>Garmin International</i></p> <p>AMC 25.671, Section 9.c</p>

	<p>This paragraph provides guidance for CS 25.671 (c) (3) (i)/(ii) jam close to the ground where the time necessary for the transfer of control might not be sufficient. Why is there no similar guidance for a disconnect that prevents the pilot-in-command from inputting a command? Would this not also warrant a transfer of control close to the ground?</p> <p>If an analysis that this failure is Extremely Improbable is acceptable, this may require that the CS 25.1309 rule retain the exception provided to CFR 25.671 (c) (1) when addressing single failures.</p> <p>It is recommended that this AMC discuss control input disconnects and whether probability is an acceptable method of addressing these types of failure. This may include addressing single failures and result in retaining the current CS 25.671 (c) (1) exception to CS 25.1309 (b) (1) (ii) (reference section 3.1, CS 25.1309, page 14).</p>
response	<p>Partially accepted.</p> <ul style="list-style-type: none"> • Disconnections (e.g. mechanical or electrical disconnections) are already addressed through the application of CS 25.671(c)(1) and CS 25.1309(b). • A probabilistic approach is not acceptable for single disconnections (i.e. single failures) leading to catastrophic repercussions (per CS 25.1309(b)) or preventing CSFL (per CS 25.671(c)(1)). <p>See NPA 2014-02 section 9 ‘Evaluation of control system failures – CS 25.671(c)’:</p> <p>‘CS 25.671(c)(1) requires the evaluation of any single failure, excluding the types of jams addressed in subparagraph CS 25.671(c)(3). CS 25.671(c)(1) requires that any single failure be considered, suggesting that an alternative means of controlling the aeroplane or an alternative load path be provided in the case of a single failure. All single failures must be considered, even if they can be shown to be extremely improbable.’</p> <ul style="list-style-type: none"> • Jamming requires specific guidance since they can be related to external events (FOD, icing, etc.). • However, it is true, as suggested in this comment, that the considerations for the assessment of continued safe flight and landing (see NPA 2014-02 section 9.e) apply to the whole CS 25.671(c), i.e. both failure and jamming cases, including the delay times definition (for recognition, reaction, e.g. transfer of control and possibly operation of a disconnect system).
comment	<p>131 comment by: <i>Garmin International</i></p> <p>AMC 25.671, Section 9.c (1)</p> <p>This paragraph states that use of “at risk time” or the exposure time associated with the last failure in the failure sequence leading to a jam close to the ground should not be used in calculating the probability of jam. At higher altitudes, it is assumed there is sufficient time to transfer control and therefore the classification close to the ground is more severe.</p> <p>It is not stated why a reduced exposure time cannot be used if the system is known to be working prior to the failure and that a jam that occurs during an earlier flight phase is mitigated to a lower classification. The sentence is not consistent with the normal application of exposure times. It is recommended that this sentence is deleted.</p>
response	<p>Not accepted.</p> <p>Jamming is not addressed via the normal system safety assessment process. EASA proposes specific dedicated criteria.</p>

comment	<p>169</p> <p>PARAGRAPH / SECTION YOUR COMMENT IS RELATED TO: AMC25.671 §9 a (1),(2),(3).</p> <p>PROPOSED TEXT / COMMENT: Delete the mentioned failure combinations in AMC25.671§9</p> <p>RATIONALE / REASON / JUSTIFICATION: If these failure combinations are to be considered within the scope of CS25.629, they should be mentioned in CS25.629 directly. An AMC to 25.671 should not specify additional requirements that are to be addressed under CS25.629. Airbus will note that the 3 examples mentioned in AMC25.671§9 deviate from the proposed update to CS25.629(d)10. See also Airbus comment on CS25.629(d)10.</p>	comment by: AIRBUS
response	<p>Accepted. The list of failure combinations has been deleted.</p>	
comment	<p>172</p> <p>PARAGRAPH / SECTION THE COMMENT IS RELATED TO: AMC25.671§9e(2)</p> <p>2. PROPOSED TEXT / COMMENT: Airbus do not agree to use CS25.302 methodology consistently for all failures considered under CS25.671c to demonstrate continued safe flight and landing. Discuss the approach first in Group of appropriate Industry and Regulatory representatives from the Structure community .</p> <p>3. RATIONALE / REASON / JUSTIFICATION: Airbus has experience on a recent certification program, where EASA proposed to use CS25.302 as an acceptable MoC for a dedicated system failure scenario covered under CS25.671c, impacting structure loads. Traditionally, Airbus has addressed this dedicated failure case with a MoC different as CS25.302. Argument has always been that MoC for a traditional system does not need to use the principles of CS25.302/ App K that are intended for complicated electronic systems that actively impact the structure loads. The way the safety factors in fig 1 and 2 are defined is such that the joint probability of structural failures due to application of loads during system malfunctions is not greater than that found in aeroplanes equipped with “earlier technology control systems”. Structure representatives both from Industry and Authorities need to be consulted and review any proposed changes to address CS25.671c failure conditions in the context of continued safe flight and landing by using Appendix K in the correct context. The proposal also leads to a dis- harmonisation with the use of FAR25 Appendix K, and therefore need to be well evaluated and coordinated with the relevant appropriate Industry and Regulatory representatives from the Structure community before accepting such a dis- harmonisation. Therefore, Airbus proposes to involve the L&DHWG to consider any update in use of Appendix K as MoC for CS25.671c.</p>	comment by: AIRBUS
response	<p>Partially accepted. The commented sentence has been revised: the possibility has been added to agree with EASA on another means of compliance.</p>	
comment	174	comment by: AIRBUS

PARAGRAPH / SECTION THE COMMENT IS RELATED TO:

AMC 25.671 §4

PROPOSED TEXT / COMMENT:

Airbus propose to modify this paragraph as follows:

4. APPLICABILITY OF CS 25.671.

CS 25.671 applies to all flight control system installations (including primary, secondary, trim, lift, drag, feel, and stability augmentation systems) regardless of implementation technique (manual, powered, fly-by-wire, or other means).

~~Some parts of CS 25.671 (and the associated AMC) also apply to all control systems. This is indicated by the use of the term 'control systems' versus 'flight control systems'.~~

-

RATIONALE / REASON / JUSTIFICATION:

Until today and according to FCHWG ARAC report, control system is only used for primary, secondary, trim, lift, drag, feel, and stability augmentation systems.

Definition of 'control systems' is not provided and must be defined in AMC 25.671 paragraph 5 – Definitions

In addition, depending on the definition for “control system” it may have a huge impact on Systems Design.

-

response

Partially accepted.

The statement has been reworded as recommended by comment #273.

comment

175

comment by: AIRBUS

PARAGRAPH / SECTION THE COMMENT IS RELATED TO:

AMC 25.671 §7 b page 22

PROPOSED TEXT / COMMENT:

Airbus propose to modify this paragraph as follow:

b. Abnormal attitude.

Compliance should be shown by evaluation of the closed loop flight control system. This evaluation is intended to ensure that there are no features or unique characteristics (including numerical singularities) which would restrict the pilot's ability to recover from any attitude. It is not the intent of this rule or Guidance Material to limit the use of envelope protection features or other systems that augment the control characteristics of the aircraft. ~~Open-loop flight control systems should also be evaluated.~~

~~This paragraph is intended to cover cases outside the protected envelope (for aircraft with flight control envelope protection).~~

RATIONALE / REASON / JUSTIFICATION:

The intent of following sentences is not understood by Airbus and needs further clarifications. “Open-loop flight control systems should also be evaluated. This paragraph is intended to cover cases outside the protected envelope (for aircraft with flight control envelope protection).”

response

Noted.

The paragraph is applicable to normal, degraded and direct-mode control. All modes should be considered.

comment

176

comment by: AIRBUS

PARAGRAPH / SECTION THE COMMENT IS RELATED TO:

AMC 25.671 §9 b 1 iii page 25

PROPOSED TEXT / COMMENT:

Airbus propose to replace this paragraph

(iii) Flare/landing: The maximum lateral control position is the peak lateral control position to maintain wings-level in response to a steady crosswind of 15 knots, in manual or autopilot mode.

By

(iii) Flare/landing: The lateral control position required to maintain wings-level with the sideslip generated to decrab 15 kts steady crosswind at approach speed and in manual and autopilot modes."

-

RATIONALE / REASON / JUSTIFICATION:

From Handling Qualities point of view, Airbus consider that the peak position is not the appropriate parameter but the sideslip value to decrab in steady crosswind. Airbus proposal is to use the wording as agreed on A350 CRI

response

Noted.

Like with any AMC, applicants may use another proposal which is shown to be equivalently safe.

comment

177

comment by: AIRBUS

PARAGRAPH / SECTION THE COMMENT IS RELATED TO:

AMC 25.671 §9 b 3 iii page 26

PROPOSED TEXT / COMMENT:

Airbus propose to replace this paragraph

(iii) Flare/landing: the maximum directional control position is peak directional control position commanded by the pilot, autopilot and/or stability augmentation system in response to a steady crosswind of 15 knots

By

(iii) Flare/landing: The directional control position required to maintain wings-level with the sideslip generated to decrab 15 kts steady crosswind at approach speed and in manual and autopilot modes."

-

RATIONALE / REASON / JUSTIFICATION:

From Handling Qualities point of view, Airbus consider that the peak position is not the appropriate parameter but the sideslip value to decrab in steady crosswind. Airbus proposal is to use the wording as agreed on A350 CRI

response

Noted.

Like with any AMC, applicants may use another proposal which is shown to be equivalently safe.

comment

178

comment by: AIRBUS

PARAGRAPH / SECTION THE COMMENT IS RELATED TO:

AMC 25.671 §9.3 ii c

PROPOSED TEXT / COMMENT:

Airbus propose to delete this paragraph

~~(c) For approach, the peak directional control position commanded by the pilot, autopilot and/or stability augmentation system in response to a steady crosswind of 15 knots.~~



response	<p>RATIONALE / REASON / JUSTIFICATION Airbus do not see any additional value from conditions described in a and b of this paragraph</p> <p>Not accepted. Comment not understood. The sentence starts with 'the greater of'. If one of the other two criteria is greater, then this third criterion would not be needed. EASA maintains the wording as it is.</p>
comment	<p>179 comment by: AIRBUS</p> <p>PARAGRAPH / SECTION THE COMMENT IS RELATED TO: AMC 25.671 §9.c page 27</p> <p>PROPOSED TEXT / COMMENT: Airbus propose to modify this paragraph as follow: For these exceptional cases the jam should be shown to be extremely improbable. This should be done either by (1) A quantitative analysis using relevant reliability data from in-service experience. The use of a risk time for this analysis is not accepted. The jam itself should be demonstrated as extremely improbable, or - RATIONALE / REASON / JUSTIFICATION During discussion for A350 TC, the FAA accepted the use of a risk time for the quantitative approach. The use of the risk is not accepted by EASA but it is not clearly explained in the AMC. Justification must be given. In addition, for (1) and (2), it is understood that on one side either quantitative or qualitative approach may be used, on the other side it is said that only qualitative approach should be used where no in-service experience. Does it mean that qualitative approach cannot be used in case of in-service experience ?</p>
response	<p>Noted. A qualitative approach may still be used.</p>
comment	<p>180 comment by: AIRBUS</p> <p>PARAGRAPH / SECTION THE COMMENT IS RELATED TO: AMC 25.671 § 10 b 3 page 30-31</p> <p>PROPOSED TEXT / COMMENT: Airbus propose to delete the paragraph AMC 25.671 paragraph 10 b (3) ii - RATIONALE / REASON / JUSTIFICATION Roll capability +/- 30° in less than 11 sec is derived from AMC 25.147(d) related to lateral control with OEI. Airbus consider this manoeuvre excessive in TEFO as no asymmetry needs to be counteracted.</p>
response	<p>Not accepted. The proposal in the AMC is based on the definition of CSFL from the ARAC WG.</p>
comment	<p>182 comment by: AIRBUS</p> <p>PARAGRAPH / SECTION THE COMMENT IS RELATED TO: AMC 25.671 § 9 e iv B page 29</p>

PROPOSED TEXT / COMMENT:

Airbus propose to modify this paragraph as follow:

(iv) *Manoeuvre Capability for Continued Safe Flight and Landing.* If, using the manufacturer's recommended procedures, the following manoeuvres can be performed following the failure, it will generally be considered that continued safe flight and landing has been shown.

(A) A steady 30° banked turn to the left or right;

~~(B) A roll from a steady 30° banked turn through an angle of 60° so as to reverse the direction of the turn in not more than 11 seconds (in this manoeuvre the rudder may be used to the extent necessary to minimise side slip, and the manoeuvre may be unchecked);~~

(C) A push-over manoeuvre to 0.8 g, and a pull-up manoeuvre to 1.3 g;

-

RATIONALE / REASON / JUSTIFICATION

Roll capability +/- 30° in less than 11 sec is derived from AMC 25.147(d) related to lateral control with OEI.

Airbus consider this manoeuvre excessive in TEFO as no asymmetry needs to be counteracted.

response

Not accepted.

The proposal in the AMC is based on the definition of CSFL from the ARAC WG.

comment

191

comment by: *Embraer - Indústria Brasileira de Aeronáutica - S.A.*

AMC 25.671 – (8)(a):

The proposed AMC states that the intent is to make incorrect assembly of system elements “impossible”. Since it is difficult to define all the assembly errors that should be considered in order to determine that something is “impossible”, Embraer believes a more tangible and useful standard would be “For control systems, the design intent should be to minimize the chance of incorrect assembly of system elements that prevent its intended function.” Rest of NPA unchanged.

response

Not accepted.

The design intent should be to make it impossible to incorrectly assemble the elements of the system.

comment

192

comment by: *Embraer - Indústria Brasileira de Aeronáutica - S.A.*

AMC 25.671 – (9)(a):

The AMC calls for consideration for specific failure combinations “within the scope of CS 25.629.” Should this reference be to 25.671?

Also, subparagraph (3) calls for the consideration of any single failure in combination with any power system failure. As we commented about CS 25.629(d)(10) and its requirement for consideration of specific failure combinations regardless of probability, Embraer recommends that the ASAWG recommendation for consideration of only combinations not shown to be extremely improbable is sufficient, and subparagraph (3) should be removed.

response

First part of the comment: Not accepted. The list of failure combinations, being inconsistent with CS 25.629(d), has been deleted.

Second part of the comment: Please refer to the response to comment #129.

comment

193

comment by: *Embraer - Indústria Brasileira de Aeronáutica - S.A.*

AMC 25.671 – (9)(e)(2)(iii):



response	<p>Embraer suggests that the mention of the need for flexible model in loads determination be revised to say “A flexible aircraft model should be used for loads calculations when structural deflection would significantly change loads distribution.” This would be in accordance with CS 25.301(c).</p> <p>Partially accepted.</p> <p>A sentence has been added to the effect that a flexible aircraft model should be used where the use of a flexible aircraft model is significant to the loads being assessed.</p>
comment	<p>217 comment by: <i>Boeing</i></p> <p>Page: 19 and 20 Paragraph: <i>AMC 25.671 -- Control Systems – General</i> <i>5. Definitions</i> <i>5.k.(1) Jam</i></p> <p>The proposed text states: “k.(1) <i>Jam</i>. A failure or event such that a control surface, pilot control, or component is fixed in one position. (i) If the control surface or pilot control is fixed in position due to physical interference, it is addressed under CS 25.671(c)(3). Causes may include corroded bearings, interference with a foreign or loose object, control system icing, seizure of an actuator, or disconnect that results in a jam by creating interference. Jams of this type must be assumed to occur and should be evaluated at positions up to and including the normally encountered positions defined in Section 9.b.”</p> <p>REQUESTED CHANGE: “k.(1) <i>Jam</i>. A failure or event such that a control surface, pilot control, or component or control system is fixed in one position. (i) If the control surface or pilot control is fixed in position due to physical interference, it is addressed under CS 25.671(c)(3). Causes may include corroded bearings, interference with a foreign or loose object, control system icing, seizure of an actuator, or disconnect that results in a jam by creating interference. Jams of this type must be assumed to occur and should be evaluated at positions up to and including the Normally encountered positions are defined in Section 9.b.”</p> <p>JUSTIFICATION: The entire system and surface needs to be addressed. The (struck-through) statement in k.(1)(i) is not a definition of a jam, but appears to be stated as a rule. As such, this would be beyond the scope of advisory material.</p>
response	<p>Partially accepted.</p> <p>The first suggestion is against the wording coming from the ARAC WG, and is more specific, hence not accepted.</p> <p>The second suggestion is accepted.</p>
comment	<p>218 comment by: <i>Boeing</i></p> <p>Page: 22 Paragraph: <i>AMC 25.671 -- Control Systems – General</i> <i>9. Evaluation of Control System Failures</i> <i>(introductory section)</i></p>

The proposed text states:

“The guidance provided in this advisory material for CS 25.671(c) is not intended to address requirement errors, design errors, software errors, or implementation errors. These are typically managed through development processes or system architecture, and are adequately addressed by SAE ARP4744A/EUROCAE ED-79A, DO-178() and AMC 25.1309.”

REQUESTED CHANGE:

“The guidance provided in this advisory material for CS 25.671(c) is not intended to address requirement errors, design errors, software errors, or implementation errors. These are typically managed through development processes or system architecture, and are adequately addressed by SAE ARP4744A/EUROCAE ED-79A, DO-178()/EUROCAE ED-12, DO 254/EUROCAE-80, and AMC 25.1309.”

JUSTIFICATION: The reference to DO-178 should include the EUROCAE equivalent document, and a reference to the hardware guidance should be included as well.

response

Noted.

Both DO-178 and ED-12 are indeed valid and were referenced in Chapter 3 of the AMC proposal. This reference has been replaced by AMC 20-115 which is the current applicable AMC referring to these standards.

The proposal to refer to DO-254/ED-80 is not deemed to be necessary in this AMC and therefore it is not accepted.

comment

219

comment by: Boeing

Page: 22-23

Paragraph: AMC 25.671 -- Control Systems – General

9. Evaluation of Control System Failures
(introductory section)

The proposed text states:

“CS 25.671(c)(3) requires the evaluation of any failure or event that results in a jam of a flight control surface or control system pilot control. This subparagraph is intended to address failure modes that would result in the surface or control system pilot’s control being fixed at the position commanded at the time of the failure due to some physical interference. The position at the time of the jam should be at any normally encountered control position encountered during take-off, climb, cruise, normal turns, descent, and landing. In some architectures, component jams within the system may result in failure modes other than a fixed surface or control system pilot control; those types of jams (such as a jammed valve) are considered under subparagraphs CS 25.671(c)(1) and (c)(2).”

REQUESTED CHANGE:

“CS 25.671(c)(3) requires the evaluation of any failure or event that results in a jam of a flight control surface or control system ~~pilot control~~. This subparagraph is intended to address failure modes that would result in the surface or control system ~~pilot’s control~~ being fixed at the position commanded at the time of the failure due to some physical interference. The position at the time of the jam should be at any normally encountered control position encountered during take-off, climb, cruise, normal turns, descent, and landing. In some architectures, component jams within the system may result in failure modes other than a fixed surface or control system ~~pilot control~~; those types of jams (such as a jammed valve) are considered under subparagraphs CS 25.671(c)(1) and (c)(2).”

JUSTIFICATION: The entire system and surface needs to be addressed.



response Not accepted.
The principle of the comment is agreed, but we prefer to stick to the well-known ARAC wording.

comment 220 comment by: Boeing
Page: 23
Paragraph: AMC 25.671 -- Control Systems – General
9. Evaluation of Control System Failures
(introductory section)

The proposed text states:

“In the past, determining a consistent and reasonable definition of normally encountered flight control positions has been difficult. A review of in-service fleet experience, to date, showed that the overall failure rate for a flight control surface jam is approximately 10-6 to 10-7 per flight hour.”

REQUESTED CHANGE:

“In the past, determining a consistent and reasonable definition of normally encountered flight control positions has been difficult. A review of in-service fleet experience, to date, showed that the overall failure rate for a flight control ~~surface~~ system jam is approximately 10-~~6~~7 to 10-~~7~~8 per flight hour. An airplane may be able to document and utilize a different jam rate based on service history or system architecture similarity to an airplane with service history.”

JUSTIFICATION: We believe that the intent of this section is to describe the history of system jams and not just surface jams. Boeing service history for jams is at least an order of magnitude better than EASA’s estimates.

response Not accepted.
These ‘probability’ values are not quoted to provide the basis of a quantitative approach. Note that a system jam could have a different consequence and probability to a surface jam. Note that these estimates are coming from the ARAC WG.

comment 221 comment by: Boeing
Page:23
Paragraph: AMC 25.671 -- Control Systems – General
9. Evaluation of Control System Failures
(introductory section)

The proposed text states:

“... Considering this in-service data, a reasonable definition of normally encountered positions represents the range of flight control surface deflections (from neutral to the largest deflection) expected to occur in 1 000 random operational flights, without considering other failures, for each of the flight segments identified in the rule.”

REQUESTED CHANGE:

“... Considering this in-service data, a reasonable definition of maximum normally encountered positions represents the ~~range~~ average of maximum flight control surface deflections ~~(from neutral to the largest deflection) expected to occur in~~ seen per flight from at least 1000 random operational flights, without considering other failures, for each of the



flight segments identified in the rule.”

JUSTIFICATION: The proposed standard in the NPA is redefining a “normally encountered position” to be “any encountered position.” The standard being set by the NPA using the maximum from 1000 flights is greater than a 3 sigma value and, thus, substantially beyond the philosophy of <10⁻⁹ being extremely improbable. Even the average of the maximum values will be extremely conservative compared to the exposure time at that deflection. Using a method that is overly conservative will yield minimal improvement in safety, while preventing manufacturers from utilizing control system designs that may have other features with their own safety benefits.

response

Not accepted.

This wording was agreed within the ARAC WG. No adverse experience has been gained since this was agreed.

Some maximum values are rare, hence 100 flights is not considered to be sufficient.

comment

222

comment by: *Boeing*

Page: 23

Paragraph: *AMC 25.671*

9. Evaluation of Control System Failures,

a. Compliance with CS 25.671(c)(2)

The proposed text states:

“a. ... The following failure combinations should be assumed to occur and The following failure combinations should be assumed to occur and should be addressed, within the scope of CS 25.629:

(1) Any dual power system failure (e.g. hydraulic, electrical)

(2) Any single failure in combination with any probable failure.

(3) Any single failure in combination with any power system failure.

The aeroelastic stability (flutter) requirements of CS 25.629 should also be considered.”

REQUESTED CHANGE: Delete this entire text.

JUSTIFICATION:

Guidance for CS 25.629 should be contained in AMC 25.629. In addition, the guidance for CS 25.629 needs to be consistent with the guidance for CS 25.671(c)(2) and CS 25.1309(b)(5).

The proposed requirements stated in this paragraph are inconsistent with what is required by CS 25.629.

- Item (1) covers dual electrical and hydraulic system failure.
- Items (2) and (3) expand the scope of failures beyond what is required in CS 25.629.
- Item (2) expands the probable failure beyond electrical/hydraulic system.
- Item (3) expands the electrical/hydraulic system failure beyond probable.

Failures should be limited to what is explicitly listed in CS 25.629 and AMC 25.629. There is no need for this explicit listing in AMC 25.671; the text therefore should be deleted.

response

Accepted.

The list of failure combinations has been deleted.



comment	<p>223</p> <p>Page:24 Paragraph: AMC 25.671 9. Evaluation of Control System Failures, b. Determination of Control System Jam Positions – CS 25.671(c)(3).</p> <p>The proposed text states: (5th paragraph) “... a reasonable crosswind level for determination of jammed lateral or directional flight control positions during take-off is 15 knots.”</p> <p>REQUESTED CHANGE: “... a reasonable determination of jammed lateral or directional flight control positions during take-off is 15 knots. <u>and consistent crosswind level commensurate with the probability of the jam condition should be utilized. The material in AC 25-7, Appendix 7, should be used in defining crosswind levels.</u>”</p> <p>JUSTIFICATION: The use of “15 knots” crosswind level is offered in the proposal without justification.</p>	comment by: <i>Boeing</i>
response	<p>Noted.</p> <p>There is a number of sources of crosswind statistical values which could be used, and each of them provides a different acceptable value. EASA has selected a reasonable value to be used, based upon these various sources.</p>	
comment	<p>224</p> <p>Page:24 Paragraph: AMC 25.671 9. Evaluation of Control System Failures, b. Determination of Control System Jam Positions – CS 25.671(c)(3).</p> <p>The proposed text states: (6th paragraph) “A similar reasoning applies for the approach and landing phase. It leads to consider that a reasonable crosswind level for determination of jammed lateral or directional control positions during approach and landing is 15 knots.”</p> <p>REQUESTED CHANGE: “A similar reasoning applies for the approach and landing phase. It leads to consider that a A reasonable crosswind level for determination of jammed lateral or directional control positions during approach and landing is 15 knots. <u>commensurate with the probability of the jam condition should be utilized. The material in AC 25-7, Appendix 7, should be used in defining crosswind levels.</u>”</p> <p>JUSTIFICATION: The use of “15 knots” crosswind level is offered in the proposal without justification.</p>	comment by: <i>Boeing</i>
response	<p>Noted.</p> <p>There is a number of sources of crosswind statistical values which could be used, and each of them provides a different acceptable value. EASA has selected a reasonable value to be used, based upon these various sources.</p>	

comment	<p data-bbox="360 277 408 309">225</p> <p data-bbox="1230 277 1485 309">comment by: <i>Boeing</i></p> <p data-bbox="360 333 1166 510">Page: 24 Paragraph: AMC 25.671 9. Evaluation of Control System Failures, b. Determination of Control System Jam Positions – CS 25.671(c)(3). [and related text in 9.b.(1)(i) and 9.b.(3)(i)]</p> <p data-bbox="360 551 671 618"><u>The proposed text states:</u> (5th paragraph)</p> <p data-bbox="360 622 1485 757">“Although 1 in 1000 operational take-offs is expected to include crosswinds of 25 knots or greater, ... Considering the flight control jam failure rate combined with the short exposure time between V_1 and V_{LOF}, a reasonable crosswind level for determination of jammed lateral or directional flight control positions during take-off is 15 knots.”</p> <p data-bbox="360 797 632 828"><u>REQUESTED CHANGE:</u></p> <p data-bbox="360 833 1485 1012">“Although 1 in 1000 operational take-offs is expected to include crosswinds of 25 knots or greater, ... Considering the flight control jam failure rate combined with the short exposure time between V_1 and V_{LOF}, a reasonable crosswind level for determination of jammed lateral or directional flight control positions during take-offs is 15 knots for a ~10-6 failure rate and 10 knots for a <10-7 failure rate.”</p> <p data-bbox="360 1052 1485 1151"><u>JUSTIFICATION:</u> Adjust the means of compliance to better reflect the philosophy of “extremely improbable” and do not penalize all airplanes/designs to the lowest common denominator.</p>
response	<p data-bbox="360 1173 443 1205">Noted.</p> <p data-bbox="360 1209 1485 1317">There is a number of sources of crosswind statistical values which could be used, and each of them provides a different acceptable value. EASA has selected a reasonable value to be used, based upon these various sources.</p>

Comment from Textron Aviation (extracted from the letter attached to comment #289):Page/Paragraph: AMC 25.671

Comment: While part of the NPA state that the 1/1000 combined with “remote” (10e-5) failure rates only need to be for two failures leading to HAZ/CAT, the example presented in the NPA has numerous failures in the fault tree, not just two.

Suggested change: Please clarify.

EASA response: Noted.

The example provides a fault tree with failure combinations of orders 2 and 3. The purpose of presenting this failure combination of order 3 is to illustrate that CS 25.1309(b)(5) does not apply to failure combinations of an order greater than 2.



Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.671

Comment: Since the “1 in 1000” criteria is new, it could potentially be miss-understood, therefore it would be useful to provided examples on how the new “1 in 1000” criteria should be interpreted and applied. This could prevent unintended interpretations/applications of “1 in 1000.”

Suggested change: Propose examples be provided on how the new “1 in 1000” criteria should be interpreted and applied.

EASA response: Not accepted.

There is already a considerable amount of guidance in the AMC. Further examples could be discussed with industry or standardisation working groups (e.g. SAE).

comment

226

comment by: *Boeing*

Page: 24

Paragraph: AMC 25.671

9. Evaluation of Control System Failures,

b. Determination of Control System Jam Positions – CS 25.671(c)(3).

(1) Jammed Lateral Control Positions.

The proposed text states:

“(ii) In-flight: The lateral control position to sustain a 12 degree/second steady roll rate from $1.23V_{sr1}$ to V_{mo}/M_{mo} or V_{fe} , as appropriate, but not greater than 50% of the control input.”

REQUESTED CHANGE:

“In-flight: The lateral control position ~~to sustain a 12 degree/second steady roll rate from $1.23V_{sr1}$ to V_{mo}/M_{mo} or V_{fe} , as appropriate, but not greater than 50% of the control input.~~ with lateral control authority corresponding to single channel autopilot.”

JUSTIFICATION: Single channel autopilots are designed to handle the normal operations of the airplane. A 12 degree/second roll rate is very high for a large transport aircraft and the result would be the 50% control input. As stated before, if a very conservative assessment is used for “normal” the gain for safety will be very small while eliminating control designs that may have other safety benefits.

response

Not accepted.

The authority of the autopilot will depend on the type of aeroplane.

The proposed text was agreed in the ARAC WG. It has also been used in EASA CRIs, with no subsequent adverse experience.

comment

227

comment by: *Boeing*

Page:25

Paragraph: AMC 25.671

9. Evaluation of Control System Failures,

b. Determination of Control System Jam Positions – CS 25.671(c)(3).

(2) Jammed Longitudinal Control Positions



The proposed text states:

“(i) Take-off: Three longitudinal flight control positions should be considered:

(A) Any flight control position from that which the flight controls naturally assume without pilot input at the start of the take-off roll to that which occurs at V_1 using the manufacturer’s recommended procedures.

(B) Note: It may not be necessary to consider this case if it can be demonstrated that the pilot is aware of the jam before reaching V_1 (for example, through a manufacturer’s recommended AFM procedure).

(C) The longitudinal flight control position at V_1 based on the manufacturer’s recommended procedures including consideration for any runway condition for which the aircraft is approved to operate.

(D) Using the manufacturer’s recommended procedures, the peak longitudinal flight control position to achieve a steady aircraft pitch rate of the lesser of 5 deg/sec or the pitch rate necessary to achieve the speed used for all-engines-operating initial climb procedures (V_2+XX) at 35 ft.”

REQUESTED CHANGE:

“(i) Take-off: Three longitudinal flight control positions should be considered:

Note: It may not be necessary to consider this case if it can be demonstrated that the pilot is aware of the jam before reaching V_1 .

(A) Any flight control position from that which the flight controls naturally assume without pilot input at the start of the take-off roll to that which occurs at V_1 using the manufacturer’s recommended procedures.

~~(B) Note: It may not be necessary to consider this case if it can be demonstrated that the pilot is aware of the jam before reaching V_1 (for example, through a manufacturer’s recommended AFM procedure).~~

~~(C)~~ The longitudinal flight control position at V_1 based on the manufacturer’s recommended procedures including consideration for any runway condition for which the aircraft is approved to operate.

~~(D)~~ Using the manufacturer’s recommended procedures, the peak longitudinal flight control position to achieve a steady aircraft pitch rate of the lesser of 5 deg/sec or the pitch rate necessary to achieve the speed used for all-engines-operating initial climb procedures (V_2+XX) at 35 f.”

JUSTIFICATION: The note appears to be equally applicable to (A) and (C). The example is not necessary and does not add any value.

response

Partially accepted.

EASA agrees that the note refers to subparagraphs A to C, and it has been moved as suggested. EASA disagrees to remove the example: the means to make the pilot aware must be provided.

comment

228

comment by: Boeing

Page: 25-26

Paragraph: AMC 25.671

9. Evaluation of Control System Failures,

b. Determination of Control System Jam Positions – CS 25.671(c)(3).

[9.b.(2)(ii)(2), 9.b.(3)(ii)(A), 9.b.(7)(i)]



The proposed text states: The proposed text contains various references to gust velocities of 15 fps to 20,000 ft., for example:

9.b.(2)(ii)(2): “The peak longitudinal flight control position commanded by the autopilot and/or stability augmentation system in response to atmospheric discrete vertical gust defined by 15 fps from sea level to 20 000 ft.”

9.b.(3)(ii)(A): “The peak directional flight control position commanded by the autopilot and/or stability augmentation system in response to atmospheric discrete lateral gust defined by 15 fps from sea level to 20,000 ft.”

9.b.(7)(i): “Gust Load Alleviation Systems: At any airspeed between 1.23VSR1(1.3VS) to VMO/MMO or Vfe, as appropriate, the flight control surfaces are assumed to jam in the maximum position commanded by the gust load alleviation system in response to a discrete atmospheric gust with the following reference velocities:

(A) 15 fps (EAS) from sea level to 20 000 ft (vertical gust);

(B) 15 fps (EAS) from sea level to 20 000 ft. (lateral gust).”

REQUESTED CHANGE: For those certifications lacking the requisite in-flight data, applying the maneuver-based criteria can be accepted; however, care must be exercised to use the appropriate levels of atmospheric turbulence and wind values to properly reflect the objective of achieving a 10E-9 outcome.

JUSTIFICATION: The universal 15 fps discrete turbulence level prescribed in the NPA is unnecessarily conservative, since it corresponds to probabilities of occurrence between 10E-4 and 10E-5 from Sea Level to 20,000 ft.

For example: For a control jam probability assessed as 10E-7/hr, an atmospheric discrete gust probability of 10E-2 is assigned (ranges from 9 fps at Sea Level to 4 fps at 20,000 ft.). If the jam probabilities were on the order of 10E-6/hr, then the turbulence level corresponding to 10E-3 (ranging from 13 fps at Sea Level to 6 fps at 20,000 ft.) is appropriate.

response

Not accepted.

EASA proposed reasonable values which originate from the ARAC WG.

It is not possible to provide a text that fits all possible system architectures.

An applicant may propose different values for their particular aeroplane project if this proposal provides for an equivalent level of safety.

comment

229

comment by: *Boeing*

Page: 27

Paragraph: *AMC 25.671*

9. Evaluation of Control System Failures,

c. Considerations for jams just before landing – CS 25.671(c)(3)(i)/(ii)

The proposed text states:

“(1) A quantitative analysis using relevant reliability data from in-service experience. The use of a risk time for this analysis is not accepted. The jam itself should be demonstrated as extremely improbable, or ..”

REQUESTED CHANGE:

~~“A quantitative analysis using relevant reliability data from in-service experience. The use of a risk time for this analysis is not accepted.~~ The jam itself should be demonstrated as extremely improbable, or ...”

JUSTIFICATION: The lack of consideration for using exposure time for jams very close to the



response	<p>ground is in contradiction to the allowance for a quantitative analysis as that analysis is dependent upon exposure time of the failure. It is impossible build a quantitative analysis solely on in-service history as the required numbers of flying hours have not been accumulated.</p> <p>Not accepted. There is in-service history for any new aeroplane type, but SSA is still performed. The AMC allows a qualitative assessment in cases where in-service history is not available.</p>
comment	<p>230 comment by: <i>Boeing</i></p> <p>Page: 27 Paragraph: AMC 25.671 <i>9. Evaluation of Control System Failures, e. Assessment of Continued Safe Flight and Landing – CS 25.671(c). 9.e.(1)(i) second paragraph</i></p> <p><u>The proposed text states:</u> “Additional means of control, such as trim system, may be used if it can be shown that the systems are available and effective. Credit should not be given for use of differential engine thrust to manoeuvre the aircraft. ...”</p> <p><u>REQUESTED CHANGE:</u> “Additional means of control, such as trim system, may be used if it can be shown that the systems are available and effective. Credit should not be given for use of differential engine thrust to maneuver the aircraft unless it is shown as part of pilot training. ...”</p> <p><u>JUSTIFICATION:</u> Excluding the ability to use engine thrust for maneuvering is short-sighted. It is possible that training in the future could use this as mitigation.</p>
response	<p>Not accepted. The proposed text originates from the ARAC WG, and there has been no subsequent negative feedback. Pilot training should be considered as an additional measure, but not as an element to justify the design.</p>
comment	<p>231 comment by: <i>Boeing</i></p> <p>Page:28 Paragraph: AMC 25.671 <i>9. Evaluation of Control System Failures, e. Assessment of Continued Safe Flight and Landing – CS 25.671(c). 9.e.(1)(ii)(D)</i></p> <p><u>The proposed text states:</u> “(ii) <i>Transient Response</i>. There should be no unsafe conditions during the transient condition following a flight control system failure. The evaluation of failures, or manoeuvres leading to jamming, is intended to be initiated at 1 g wings-level flight. For this purpose, continued safe flight and landing (within the transition phase) is generally defined as not exceeding any one of the following:</p>

	<p>... (D) Catastrophic Flutter or vibration”</p> <p><u>REQUESTED CHANGE:</u> “... (D) Catastrophic Flutter or excessive vibration”</p> <p><u>JUSTIFICATION:</u> This suggested change should be made for improved clarity. Vibration is covered by current design practices.</p>
response	<p>Partially accepted. Vibration is to be considered separately. A new subparagraph is therefore created to read: (...)’ (D) catastrophic flutter, (E) vibration and buffeting conditions, (F) bank angle (...)</p>
comment	<p>232 comment by: <i>Boeing</i></p> <p>Page:29 Paragraph: <i>AMC 25.671</i> <i>9. Evaluation of Control System Failures,</i> <i>e. Assessment of Continued Safe Flight and Landing – CS 25.671(c).</i></p> <p><i>9.e.(1)(iv)(E)</i></p> <p><u>The proposed text states:</u> “(iv) <i>Manoeuvre Capability for Continued Safe Flight and Landing.</i> If, using the manufacturer’s recommended procedures, the following manoeuvres can be performed following the failure, it will generally be considered that continued safe flight and landing has been shown. ... (E) The aircraft remains on the paved runway surface during the landing roll, until reaching a complete stop.”</p> <p><u>REQUESTED CHANGE:</u> “... (E) <u>The aircraft remains on the paved runway surface during the landing roll, until reaching a complete stop. Assuming that a suitable runway is available, it should be possible to control the aeroplane until it comes to a complete stop on the runway.</u>”</p> <p><u>JUSTIFICATION:</u> The flight controls that are the subject of CS 25.671 are only one contributor to the airplane’s capability to remain on the paved surface to a complete stop. Other systems (thrust reversers, brakes, nose wheel steering) have significant contributions. While desirable, recent aircraft would probably not be able to remain on the paved surface for all flight control failures not shown to be extremely improbable. We suggest the criterion be similar to (proposed) AMC 25.671, paragraph 10.b.(5).</p>
response	<p>Not accepted. The commented topic is not linked to CS 25.671(d).</p>

This refers to the destination (or diversion) runway — the aeroplane must remain on that runway under the conditions defined.

comment

233

comment by: *Boeing*

Page:29

Paragraph: AMC 25.671

9. Evaluation of Control System Failures,

e. Assessment of Continued Safe Flight and Landing – CS 25.671(c).

9.e.(1)(iv)

The proposed text states:

“(iv) *Manoeuvre Capability for Continued Safe Flight and Landing*. If, using the manufacturer’s recommended procedures, the following manoeuvres can be performed following the failure, it will generally be considered that continued safe flight and landing has been shown.

(A) A steady 30° banked turn to the left or right;

(B) A roll from a steady 30° banked turn through an angle of 60° so as to reverse the direction of the turn in not more than 11 seconds (in this manoeuvre the rudder may be used to the extent necessary to minimise side-slip, and the manoeuvre may be unchecked);

(C) A push-over manoeuvre to 0.8 g, and a pull-up manoeuvre to 1.3 g;

(D) A wings level landing flare in a 90° crosswind of up to 10 knots (measured at 10 meters above the ground).

(E) The aircraft remains on the paved runway surface during the landing roll, until reaching a complete stop.”

REQUESTED CHANGE:

“(iv) *Manoeuvre Capability for Continued Safe Flight and Landing*. If, using the manufacturer’s recommended procedures, the following manoeuvres can be performed following the failure, it will generally be considered that continued safe flight and landing has been shown.

(A) A steady 30° banked turn to the left or right;

(B) A roll from a steady 30° banked turn through an angle of 60° so as to reverse the direction of the turn in not more than 11 seconds (in this manoeuvre the rudder may be used to the extent necessary to minimise side-slip, and the manoeuvre may be unchecked);

(C) A push-over manoeuvre to 0.8 g, and a pull-up manoeuvre to 1.3 g;

(D) A wings level landing flare in a 90° crosswind of up to 10 knots (measured at 10 meters above the ground).

* (E) The aircraft remains on the paved runway surface during the landing roll, until reaching a complete stop.

Alternatively, a closed-loop piloted demonstration of continued safe flight and landing can also be used, including through simulation per paragraph 13(b)."

[* See our separate comment to this paragraph 9.e.(1)(iv)(E)]

JUSTIFICATION: The conditions listed in (A) through (E) are all open-loop maneuvers. It may well be the case that a closed-loop pilot-in-the-loop evaluation will demonstrate the capability of continued safe flight and landing while not necessarily meeting all of these conditions. In addition, these do not recognize that recommended procedures may call for other conditions than these (for example limiting bank angle to less than 30 degrees).). The proposed AMC 25.671, Section 13, “Acceptable Means of Compliance,” recognizes and



accepts piloted “closed loop” flight simulation evaluations of failures where such closed loop performance is important. This both complements and alleviates the potentially restrictive “open loop” criteria outlined in Section 9 of the proposed AMC. It is appropriate that continued safe flight and landing compliance be based on more than open loop control parameters.

response

Not accepted.
EASA prefers to maintain the proposed text without supplement.
However, any applicant may propose other means of compliance for their specific design.

comment

234

comment by: *Boeing*

Page: 30
Paragraph: *AMC 25.671*
9. Evaluation of Control System Failures,
e. Assessment of Continued Safe Flight and Landing – CS 25.671(c).
9.e.(2)(iii)(B)

The proposed text states:

“(B) Vertical and lateral discrete gusts corresponding to 40 % of the limit gust velocity specified at Vc in CS 25.341(a) with high-lift devices fully retracted, and a 17 fps vertical and 17 fps head-on gust with high-lift devices extended.”

REQUESTED CHANGE:

“(B) Vertical and lateral discrete gusts corresponding to 40 % of the limit gust velocity specified at Vc in CS 25.341(a) with high-lift devices fully retracted, and a ~~17~~ **10** fps vertical and ~~17~~ **10** fps head-on gust with high-lift devices extended.”

JUSTIFICATION: To be consistent with the approach used for high-lift devices fully retracted, use 40% of the limit gust velocities specified in CS 25.345(a)(2) and CS 25.345(b)(2) with high-lift devices extended.

response

Not accepted.
‘17 fps’ was agreed many years ago during previous harmonisation activities among aviation authorities. It has been applied on every subsequent certification project.
The ARAC WG considered it with no further discussion or adverse experience.
Please note that ‘17 fps’ applies to the ‘retracted’ configuration.

comment

235

comment by: *Boeing*

Page:32
Paragraph: *AMC 25.671*
13. ACCEPTABLE MEANS OF COMPLIANCE DEMONSTRATION
a. Acceptable Use of Simulations
13.a.(2)(ii)

The proposed text states:

“(2) Simulation may be an acceptable alternative to flight demonstrations, especially when:
...

(ii) The required environmental conditions are too difficult to attain (e.g., wind shear, high crosswinds); ...”

REQUESTED CHANGE:

	<p>“... (ii) The required environmental conditions, or representation of the failure states are too difficult to attain (e.g. wind shear, high crosswinds, system failure configuration).”</p> <p>JUSTIFICATION: Sometimes it becomes problematic to arrange the specific failure condition on the test airplane where the system/architecture does not lend itself to reasonably be constructed to accurately represent the failure condition. In these cases, simulation may be the only means to evaluate controllability and the continued safe flight and landing capability of the airplane. Consequently, the text in paragraph 13.a.(2)(ii) should be expanded to include circumstances where it is too difficult to safely construct the failed condition on a test airplane.</p>
response	<p>Accepted. Please note that the applicant must propose and justify under which conditions they wish to use a simulation.</p>
comment	<p>260 comment by: <i>Embraer - Indústria Brasileira de Aeronáutica - S.A.</i></p> <p>AMC 25.671 – (9)(c)(1): A quantitative analysis using relevant reliability data from in-service experience. The use of a risk time for this analysis is not accepted. The jam itself should be demonstrated as extremely improbable, or</p> <p>The “at risk time” is an inherent part of the definition of the failure condition, and, of course, of its criticality and probability. So there is no sense in not accepting it while calculating the probability. The question maybe how it is used...</p> <p>For instance, a jam of the pilot column, if occurred during flare, is potentially catastrophic; if occurred during descent, it is not catastrophic. The relevant factor here is the height of the aircraft when the jam occurs. During descent there is enough height to allow coordination between the crew without hitting an obstacle; during flare, there is not. If the jam occurs during the flare, then it was not present at start of the flare. This fact is relevant in determining the probability of the failure condition, and it seems strange not accepting it.</p> <p>Therefore Embraer suggests the sentence "The use of a risk time for this analysis is not accepted" should be excluded.</p>
response	<p>Not accepted. Jams can be caused by a single event. Therefore, it is appropriate not to use the risk time.</p>
comment	<p>263 comment by: <i>AIRBUS</i></p> <p>PARAGRAPH / SECTION THE COMMENT IS RELATED TO: AMC25.671§9e(2)iii</p> <p>PROPOSED TEXT / COMMENT: Airbus do not agree to include the sentence: A flexible aircraft model should be used for loads calculations, and therefore propose to delete this sentence.</p> <p>3. RATIONALE / REASON / JUSTIFICATION: A flexible aircraft model for loads analysis is used in the context of dynamic loading conditions or unsteady aerodynamics. Airbus do not understand why the reference to a</p>

flexible aircraft model is made in terms of considering the referenced failure conditions, and see no additional benefit in applying considering the additional costs made to perform these highly complicated and extensive analysis methods.

Structure representatives both from Industry and Authorities need to be consulted and review any proposed changes to address the loads analysis for these failure conditions in the context of continued safe flight and landing.

Therefore, Airbus proposes to involve the L&DHWG to consider this loads analysis.

response

Partially accepted.

A sentence has been added to the effect that a flexible aircraft model should be used where the use of a flexible aircraft model is significant to the loads being assessed.

comment

271

comment by: *Transport Canada Standards Branch*

p.20, AMC 25.671 section 5.k.(2)

In the definition of “Loss of control of surface”, consider adding wording at the end of the second sentence to better reflect fly-by-wire designs:

“(…) ~~or~~ loss of hydraulic power, or loss of control commands due to computers, data path or actuator electronics failures.”

p.20, AMC 25.671 item 5.m

Definition of “Flight Control System”:

a) a) While hinges are listed in the examples, the definition itself would exclude hinges as currently written. TCCA recommend including in the definition wording along the lines of what is found in FAA AC 25-22 (section 3.d): “For the purpose of compliance with CS25.671, the control system ends where the control surface attaches to fixed structure such as the wing or fuselage.” This would inherently include surface hinges.

b) b) Control surfaces are included in the flight control system per current definition and examples. However 25.671 requirements have not typically been applied to flight control surfaces themselves, and it is unclear how they could be applied – e.g. how would surfaces be addressed under 25.671(c)(1) and (c)(2)? TCCA therefore recommends removing flight control surfaces from the list of examples provided with the definition. If EASA elects to keep control surfaces in the definition, it would be helpful to provide clarification in the AMC as to whether / how each sub-paragraph of CS25.671 would apply to control surfaces.

c) c) It is noted the examples include flaps/slats movable tracks. TCCA would recommend adding clarification in the AMC regarding acceptable compliance means against paragraph CS 25.671(c)(1) for high lift systems movable tracks (slats) and carriages (flaps). This is perceived as an area where further harmonization would be beneficial.

response

Partially accepted.

The proposed change to 5.k.(2) is accepted.

The other proposed changes are not accepted. These items were already discussed during conference calls between EASA and the TCCA, at the end of which the proposed text was retained by EASA.

comment

272

comment by: *Transport Canada Standards Branch*

p.21, AMC 25.671 item 5.o

This item (AMC 25.671 5.o) appears to contain two definitions, “take-off” and “in-flight”. Consider documenting as two separate definitions in section 5, to improve clarity.

p.21, AMC 25.671 section 6.c.

The last sentence of this paragraph reads as follows: “(…) *the requirements specified in*



response	<p>CS25.671(c) are now intended to be identical with the corresponding requirements in CS25.1309 and rely on the same methods of compliance.”</p> <p>TCCA questions this statement, as the proposed CS25.671(c)(2)(ii) requirement is not aligned with the corresponding requirements in CS25.1309.</p> <p>Accepted. Subparagraph 6.c has been deleted.</p>
comment	<p>273 comment by: Transport Canada Standards Branch</p> <p>p.12, CS25.671(a) p.19, AMC 25.671 section 4 AMC 25.671 sections 7.a., 8.a., 8.b., 9 and 9.b.</p> <p>a) a) Per section 4 of AMC 25.671: <i>“Some parts of CS 25.671 (and the associated AMC) also apply to all control systems. This is indicated by the use of the term ‘control system’ versus ‘flight control system’.”</i></p> <p>TCCA’s understanding is that except for CS25.671(d), CS25.671 is intended to address <u>flight</u> control systems. It is recommended to reword the 2nd paragraph of AMC 25.671 section 4 to be more specific in this regard: <i>“While CS25.671 applies to flight control systems, paragraph CS25.671(d) does apply to all control systems required to provide control, including deceleration, for the phases specified.”</i></p> <p>b) b) Wording throughout CS 25.671 and AMC 25.671 has been changed to reference “flight control system”, instead of “system” or “control system” – this is improving clarity. However, it is noted that similar consistent wording has not been used in some instances:</p> <ul style="list-style-type: none"> - CS 25.671(a) refers to “each control and control system” - AMC 25.671 section 7.a. refers to “control systems for essential services” - AMC 25.671 sections 8.a. , 8.b. , 9. (title) and 9.b. (title) refer to “control system(s)” <p>TCCA believe the above cases are also intended to apply to flight control systems only, and therefore recommend that they be changed to “flight control system(s)”, to improve clarity and consistency.</p>
response	<p>Accepted. Paragraph 4: the second statement has been amended as proposed. The terms have been clarified as suggested in the other parts of the AMC.</p>
comment	<p>274 comment by: Transport Canada Standards Branch</p> <p>p.22, AMC 25.671 section 7.b.</p> <p>The last sentence of this paragraph reads as follows: <i>“This paragraph is intended to cover cases outside the protected envelope (for aircraft with flight control envelope protection).”</i></p> <p>TCCA concurs that 25.671(a) does include cases outside of the protected envelope, but is concerned the sentence as written could be interpreted as 25.671(a) applying only to these cases. TCCA would recommend re-wording as follows:</p> <p><i>“This paragraph is intended to <u>include</u> cases outside of the protected envelope [...].”</i></p> <p>p.22, AMC 25.671 section 8.b.</p> <p>Regarding the last portion of this paragraph starting with “The applicant should [...]” and including the three bullets (i), (ii) and (iii):</p> <p>As written TCCA sees this guidance (i.e. different compliance means based on criticality) as contradicting the text of the rule, which requires that marking may be used only where design means are impractical. While agreeing that in certain cases minor criticality could be weighted in when assessing the overall practicality of specific design means, this would</p>

remain subject to a case by case assessment by the certification authority. TCCA would recommend removing entirely the last portion of AMC 25.671 section 8.b. and keeping only the first paragraph of this section: *“Adequate precautions should be taken [...].”*

p.22, AMC 25.671 section 9.

TCCA concurs with the intent of the 1st paragraph in section 9 on development errors. However experience suggests this paragraph (initially from the ARAC FCHWG draft) has not always been understood as intended. TCCA would suggest the following re-wording to improve clarity:

“Development errors (i.e. errors in requirement, design, software, or implementation) should be considered when showing compliance with CS 25.671(c). However, the guidance provided in this advisory material for CS 25.671(c) is not intended to address means of compliance related to development errors. ~~requirement errors, design errors, software errors, or implementation errors.~~ These are typically managed through development processes and ~~or~~ system architecture, and are adequately addressed by SAE ARP 4754A/EUROCAE ED-79A, DO-178() and AMC 25.1309.

p.22, AMC 25.671 section 9

In the paragraph addressing CS25.671(c)(3) (bottom of page 22), TCCA would recommend adding a clarification similar to that CS25.671(c)(1) a few paragraphs above: *“All single jams must be evaluated, even if they can be shown to be extremely improbable.”*

response

Accepted.

First point: Accepted.

Second point: 8.b(iii) is deleted in order to be more consistent with the rule.

Third point: Accepted in principle, although it is generally required to raise a CRI on this topic and the industry guidance alone is not considered to be sufficient. It is proposed to state ‘typically addressed [...] with additional EASA guidance’, rather than ‘adequately addressed’.

Fourth point: Accepted.

comment

275

comment by: *Transport Canada Standards Branch*

p.23, AMC 25.671 section 9.

TCCA questions the inclusion of *“means of preventing a runaway”* as one type of *“means to alleviate a runaway”*. It is unclear what this reference to runaway prevention means is intended to address. Monitoring other features such as trim timers/inhibit would presumably be considered system deactivation. TCCA is concerned that this reference to runaway prevention means could be interpreted as an acceptance of *“extremely improbable”* arguments where the runaway could be due to a single failure – which is contrary to the intent of CS25.671(c)(1).

TCCA would therefore recommend removing references to *“runaway prevention means”* in AMC 25.671.

response

Accepted.

comment

276

comment by: *Transport Canada Standards Branch*

p.23, AMC 25.671 section 9.

TCCA questions the following statement, in the paragraph addressing flight control runaways: *“Without suitable means to alleviate or prevent the runaway, an adverse position would represent any position for which they are approved to operate.”*

Depending on the system design and specific failure leading to runaways, the resulting surface position after a runaway may not be limited to within the positions for which the



surface is approved to operate. This statement is seen as too limiting. TCCA would recommend using the wording from the FCHWG recommendation which is more general in applicability, as follows:
“Consideration of a control runaway will be specific to each application and a general interpretation of an adverse position cannot be given. Where applicable, the applicant is required to assess the resulting surface position after a runaway, if the failure condition is not extremely improbable or can occur due to a single failure.”

response Accepted.

comment 277 comment by: Transport Canada Standards Branch

p.23, AMC 25.671 section 9.a.
 The reference to CS 25.629 near the bottom of p.23 appears to be a typo, and should presumably read instead “within the scope of CS 25.671”. The reference to CS 25.629 near the top of p.24 is correct.
 AMC 25.671 section 9
 No guidance has been provided in AMC 25.671 to address means of compliance to paragraph CS25.671(c)(2)(ii). As the criteria proposed by EASA in this paragraph differs from that defined in CS 25.1309(b)(5), the addition of guidance material in AMC 25.671 would be beneficial.

response Accepted.
 The reference to CS 25.629 is correct; however, the list of failure combinations was inconsistent with CS 25.629(d) and has been deleted.

comment 278 comment by: Transport Canada Standards Branch

p.24, AMC 25.671 section 9.b.
 Near the middle of p.24: *“The manoeuvres and conditions described in this section are only to provide the flight control surface deflection to evaluate continued safe flight and landing capability [...].”*
 As CS 25.671(c)(3) addresses jams of flight control surface or pilot control, TCCA would recommend revising the wording as follows:
“The manoeuvres and conditions described in this section are only to provide the flight control surface and pilot control deflections to evaluate continued safe flight and landing capability [...].”

response Accepted.

comment 279 comment by: Transport Canada Standards Branch

p.25, AMC 25.671 section 9.b.(2)(i)(B)
 The note currently written as item 9.b.(2)(i)(B) pertains to item 9.b.(2)(i)(A); documenting is as a separate bullet (B) may result in confusion.

response Accepted.

comment 280 comment by: Transport Canada Standards Branch

p.27, AMC 25.671 section 9.c. (1) and (2)



	<p>As written, the AMC text indicates that a quantitative analysis per (1) or qualitative analysis per (2) would be equally acceptable to demonstrate compliance via an “extremely improbable argument”, for jam cases just prior to landing where continued safe flight and landing cannot otherwise be shown.</p> <p>This does not appear consistent with material applied on recent certification programs. TCCA would recommend revising this section of the AMC to align with the expected gradual approach to compliance means in such cases, i.e.</p> <ol style="list-style-type: none"> 1. Demonstrate continued safe flight and landing with a jam occurring just prior to landing (already well addressed in current text). 2. If CSF&L cannot be shown, perform a qualitative assessment of the design, relative to jam prevention features and jam alleviation means. 3. As a last resort, with concurrence by the certification authority, use in-service data to support an extremely improbable argument (without use of at-risk time).
response	Accepted.
comment	<p>281 comment by: <i>Transport Canada Standards Branch</i></p> <p>p.27, AMC 25.671 section 10.a. <i>“CS 25.671(d) effectively requires aeroplanes with fully powered or electronic flight control systems to have a source for emergency power, such as an air-driven generator, windmilling engines, batteries, or other power source capable of providing adequate power to the flight control system.”</i></p> <p>TCCA understand paragraph CS 25.671(d) applies to the aeroplane as a whole, and therefore also to systems other than flight controls. Given this, the paragraph quoted above appears too specific to flight controls. It is expected, for example, that power sources would also be adequate to allow deceleration to a stop on the ground (e.g. in the case of electric brakes, electrical power should be sufficient to allow both control in flight, and braking once on the ground). It is recommended to re-word this sentence along the following lines: <i>“CS 25.671(d) effectively requires aeroplanes with fully powered or electronic flight control systems to have a source for emergency power, such as an air-driven generator, windmilling engines, batteries, or other power source capable of providing adequate power to <u>the systems necessary for control as specified under paragraph 25.671(d) flight control system.</u>”</i></p>
response	Accepted.
comment	<p>282 comment by: <i>Transport Canada Standards Branch</i></p> <p>p.27, AMC 25.671 section 10.b.(5) Controllability on ground and deceleration capability are currently addressed separately under bullet (5). TCCA recommends either adding considerations of controllability on ground and deceleration capability under bullet (2), or expanding bullet (5) to more clearly capture the applicable consideration in these phases (sufficient power, transients in critical phases, demonstration means).</p>
response	<p>Not accepted.</p> <p>Point 2 deals with how to perform the demonstration. Points 3, 4 and 5 follow this sequentially. EASA, therefore, prefers to keep it as is.</p>
comment	<p>299 comment by: <i>Rockwell Collins, Inc.</i></p>

	<p>4. For the statement, “Some parts of CS 25.671 (and the associated AMC) also apply to all control systems. This is indicated by the use of the term ‘control systems’ versus ‘flight control systems’.”, all non-flight control specific risk items should be moved to AMC 25.1309. For consistency of coverage, please consider concentrating all specific risk items that are applicable to all systems in the AMC 25.1309.</p>
response	<p>Partially accepted. Except CS 25.671(d), CS 25.671 applies to the flight control system only. The statement has been reworded.</p>
comment	<p>300 comment by: <i>Rockwell Collins, Inc.</i></p>
	<p>9. For the statement, “The guidance provided in this advisory material for CS 25.671(c) is not intended to address requirement errors, design errors, software errors, or implementation errors. These are typically managed through development processes or system architecture, and are adequately addressed by SAE ARP 4754A/EUROCAE ED-79A, DO-178() and AMC 25.1309.”, is EASA indicating that FDAL and IDAL = A is sufficient alone to address “errors”? If that is not the intent of that paragraph, why did EASA include the word “typically” here? Please add more clarifying statements as to the intent of this paragraph.</p>
response	<p>Not accepted. This is not the intent of the statement. Development errors are addressed by CS 25.1309. CS 25.671(c) does not apply to development errors. The term ‘typically’ has been deleted to avoid any confusion.</p>
comment	<p>301 comment by: <i>Rockwell Collins, Inc.</i></p>
	<p>9.a 3rd paragraph For the statement, “The following failure combinations should be assumed to occur and should be addressed, within the scope of CS 25.629: (1) Any dual power system failure (e.g. hydraulic, electrical) (2) Any single failure in combination with any probable failure. (3) Any single failure in combination with any power system failure.”, This seems to go beyond the other ‘Specific Risk’ considerations of assuming any single latent failure has occurred. Why did EASA add these new combinations to address? Please provide justification for this addition.</p>
response	<p>Noted. The intent is to indicate that EASA would expect CSFL to be shown (at least) with these combinations. The list of failure combinations was inconsistent with CS 25.629(d) and has been deleted. Only the reference to the aeroelastic stability requirements of CS 25.629 has been maintained.</p>
comment	<p>322 comment by: <i>Boeing</i></p>
	<p>Page:30 Paragraph: <i>AMC 25.671 - Control Systems – General</i></p>

10. EVALUATION OF ALL ENGINES FAILED CONDITION – CS 25.671(d).
10.a. and b.

REQUESTED CHANGE: We request this section be revised as follows:

a. *Explanation.*

CS 25.671(d) states that,

...

(d) The aeroplane must be designed so that, if all engines fail at any point of the flight and a suitable hard surface runway or equivalent is available for which the distance available following the flare to landing is consistent with the available aeroplane deceleration capability with all engines failed, then it is controllable: if all engines fail.

(1) In flight;

(2) On approach;

(3) During the flare to a landing, and

(4) During ~~the ground phase;~~ and ground deceleration to a stop.

~~(5) The aeroplane can be stopped.~~

The intent of CS 25.671(d) is to assure that in the event of failure of all engines and given the availability of a suitable ~~an adequate~~ runway, the aeroplane will be controllable inflight during, ~~an~~ approach and flare to a landing, and during ground deceleration to a stop ~~is possible and the aeroplane can be stopped~~. In this context, ‘flare to a landing’ refers to the time until touchdown. Although the rule refers to ‘flare to a landing’ with the implication of being on a runway, it is recognised that with all engines inoperative it may not be possible to reach an adequate runway or landing surface; in this case the aircraft must still be able to make a flare to landing attitude. CS 25.671(d) effectively requires aeroplanes with fully powered or electronic flight control systems to have a source for emergency power, such as an air-driven generator, windmilling engines, batteries, or other power source capable of providing adequate power to the flight control system.

Analysis, simulation, or any combination thereof may be used to show compliance where the methods are shown to be reliable.

b. *Procedures.*

...

(5) Finally, assuming that a suitable runway is available, it should be possible to control the aeroplane until it comes to a complete stop on the runway. ~~A means of positive deceleration should be provided.~~

JUSTIFICATION: Our suggested revisions reflect and are consistent with our separate recommended changes to the NPA’s proposed 2.4.2.(f) and 25.671(d).

Additionally, the last sentence in (5), which appears to be an inappropriate and unnecessary regulation placed within the AMC, becomes redundant if the change we have recommended to the definition of “suitable runway” is accepted.

response

Partially accepted.

The first paragraph quoting the rule has been deleted.

Guidance has been added regarding ‘suitable runway’.



Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: CS 25.671(d)(4)-(5), AMC 25.671 Section 10b5

Comment: NPA AMC 25.671 Section 10b5 adds the ground controllability and deceleration capability. However, the NPA is vague in its acceptance criteria for ground control and deceleration: How much lateral deviation is allowed for ground control and still be acceptable? How much deceleration is needed to be acceptable? NPA AMC 25.671 Section 10b5 states “positive deceleration” must be provided, but if that deceleration was only 5% of normal braking deceleration, would that be acceptable?

Suggested change: Propose removal of ground controllability and deceleration capability from the effect of all-engines out on the flight control systems and leave “aircraft controllability up to the point of touchdown in a landing flare”. Reinstate the “to the point of touchdown” language from FCHWG FAR 25.671(d) and FCHWG AC 25.671 Section 10a and Section 10b1-4

EASA response: Not accepted.

Setting performance objectives for such a case is not considered to be appropriate. The demonstration of compliance is expected to be performed via a qualitative assessment of the system architecture and the system availability following total engine loss.

comment

328

comment by: Gulfstream Aerospace Corporation

8. EVALUATION OF CONTROL SYSTEM ASSEMBLY – CS 25.671 (b).

“(…)a. For control systems, the design intent should be such that it is impossible to assemble elements of the system so as to prevent its intended function. Examples of the consequences of incorrect assembly include the following:

- (1) an out-of-phase action, or
- (2) reversal in the sense of the control, or
- (3) interconnection of the controls between two systems where this is not intended, or
- (4) loss of function.”

- GAC Response:

CS 25.671(b) applies to flight control systems, the same scope should be preserved here. This section should clarify that the intent of the rule is to prevent mis-assembly from affecting the safety of flight. It may be possible to incorrectly assemble a system in such a way that the resulting installation is evidently non-functional. Aircraft with such conditions would never plausibly be dispatched.

The current text does not make it clear that the listed consequences are not acceptable.

Recommended:

a. For flight control systems, the design intent should be that it is impossible to assemble elements of the system such that the aircraft could be dispatched in a condition where the system is not capable of performing its function as intended.

b. Examples of unacceptable consequences for incorrect assembly include the following:

- (1) an out-of-phase action, or*
- (2) reversal in the sense of the control, or*
- (3) interconnection of the controls between two systems where this is not intended, or*
- (4) uncommanded motion, or*
- (5) loss of function or redundancy.*

c. Where the effects of incorrect assembly would be unmistakably evident during normal pre-flight procedures, it may be considered that the aircraft would not be dispatched in that condition.

d. Examples of unmistakably evident effects include the following:



	<p><i>(1) Jammed cockpit controls,</i> <i>(2) Severely off center cockpit controls,</i> <i>(3) Conditions resulting in caution or warning alerts that cannot be circumvented by normal operating procedures.</i></p>
response	<p>Partially accepted. There have been occurrences where conditions considered to be ‘obvious’ or ‘unmistakable’ were not identified. We agree to make it clear that the list of examples are of ‘unacceptable consequences’.</p>
comment	<p>329 comment by: Gulfstream Aerospace Corporation</p> <p>CS 25.671 (b) <i>“b. (...) The applicant should:</i> <i>(i) Analyse the assembly and maintenance of the system to assess the classification of potential failures.</i> <i>(ii) For Cat/Haz/Maj failures: Introduce Physical Prevention against mis-assembly or discuss with the Authority if Physical Prevention is not possible.</i> <i>(iii) For Minor failure or No Safety Effect: Marking alone is generally considered sufficient to prevent incorrect assembly.”</i></p> <ul style="list-style-type: none"> • GAC Response: The current text equivocates between the assembly or maintenance error and the failure condition resulting from the error. Recommended: <i>The applicant should:</i> <i>(i) Analyze the system to assess the failure conditions that could be caused by incorrect assembly or maintenance.</i> <i>(ii) For assembly or maintenance errors resulting in Cat/Haz/Maj failures, introduce physical prevention against mis-assembly, or an indication to the flight crew capable of preventing dispatch with the condition. Discuss with the Authority if neither of these solutions is possible.</i> <i>(iii) For assembly or maintenance errors resulting in Minor or No Safety Effect failure conditions marking alone is generally considered sufficient to prevent incorrect assembly.</i>
response	<p>Not accepted. An indication to the flight crew is not considered to be acceptable. There have been occurrences where conditions considered to be ‘obvious’ or ‘unmistakable’ were not identified.</p>
comment	<p>330 comment by: Gulfstream Aerospace Corporation</p> <p>CS 25.671 (c) <i>“CS 25.671(c) requires that the aeroplane be shown by analysis, tests, or both, to be capable of continued safe flight and landing following failures in the flight control system within the normal flight envelope.”</i></p> <ul style="list-style-type: none"> • GAC Response: Typo <i>“...flight envelope.”</i>
response	<p>Accepted.</p>

comment	331	comment by: Gulfstream Aerospace Corporation
	<p>10. EVALUATION OF ALL ENGINES FAILED CONDITION – CS 25.671 (d)(b)(3)(iv)</p> <p><i>“Note: If the loss of all engines has no effect on the flight control authority of the aircraft (e.g., manual controls), then the results of the basic handling qualities flight tests with all engines operating may be used to demonstrate the satisfactory handling qualities of the aeroplane with all engines failed.”</i></p> <ul style="list-style-type: none"> GAC Response: <p>Note: Loss of engines can have an effect on control authority for manually controlled propeller driven aircraft.</p>	
response	<p>Noted.</p> <p>The wording only applies when there is NO effect. The example on ‘manual controls’ has been deleted.</p>	

3. Proposed amendments - CS-25 - Book 2 - AMC 25.933(a)(1)

p. 33

comment	132	comment by: Garmin International
	<p>AMC 25.933(a)(1), Section 8.b.(2) and 8.b.(3)</p> <p>The rule recommendation proposed by the ASAWG to address specific risk had associated guidance that latent failures were to be avoided by monitoring or that dual failure combinations were to consider the addition of redundancy to reduce the effect of latency. Given that NPA section 2.4.3 and AMC 25.933(a)(1) section 8.b implies current practices have resulted in designs where neither of the dual failures is pre-existing, it would be difficult given this design precedence to use ASAWG recommendations to reduce the level of safety below that provided by AMC 25.933(a)(1) section 8.b.(2). The argument in NPA section 2.4.3 should be modified to not imply the ASAWG proposal would allow design configurations that would be avoided by current practices.</p> <p>The ASAWG limited the scope of specific risk to dual failures. It was felt by many members of the ASAWG working group that average risk adequately dealt with specific risk when considering multiple failure combinations. Given that the ASAWG rule proposal did not include multiple failure combinations, it would be possible for individual system regulations to retain guidance such as AMC 25.933(a)(1) section 8.b.(3) as it is legacy guidance that is outside the scope of the ASAWG proposed rule.</p> <p>However, on page 15, this NPA introduces CS 25.1309 (b) (4) and associated AMC material. New CS 25.1309 (b) (4) does address multiple failure combinations. It was the intent of ASAWG to have one methodology for addressing specific risk to ensure consistency and to simplify certification. If CS 25.1309 (b) (4) is retained then it is recommended that AMC 25.933(a)(1) section 8.b.(3) be removed since it involves a different methodology.</p>	
response	<p>Not accepted.</p> <p>The NPA Section 2.4.3 is part of the explanatory note and will not be republished, so no change is foreseen to be made to this section.</p> <p>It is nevertheless agreed that there was no intent in the NPA to use the ASAWG proposal in order to allow design configurations that have been avoided by current practices. This approach is reflected in the changes that have been proposed in the text of the CS and AMC of the NPA.</p> <p>Design configurations in paragraph 8.b.(2) and 8.b.(3) of AMC 25.933(a)(1) have traditionally been considered to be practicable and acceptable to EASA. This position is clearly reminded</p>	

in paragraph 8.b. of AMC 25.933(a)(1). These design configurations are not considered to involve a different methodology from the specific risk laid down in the NPA text for CS 25.1309.

Design configurations in paragraph 8.b.(2) and 8.b.(3) provide acceptable means of compliance to CS 25.1309(b)(4). No dual failure combination, either of which is latent for more than one flight, leading to a catastrophic unwanted in-flight thrust reversal, should then remain in the thrust reverser system design. As such, CS 25.1309(b)(5) is not applicable.

comment 194

comment by: *Embraer - Indústria Brasileira de Aeronáutica - S.A.*

AMC 25.933(a)(1):

As discussed during the deliberations of the ASAWG, Embraer believes that there is no technical or safety justification for the safety requirements for the thrust reversers to be more conservative than that applied to other equally critical systems. Embraer recommends that the acceptable means of compliance for CS 25.1309(b) be used for compliance to CS 25.933(a)(1)(ii).

response

Not accepted.

The NPA proposal states for CS 25.933(a)(1)(ii): 'It can be demonstrated that any in-flight thrust reversal complies with CS 25.1309(b).'

It is not intended to assign to the thrust reverser system more conservative safety requirements than the ones applied to other equally critical systems. However, in accordance with the dissenting opinions of EASA and the FAA expressed in the ASAWG report, the NPA did not make use of the ASAWG proposal to allow design configurations that have been avoided by current practices. Hence, the AMC 25.933 sections 8.b.(2) and 8.b.(3) are maintained, describing design configurations which have traditionally been considered to be practicable and deemed to be acceptable to EASA.

comment 266

comment by: *AIRBUS*

PARAGRAPH / SECTION YOUR COMMENT IS RELATED TO:

AMC 25.933(a)(1) Unwanted in-flight thrust reversal of turbojet thrust reversers

PROPOSED TEXT / COMMENT:

Replace Sections 8.b.2 and 8.b.3 of the attached with a Section 8.b.2 as follows:

whenever practical, latent failures should be avoided. It has traditionally been deemed practical to avoid catastrophic in-flight thrust reversal failure conditions due to any "single latent plus single active" (a.k.a "latent plus one") failure combination.

RATIONALE / REASON / JUSTIFICATION:

To be consistent with ASAWG recommendations.

Rationale from ASAWG Report:

QUOTE

A change to FAR/CS 25.933(a)(1)(ii) was recommended because the rule combined with recent policy implies latent specific risk criteria should be applied to thrust reversers. This policy is based on earlier ARAC recommendations currently being used and requires the review of latent related specific risk. Therefore, the introduction of the ARAC PPIHWG version of AC/ACJ 25.933 with the deletion of Sections 8.b.2 and 8.b.3 was provided to ensure consistency across the Industry and systems.

ASAWG Recommends adoption of the related ARAC PPIHWG and SDAHGW Recommendations as modified by the ASAWG recommendations made elsewhere in this report. Adoption of the ASAWG recommendations regarding FAR/CS 25.1309 would result in



a level of safety for powerplant systems at least equivalent to that provided by the current interpretation of FAR/CS 25.933(a)(1)(ii) while facilitating a more consistent and objective means of demonstrating compliance. For example, the “no single failure” requirement would be covered by the revision to FAR/CS 25.1309(b) proposed by ARAC SDAHWG and clarified by ASAWG recommendations. The avoidance of “latent plus one” failure conditions would be covered by the ASAWG recommendation to eliminate significant latent failures wherever practical. In addition the ASAWG recommendation would provide a more objective and hence consistent maximum acceptable residual risk when operating one failure away from a catastrophe.
UNQUOTE

response

Not accepted.
The NPA states for CS 25.933(a)(1)(ii): ‘It can be demonstrated that any in-flight thrust reversal complies with CS 25.1309(b).’
In accordance with the dissenting opinions of EASA and the FAA expressed in the ASAWG report, the NPA did not make use of the ASAWG proposal to allow design configurations that have been avoided by current practices. Hence, the AMC 25.933 sections 8.b.(2) and 8.b.(3) are maintained, describing design configurations which have traditionally been considered to be practical and deemed to be acceptable to EASA.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC Subpart E Powerplant

Comment: “RELIABILITY OPTION”: PROVIDE CONTINUED SAFE FLIGHT AND LANDING BY PREVENTING ANY IN FLIGHT THRUST REVERSAL, It should be pointed out that no credit is given for the consideration of fuselage mounted engines and the moments that they can produce compared to wing mounted engines. In our recent certification activity dealing with thrust reversers, the reliability option was not allowed, and Cessna had to demonstrate an in flight deployment. The effect on the aircraft and crew was not worse than minor for some flight phases, but we were not allowed to change the functional failure condition to agree with the results from flight test (!). This is not a consistent application of the requirements, and Cessna’s position that the following change “Latent failures involved in unwanted in-flight thrust reversal should be avoided whenever practical. The design configurations in paragraphs 8.b. (2) and 8.b. (3) have traditionally been considered practical and deemed acceptable to the Agency.” Cessna’s position is that this statement is not clear and unambiguous. As a result this will introduce more inconsistency from aircraft OEM to OEM and not increase the overall level of safety.

Suggested change: Recommends that this be struck or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Not accepted.

The NPA did not introduce any novelty as regards the four different means or methods regarding the specific aspects of compliance with CS 25.933(a). The changes in paragraph 8.b. only reflect that, in accordance with the dissenting opinions of EASA and the FAA expressed in the ASAWG report, the NPA did not make use of the ASAWG proposal to allow design configurations that have been avoided by current practices.

3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309 p. 33-47

comment

2

comment by: Lockheed Martin Aeronautics

6. b (1) (ii) Fail safe design concept



The changes to the wording of Paragraph 6.b (ii) on page 37, Fail-Safe Design Concept appears to be missing text, specifically; “Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless and their joint probability with the first failure is shown to be extremely improbable. The effect of combinations of failures that are not extremely improbable should not be catastrophic.” This last sentence contains a double negative and appears to be redundant since catastrophic failures are required to be extremely improbable.

response

Noted.
This last sentence has been deleted.

comment

3

comment by: Duane Kritzinger

Page 35 of 60: In para 4h I would caution against the use of the word “risk”. Risk = Probability x Severity. Furthermore, the severity criteria in 25.1309 does not cater for various degree of occupational hazards

Page 40 of 60: Para (ii) brings in the “risk” term again (where Risk should be the product of severity and probability). I suggest Residual Risk” should rather be replaced with “Residual Probability” (i.e. the average probability/FH of the failure condition given the presence of a single latent failure).

Page 41 of 60: Para c(2) states “loss of annunciation....” is a Major failure condition. I think we should also discuss the more severe “misleading annunciation” failure mode (because if the combination of misleading is CAT, then what should the single failure severity be? I think this para should maybe reference out to AC25-11 for more examples)

Page 42 of 60: Para b(4). I think it will be desirable to clarify that the “bottom up approach” is not an FHA , but probably an FMEA.

Page 42 of 60: Para (c)(2)(ii). Different phases of flight will most probably require individual FHA line entries (e.g. see evaluating the ‘all engines failed condition’ introduced by this NPA as part of changes to CS 25.671)

Page 43 of 60: Para 11(a)(4). I would replace the new word “item” with “system” instead.

response

Partially accepted.

Page 35 of 60 — Para 4h: Accepted. The word ‘risk’ is not appropriate and has been replaced by ‘effects’.

Page 40 of 60 — Para (ii): Accepted.

Page 41 of 60 — Para c(2): Noted. The purpose of the change is actually to highlight to the applicants that in such dual functional failure combination, the failure condition ‘loss of annunciation’ is expected to be classified as ‘major’, and not ‘no safety effect’ (as it has already been detected during certification reviews).

Page 42 of 60 — Para b(4): Noted. The purpose of the change reflects the current situation where increasing integrated system architectures have led applicants to perform SFHAs on shared data and resources systems, e.g. air data system, flight/ground status information.

Page 42 of 60 — Para (c)(2)(ii): Noted.

Page 43 of 60 — Para 11(a)(4): The term ‘item’ is used here in accordance with EUROCAE ED79A/SAE ARP4754A.

comment

50

comment by: UK CAA



Page No: 35**Paragraph No:** 4h

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.

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.

Proposed Text: Replace each instance of “Airplane” with “Aeroplane”.

response Accepted.

Comment from Textron Aviation (extracted from the letter attached to comment #289):Page/Paragraph: AMC 25.1309 Section 4h

Comment: Does the addition of NPA AMC 25.1309 Section 4h mean that the airplane OEM now has to consider means within the airplane/systems to prevent such external hazards? If so, does that mean some sort of sensor forward of the nacelle which would be tied into an engine’s run/stop logic? While this may potentially address the risk to ground crew, it may increase the risks to the airplane/occupants by yielding additional failure modes which could shutdown an engine in-flight. This seems to overreach the control that an OEM would have on such ground operations.

Suggested change: Propose removing external ground operations hazards to persons other than the occupants/crew. Ground operational procedures (i.e., beacons on when engines running, ground crews clearing the area around the nacelle prior to engine start, ramp markings for engine ingestion zones) are better suited to such hazards than additional airplane systems.

EASA response: Noted.

The purpose of the change is not to address workplace safety or assess ground operational procedures. The aim of paragraph 4.h is to not disregard, on a systematic basis, the effects on persons other than aeroplane occupants during ground operations, when assessing the failure conditions of the aeroplane and its systems identified in the AFHA/SFHAs.

comment 51

comment by: UK CAA

Page No: 36**Paragraph No:** 5f

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.

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.

“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.

Many entries are still made within the document to things that are “complex”; if the definition is lost, these lose their meaning.

Proposed Text: Retain the definition for Complex; include the new definition for complexity



response	<p>as a measure of how complex a function, system or item is.</p> <p>Accepted.</p> <p>'Complex' (definition deleted in the NPA): A system is complex <u>when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods.</u></p> <p>'Complexity' (definition added in the NPA): An attribute of functions, systems or items, <u>which makes their operation, failure modes, or failure effects difficult to comprehend without the aid of analytical methods.</u></p> <p>Since many entries related to the term 'complex' in the existing AMC 25.1309 were not addressed in the NPA, it has been decided to retain both definitions in the resulting text.</p>
comment	<p>52 comment by: UK CAA</p> <p>Page No: 37 Paragraph No: 8 c. (3) 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. 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. 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>
response	<p>Not accepted.</p> <p>The proposed text does not cover the case where LAT 3 pre-exists (ref. Table A5-2 of the NPA example). When LAT 3 pre-exists, the catastrophic failure condition is actually not compliant with the residual probability criterion. The non-compliance would not be identified with the proposed text.</p>
comment	<p>53 comment by: UK CAA</p> <p>Page No: 40 Paragraph No: (6) compliance with CS 25.1309(b)(4) and (5) 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. 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. 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? 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>

response	<p>Proposed Text: Revise text such that compliance is shown by the applicant</p> <p>Partially accepted. Third and fourth paragraph: entirely deleted. The paragraph that deals with compliance with CS 25.1309(b)(5) is specific to the 1 active + 1 latent combinations leading to a catastrophic failure condition. These combinations, when existing, are requested to be highlighted to EASA for acceptance early in the development and the rationale for acceptance is requested to be recorded in the system safety assessment.</p>
comment	<p>54 comment by: UK CAA</p> <p>Page No: 41 Paragraph No: c (2) Compliance with CS 25.1309(c) 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. 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. 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>
response	<p>Partially accepted. Failure conditions related to loss of protection, loss of crew alerting, or loss of systems only used as mitigations to other failure conditions or events, are on a regularly basis classified as ‘minor’ or ‘no safety effect’. The rationale used is that there is no reduction in the performance of the aeroplane (e.g. reduction in thrust), increased crew workload or reduction in safety margins (e.g. reduction in control authority, increased loads). While EASA agrees with the UK CAA comment, the intent of the proposed approach was to challenge the above rationale, particularly when the system failure/event is ‘catastrophic’ if not annunciated/mitigated. The resulting text reads: ‘[...] For example, if the effects of having a system failure and not annunciating that system failure are ‘catastrophic’, the combination of the system failure with the failure of its annunciation must be ‘extremely improbable’. The loss of annunciation should be considered to be a failure condition in itself, and particular attention should be paid to the impact on the ability of the crew to cope with the subject system failure. In addition, unwanted operation (e.g. nuisance warnings) should be assessed. [...]’</p>
comment	<p>55 comment by: UK CAA</p>

	<p>Page No: 42 Paragraph No: c. (2)(ii) 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. Justification: Output of FHA here would be the FFCC Proposed Text: Change to: “... or diversion time can adversely affect the functional failure condition classification, ...”</p>
response	<p>Partially accepted. The resulting text reads: ‘Where flight duration, flight phase, or diversion time can adversely affect the “failure condition” classification, they must be considered as intensifying factors.’</p>
comment	<p>56 comment by: UK CAA</p>
	<p>Page No: 44 Paragraph No: 11 g 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. 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 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.</p>
response	<p>Partially accepted. The wording was added to the original ASAWG sentence in order to prevent applicants from taking credit of the ‘extremely remote’ operational event/environmental condition for alleviating to the maximum extent the reliability requirements on the protection system. The concern is actually similar to the one expressed in comment #54. The referenced sentence is considered to be inadequate in the context of paragraph 11.g, and is therefore deleted in the resulting text.</p>
comment	<p>57 comment by: UK CAA</p>
	<p>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,</p>

	<p>but it cannot contain all expected crew actions which could be much higher... it should actually dictate what should be done.</p> <p>Proposed Text: "The applicant should provide a means to ensure the AFM will contain all the required crew actions."</p>
response	<p>Partially accepted.</p> <p>The resulting text reads: 'The applicant should provide a means to ensure that the AFM will contain these required crew actions that [...].'</p>
comment	<p>58 comment by: <i>Alvaro Esteban</i></p> <p><i>"(iv) the relevant 'at risk' time if an event is only relevant during certain flight phases; This should be based on the probability per flight, rather than per flight hour, for failure conditions that have a very short exposure window."</i></p> <p>Related to the new text added in paragraph (iv) it is not clear enough which is the purpose of the remark:</p> <ul style="list-style-type: none"> · Paragraph (iv) is to state that a correct "time exposure" have to be taken into account in the calculation. Why the remark is about probability? If a remark is needed, this remark should be related to the used of "time exposure" and not to the "probability per flight". <u>The "probability" of a basic event is based on the "time exposure" (and the failure rate), but the "time exposure" can never be based on the "probability".</u> · Maybe the purpose of the remark is to establish that <u>the probability of "events only relevant during certain flight phases" (e.g. takeoff, landing, etc) should be based and expressed in "probability per flight" instead of "probability per flight hour".</u> This is in accordance with former AMJ 25.1309 (see paragraph 10.b) and actual AC 25.1309.1A (see paragraph 10.b). Is this the intention of the remark for new NPA 2014-02? If answer is affirmative, which should be the quantitative safety objective for these type of "events only relevant during certain flight phases"? · This last question is also in line with "ARAC ASAWG Report Specific Risk Tasking" (see conclusions in paragraph 6.3.4.3.3), where it should be determine if AC 25.1309-1A criteria should be used or other criteria developed for latent and active failures (see paragraph 6.3.4.5.3). It is kindly requested to clarify which is EASA recommendation for these <u>"events only relevant during certain flight phases"</u>: <ol style="list-style-type: none"> 1. It is better to express probability in terms of "probability per flight", or, 2. It is better to express probability in terms of "probability per flight hour" (despite these types of events do not depend on the duration of the flight). <p>With these comments, it is considered that actual NPA 2014-02 is not clear enough regarding <u>"events only relevant during certain flight phases"</u>. Adequate update of paragraphs "11.e Calculation of Average Probability per Flight Hour (Quantitative Analysis)." and/or "APPENDIX 3 CALCULATION OF THE AVERAGE PROBABILITY PER FLIGHT HOUR" are needed in order to clarify quantitative safety objective.</p>
response	<p>Partially accepted.</p> <p>a) Accepted. The 'at risk' time is not based on probability. The remark, as written in the NPA, does not clearly convey the concern.</p> <p>b) Correct. This was the intent of the remark. For these cases where the probability per flight was requested, quantitative safety objectives were expected to be aligned with the actual AC 25.1309-1A, as currently applied per Issue Papers 'Equipment, Systems, and Installation Requirements: Use of ARAC Recommendations'. These Issue Papers recognise the AC 25.1309 Arsenal with a reservation on the probability calculation where the failure</p>

repercussions are different over the entire flight profile (i.e. to the extent that distinct failure conditions — with different classifications — are identified for specific flight phases).

c) The Systems Design and Analysis Harmonization Working Group (SDAHWG) phase I report on 25.1309, dated June 2002, mentions 'The SDAHWG recognized that the current AC25.1309-1A section 10.b could be interpreted as quantitatively considering specific risk during specific flight operations such as takeoff, landing, etc. The interpretation and application of this paragraph by industry and regulators has been inconsistent. Further, this interpretation of the paragraph was deemed to be more conservative than necessary to meet 25.1309(b) as it used the same probability criteria for specific risk and average risk. The working group agreed it should be reviewed in Phase 2 as a sub-topic of "deviation from average risk".'

In Appendix C, the SDAHWG report details the rationale for postponing the rulemaking activity to phase II, when addressing deviation from average risk concerns:

'The sentence highlighted by the FAA has been interpreted in different ways. The method outlined in the ARAC diamond AC is consistent with the accepted method used by many manufacturers today and is also presented in ARP 4761. Basically the probability calculations at FC level is made to show compliance with the quantitative objectives associated to the classification of the concerned FC.

In the proposed regulation (AC/AMJ) these quantitative requirements are expressed in "average probability per flight hour" (ex: Extremely Improbable Failure Conditions are those having an Average Probability Per Flight Hour of the order of 1×10^{-9} or less. Catastrophic Failure Conditions must be Extremely Improbable).

The existing AC allows an interpretation that specific risk methodologies should be applied. It is believed that this is too conservative for a specific operation when compared to the average probability calculation for a non-specific phase of operation.

This normalisation of the average probability calculation per flight hour allows a common base for comparison between FC, it allows also to sum the FC expected probability per system and at aircraft level. It shows that the quantitative requirements are met, on average, during the fleet life. The use of 1×10^{-9} per flight hour is derived from historical basis. If probability was expressed per flight or per flight phase, another number would have to be determined as 1×10^{-9} has no basis when quoted as a per flight probability.

Nevertheless while meeting the average per flight hour probability, one can argue that this kind of calculation is hiding the risk taken during specific flight operations like take-off and landing. This is typically a problem of specific risk calculation and limitation like the one associated with latent failure, dispatch under MMEL conditions, Consideration of maximum flight time instead of average flight time.

It is agreed that the removal of the sentence from the AC may have removed the ability for the "specific risk" interpretation to be used. It is agreed that this needs to be revisited in phase 2 with all the other issues associated with Deviation from Average Risk concern.'

As reminded in this comment (#58), the ASAWG Specific Risk Tasking report, dated April 2010, whose aim was to address the 'issues associated with Deviation from Average Risk concern', indicates in Section 6.3.4.5.3. Risk during actual at-risk time versus normalising by flight length (AC 25.1309-1A v AC 25.1309 Arsenal Version): 'The recommendation to resolve the third fundamental issue is to use AC 25.1309 Arsenal Version paragraph 11.e.(1) for average risk. For specific risk, determine if AC 25.1309-1A criteria should be used or other criteria developed for latent and active failures.'



For the time being, without any additional material to substantiate a change back to 'probability per flight', EASA accepts not to modify the current calculation of average probability per flight hour, i.e. as introduced by the AC 25.1309 Diamond version.

comment 62 comment by: *Thales Avionics- JD Chauvet*

AMC25.1309 4.g. "CS 25.1309 is always applicable to flight conditions, but only applicable to ground conditions when the airplane is in service": this sentence is unclear, should the term "only" term be replaced by "also"?
=> clarify the sentence

response Noted.
CS 25.1309 is proposed to be applicable to ground conditions only when the aeroplane is in service.

comment 63 comment by: *Thales Avionics- JD Chauvet*

AMC25.1304.h. to avoid confusion, avoid the term "threat" which is now a term dedicated to security domain
=> replace "threat" for example by "fear"

response Not accepted.
The term 'fear' is not considered to be adequate.

comment 64 comment by: *Thales Avionics- JD Chauvet*

CS25.13094.h. considering that "threats to people on the ground or adjacent to the airplane during ground operations" can induce that "designs may be considered non-compliant", it is unacceptable for industrials to let this section with such uncertainty within the risk acceptability level.
=> clarify the acceptability level or remove the section

response Please refer to the response to comment #151.

comment 65 comment by: *Thales Avionics- JD Chauvet*

6. b. (ii) "The effect of combinations of failures that are not extremely improbable should not be catastrophic": such demonstration is industrially not feasible in term of workload considering that "failures" can be understood at any design level (equipment, board, electronic component, gate, etc.), that each probability combination would have to be evaluated in term of exposure time and dormancies, etc..
=> remove this sentence

response Partially accepted.
EASA agrees with the concern. Please refer to the response to comment #2 for the resulting text.

comment 66 comment by: *Laurent Lalaque*

Proposed change



In the top of page 37 of 60, paragraph 6. b. (1) (ii), we strongly disagree with the proposed text and we propose to remove the last sentence which is a trap:

"The effect of combinations of failures that are not extremely improbable should not be catastrophic."

Justification

Indeed, in order to verify this requirement on the analyzed system, a new "bottom up" activity will be required. This will consist in combining all the potential failures of the system, evaluating the effects of this double failure state of the system and, in case of catastrophic effect, checking that the quantitative combination is extremely improbable. Imagine the number of combinations to be analyzed for a system with only 1000 failure modes => Practically not feasible.

response

Partially accepted.

EASA agrees with the concern. Please refer to the response to comment #2 for the resulting text.

comment

67

comment by: *Thales Avionics- JD Chauvet*

8. (3) "when either one is pre-existing": by definition, for scenarios including latent failures, the latent failures shall always occur before the none latent failures. This part of the sentence may be confusing for the reader.

==> remove "when either one is pre-existing"

response

Partially accepted.

The phrase 'when either one is pre-existing' was considered to be adequate for that sentence. However, CS 25.1309(b)(5)(ii) being revised as a result of other comments, the sentence of concern in section 8.c.(3) of the AMC is modified accordingly.

The resulting text reads: '(3) Given that a single latent failure has occurred on a given flight, each *catastrophic failure condition*, resulting from two failures, either of which is latent for more than one flight, is remote.'

comment

68

comment by: *Laurent Lalaque*

Proposed change

In addition to the pages 39, 40 and 41, in the paragraph (6) Significant Latent Failures, a guidance should be defined for the particular case of the power plant system. Should the engine manufacturer during engine certification define the list, details, and justification of all latent failures that could be involved in a CAT aircraft level FC ? Note that CS-E does not consider, at present time, any CAT failure condition.

Justification

When analyzing the power plant system of a twin-engine aircraft, a case of CAT failure condition, in particular flight phases, is the complete loss of one engine (due to a single failure) combined with a latent failure that leads to a non-availability of the maximum power on the remaining engine on request. The presence of latent failures is a particular concern for engines for which the maximum rating power cannot be directly tested in service (example: OEI ratings, the worst case being 30 second OEI ratings) and remains a concern for engines periodically tested at that maximum power. Note that the list of possible latent failures precipitated during the usage of the maximum power could be quite significant for a complete engine. The justification of the acceptability for each one at aircraft level Authority, should require early coordination between Aircraft level Authority, Engine level Authority, Aircraft manufacturer and Engine manufacturer. Note that a case by case combination

	<p>analysis of all the combinations is probably a heavy activity due to the number of possible combinations of failures between both engines (the number of order 2 minimal cut sets is largely higher than one hundred for above mentioned FC). Note that the latent failures precipitated during a maximum power rating usage could be caused by a significant list of parts from various engine modules or accessories : compressors, combustion chamber, turbines, sensors, actuators,</p>
response	<p>Not accepted.</p> <p>The NPA does not introduce any new approach/concept when certifying an aeroplane against CS-25. The aeroplane manufacturer remains responsible for demonstrating compliance with CS 25.1309.</p> <p>The aeroplane manufacturer may issue additional specifications to the engine manufacturer to address significant latent failures, particularly for compliance with CS 25.1309(b)(5).</p>
comment	<p>69 comment by: <i>Thales Avionics- JD Chauvet</i></p> <p>8.b.(6)(i): according to definition 4.v. "significant latent failure" concept applies to hazardous and catastrophic FCs. Considering that 9.b.(6)(ii) addresses catastrophic FCs, it must be clarified that 9.b.(6)(i) applies to hazardous FCs.</p> <p>==> at the beginning of 9.b.(6)(i) clarify that it applies to hazardous FCs</p>
response	<p>Not accepted.</p> <p>It is agreed that according to definition 4.v., the 'significant latent failure' concept is limited to latent failures involved in hazardous and catastrophic failure conditions.</p> <p>However, section 9.b.(6)(i) applies to any significant latent failure, not only to hazardous failure conditions.</p>
comment	<p>70 comment by: <i>Laurent Lalaque</i></p> <p><u>Proposed change</u></p> <p>At the bottom of page 43, paragraph e. (1) (v) Calculation of average probability per flight hour (Quantitative Analysis), we strongly disagree and we propose to leave "average" instead of "maximum" in the sentence "the maximum exposure time if the failure can persist for multiple flights."</p> <p>In the page 56, in the paragraph 4.5.4, the assessment of the economic impact for options 1, 2 and 3 does not reflect the very significant additional costs of dividing by 2 the periodicity of preventive maintenance inspections, induced by replacing "average" by "maximum" (see the justification hereafter).</p> <p><u>Justification.</u></p> <p>1 - As mentioned in another Turbomeca comment on pages 39, 40 and 41, the number of latent failures is significant, and the dormancies are not all the same due to different kind and different periodicity of preventive maintenance actions that are requested to limit at a certain level the non-availability of the maximum rating power when requested. It is not realistic to consider that, simultaneously on the same engine, all latent failures are in the same engine, the same flight, at their maximum of dormancy, that is to say just the flight before the maintenance action.</p> <p>2 - Even for just one order two minimum cut set leading to a CAT FC, using the "maximum exposure time" is not consistent with the spirit of computing an "average probability".</p> <p>3 - With this new practice, taking into account the maximum exposure time into the SSA would lead to divide by 2 the periodicity of most of the periodic preventive maintenance</p>

	inspections. This would lead to a serious impact at operators level, organizations, maintenance costs ...and then a significant economic impact has to be taken into account in the paragraph 4.5.4 economic impact.
response	Please refer to the response to comment #61.
comment	<p>71 comment by: <i>Laurent Lalaque</i></p> <p><u>Proposed change</u> Page 46, in the appendix 3 paragraph b (1), the added text underlined in grey should be removed, or completed by developing more accurately what is recommended for non constant failure rates in the cases of a simple failure, a combination of failures, ..., on one aircraft computation risk, for the fleet risk, etc</p> <p><u>Justification</u> Considering the failure rates after infant mortality and prior to wear-out supports the modelling of a constant and mature failure rate, which simplifies a lot the computation specially when the FC results from combinations of failures. This modelling fits relatively well the field data for electronic components. But for non-electronic components/parts/equipment/accessories, for a particular failure mode of a part, this modelling is a simplification. Most mechanical components cumulate damage via different and concurring failure mechanisms up to one failure. On a given aircraft, a combination of non-electronic component failures is quite difficult to compute as the computation should consider the history of each component. And as a part of this history is often common to all components, due to the fact that they are exposed to the same ageing conditions (same environmental conditions, stresses, cycling, etc) their ageing/wearing processes are stochastically dependent. The computation is not simple and can be approached by different methods, assumptions, conditions, etc. If you open the door to such more realistic estimation, you should better define the related conditions and criteria of acceptability. For instance, in this case, is the general failure rate traditional approach (with the 1.0 10⁻⁹ per flight hour criteria for CAT events) appropriate and sufficient? Concerning the wording "average probability per flight hour", is it for the last flight of one aircraft before the inspection (repair)? In which configuration are the aged parts for this particular aircraft? Is it for the whole fleet and at which age (age distribution)? A lot of questions arise. Note that as far as we know, integrating wearing into the SSA computation is, at present time, not the intent of the current draft of the ARP4761A, nor an industry current practice. But it seems obvious that any intent to harmonize methods, conditions, assumptions, criteria would be appreciated.</p>
response	<p>Partially accepted.</p> <p>As discussed in the ASAWG report, the first paragraph of Appendix 3.b.(1) along with the NPA proposed text intends to convey that conducting an analysis using a time-dependent failure rate is not required if the applicant has established life limits or other restrictions to ensure that the failure rate is constant.</p> <p>The Weibull analysis is an example of reliability analysis as meant in that paragraph. This analysis is added as an example in the resulting text.</p>
comment	<p>72 comment by: <i>Thales Avionics- JD Chauvet</i></p> <p>8.b.(6)(i): according to definition 4.v. "significant latent failure" concept applies : 1) to hazardous and catastrophic FCs. Considering that 9.b.(6)(ii) addresses catastrophic FCs,</p>

	<p>it must be clarified that 9.b.(6)(i) applies to hazardous FCs. 2) to dual failure scenarios. This cutset order is not clearly recall in 9.b.(6)(i) ==> at the beginning of 9.b.(6)(i) clarify that it applies to hazardous FCs and dual failure scenarios</p>
response	Please refer to the response to comment #69.
comment	<p>73 comment by: <i>Thales Avionics- JD Chauvet</i></p> <p>8.b.(6)(i): use of "maximum time" is inconsistent with average probability computation detailed in AMC25.1309 11.e. and Appendix3 ==> replace "maximum time" per "average time"</p>
response	Please refer to the response to comment #61.
comment	<p>74 comment by: <i>Thales Avionics- JD Chauvet</i></p> <p>8.b.(6)(ii): use of "maximum time" is inconsistent with average probability computation detailed in AMC25.1309 11.e. and Appendix3 ==> replace "maximum time" per "average time"</p>
response	Please refer to the response to comment #61.
comment	<p>75 comment by: <i>Thales Avionics- JD Chauvet</i></p> <p>11.e.(iv) "This should be based on the probability per flight, rather than per flight hour, for failure conditions that have a very short exposure window.": this approach is in complete contradiction with the quantitative safety objective definition and equations established in Appendix3 c. and d. ==> remove the sentence</p>
response	Please refer to the response to comment #58.
comment	<p>76 comment by: <i>Thales Avionics- JD Chauvet</i></p> <p>11.e.(v) removal of "average" and replacement by "maximum" this approach is inconsistent with average probability computation detailed in AMC25.1309 11.e. and Appendix3 ==> come back to previous sentence</p>
response	Please refer to the response to comment #61.
comment	<p>77 comment by: <i>Thales Avionics- JD Chauvet</i></p> <p>11.g. "Single failures ...provide protection against the events." too constraining comparing to current architectures and unrealistic considering that some failures of the protection system may be annunciated to flight crew who may limit aircraft exposure to associated environmental conditions or apply specific procedures ==> remove the sentence.</p>
response	Partially accepted.

For the reasons detailed in the response to comment #56, the referenced sentence is considered to be inadequate in the context of paragraph 11.g, and therefore it has been deleted in the resulting text.

comment	<p>78 comment by: <i>Thales Avionics- JD Chauvet</i></p> <p>Appendix 3 b.(1) "For components whose probability of failure may be associated with non-constant failure rates within the operational life of the aircraft, reliability analysis may be used to determine component replacement times. and In either case, the failure rate" it is unrealistic to generalize the principle of replacement time to all failures without the restriction to their contribution to catastrophic or hazardous FC and when contributing to a first or second order cutset ==> remove the sentence</p>
response	<p>Not accepted. The first paragraph of Appendix 3.b.(1) is of general nature, applicable to any failure condition for which a quantitative analysis is performed.</p>
comment	<p>133 comment by: <i>Garmin International</i></p> <p>AMC 25.1309, Section 4.b The changes to AMC 25.1309 section 4.b are not part of the ASAWG recommendations. The particular concern with these changes relates to deletion of text referencing CS 25.571. It is assumed that the reference to CS 25.571 is used to justify that certain failure modes are not credible. For example, a longitudinal concentric crack of a ball screw nut that would allow the nut to move independently of the actuator screw. However, without a rationale for the proposed change the impact of this change cannot be fully assessed. It is recommended that this change is not made without justification.</p>
response	<p>Noted. The above-referenced change to AMC 25.1309 reflects the NPA changes to CS 25.671(c) and AMC 25.671(c)(1).</p>
comment	<p>134 comment by: <i>Garmin International</i></p> <p>AMC 25.1309, Section 6.b.(1)(ii) The changes to AMC 25.1309 section 6.b.(1)(ii) are not part of the ASAWG recommendations. The particular concern relates to the replacement of the word "unless" with the word "and". The original text is well understood as it has been present in the advisory material for a considerable period of time. It is not clear why a change is necessary. The proposed change implies that subsequent failures should be assumed and be shown to be extremely improbable even if the failure effect is not catastrophic. It is recommended that the original text (i.e., "and") be retained.</p>
response	<p>Partially accepted. Some applicants have used the original text as rationale for not performing FHAs on combinations of related systems. The sentence —as proposed in the current AMC 25.1309— is then considered to be misleading. It is agreed that the current NPA text needs clarification. The original text will, however, not be reinstated. Please refer to the response to comment #2 for the resulting text.</p>

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: § AMC 25.1309 6.b.(1)(ii)

Comment: “Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, ~~unless~~ **and** their joint probability with the first failure is shown to be extremely improbable.”

The wording of this sentence seems awkward as indicated by the mark-up. It could be read to imply that all subsequent failures, regardless of probability, must be assumed to happen on the same flight. This would be an unbounded requirement with no real value to the safety process so we assume this is a wrong reading of it and request that it be clarified.

Suggested change: Correct and/or clarify requirement

EASA response: Partially accepted.

Please refer to the response to comment #2 for the resulting text.

comment	<p>135</p> <p style="text-align: right;">comment by: <i>Garmin International</i></p> <p>AMC 25.1309, Section 6.c.(1)</p> <p>The changes to AMC 25.1309 section 6.c.(1) are not part of the ASAWG recommendations. The particular concern relates to the replacement of the words “non-complex” with “non-integrated”, and “complex” with “integrated”. Complexity and integration are different aspects of a design. Although integration and complexity show a level of correlation, it is inappropriate to equate the two as the same. It is quite possible for a non-integrated system to be complex and integrated system to be non-complex. For example, deterministic risk assessment can still be applied to integrated systems which involve analog and discrete signals. The limitations of deterministic risk assessment and application of assurance techniques depends more on whether the system contains complex components rather than the level of integration. The effects of integration are more relevant to independence between functions. It is recommended that the original text (i.e., “non-complex” and “complex”) be retained.</p>
response	<p>Partially accepted.</p> <p>The resulting text reads:</p> <p>‘A concern arose regarding the efficiency and coverage of the techniques used for assessing safety aspects of aeroplane and system functions implemented through the use of electronic technology and software-based techniques. The concern is that design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for these aeroplane and system functions. Thus, other assurance techniques, such as development assurance utilising a combination of integral processes (e.g. process assurance, configuration management, requirement validation and implementation verification), or structured analysis or assessment techniques applied at the aeroplane level and across integrated or interacting systems, have been requested. Their systematic use increases confidence that development errors, and integration or interaction effects, have been adequately identified and corrected.’</p>
comment	<p>136</p> <p style="text-align: right;">comment by: <i>Garmin International</i></p>

	<p>AMC 25.1309, Section 9.b (1)(vii)</p> <p>The change to AMC 25.1309 section 9.b (1)(vii) is not part of the ASAWG recommendations. This paragraph seems to be related to FHA failure effects. What is meant by the term “operational sequences” added to this paragraph? Crew cues and corrective action are mentioned in the preceding paragraph so it does not seem to be related to the crew response to failures. If this text is not in reference to crew procedures then this should be clarified.</p>
response	<p>Partially accepted.</p> <p>It is correct that the text does not refer to crew procedures. The aim of the change is to address the sequences of events/failures when relevant.</p> <p>E.g. System failure A occurs before system failure B --> this sequence leads to one failure condition versus system failure B occurs before system failure A --> this sequence leads to another failure condition since here the consequences can be mitigated by crew action, thanks to a specific flight deck effect displayed when system failure B occurs first.</p> <p>The resulting text is clarified and reads as follows: ‘(vii) The resulting effects on the aeroplane and occupants, considering the stage of flight, the sequence of events/failures occurrence when relevant, and operating and environmental conditions.’</p>
comment	<p>137 comment by: <i>Garmin International</i></p> <p>AMC 25.1309, Section 9.b (4)</p> <p>The changes to AMC 25.1309 section 9.b (4) are not part of the ASAWG recommendations. The particular concern relates to deleting the words “more complex”. As is implied by the definition, complexity is an attribute of system which makes failure modes difficult to identify, which therefore makes it difficult to determine all system states, etc. It is recommended that the original text (i.e., “more complex”) be retained.</p>
response	<p>Accepted.</p> <p>The original text is retained.</p>
comment	<p>138 comment by: <i>Garmin International</i></p> <p>AMC 25.1309, Section 9.b (6)(i)</p> <p>The AMC established hierarchy of safety objectives for managing exposure time and the definition of significant latent failure does not account for the number of failures in the failure sequence leading to the failure condition. The scope of AMC 25.1309 section 9.b (6)(i) is not bounded. At what point is a latent failure no longer considered “significant”? It is recommended that if the associated rule is retained, that this AMC provide additional guidance regarding what latent failures are significant.</p>
response	<p>Not accepted.</p> <p>A latent failure is considered to be significant as soon as it contributes to a failure condition the classification of which is more severe than ‘major’.</p>
comment	<p>139 comment by: <i>Garmin International</i></p> <p>AMC 25.1309, Section 9.b (6)(i)</p> <p>The AMC 25.1309 section 5.v definition of “significant latent failure” addresses both Hazardous and Catastrophic failure conditions and the number of failures in a failure sequence is not restricted when determining that a latent failure is significant. This covers all</p>

latent failures. Is the AMC 25.1309 section 9.b (6)(i) 1/1000 criteria associated with maintenance intervals required to be tracked as certification maintenance requirements (CMRs)? This is a method of compliance to a new rule.

It is recommended that if the associated rule is retained that this AMC provide guidance whether or not the maintenance intervals associated with the 1/1000 criteria are to be tracked as CMRs.

response

Not accepted.

The scheduled maintenance tasks derived from the '1/1000' criterion of AMC 25.1309 section 9.b (6)(i) are required to be tracked as candidates for certification maintenance requirements (CCMRs).

comment

140

comment by: *Garmin International*

AMC 25.1309, Section 9.b (6)(i) & (6)(ii)

AMC 25.1309 section 9.b (6)(ii) guidance has been modified from the ASAWG recommended guidance. It is the method of calculation associated with latent failures that determines whether a fault tree analyses top event probability represents average probability. Both AMC 25.1309 section 9.b (6)(i) and (6)(ii) change this method of calculation when performing specific risk. The analysis of specific risk criteria will likely be based on the data output from fault tree analyses. Since an applicant is not going to go back and forth changing how latent probabilities are calculated, from a practical implementation perspective, AMC 25.1309 section 9.b (6)(i) and (6)(ii) are forcing a change in the method of calculation in meeting 10-9, 10-7. This proposed change is not necessary to control deviation and, therefore, is not recommended.

response

Please refer to the response to comment #61.

comment

141

comment by: *Garmin International*

AMC 25.1309, Section 9.c

The change to AMC 25.1309 section 9.c is not part of the ASAWG recommendations. There are failure conditions where there is no dedicated warning (e.g. misleading navigation). In such situations, indications (e.g., course deviation) or the system operating condition (e.g., blank display) are used by the crew to recognize an unsafe condition. Such failures are considered inherently detectable by the crew.

The current discussion is limited to airplane responses such as control loads, aerodynamic response and aircraft noise, etc. It is recommended that AMC 25.1309 section 9.c should expand on inherent detection. For example:

The required information can be provided by annunciation or be inherently detectable. Annunciations are defined as any crew alerting mechanism (e.g., acoustic, visual or feel) purposely included in the design of the aircraft to inform the crew of an existing or impending problem. Inherent detection is defined as determinations that the crew may make of the status of the aircraft from instrument crosscheck, obvious loss of equipment, or cues that result from the process of flying the aircraft, such as visual references, control loads, aerodynamic response, and aircraft noise.

response

Partially accepted.

Using the term 'aeroplane responses' was not meant to be limited to responses such as control loads, aerodynamic response and aircraft noise, etc. The text is amended so that the ambiguity is removed.



The resulting text reads: 'The required information may be provided by dedicated indication and/or annunciation or made apparent to the crew by the inherent aeroplane/systems responses.'

comment

142

comment by: *Garmin International*

AMC 25.1309, Section 9.c (2)

The change to AMC 25.1309 section 9.c (2) is not an ASAWG recommendation. The Major Classification requirement for loss of annunciation is not consistent with the AFHA and SFHA process or the AMC 25.1309 classification definitions.

The assessment of the loss of annunciation by itself would not necessarily be considered Major. This is because the failure of annunciation does not necessarily create a Major condition because here has been no system failure; therefore, there is no reduction in capability of the airplane (e.g. reduction in thrust), increased crew workload or reduction in safety margins (e.g. reduction in control authority, increased loads).

Differences in classification can occur such as when considering loss of annunciations for systems that can increase situational awareness to crew error, terrain or proximity to ground since these situational awareness problems are not necessarily associated with system functional failures. However these cases would be identified and addressed during the AFHA/SFHA process. Each failure condition effect and applicable classification is addressed on its own merit.

More severe probability requirements are allocated based on the combined failure condition in a similar manner to how AFHA requirements are allocated to the systems that contribute to a specific airplane level function. The SSA process will ensure both the individual and combined failure condition requirements are met. Therefore, the requirement for the annunciation system to meet Major for a Catastrophic failure condition that includes loss of annunciation is arbitrary and outside the AMC 25.1309 process and thus should be deleted.

response

Please refer to the response to comment #54.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: § AMC 25.1309 9(c)

Comment: "The required information may be provided by dedicated indication and/or annunciation or made apparent by the inherent airplane responses."

This is a reasonable statement but it directly conflicts the proposed language of the rule which does not allow for "inherent airplane responses". We would suggest changing the rule to recognize additional methods of providing information to the flight crew.

Suggested change: Modify 25.1309(c) to allow credit for crew information from sources other than "alerting systems" per 25.1322.

EASA response: Accepted.

CS 25.1309(c) has been amended to include: 'When flight crew alerting is required, it must be provided in accordance with CS 25.1322.'

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: § AMC 25.1309 9(c)



Comment: “Any system operating condition which, if not detected and properly accommodated by crew action, would contribute to or cause one or more serious injuries should be considered as an ‘unsafe system operating condition’.”

This would seem to require yet another system of classification for the hazards to the aircraft. Is there a compelling safety case for not aligning this requirement with established hazard classifications under 25.1309?

Suggested change: Align unsafe system operation condition effects with other 25.1309 criteria.

EASA response: Please refer to the response to comment #251.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: § AMC 25.1309 9(c)(2)

Comment: “but the loss of annunciation should be considered a major failure condition”

The NPA provides no real justification for this requirement. There are many cases where the best design solution is a robust means of providing a function (like 10E-7) and then a single path warning system (10E-4) for the rare3 time that robust solution fails. How is this less safe (note that the example actually meets 10E-11 if adequately independent) than a 10E-5 solution with a 10E-5 annunciation?

Suggested change: Remove added requirement of annunciation being “major”.

EASA response: Please refer to the response to comment #54.

comment 143

comment by: *Garmin International*

AMC 25.1309, Section 10.b (4)

The change to AMC 25.1309 section 10.b (4) is not an ASAWG recommendation. It is recommended that the new sentence be removed based on the following discussion.

The FHA is a top-down thought process that starts with the description of the aircraft/system functions. One interpretation or application of the new sentence would be to turn the FHA into a bottom-up FMEA type activity. If functions are expressed at too detailed a level this would increase the FHA development process significantly. The objective of the FHA is not to describe detailed aspects of the design. The new statement is more relevant to Common Cause Analysis.

CCA addresses the following type of failures, errors or external events:

- A cause that can trigger several failures occurring (almost) simultaneously
- A cause that can lead to cascading unit or system failures
- A cause in which several units fail in the same way.

The CCA analysis can identify failure conditions in addition to those previously identified during the FHA process since the CCA methodologies can trace failure mode effects across multiple system boundaries where the interactions between functions, system and items are complex. The CCA validates that the common cause failure, error or event is within the assigned probabilities objective and, is minimized or precluded in accordance with the relevant regulatory guidance. Typical CCA activities include common connector analysis, common sensor analysis, rotorburst, etc.

response Partially accepted.

EASA recognises that the term ‘bottom-up’ may be misleading when used in the context of functional hazard assessment.

As described above, new failure conditions may be identified due to the implementation.



These failure conditions need to be assessed and classified in accordance with CS 25.1309. The resulting text reads: ‘However, with the increasing integrated system architectures, this traditional top-down approach should be performed in conjunction with common-cause considerations (e.g. common resources) in order to properly address where one system contributes to several aeroplane-level functions.’
This text is consistent with the draft ARP4761A Appendix B PASA.

comment 144 comment by: *Garmin International*

AMC 25.1309 section 10.c. (2)(ii) includes proposed text that was not part of the ASAWG recommendations. Specifically the sentences: “To correlate with the crew’s annunciation requirements in CS 25.1309(c), consider the case of the crew taking action and also the effects if they do not. If their inability to take action results in an unsafe system operating condition, crew annunciations and evaluation of crew responses should be considered. See CS 25.1309(c) and paragraph 9c of this AMC for more detailed guidance on those considerations.”

These sentences are included under a discussion related to FHA effects and associated classifications. Typically, when assessing flight crew actions in the FHA it is normal practice to assume that credit can be taken for crew corrective action (e.g. follow the AFM procedure) if the crew is not under excessive workload and the actions are not considered complicated. The un-annunciated failure condition addresses the scenario when corrective crew action is not performed in a timely manner or not at all.

The location of the quoted proposed text in this section is potentially contradictory. The first sentence “To correlate with the crew’s annunciation requirements in CS 25.1309(c), consider the case of the crew taking action and also the effects if they do not” can be interpreted that for the annunciated failure conditions, no alleviation can be provided for crew action.

The proposed text is more relevant to the CS 25.1309 (c) discussions and should be moved to AMC 25.1309 section 9.c. Additionally, it is recommended that the proposed text be clarified to indicate that the crew taking action corresponds to the annunciated failure conditions and the crew not taking corrective action refers to the un-annunciated failure conditions.

response Please refer to the response to comment #255.

comment 145 comment by: *Garmin International*

AMC 25.1309 section 11.e (1)(iv) includes proposed new text that “[‘at risk’ time] should be based on the probability per flight, rather than per flight hour, for failure conditions that have a very short exposure window.”

The proposed new text reverses a SDAHWG change to the AC/AMC 25.1309 advisory circular, which related to when and when not to normalize the average probability per flight. For a system, a 10-hour flight will always provide a worse probability per flight than a 1-hour flight, assuming the same operational conditions. The “per flight hour” expression provides a more accurate apples-to-apples comparison of aircraft design across different model types. When addressing average probability there are typically multiple failures making up each failure sequence. A failure that occurs during a short exposure window weights less when considering an airplane model with a long average flight duration versus another airplane model with a shorter average flight duration. However, the longer flight time increases the probability of failure per flight.

The AMC 25.1309 section 11.e (1)(iv) change to how average probability is expressed does not fall within the NPA section 2.2 objectives and it is recommended that it be deleted.



response Please refer to the response to comment #58.

comment 146 comment by: *Garmin International*

AMC 25.1309, Section 11.e (1)(v)

The change to AMC 25.1309 section 11.e (1)(v) strikes out “average” exposure time and replaces it with “maximum” exposure time. The ASAWG did not recommend changing the average probability per flight hour calculation. If this change is made then all references to average probability will have to be removed from this AMC since average probability is no longer being calculated. The NPA section 2.2 objectives do not include replacing average probability as a means of showing compliance to 10-9, 10-7, etc. Therefore, the AMC 25.1309 section 11.e (1)(v) change is not recommended.

response Please refer to the response to comment #61.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: § AMC 25.1309 11e.(1)(v)

Comment: Note that the title of 11.e is “Calculation of average [emphasis added] Probability per Flight Hour”: what is the justification for using “maximum” exposure time for latent failures?

Suggested change: Remove change to “maximum” exposure time for latent failures; return it to “average”.

EASA response: Please refer to the response to comment #61.

comment 147 comment by: *Garmin International*

The AMC 25.1309 section 11.g changes include a change that was not part of the ASAWG recommendations. Specifically the sentence “In these limited cases, it is acceptable to classify the single failure as at least major, to ensure adequate development assurance and reliability for the systems that provide protection against the events.”

It should be noted that most individual avionics units do not have a MTBF>100,000 (FR<1E-5). Further, the Major classification would actually be correlated to a function which would be implemented by multiple components whose sum would have to be <1E-5. This new Major classification requirement basically prohibits single failures in combination with operational or environmental conditions and is not consistent with ASAWG recommendations. How would existing systems such as loss of stick pusher meet this requirement? Typically loss of stick pusher is 1E-4 when in combination with entry into stall (Remote). It is recommended that the quoted text be deleted.

response Partially accepted.
For the reasons detailed in the response to comment #56, the referenced sentence is considered to be inadequate in the context of paragraph 11.g, and is therefore deleted in the resulting text.

comment 148 comment by: *Garmin International*

AMC 25.1309, Section 11.g

HIRF and lightning should not be considered as one of the environmental conditions required to be met in combination with a single point failure. While the NPA has removed HIRF and



lightning from the Appendix 4 list, it may not be clear once the final guidance is published that HIRF and lightning was considered and removed since it is not intended to apply to it. To address this issue, it is recommended that a new sentence be added as follows (the new sentence is in red):

“Appendix 4 is provided for guidance and is not intended to be exhaustive or prescriptive. **HIRF and lightning does not need to be considered in combination with a single failure. ...**”

Concerns related to the need to meet single failure in combination with HIRF & Lightning include:

The assessment required in determining the single point failures under HIRF & lightning are endless due to numerous protections that the aircraft and equipment have. The requirement for Level A systems is to have an integrated test, to show compliance, that often includes a significant number of LRUs with complex architectures. It would be very difficult to quantify single point failures for assessment for a LRU and is further complicated by integrated systems. For any single point failures that can be identified, the assessment is difficult to analyze and would most likely force additional testing with simulated failures. This effort of testing for single point failures would lead to high cost and the time to do the testing would be impractical to support Certifications given the typical long times it takes to run testing. Garmin does not believe that the benefit of meeting such a requirement warrants the cost and complexity with which the systems would need to be designed, tested and Certified.

Some examples of consideration for single point failure that is considered to be impractical include:

1. Does the loss of shielding on wire cause it to be susceptible? Which wire or wires? Is it at the unit connector, at the interposing connector (which one if more than one)? etc.
2. Degraded or loss of electrical bonding (within LRU and on aircraft).
3. Does the failure of any filtering component on the I/O cause the unit to not function? If so, which component? Note in many cases it is unknown whether the IO protection (EMI filtering, lightning suppressors, etc.) is helping or whether something further downstream is preventing the upset. Often these protection devices are inherently incorporated as good design practices. The only true way to know if they help is to test with and without this I/O protection.
4. Is there anything downstream of the I/O protection that can lead to the unit upsetting?
5. Aircraft level HIRF and lightning testing that determines equipment and wiring test level will need to take into account single failures at the installation level that may lead to higher threats on the aircraft.

response

Not accepted.

The concern is acknowledged, but the proposed change is not accepted. Indeed, although the ASAWG deliberated on the exception of HIRF and Lightning from CS 25.1309, a consensus was not achieved due to dissension from all the involved certification authorities (ANAC, EASA, FAA, and TCCA).

The conclusion from the ASAWG report on the related Garmin dissenting opinion (5) reads: ‘With the exception of removing HIRF and Lightning from the Appendix 4 table for reasons noted above, status quo for H/L considerations should be maintained until that proposed future committee addresses them.

Because the failures of HIRF and Lightning protection features are often latent, clear guidance should be provided as to whether qualitative evaluation of failure conditions involving protection features is adequate, and if so, how should such qualitative evaluation



be performed. Establish a basis for a qualitative assessment of the architecture to confirm that it is robust and it can withstand such risk [...].’

comment

151

comment by: Dassault Aviation

Dassault-Aviation comment page #35

Extract:**AMC 25.1309(4) Applicability of CS 25.1309.**

(g) CS 25.1309 is always applicable to flight conditions, but (...)

(h) Risks to persons other than airplane occupants should be taken into account when assessing failure conditions in compliance with CS 25.1309. Such risks include threats to people on the ground or adjacent to the airplane during ground operations, electric shock threats to mechanics, and other similar situations. Because such risks are usually less significant in comparison with the risk to the airplane and its occupants, applicants have not typically addressed these risks in demonstrating compliance with CS 25.1309. However, designs may be considered non-compliant due to an unacceptable potential threat to persons outside the airplane or to line mechanics.

Comment:

Dassault-Aviation do not concur with this amended text. It is not consistent with the current criteria established for determining the failure condition severity based exclusively upon the effects on the aeroplane and its occupants (passengers and flight crew).

Such a proposition would require revising deeply AMC 25.1309. Particularly it would mean to revise all the severity definitions to be consistent with the consideration of the effect on ground people.

Requested Change:

Remove these paragraphs. Note that design rules basically take into account potential threat to persons outside the airplane. So it does not bring any significant gap in safety improvement. Also such an amendment would lead to multiple inconsistencies in AMC 25.1309.

response

Not accepted.

As explained in the FAA NPRM draft preamble from 2002, there has long been a question as to whether risks to persons other than aeroplane occupants should be taken into account when assessing compliance with FAR/CS 25.1309.

Without being prescriptive on the failure condition classification, the AMC 25.1309 paragraph 4.h. is meant to request the applicants not to ignore the effects on persons other than aeroplane occupants, particularly when these effects are significantly more severe than the ones on the aeroplane and its occupants.

comment

152

comment by: Dassault Aviation

Dassault-Aviation comment page #36

Extract:**AMC 25.1329(4)(r)**

r. *Latent Failure*. A failure is latent until it is made known to the flight crew or maintenance personnel. ~~A significant latent failure is one, which would in combination with one or more specific failures, or events result in a Hazardous or Catastrophic Failure Condition.~~

Comment:

Dassault-Aviation suggests distinguishing short-term latent failures from long-term ones that may help the safety practitioners when applying the specific risks criteria.



response	<p>Requested Change: Dassault-Aviation propose to introduce these additional definitions: <i>Short-term Latent Failure.</i> A latent failure whose exposure time is not longer than one flight duration (e.g. detected and signaled to the flight crew before the beginning of next flight thanks to a preflight test). <i>Long-term Latent Failure.</i> A latent failure that cannot be qualified as “short-term latent”.</p> <p>Not accepted. The proposed change would lead to inconsistencies in CS-25, and would adversely affect harmonisation efforts with foreign authorities.</p>
comment	<p>153 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment page #37</p> <p>Extract: AMC 25.1309(6)(b)(1)(ii) (ii) Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless and their joint probability with the first failure is shown to be extremely improbable. The effect of combinations of failures that are not extremely improbable should not be catastrophic.</p> <p>Comment: Last sentence (as it is worded) may imply a “bottom up” activity requiring to assess every failure combinations. It would be a heavy task with a non-negligible economic impact. The usual approach consists in checking that any catastrophic failure condition is extremely improbable (top down).</p> <p>Requested Change: Dassault-Aviation suggests the removal of the added sentence.</p>
response	<p>Partially accepted. EASA agrees with the concern. Please refer to the response to comment #2 for the resulting text.</p>
comment	<p>154 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment page #37</p> <p>Extract: AMC 25.1309(8)(c)(3) (3) each Catastrophic Failure Condition, resulting from two failures, either of which is latent for more than one flight, is remote when either one is pre-existing.</p> <p>Comment: This paragraph is not fully consistent with the specific risk criteria proposed in CS 25.1309(b)(5).</p> <p>Requested Change: Dassault-Aviation suggest to reuse the same wording than the one used for CS 25.1309(b)(5) to be homogeneous.</p>
response	<p>Accepted. The sentence of concern in the AMC section 8.c.(3) is modified in accordance with the revised CS 25.1309(b)(5)(ii).</p>

comment	<p>155 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment page #40</p> <p>Extract: AMC 25.1309(9)(b)(6)(i) (B) For each significant latent failure_which cannot be practically eliminated, the latency should be limited to a probability of 1/1000, and (C) For each remaining significant latent failure where the 1/1000 criterion cannot be practically met, the latency should be minimised.</p> <p>Comment: A significant latent failure is defined as a latent failure that would, in combination with one or more specific failures or events, results in Hazardous or Catastrophic Failure Condition. No additional criterion is provided to delimitate the analysis on the failure combinations involved in Hazardous or Catastrophic Failure Conditions. Being the huge quantity of minimal cutsets that may exist, it means compliance with AMC 25.1309(9)(b)(6)(i) would be impracticable without excessive extra costs so as to deal with all possible combination failures. To reasonably limit the analysis to carry out, Dassault-Aviation suggests to focus only on dual-failure situations (it is consistent with CS 25.1309(b)(5)) and whose occurrence probability is more than 1E-12/fh. This latter proposition is consistent with ARAC ASAWG results.</p> <p>Requested Change: State that verifying CS 25.1309(b)(5) is an acceptable means of compliance for CS.251309(b)(4) and revise AMC associated to 25.1309(b)(5) to exclude dual-failure combinations whose probability occurrence is less than 1E-12/fh (as being far from extremely improbable).</p>
response	<p>Not accepted.</p> <p>AMC 25.1309 section 9.b(6)(i) deals with compliance with CS 25.1309(b)(4). This part of the AMC only addresses the significant latent failures taken individually. There is therefore no investigation to be performed on combinations other than the ones being within the scope of CS 25.1309(b)(5).</p>
comment	<p>156 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment page #40</p> <p>Extract: AMC 25.1309(9)(b)(6)(i) The probability value 1/1000 is the product of the <u>maximum time</u> the failure is allowed to be present and its failure rate.</p> <p>Comment: Dassault-Aviation position for computing the occurrence probabilities of latent failures is to use the average probability, that is to say the product of the average time (and not the maximum time) the latent failure is expected and its failure rate. A different approach would be not consistent with ARP 4761, ARAC ASAWG and more particularly with the 25.1309 probability criteria that are defined as average probabilities per flight hour. It may also lead to unjustified constraints on maintenance (economic impact).</p> <p>Requested Change: Modify “maximum time” by “average time”.</p>
response	<p>Please refer to the response to comment #61.</p>

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.1309 Section 9b6i

Comment: NPA AMC 25.1309 Section 9b6i seems needlessly circular and vague, with opportunities for inconsistent application among OEMs.

First, “A” says significant latents should be eliminated to the extent practical. “B” says if it cannot be practically eliminated, the latency should be $<1/1000$ (i.e., failure rate * inspection interval). “C” says that if “1/1000” cannot be practically met, it should be minimized. This seems like a circular argument: minimize to be less than 1/1000 unless it can't be less than 1/1000, in which case minimize.

Second, if the “Significant Latent Failure” definition of NPA AMC 25.1309 5v really is intended to capture ALL latent failures in ANY fault tree leading to HAZ/CAT are considered Significant, imposing the 1/1000 criteria on EACH of those Significant latent failures in the fault tree will likely force shorter inspection intervals (which may increase chances to introduce failures as part of the inspection). Furthermore, the resulting top event probability is likely to be significantly less than $10e-9$; and what is gained by making an extremely improbable event even more extremely improbable?

Third, the last paragraph of NPA AMC 25.1309 Section 9b6i says that dedicated compliance with the “significant latent failures” provisions above is not expected to be a dedicated demonstration of compliance, but rather only “where the Agency identifies a...failure of concern and deems it practical to eliminate or further reduce the exposure...” This seems to mean that compliance is “not required, until it is required by the agency” with the onus on the applicant to justify impracticality of meeting 1/1000.

If minimization criteria are to be the standard, then it should state such. If a 1/1000 criteria is to be the standard, then it should state such.

Suggested change: Propose the 1/1000 standard be applied (per the FCHWG) at the top-event level, not at the component failure level of the latent failure. As worded, it is neither. Furthermore, if it is to be a standard, then it should be applied rather than to state a “standard” which later is described as “not expect a demonstration of compliance” which seems to not be a standard.

EASA response: Partially accepted.

First point: Not accepted. The draft AMC is not considered to provide a circular argument: 1) eliminate the significant latent failure, 2) reduce the exposure time so that the occurrence probability of the significant latent failure does not exceed 1/1000, 3) should the maintenance task be too complex or invasive so that it cannot be performed safely during an A- or B-check, propose an exposure time where the latent failure may be serviced at a suitable maintenance facility.

Second point: Accepted. Section 9.b.(6) is completely reviewed. The 1/1000 criterion is withdrawn from compliance with CS 25.1309(b)(4). It is however kept for compliance with CS 25.1309(b)(5). The intent of CS 25.1309(b)(4) is better served by 1) eliminating significant latent failures to the extent practicable (refer to AMC 25-19 paragraph 8), and 2) limiting the latency of the remaining significant latent failures for compliance with CS 25.1309(b) (refer to AMC 25-19 paragraph 10).

Third point: Accepted. The paragraph is deleted.



Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC Subpart F – Equipment, AMC 25.1309 (b) (6)(i)

Comment: Last paragraph. “The Agency does not expect a dedicated demonstration of compliance with CS 25.1309(b) (4). The minimization of significant latent failures is rather expected to be an integral part of each applicant’s normal design practices. During review of the system safety analyses that demonstrate compliance with the other provisions of CS 25.1309(b), if the Agency identifies a significant latent failure of concern and deems it may be practical to eliminate or further reduce the exposure to that latent failure, then the applicant will be required to provide justification of impracticality. Justifications should be based on past experience, sound engineering judgment, or other reasonable arguments”. Cessna does not support this position for several reasons; first, it is subject to interpretation by the regulatory agency. So it will not be uniformly applied, what may be OK for one applicant based on subjective criteria, may not be acceptable for another. This does not support the goal of a harmonized approach for safety and could drive changes to type design after a product has entered into service on one design, adding costly design changes without a commiserate benefit to safety, while not requiring any design changes to the other. Second, EASA seems to blurring the lines between the finding of compliance and the showing of compliance. This will likely lead to a discussion with the authorities on when an applicant is done. Again, both of these requirements for showing compliance to the rule are not clear and unambiguous

Suggested change: Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Accepted.

The referenced paragraph has been deleted.

comment	157	comment by: <i>Dassault Aviation</i>
	<p>Dassault-Aviation comment page #40</p> <p>Extract:</p> <p>AMC 25.1309(9)(b)(6)(ii)</p> <p>(ii) Compliance with CS 25.1309(b)(5)</p> <p>(...)</p> <p>Comment:</p> <p>No probability limitation is retained in this guidance whereas ARAC ASAWG proposed a quantitative threshold for the dual-failure combinations to address (based on a cost benefit analysis).</p> <p>Requested Change:</p> <p>Dassault-Aviation suggest to take credit from the ARAC ASAWG results concluding that the failure combinations whose probability is less than 1E-12/FH may not be addressed. It should be added to this AMC.</p>	
response	<p>Not accepted.</p> <p>The applicability of CS 25.1309(b)(5) is limited to the combination of two failures, either of which is latent for more than one flight, resulting in a catastrophic failure condition. The 10⁻¹² statistical fallout was therefore no longer considered.</p>	
comment	158	comment by: <i>Dassault Aviation</i>
	<p>Dassault-Aviation comment page #40</p> <p>Extract:</p>	

AMC 25.1309(9)(b)(6)(ii)

(ii) Compliance with CS 25.1309(b)(5)

(...)

Comment:

This AMC may involve an excessive effort in additional substantiations to provide because the amount of failures and failure combinations may be in some cases very important.

Especially, it requires processing the minimal cutset sorting so as to be able to identify those where a common latent failure may be involved. When a failure condition includes hundreds or thousands of minimal cutsets, it may become a very expensive task with a non-negligible economic impact.

Requested Change:

Dassault-Aviation suggests the revision of this AMC (and the attached appendix 5) so as to include an alternative method based on the study of significant minimal cutsets considered individually. As a proposition, the use of a 10^{-6} /fh criterion (on each minimal cutset) instead of 10^{-5} /fh (on the summed minimal cutsets given a common latent failure) may be considered as an acceptable means of compliance.

response

Noted.

This AMC describes the acceptable means for demonstrating compliance with the requirement of CS 25.1309(b)(5)(ii). As usual, the means described in this AMC are not mandatory. Other means may be proposed by the applicant to demonstrate compliance with CS 25.1309(b)(5)(ii).

Comment from Textron Aviation (extracted from the letter attached to comment #289):Page/Paragraph: AMC 25.1309 Section 9b6ii

Comment: NPA AMC 25.1309 Section 9b6ii also applies a dual standard of 1/1000 on the latency itself (as does Section 9b6i), as well as “remote” on the other failure of the dual failure combination leading to HAZ/CAT. Assuming Section 9b6i stands and the circular argument with it resolved the 1/1000 on the latency in Section 9b6ii is redundant as it is already covered under Section 9b6i. Furthermore, imposing an additional “remote” criteria is more severe than the former “single + probable” interpretation, which only required failure rates less than $10e-5$, since existing AMC 25.1309 Section 7c1ii defines “remote” as a failure rate less than $10e-5$ but greater than $10e-7$. However, the last paragraph of NPA AMC 25.1309 Section 9b6ii seems to redefine “remote” as being $10e-6$, not $10e-5$.

The language of NPA AMC 25.1309 Section 9b6ii is confusing as it speaks to “the sum of all subsequent single active failures” and yet the opening sentence of Section 9b6ii says it’s for “CAT...involving two failures...” If it were conditions of two failures, one of which could be remote, then there would be no “sum of subsequent failures”...there would be merely “the remaining active failure.” Either this applies to specific cases of two failures leading to a CAT, in which case the remaining failure would have to pass the “remote” criteria (i.e., there would be no “summing” of one failure rate), or if the “sum of subsequent failures” must pass “remote” criteria, then is this really limited to special cases where only two failures could lead to CAT?

The math at the end of NPA AMC 25.1309 Section 9b6ii 4th paragraph mixes probability and failure rate, which neglect the flight duration. The original intent of FCHWG’s “1/1000” was to also capture the remaining flight time in the calculation. Meaning that the top event probability be 1/1000, which for a long duration flight would drive the need for lower failure rates depending on the flight duration. In other words, flight duration is taken into account in the 1/1000 probability. The NPA places a “probability of 1/1000” on the latent failure, claiming that it would drive the active failure’s failure rate...as well as stating that the “remote” criteria on the active failure could drive the failure rate of latency in order to meet its 1/1000...but neither description considers the flight duration.



Suggested change: Propose striking the NPA language in favor of a broad “1 in 1000” criteria, as proposed by FCHWG, which inherently includes the flight duration, and would cover the underlying reason for the NPA addition, in a more straightforward manner. There appears to be nothing gained by a “remote” as well as a “1/1000” criteria.

EASA response: Not accepted.

Two criteria are implemented in the CS: limit latency and limit residual probability. Limit latency is intended to limit the time of operating with a latent failure present. This is achieved by requiring that the occurrence probability of the latent failure does not exceed 1/1000. Limit residual probability is intended to limit the average probability per flight hour of the failure condition given the presence of a single latent failure. This is achieved by defining the residual probability to be remote. Residual probability is the combined average probability per flight hour of all the single active failures that result in the catastrophic failure condition assuming one single latent failure has occurred.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC Subpart F – Equipment, AMC 25.1309 (b) (6)(ii)

Comment: Do not support the following statement, “In numerical terms, compliance with CS 25.1309(b)(1) and CS 5.1309(b)(5) together means the residual risk, i.e. the sum of all subsequent single active failures, must be on the order of 1×10^{-6} per flight hour when the latency is limited to 1/1000 to satisfy the Extremely Improbable safety objective. Conversely, if the reliability of the only residual component is 1×10^{-5} per flight hour, then latency is limited to a maximum probability of 1×10^{-4} ”. During the ASAWG tasking, no consensus could be reached on what was meant by “on the order of”. Industry had one perspective that worked for their sized product and the regulators had a different perspective that “would be acceptable” but there was no overlap between the two groups. Since there was no consensus, an industry member that signs up for this does not have a clear set of requirements to design to. So again, harmonization does not apply; the pass fail criteria are not clear and unambiguous.

Suggested change: Recommend that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Not accepted.

The term ‘on the order of’ has already been used for many years in AMC 25.1309. The NPA does not intend to change the current interpretation of this term. Please refer to AMC 25.1309, section 11.e.(4). In the example, when the occurrence probability of the significant latent failure is 1/1000, the extremely improbable safety objective (on the order of 1.10^{-9} per FH) is developed into a safety requirement of the same nature towards the residual probability part (i.e. on the order of 1.10^{-6} per FH).

comment 159

comment by: Dassault Aviation

Dassault-Aviation comment page #41

Extract:

AMC 25.1309(9)(c)(2)

For example, if the effects of having a failure and not annunciating that failure are Catastrophic, not only must the combination of the failure with the failure of its annunciation must be Extremely Improbable, but the loss of annunciation should be considered a major failure condition in and of itself due to the impact on the ability of the crew to cope with the subject failure.

Comment:

Dassault-Aviation do not concur with this proposal (out of the scope of the ARAC ASAWG and



FCHWG results).

Especially the new added criterion may have some adverse effects on safety interests because it may lead to transfer effort for demonstrating compliance to 25.1309 towards the annunciation system rather than the system function itself whose failure is undesired.

Indeed, in the example given, it is requested that the loss of a failure annunciation should have a probability less than 1E-05/FH (consistent with major severity) if, this failure not detected can lead to catastrophic effects whose safety target is set to 1E-09/FH.

Dassault-Aviation position is that it is preferable to privilege the system robustness to the undesired failure whereas the amendment proposed tends to balance demonstrating efforts between the system function and its failure annunciation means.

Also from a DAL point of view, this change in AMC 25.1309 do not support any improvement since ED79A already requires DAL no lower than C for contributors involved in a catastrophic FC.

Requested Change:
Dassault-Aviation suggest not adding any change to this paragraph.

response Please refer to the response to comment #54.

comment 160 comment by: Dassault Aviation

Dassault-Aviation comment page #41

Extract:

AMC 25.1309(9)(c)(6)

Comparison with similar, previously approved systems is sometimes helpful. However, what is feasible and practical can change with time and circumstances.

Comment:

Only a minor remark on wording. The added sentence is deemed to have a too general sense to be exploitable. Dassault-Aviation understand that technical context may evolve and should be taken into account if new reliable failure monitoring and indication systems are available.

Requested Change:

Dassault-Aviation suggests the alternative wording:

“Comparison with similar, previously approved systems is sometimes helpful. However the use of periodic maintenance or flight crew checks may have been preferred at a given time, because the technical context did not offer any other alternative. But if new technical context allows practical and reliable failure monitoring and indications, such solutions should be preferred in lieu of periodic maintenance or flight crew checks previously retained.”

response Partially accepted.
There is indeed room for improvement in the current NPA text.
The resulting text reads: ‘Comparison with similar, previously approved systems is sometimes helpful. However, if a new technical context allows practical and reliable failure monitoring and indications, such solutions should be preferred in lieu of periodic maintenance or flight crew checks.’

comment 161 comment by: Dassault Aviation

Dassault-Aviation comment page #40

Extract:

AMC 25.1309(11)(e)(1)

The calculation of the Average Probability per Flight Hour for a Failure Condition should consider:



	<p>(...)</p> <p>(iv) the relevant 'at risk' time if an event is only relevant during certain flight phases;</p> <p>This should be based on the probability per flight, rather than per flight hour, for failure conditions that have a very short exposure window.</p> <p>Comment: Interpretation of this extract is not evident. Especially "This should be based". With what refers the word "this"? Do we have to understand that normalizing per flight hour may be done or not?</p> <p>Requested Change: No requested change. Additional explanation request only.</p>
response	<p>Noted.</p> <p>The NPA text was meant to convey that the normalisation by the mean flight duration should not be done for very short exposure window.</p>
comment	<p>162 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment page #43</p> <p>Extract: AMC 25.1309(11)(e)(v) the average maximum exposure time if the failure can persist for multiple flights.</p> <p>Comment: Dassault-Aviation position for computing the occurrence probabilities of latent failures is to use the average probability, that is to say the product of the average time (and not the maximum time) the latent failure is expected and its failure rate. A different approach would be not consistent with ARP 4761, ARAC ASAWG and more particularly with the 25.1309 probability criteria that are defined as average probabilities per flight hour. It may also lead to unjustified constraints on maintenance (economic impact).</p> <p>Requested Change: Keep the wording "average exposure time".</p>
response	<p>Please refer to the response to comment #61.</p>
comment	<p>163 comment by: Dassault Aviation</p> <p>Dassault-Aviation comment page #45</p> <p>Extract: AMC 25.1309(12)(a) The applicant should provide a means to ensure that the AFM will contain all the expected crew actions.</p> <p>Comment: In the CS 25.1309 perimeter, it should be precised that it should be provided a means to ensure that the AFM will contain all the expected crew actions that are used as mitigation factor in the hazard classification or that are taken as assumptions to limit the exposure time of failures.</p> <p>Requested Change: Dassault-Aviation propose the following text: "The applicant should provide a means to ensure that the AFM will contain all the expected crew actions that may be used as mitigation factor in the hazard classification or that may be taken as assumptions to limit the exposure time of failures."</p>

response	Partially accepted. The resulting text reads: 'The applicant should provide a means to ensure the AFM will contain these required crew actions that have been used as mitigation factors in the hazard classification or that have been taken as assumptions to limit the exposure time of failures.'
comment	164 comment by: Dassault Aviation Dassault-Aviation comment page #46 Extract: AMC 25.1309(appendix 3) For components whose probability of failure may be associated with non-constant failure rates within the operational life of the aircraft, reliability analysis may be used to determine component replacement times. (...) Ageing and wear of similarly constructed and similarly loaded redundant components directly leading to or when in combination with one other failure leads to a catastrophic or hazardous failure condition should be assessed when determining scheduled maintenance tasks for such components. Comment: Current analyses are based with the assumption that the failure rates are constant. Maintenance policy ensures that failure rates remain constant within the aircraft operation life. Basically, the determination of replacement times are based upon manufacturer experience supported by tests such as endurance or stress tests. This is part of the state of the art. Some items have failure modes due to aging and wear that could lead directly or in combination with one other failure to a Catastrophic Failure Condition. Scheduled mandatory replacements of these items during the operational life of the aircraft ensure that safety requirements are met. The Airworthiness Limitation Items (ALI) are documented in the Airworthiness Limitation Section. Requested Change: Developing model to determine non-constant failure rates may involve economic impacts as it will require revising the current computation methods. For this reason, Dassault-Aviation suggest to remove this text or to provide a detailed guidance to be discussed.
response	Please refer to the response to comment #71.
comment	195 comment by: Embraer - Indústria Brasileira de Aeronáutica - S.A. AMC 25.1309 – 9(b)(4): To more clearly define what is impractical or impossible, Embraer suggests that Paragraph 9.b.4 of the AMC 25.1309 be revised to say "For integrated systems, exhaustive testing may be impractical, or even impossible, because all of the system states cannot be determined, or be impractical because of the number of tests which must be accomplished."
response	Not accepted. Paragraph 9.b(4) is considered to be sufficiently clear to convey the concern.
comment	236 comment by: Boeing Page: 35



Paragraph: AMC - SUBPART F - EQUIPMENT
 AMC 25.1309 -- System Design and Analysis
 4. APPLICABILITY OF CS 25.1309

The proposed text states:

“g. CS 25.1309 is always applicable to flight conditions, but only applicable to ground conditions when the airplane is in service (that is, from the time the airplane arrives at a gate or other location for pre-flight preparations, until it is removed from service for shop maintenance, storage, etc.). While this does include conditions associated with line maintenance, dispatch determinations, embarkation and disembarkation, taxi, or the like, it does not include periods of shop maintenance, storage, or other out of service activities.”

REQUESTED CHANGE:

“g. CS 25.1309 is always applicable to flight conditions, but only applicable to ground conditions when the airplane is in service (that is, from the time the airplane ~~arrives at a~~ pushes back from the gate ~~or other location for pre flight preparations,~~ until it returns to the gate. ~~is removed from service for shop maintenance, storage, etc.). While this does include conditions associated with line maintenance, dispatch determinations, embarkation and disembarkation, taxi, or the like, it does not include periods of shop maintenance, storage, or other out of service activities.”~~”

JUSTIFICATION: When the airplane is at the gate under maintenance control/operation, the airplane may not be configured for normal part 25 operation and, as such, part 25 requirements should not be made to apply during such operation. If there is a specific concern during this phase of airline maintenance, then perhaps that is what should be addressed.

response

Not accepted.

As explained in the FAA NPRM draft preamble from 2002, there has long been a question as to whether effects on persons other than aeroplane occupants should be taken into account when assessing compliance with FAR/CS 25.1309. Such effects include, for example, threats to people overflown or adjacent to the aeroplane during ground operations, electric shock threats to mechanics, and other similar situations. Because such effects are usually insignificant when compared with the effects to the aeroplane and its occupants, applicants have not typically addressed these effects in demonstrating acceptable means of compliance with CS 25.1309. Consequently, this has been mistakenly interpreted to mean that such effects need not be considered at all.

The period of time as proposed by Boeing ‘from the time the airplane pushes back from the gate until it returns to the gate’ would not include preflight phase where the APU is operated.

comment

237

comment by: Boeing

Page:35

Paragraph: AMC - SUBPART F - EQUIPMENT
 AMC 25.1309 -- System Design and Analysis
 4. APPLICABILITY OF CS 25.1309

The proposed text states:

“h. Risks to persons other than airplane occupants should be taken into account when assessing failure conditions in compliance with CS 25.1309. Such risks include threats to



people on the ground or adjacent to the airplane during ground operations, electric shock threats to mechanics, and other similar situations. Because such risks are usually less significant in comparison with the risk to the airplane and its occupants, applicants have not typically addressed these risks in demonstrating compliance with CS 25.1309. However, designs may be considered non-compliant due to an unacceptable potential threat to persons outside the airplane or to line mechanics.”

REQUESTED CHANGE: Delete this entire text.

JUSTIFICATION: This proposed text goes beyond the current regulatory requirements. CS 25.1309 requirements apply to occupants of the airplane. The proposed text in this advisory material expands the requirements of CS 25.1309 outside of the intended operation of the airplane.

response Please refer to the response to comment #151.

comment 238 comment by: *Boeing*

Page: 36
Paragraph: *AMC - SUBPART F - EQUIPMENT*
AMC 25.1309 -- System Design and Analysis
5. Definitions

The proposed text states:

“k. Error. An omission or incorrect action by a crewmember or maintenance personnel, or a mistake in requirements, design, or implementation.”

REQUESTED CHANGE:

“k. Error. An omission or incorrect action by a crewmember or maintenance personnel, or a **development error** [a mistake in requirements, design, or implementation].”

JUSTIFICATION: Make use of the new definition for "development error."

response Partially accepted.
The resulting text reads: ‘k. Error. An omission or incorrect action by a crewmember or maintenance personnel, or a development error (i.e. a mistake in requirements determination, design, or implementation).’

comment 239 comment by: *Boeing*

Page: 36
Paragraph: *AMC - SUBPART F - EQUIPMENT*
AMC 25.1309 -- System Design and Analysis
5. Definitions

The proposed text states:

“v. Significant Latent Failure. A latent failure that would, in combination with one or more specific failures or events, results in a Hazardous or Catastrophic Failure Condition.”

REQUESTED CHANGE:

“v. Significant Latent Failure: A **latent** failure that ~~would, in combination with one or more specific failures or events,~~ **can be latent and could** results in a ~~Hazardous or~~ Catastrophic



Failure Condition [when combined with another single failure on a given flight.](#)"

JUSTIFICATION: The concept of "significant latent failure" is unique to catastrophic failure conditions per CS 25.1309(b)(5). There are no proposed criteria for hazardous two failure combinations. There are no proposed criteria for three (or more) failure combinations.

response

Not accepted.

The concept of 'significant latent failure' is not unique to catastrophic failure conditions. This is not a novelty brought by this NPA that the term 'significant latent failure' also addresses latent failures involved in hazardous failure conditions.

comment

240

comment by: Boeing

Page: 36

Paragraph: AMC - SUBPART F - EQUIPMENT
AMC 25.1309 -- System Design and Analysis
5. Definitions

REQUESTED CHANGE:

In the Definitions section and several other places throughout the proposed AMC, correct the use of the term "latency" to address probability (since this is how it is used in the rule), and not both probability and exposure time (as it is currently used in this proposed AMC). Revise "latency period" in definitions to read "**latent exposure time**" and use this throughout when describing the exposure time for latent failures.

JUSTIFICATION: The word "latency" is sometimes used for the exposure time and sometimes used for the probability of the significant latent failure in the AMC. Examples:

- Page 40, First Paragraph, latency is used as probability: "For each significant latent failure which cannot be practically eliminated, the latency should be limited to probability of 1/1000."

- Page 40, Last Para: latency is used to relate to exposure: "Two criteria are implemented in the CS, limit latency and residual risk. Limit latency is intended to limit the time of operating with a latent failure present."

Use of this term should be correct and consistent throughout the proposed document.

response

Accepted.

The use of the term 'latency' will be corrected and made consistent throughout AMC 25.1309. The term is meant to describe the exposure time of the latent failure. Section 9.b.(6) is updated accordingly. The resulting text reads:

'The rationale should be based on past experience, sound engineering judgment or other arguments, which led to the decision not to implement other potential means of avoidance (e.g. eliminating the significant latent failure or adding redundancy).'

'In numerical terms, compliance with CS 25.1309(b)(1) and CS 25.1309(b)(5) together means that the residual probability, i.e. the sum of all subsequent single active failures, must be in the order of 1×10^{-6} per flight hour when the occurrence probability of the significant latent failure is limited to 1/1000 to satisfy the *extremely improbable* safety objective. Conversely, if the residual probability is 1×10^{-5} per flight hour, then the occurrence probability of the significant latent failure is limited to a maximum probability of 1×10^{-4} .'

comment

241

comment by: Boeing



Page: 37
 Paragraph: AMC - SUBPART F - EQUIPMENT
 AMC 25.1309 -- System Design and Analysis
 6. Background
 b. Fail-Safe Design Concept.
 6.b.(1)(ii)

The proposed text states:

“(ii) Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, ~~unless~~ **and** their joint probability with the first failure is shown to be extremely improbable.”

REQUESTED CHANGE:

Return to the original wording:

“(ii) Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, ~~unless~~ ~~and~~ their joint probability with the first failure is shown to be extremely improbable.”

JUSTIFICATION: The change as proposed makes the sentence incorrect; the original wording should be retained.

response Please refer to the response to comment #134.

comment 242

comment by: Boeing

Page:37
 Paragraph: AMC - SUBPART F - EQUIPMENT
 AMC 25.1309 -- System Design and Analysis
 6. Background
 c. Development of Aeroplane and System Functions
 6.c.(1)

The proposed text states:

“(1) A concern arose regarding the efficiency and coverage of the techniques used for assessing safety aspects of systems that support aeroplane-level functions and have failure modes with the potential to affect the safety of the aeroplane. The current trend in aeroplane and system design is an increasing level of integration between aeroplane functions and the systems that implement them, particularly through the use of electronic technology and software-based techniques. While there can be considerable value gained when integrating systems with other systems, the increased complexity yields increased possibilities for development errors. The concern is that design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex non-integrated systems may not provide adequate safety coverage for more complex integrated systems. Thus, other assurance techniques, such as development assurance utilising a combination of integral processes (e.g. process assurance, configuration management, requirement validation and implementation verification or structured analysis or assessment techniques applied at the aeroplane level and across integrated or interacting systems, have been applied. Their systematic use increases confidence that development errors and integration or interaction effects have been adequately identified and corrected.”

REQUESTED CHANGE:

“(1) ~~A concern arose regarding~~–The efficiency and coverage of the techniques used for



assessing safety aspects of ~~systems that support aeroplane-level functions and have failure modes with the potential to affect the safety of the aeroplane~~ highly integrated systems that perform complex and interrelated functions may not adequately address development errors. The current trend in aeroplane and system design is an increasing level of integration between aeroplane functions and the systems that implement them, particularly through the use of electronic technology and software-based techniques. While there can be considerable value gained when integrating systems with other systems, the increased complexity may yields increased possibilities for development errors. ~~The concern is that design and analysis~~ Deterministic techniques traditionally applied to ~~deterministic risks or to~~ conventional, ~~non-integrated~~ systems may not provide adequate safety coverage for more integrated systems. Thus, other assurance techniques, such as development assurance utilising a combination of integral processes (e.g. process assurance, configuration management, requirement validation, and implementation verification) or structured analysis or assessment techniques applied at the aeroplane level and across integrated or interacting systems, have been applied. Their systematic use increases confidence that development errors and integration or interaction effects have been adequately identified and corrected.”

JUSTIFICATION: The proposed wording makes the “concern” too broad, as it loses its tie to complexity and tends to broad-brush all systems related to an airplane-level function. All systems are related to an airplane-related function, even if that function is, for example, to entertain and accommodate passengers.

response Please refer to the response to comment #135.

comment

243

comment by: Boeing

Page: 37
 Paragraph: *AMC - SUBPART F - EQUIPMENT*
AMC 25.1309 -- System Design and Analysis
8. Safety Objective
8.c.(3)

The proposed text states:

“(3) Each Catastrophic Failure Condition, resulting from two failures, either of which is latent for more than one flight, is remote when either one is pre-existing.”

REQUESTED CHANGE:

“(3) Each Catastrophic Failure Condition, resulting from two failures, either of which is latent for more than one flight, is remote. when either one is pre-existing. **For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, (1) it is impractical to provide additional fault tolerance; and (2) given any single latent failure has occurred, the catastrophic failure condition due to the sum of all subsequent single failures is remote, and (3) the product of the maximum time the latent failure is expected to be present (per occurrence) and its rate of occurrence does not exceed 1/1000.**”

JUSTIFICATION: As proposed, paragraph 8.c.(3) is confusing in that it paraphrases only part of the CS 25.1309 (b)(5) requirement [i.e., (CS 25.1309 (b)(5)(ii)]. We recommend repeating the requirement verbatim.

[Note in that our previous comments we recommend deleting 25.1309.b.5.(i); if that recommendation is accepted, then it should be deleted here as well.]



response Partially accepted.
 Section 8. ‘Safety Objective’ mainly describes the inverse relationship between the average probability per flight hour and the failure condition classification. The additional value of section 8.c is to introduce the ‘no single failure criterion’ as a safety objective for Catastrophic Failure Conditions.
 While CS 25.1309(b)(5)(i) and CS 25.1309(b)(5)(iii) must be complied with (fully addressed in section 9.b), it was considered to be equally confusing to present these requirements as safety objectives for catastrophic failure conditions. These two requirements are indeed applicable at the level of the contributing failures rather than the top-level event.
 The text has nevertheless been revised so that consistency is ensured with CS 25.1309(b)(5)(ii).

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC Subpart F – Equipment, AMC 25.1309

Comment: “8. SAFETY OBJECTIVE (c) (3) Each Catastrophic Failure Condition, resulting from two failures, either of which is latent for more than one flight, is remote when either one is pre –existing”. Cessna objects to the change based on the industry position voiced by ASAWG that this could lead to a “balanced fault tree” requirement where, for small part 25 business jets, the business model (i.e. warranty costs) drive us to design systems in that manner. Other, larger, OEMs don’t have the same business model (scheduled airlines) and the “balanced trees” concept was not identified by ASAWG as a problem that ASAWG needed to address. This appears to be an attempt by EASA to “back door” a requirement to address a perceived problem. Again, where is the problem statement?

Suggested change: Recommends that this be struck or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Not accepted.

The AMC section 8.c.(3) is considered to reflect the ASAWG recommendation on residual probability.

comment	<p>244</p> <p>Page:38 Paragraph: AMC - SUBPART F - EQUIPMENT AMC 25.1309 -- System Design and Analysis 9. Compliance with CS 25.1309 a. Compliance with CS 25.1309(a)</p> <p>The proposed text states: “(4)... If the possible impacts, including failure modes or effects, are questionable, or isolation between systems is provided by complex means, more formal structured evaluation methods may be necessary.”</p> <p>REQUESTED CHANGE: Delete the sentence.</p> <p>JUSTIFICATION: As proposed, this is a potential expansion of CS 25.1309(a) that is already addressed by CS 25.1309(b). This is an unnecessary change.</p>	comment by: <i>Boeing</i>
response	<p>Not accepted.</p> <p>This sentence is deemed to be adequate when considering the complete change proposed in the NPA, i.e. including the sentence right before ‘Normal installation practices should result</p>	

in sufficiently obvious isolation of the impacts of such equipment on safety that substantiation can be based on a relatively simple qualitative installation evaluation.'

comment

245

comment by: Boeing

Page:38

Paragraph: AMC - SUBPART F - EQUIPMENT

AMC 25.1309 -- System Design and Analysis

9. Compliance with CS 25.1309

b. Compliance with CS 25.1309(b)

9.b.(1)(vii)

The proposed text states:

“(vii) The resulting effects on the airplane and occupants, considering the stage of flight, the operational sequences, and operating and environmental conditions.”

REQUESTED CHANGE:

“(vii) The resulting effects on the airplane and occupants, considering the stage of flight, ~~the operational sequences~~ operating procedures, and operating and environmental conditions.”

JUSTIFICATION: The proposed NPA text adds the new phrase “*the operational sequences*,” it is not clear what is intended, as this is a vague term not used elsewhere in the AMC. We recommend using more familiar and consistent wording, such as procedures, crew interactions, etc., if that is what is intended.

response

Please refer to the response to comment #136.

comment

246

comment by: Boeing

Page: 39

Paragraph: AMC - SUBPART F - EQUIPMENT

AMC 25.1309 -- System Design and Analysis

9. Compliance with CS 25.1309

b. Compliance with CS 25.1309(b)

9.b.(4) [second unnumbered paragraph]

The proposed text states:

“Guidelines, which may be used for the assignment of Development Assurance Levels of aeroplanes and system functions up to items (hardware and software elements), are described in the document referenced in paragraph 3b(2). Through this document, the Agency recognises that system architecture (e.g. functional or item development independence) may be considered for the assignment process.”

REQUESTED CHANGE:

“Guidelines, which may be used for the assignment of Development Assurance Levels of aeroplanes and system functions ~~up to items~~ including ~~(hardware and software items elements)~~, are described in the document referenced in paragraph 3b(2). Through this document, the Agency recognises that system architecture (e.g. functional or item development independence) may be considered for the assignment process.”

JUSTIFICATION: ARP 4754A includes techniques to assign hardware and software Development Assurance Levels (DAL) also. Additionally, the phrase “up to” is confusing, as



response	<p>DALs are assigned top-down from airplane functions.</p> <p>Noted.</p> <p>The commented text of AMC 25.1309 has evolved at Amendment 19 of CS-25 to read: 'Guidelines, which may be used for the assignment of development assurance levels to aeroplanes and system functions (FDAL) and to items (IDAL), are described in the document referenced in 3.b(2) above. Through this document, EASA recognises that credit can be taken from system architecture (e.g. functional or item development independence) for the FDAL/IDAL assignment process.'</p>
comment	<p>247 comment by: <i>Boeing</i></p> <p>Page: 39 Paragraph: <i>AMC - SUBPART F - EQUIPMENT</i> <i>AMC 25.1309 -- System Design and Analysis</i> 9. <i>Compliance with CS 25.1309</i> b. <i>Compliance with CS 25.1309(b)</i> (4) <i>[third unnumbered paragraph]</i></p> <p>The proposed text states: "... There is currently no agreed Development Assurance standard for airborne electronic hardware." REQUESTED CHANGE: Either properly reference RTCA DO-254/EUROCAE ED-80, or delete this sentence, as it is incorrect.</p> <p>JUSTIFICATION: This sentence in the proposed NPA is an old artifact from the "Diamond" draft AC/AMJ from long before DO-254/ED-80 was completed; but this standard is now 14 years old! It seems ironic to update the terminology with newer nomenclature (implying there is indeed a standard to follow) yet retaining the same outdated sentence.</p>
response	<p>Not accepted.</p> <p>EASA recognises that DO-254/ED-80 provides some guidance for the development of custom Airborne Electronic Hardware, but EASA also recognises that this standard might be insufficient for some other Airborne Electronic Hardware. A new AMC-20 item is under development (AMC 20-152). AMC 25.1309 will be updated once this new AMC 20-152 is published.</p>
comment	<p>248 comment by: <i>Boeing</i></p> <p>Page:39 Paragraph: <i>SUBPART F - EQUIPMENT</i> <i>AMC 25.1309 -- System Design and Analysis</i> 9. <i>Compliance with CS 25.1309</i> b. <i>Compliance with CS 25.1309(b)</i> (5)(i)1 <i>Crew and Maintenance Actions.</i></p> <p>The proposed text states: "1 Verify that any identified indications are actually provided by the system. This includes verification that the sensor coverage and logic that detects the situations and triggers the indicator is sufficient to always detect the situations considering various causes, flight phases, operating conditions, operational sequences, and environments."</p>

REQUESTED CHANGE:

“1 Verify that any identified indications are actually provided by the system. This includes verification that ~~sensor coverage and logic that detects the situations and triggers the indicator is sufficient to always detect~~ the elements that provide detection (e.g. sensors, logic) properly trigger the indication under the relevant situations considering various causes, flight phases, operating conditions, operational sequences, and environments.”

JUSTIFICATION: Sensors and logic are just examples, but the text also misses the broader intent while being too prescriptive. While some indications may be driven by sensors and logic, others may not or they may be influenced by other implementations. Additionally, the term “always” is too restrictive; we have reworded it to cover the intent for the credit being claimed of such indications.

response

Accepted.

The resulting text reads: ‘Verify that any identified indications are actually provided by the system. This includes verification that the elements that provide detection (e.g. sensors, logic) properly trigger the indication under the relevant situations considering various causes, flight phases, operating conditions, operational sequences, and environments.’

comment

249

comment by: Boeing

Page: 40

Paragraph: *SUBPART F - EQUIPMENT*AMC 25.1309 -- *System Design and Analysis*9. *Compliance with CS 25.1309*b. *Compliance with CS 25.1309(b)*(6) *Significant Latent Failures*(i) *Compliance with CS 25.1309(b)(4)***The proposed text states:**

“(i)... This AMC establishes a hierarchy of safety objectives for managing exposure to significant latent failures:

(A) Significant latent failures should be eliminated to the extent practical,

(B) For each significant latent failure which cannot be practically eliminated, the latency should be limited to a probability of 1/1000, and

(C) For each remaining significant latent failure where the 1/1000 criterion cannot be practically met, the latency should be minimised.”

REQUESTED CHANGE:

“(i)... This AMC establishes a **A** hierarchy of safety objectives for managing exposure to significant latent failures:

(A) Significant latent failures should be eliminated to the extent practical,

(B) For each significant latent failure which cannot be practically eliminated, **catastrophic failure condition that results from two failures, either of which is latent**, the latency should be limited to a probability of 1/1000 **by requiring the average probability for the latent failure to be on the order of 1/1000 or less**, and

(C) For each remaining significant latent failure **catastrophic failure condition that results from two failures, either of which is latent**, where the 1/1000 criterion cannot be practically met, the latency should be minimised.”

JUSTIFICATION: The proposed AMC does not align with the rule; paragraph (B) and (C) apply



only to a catastrophic failure condition that results from two failures, either of which is latent. Imposing 1/1000 criteria to significant latent failures that could result from more than 2 failures or in a hazardous failure condition, is not in concert with the rule and is specific enough to appear as a new requirement within the AMC. Using the average probability and “on the order of” matches the intent of the ASAWG’s recommendations.

[See our separate comments on CS 25.1309(b)(4) and (b)(5)(i).]

response

Not accepted.

Paragraphs (A), (B) and (C) are related to the demonstration of compliance with CS 25.1309(b)(4). They apply to any significant latent failure. As such, this includes latent failures contributing to Hazardous failure conditions.

comment

250

comment by: Boeing

Page: 40

Paragraph: *SUBPART F - EQUIPMENT*

AMC 25.1309 -- System Design and Analysis

9. Compliance with CS 25.1309

b. Compliance with CS 25.1309(b)

(6) Significant Latent Failures

(ii) Compliance with CS 25.1309(b)(5) [third and fourth unnumbered paragraphs]

The proposed text states:

“Two criteria are implemented in the CS, limit latency and residual risk. Limit latency is intended to limit the time of operating with a latent failure present. This is achieved by requiring the product of the maximum time the latent failure is expected to be present and its failure rate to not exceed 1/1000. Residual risk is intended to limit the average probability per flight hour of the failure condition given the presence of a single latent failure. This is achieved by defining the residual risk to be remote. Residual risk is the sum of single active failure(s) that have to be combined with the single latent failure to result in the Catastrophic Failure Condition.

“In numerical terms, compliance with CS 25.1309(b)(1) and CS 25.1309(b)(5) together means the residual risk, i.e. the sum of all subsequent single active failures, must be on the order of 1×10^{-6} per flight hour when the latency is limited to 1/1000 to satisfy the Extremely Improbable safety objective. Conversely, if the reliability of the only residual component is 1×10^{-5} per flight hour, then latency is limited to a maximum probability of 1×10^{-4} .”

REQUESTED CHANGE:

“Two criteria are implemented in the CS, limit latency and residual risk. Limit latency is intended to limit the time of operating with a latent failure present. This is achieved by requiring ~~the product of the maximum time~~ **the average probability of** the latent failure ~~is expected to be present and its failure rate to not exceed~~ to be on the order of 1/1000 **or less**. Residual risk is intended to limit the average probability per flight hour of the failure condition given the presence of a single latent failure. This is achieved by defining the residual risk to be remote. Residual risk is the ~~sum of single active failures~~ **combined probability per flight hour of all active failures** that ~~have to be combined with the single latent failure to may~~ result in ~~the a~~ Catastrophic Failure Condition **assuming the latent failure has occurred**.

In numerical terms, compliance with CS 25.1309(b)(1) and CS 25.1309(b)(5) together means the residual risk, i.e. the sum of all subsequent single active failures, must be on the order of 1×10^{-6} per flight hour when the latency is ~~limited to~~ **on the order of** 1/1000 to satisfy the



Extremely Improbable safety objective. Conversely, if the **reliability probability of occurrence** of the only residual **component event** is 1×10^{-5} (per flight hour), then **latency** probability of the latent **cy event** is limited to a maximum **probability** of 1×10^{-4} ."

JUSTIFICATION:

- Using the average probability and "on the order of" matches the intent of the ASAWG's recommendations.
- Clarification of residual risk probability is needed.
- It is not "reliability" but "unreliability" of the residual component that is 1×10^{-5} per flight hour.
- Remove the word "component" from the last sentence as it implies the residual event is failure of a component, when it can be any event.

response

Partially accepted.

The resulting text reads: 'Two criteria are implemented in the CS: limit latency and limit residual probability. Limit latency is intended to limit the time of operating with a latent failure present. This is achieved by requiring that the occurrence probability of the latent failure does not exceed 1/1000. Limit residual probability is intended to limit the average probability per flight hour of the failure condition given the presence of a single latent failure. This is achieved by defining the residual probability to be remote. Residual probability is the combined average probability per flight hour of all the single active failures that result in the catastrophic failure condition assuming one single latent failure has occurred.

In numerical terms, compliance with CS 25.1309(b)(1) and CS 25.1309(b)(5) together means the residual probability, i.e. the sum of all subsequent single active failures, must be in the order of 1×10^{-6} per flight hour when the occurrence probability of the significant latent failure is 1/1000 to satisfy the extremely improbable safety objective. Conversely, if the residual probability is 1×10^{-5} per flight hour, then the occurrence probability of the significant latent failure is limited to a maximum of 1×10^{-4} .'

comment

251

comment by: Boeing

Page:41

Paragraph: : SUBPART F - EQUIPMENT

AMC 25.1309 -- System Design and Analysis

9. Compliance with CS 25.1309

c. Compliance with CS 25.1309(c) [first unnumbered paragraph]

The proposed text states:

"... Any system operating condition which, if not detected and properly accommodated by crew action, would contribute to or cause one or more serious injuries should be considered as an 'unsafe system operating condition. ..."

REQUESTED CHANGE: Remove this text from 9.c.

~~Any system operating condition which, if not detected and properly accommodated by crew action, would contribute to or cause one or more serious injuries should be considered as an 'unsafe system operating condition.~~

Add the relevant text to AMC 25.1309, Section 5. Definitions, as follows:

"[x.] **Unsafe System Operating Condition.** Any system operating condition which, if not detected and properly accommodated by crew action, ~~would contribute to or cause one or more serious injuries should be considered as an 'unsafe system operating condition.~~ **has the potential to result in a hazardous or catastrophic failure condition.**"



response

JUSTIFICATION: This appears to be a new definition that is not in line with the hazard classifications defined in the AMC. Additionally, manufacturers (OEMs) have worked with the Agencies to use words like “contribute” judiciously as it has shown itself open to varied interpretations. Since “Unsafe System Operating Condition” is used in CS 25.1309(c) it should be moved to Section 5 (Definitions) of AMC 25.1309 where it is more visible, and use the hazards classifications previously defined in the AMC.

Partially accepted.

The term ‘unsafe system operating conditions’ is already used in current CS/FAR 25.1309, but with no proper explanation. The intent of the NPA was to propose a common understanding of this term rather than introducing a new definition in Section 5. The resulting text is now in line with the hazard classification defined in the AMC. The combination of words ‘would contribute to or cause [...]’ was used on purpose in the NPA text, and was actually thought to be judicious. Without any additional information, the wording is unchanged on this aspect.

The resulting text reads: ‘Any system operating condition which, if not detected and properly accommodated by crew action would contribute to or cause a hazardous or catastrophic failure condition, should be considered to be an “unsafe system operating condition”.’

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC Subpart F – Equipment, AMC 25.1309 (c)

Comment: Do not support the proposal that loss of annunciation is no worse than Major, and proposes that the crew action based on the annunciation be dealt with by showing compliance to 25.1302 (Human Factors). Cessna does not support the use of the term “unsafe operating condition” and in the interest of increasing safety or at least keeping the approach uniform across applicants, proposes that EASA and FAA coordinate on a term and definition that is usable and consistent. Such as “conditions requiring warning”, and limit those to functional failure conditions that are Hazardous, since Catastrophic failure conditions are not required to be annunciated, and for our class business jets, the death of a single individual has been defined as Catastrophic by the FAA.

Suggested change: Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Not accepted.

The combination of system failure and loss of annunciation is Catastrophic. The paragraph does not require to ‘annunciate catastrophic failure conditions’. The ‘major’ classification applies to the loss of annunciation. The comment refers to demonstration of compliance with CS 25.1302, but in this case there is no crew action based on the annunciation since there is no annunciation. The comment would be valid for the system failure (annunciated).

The term ‘unsafe system operating condition’ was not introduced through the NPA. This term was already used by EASA and the FAA in CS/FAR 25.1309(c) — however, without a proper explanation. The intent of the NPA was therefore to propose a common understanding of this term in the AMC. The wording was discussed and agreed with the FAA before publishing the NPA. An additional cross-check will nonetheless be performed once the FAA NPRM is published.

comment

252

comment by: Boeing

Page:41

Paragraph: SUBPART F - EQUIPMENT



AMC 25.1309 -- System Design and Analysis
 9. Compliance with CS 25.1309
 c. Compliance with CS 25.1309(c)
 9.c.(2)

The proposed text states:

“(2) When failure monitoring and indication are provided by a system, its reliability should be compatible with the safety objectives associated with the system function for which it provides that indication. For example, if the effects of having a failure and not annunciating that failure are Catastrophic, not only must the combination of the failure with the failure of its annunciation be Extremely Improbable, but the loss of annunciation should be considered a major failure condition in and of itself due to the impact on the ability of the crew to cope with the subject failure. ...”

REQUESTED CHANGE:

“(2) When failure monitoring and indication are provided by a system, its reliability should be compatible with the safety objectives associated with the system function for which it provides that indication. For example, if the effects of having a failure and not annunciating that failure are Catastrophic, ~~not only must the combination of the failure with the failure of its annunciation~~ **must** be Extremely Improbable. ~~, but t~~The loss of annunciation should be considered a ~~major~~ failure condition in and of itself. ~~due to the impact on the ability of the crew to cope with the subject failure.~~ ...”

JUSTIFICATION: The proposed text uses the term “a failure,” so it is presumably addressing a two-failure condition. This results in a disagreement with the guidance for a catastrophic failure condition that results from two failures, either of which is latent. In cases where the annunciation could fail latently, it is required to have a probability of 1/1000, while this guidance would require a probability on the order of 1E-5. If this is a requirement, it has the effect that latent failure of an annunciation and its residual risk must meet $1E-5 \times 1E-5 = 1E-10$. This argument would say that any failure that leaves a system one failure away from a catastrophic condition should be classified as “major;” however, this is in contradiction with the new guidance for catastrophic failure conditions where a latent failure could be 1/1000, by definition impacts the crews ability to cope (since the next failure is catastrophic), and should not be added.

response Please refer to the response to comment #54.

comment 253

comment by: Boeing

Page:42
 Paragraph: SUBPART F - EQUIPMENT
 AMC 25.1309 -- System Design and Analysis
 10. Identification of Failure Conditions and Considerations When Assessing their Effects.
 b. Identification of Failure Conditions Using a Functional Hazard Assessment.
 10.b.(4) [last sentence]

The proposed text states:

“(4)... With the increasing integrated system architectures, this traditional top down approach should also be complemented with a bottom up approach in order to properly address where one system contributes to several aeroplane level functions.”

REQUESTED CHANGE:



“(4)... With the increasing integrated system architectures, this traditional top down approach should ~~also be complemented with a bottom up approach in order to properly address where one system contributes to several aeroplane level functions~~ validated against system level Functional Hazard Assessments and the other safety assessments.”

JUSTIFICATION: The proposed sentence is out of place, as it implies there is something like a “bottom up” Functional Hazard Assessment. We suggest rewording it as indicated.

response Please refer to the response to comment #143.

comment

254

comment by: Boeing

Page:42

Paragraph: *SUBPART F - EQUIPMENT*

AMC 25.1309 -- System Design and Analysis

10. Identification of Failure Conditions and Considerations When Assessing their Effects.

c. Considerations When Assessing Failure Condition Effects

10.c.(1)(i)

The proposed text states:

“(1) The severity of Failure Conditions should be evaluated according to the following:

(i) Effects on the aeroplane, such as reductions in safety margins, degradation in performance, loss of capability to conduct certain flight operations, reduction in environmental protection, or potential or consequential effects on structural integrity. When the effects of a Failure Condition are complex, the hazard classification may need to be validated by tests, simulation, or other appropriate analytical techniques.”

REQUESTED CHANGE:

“(1) The severity of Failure Conditions should be evaluated according to the following:

(i) Effects on the aeroplane, such as reductions in safety margins, degradation in performance, loss of capability to conduct certain flight operations, reduction in environmental protection, or potential or consequential effects on structural integrity. When the effects of a Failure Condition are ~~complex~~ **difficult to assess**, the hazard classification may need to be validated by tests, simulation, or other appropriate analytical techniques.”

JUSTIFICATION: The term “complex” does not properly describe the situation. More appropriately, it is when there is difficulty assessing the failure condition that some additional validation may be required.

response Accepted.

comment

255

comment by: Boeing

Page:43

Paragraph: *SUBPART F - EQUIPMENT*

AMC 25.1309 -- System Design and Analysis

10. Identification of Failure Conditions and Considerations When Assessing their Effects.

c. Considerations When Assessing Failure Condition Effects

10.c.(2)(ii)

The proposed text states:

(ii)... Another example of an alleviating factor is the flight crew’s ability to recognise the



Failure Condition and take action to temper its effects. Whenever this is taken into account, attention to the detection means should be given to ensure the crew's ability (including physical and timeliness) to detect and take corrective action is sufficient. To correlate with the crew's annunciation requirements in CS 25.1309(c), consider the case of the crew taking action and also the effects if they do not. If their inability to take action results in an unsafe system operating condition, crew annunciations and evaluation of crew responses should be considered. See CS 25.1309(c) and paragraph 9c of this AMC for more detailed guidance on those considerations. ..."

REQUESTED CHANGE:

"(ii) Another example of an alleviating factor is the flight crew's ability to recognise the Failure Condition and take action to temper its effects. Whenever this is taken into account, attention to the detection means should be given to ensure the crew's ability (including physical and timeliness) to detect and take corrective action is sufficient. To correlate with the crew's annunciation requirements in CS 25.1309(c), consider the case of the crew taking action and also the effects if they do not. ~~If their inability to take action results in an unsafe system operating condition, crew annunciations and evaluation of crew responses should be considered. See CS 25.1309(c) and paragraph 9c of this AMC for more detailed guidance on those considerations. ..."~~

JUSTIFICATION: This text is not appropriate for discussion of alleviating action, and is redundant to CS 25.1309(c) already referenced in the paragraph.

response

Partially accepted.

The resulting text reads: 'Another example of an alleviating factor is the flight crew's ability to recognise the failure condition and take action to mitigate its effects. Whenever this is taken into account, attention to the detection means should be given to ensure that the ability of the flight crew (including physical ability and timeliness of the response) to detect the failure condition and take corrective action(s) is sufficient. See CS 25.1309(c) and paragraph 9c of this AMC for more detailed guidance on crew annunciations and crew response evaluation.'

comment

256

comment by: Boeing

Page: 45

Paragraph: *SUBPART F - EQUIPMENT*

AMC 25.1309 -- System Design and Analysis

12. Operational and Maintenance Considerations.

a. Flight Crew Action [first unnumbered paragraph]

The proposed text states:

"a. ... When considering the information provided to the crew, refer also to the guidance on CS 25.1309(c). Credit for crew actions, and considerations of flight crew errors, should be consistent with relevant service experience and acceptable human factors evaluations. ..."

REQUESTED CHANGE:

"a. ... When considering the information provided to the crew, refer also to the guidance on CS 25.1309(c). ~~Credit for crew actions, and considerations of flight crew errors, should be consistent with relevant service experience and acceptable human factors evaluations. ..."~~

JUSTIFICATION: The second sentence is not needed because it is redundant to compliance with CS 25.1309(c), which allows demonstration by analysis (see paragraph 9.c. on page 41).



	The guidance for 25.1309(c) has proposed wording which references CS 25.1302. That reference is adequate to cover guidance on appropriate information and control design to manage crew error.
response	Not accepted. The sentence contributes to the illustration of the requirement.
comment	<p>257 comment by: Boeing</p> <p>Page:45 Paragraph: <i>SUBPART F - EQUIPMENT</i> AMC 25.1309 -- <i>System Design and Analysis</i> 12. <i>Operational and Maintenance Considerations.</i> a. <i>Flight Crew Action [last sentence]</i></p> <p><u>The proposed text states:</u> “a. ... The applicant should provide a means to ensure the AFM will contain all the expected crew actions.”</p> <p><u>REQUESTED CHANGE:</u> “a. ... The applicant should provide a means to ensure the AFM will contain a the expected crew actions, as required by CS 25.1585.”</p> <p><u>JUSTIFICATION:</u> CS 25.1585 already describes the required operating procedures to be included in the AFM. The guidance of this AMC should not contradict the requirements of this regulation. Referencing the applicable regulation here will help clarify the guidance of this AMC.</p>
response	Partially accepted. The resulting text reads: ‘Unless flight crew actions are accepted as normal airmanship, they should be described in the approved aeroplane flight manual in accordance with CS 25.1585.’

Comment from Textron Aviation (extracted from the letter attached to comment #289):Page/Paragraph: For AMC Subpart F – Equipment, AMC 25.1309 (d)Comment: Do not support the proposal “When more than one flight is made with equipment known to be inoperative and that equipment affects the probabilities associated with hazardous and/or catastrophic failure conditions, time limits may be needed for the number of flights or allowed operation time in that aircraft configuration. These time limits should be established in accordance with the recommendations contained in CS-MMEL”. Again, the pass fail criteria are not clear and unambiguous.Suggested change: Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.EASA response: Not accepted.

The pass–fail criteria are provided in CS-MMEL, and will not be duplicated in AMC 25.1309.

comment	261 comment by: Alvaro Esteban
---------	---



"5. DEFINITIONS."

Related to the new definitions added in the **AMC 25.671 Control Systems – General**, some of them are closely related to Safety Process. It is kindly requested to include the following definitions in the AMC 25.1309:

n. *Probability vs. Failure Rate.* Failure rate is typically expressed in terms of average probability of occurrence per flight hour. In cases where the failure condition is associated with a certain flight condition that occurs only once per flight, the failure rate is typically expressed as average probability of occurrence per flight (or per take-off, or per landing). Failure rates are usually the 'root' numbers used in a fault tree analysis prior to factoring in latency periods, exposure time, or at risk time. Probability is non-dimensional and expresses the likelihood of encountering or being in a failed state. Probability is obtained by multiplying a failure rate by the appropriate exposure time.

i. *Exposure Time.* The period of time between when an item was last known to be operating properly and when it will be known to be operating properly again. See also SAE ARP 4761/EUROCAE ED-135.

a. *At Risk Time.* The period of time during which an item must fail to cause the failure effect in question. This is usually associated with the final fault in a fault sequence leading to a specific failure condition. See also SAE ARP 4761/EUROCAE ED-135.

response Partially accepted.
'Probability versus failure rate' is rather an explanation, not a definition.
The definitions of 'exposure time' and 'at-risk time' are added to the resulting text as proposed.

comment 285 comment by: *Bombardier Aerospace*

Re. Applicability of CS 25.1309 in AMC 25.1309 4.(g) and (h) (page 35):
While the proposal to consider failure effects outside of flight operations is certainly reasonable, the proposed guidance is unclear. The risk/safety assessment approach/process that has to be used to address this item should be clarified. For instance, it should be stated if the expected analysis should be qualitative or quantitative.

response Noted.
Paragraph 4.g aims to inform on the conditions expected to be considered in the hazard assessment. Paragraph 4.h is more specific and presents the effects to be considered on persons other than the occupants of the aeroplane. The main goal of the proposed changes is to ensure that the applicant will not disregard the effects on persons other than aeroplane occupants during ground operations.
These two paragraphs deal with the qualitative aspects of the safety assessment.

comment 286 comment by: *Bombardier Aerospace*

For consistency, the same wording should be used in the Safety Objectives in AMC 25.1309 8.(c)(3) as in CS-25.1309 (b)(5)(ii):
(ii) given any single latent failure has occurred, the catastrophic failure condition due to the sum of all subsequent single failures is remote;

response Please refer to the response to comment #154.



comment	287	comment by: <i>Bombardier Aerospace</i>
	<p>The calculation of average probability per flight hour calculation in AMC 25.1309 11.(e)(1)(v) is intended to describe how to compute the average probability per flight hour. To compute the average probability the FTA model must use the average exposure time, and not the maximum exposure time as proposed.</p> <p>We suggest retaining the original text: <i>(v) the average exposure time if the failure can persist for multiple flights.</i></p>	
response	Please refer to the response to comment #61.	
comment	288	comment by: <i>Bombardier Aerospace</i>
	<p>In AMC 25.1309 10.(c)(2)(ii), "temper" should be changed to "mitigate" to maintain consistent terminology.</p>	
response	Accepted.	
comment	291	comment by: <i>Rockwell Collins, Inc.</i>
	<p>9.b.(6).(i).(C): For the statement, “(C) For each remaining significant latent failure where the 1/1000 criterion cannot be practically met, the latency should be minimised.” Is this statement implying: (a) a <u>waiver</u> as a subsequent paragraph seems to imply, or (b) a <u>mandatory design change</u>? a <u>CCMR</u> to be proposed to <u>limit the total exposure time</u> of the significant latent failure? Please provide clarifying text.</p>	
response	<p>Noted. The statement is meant to provide a waiver, as implied by the subsequent paragraph starting with ‘There can be situations where it is not practicable to meet the 1/1000 criterion [...].’</p>	
comment	292	comment by: <i>Rockwell Collins, Inc.</i>
	<p>9.b.(6).(ii) fourth paragraph For the statement, “In numerical terms, compliance with CS 25.1309(b)(1) and CS 25.1309(b)(5) together means the residual risk, i.e. the sum of all subsequent single active failures, must be on the order of 1×10^{-6} per flight hour when the latency is limited to 1/1000 to satisfy the Extremely Improbable safety objective. Conversely, if the reliability of the only residual component is 1×10^{-5} per flight hour, then latency is limited to a maximum probability of 1×10^{-4}.” CS 25.671 (c).(2).(ii) on page 13 of 60 mentions 1×10^{-5} instead without the trade-off of 1×10^{-4} for the latent failure. Are those numbers final? Isn't that a contradiction between the CS 25.671 and the AMC 25.1309? Please provide text that clarifies or otherwise eliminates this apparent conflict.</p>	
response	<p>Not accepted. There is no contradiction between CS 25.671 and CS 25.1309 on this specific subject. Both</p>	



requirements specify a residual probability to be remote assuming that one single latent failure pre-exists for a given flight.

comment	<p>295</p> <p>4.h</p> <p>Paragraph “h” – if the TC or STC applicant is going to have to analyze potential threat or risks to persons outside the airplane at the aircraft level, then will EASA be publishing additional guidance for how to accomplish this type of assessment? Will EASA be working with the SAE S-18 Committee in order to get this “additional guidance” within ARP4761 Rev. A? Please provide information on how EASA intends to inject this analysis requirement within the industry as a best practice.</p>	comment by: <i>Rockwell Collins, Inc.</i>
response	<p>Noted.</p> <p>The goal of this change is not to introduce a new type of assessment, or inject a new type of analysis within the industry as a best practice. The scope of the assessment remains the aircraft and system failure conditions.</p> <p>Paragraph 4.g aims to inform on the conditions expected to be considered in the hazard assessment. Paragraph 4.h is more specific and presents the effects to be considered on persons other than the occupants of the aeroplane. The main goal of the proposed changes is to ensure that the applicant will not disregard the effects on persons other than aeroplane occupants during ground operations. These two paragraphs deal with the qualitative aspects of the safety assessment.</p>	
comment	<p>296</p> <p>8.c.(3)</p> <p>For the statement, “(3) Each Catastrophic Failure Condition, resulting from two failures, either of which is latent for more than one flight, is remote when either one is pre-existing.”, does this imply that</p> <p>(a) each permutation will need to meet a numerical safety objective of 5E-10 (so that catastrophic failure condition still complies with 1E-09)?</p> <p>(b) all latent failures (as appropriate based on the architecture) must be FDAL/IDAL = A?</p> <p>Please provide clarifying text.</p>	comment by: <i>Rockwell Collins, Inc.</i>
response	<p>Noted.</p> <p>(a): It implies that the catastrophic failure condition needs to meet the safety objective ‘remote’ when the probability of one single latent failure of concern is set to 1. Single latent failures of concern are these latent failures involved in two-failure combinations.</p> <p>(b): There is no link between the occurrence probability objectives and the development assurance levels. The assignment of FDAL/IDAL is based on the classification of sizing failure conditions and on aircraft/system architecture considerations, if any.</p>	
comment	<p>302</p> <p>5.v.</p> <p>For the definition, “v. Significant Latent Failure. A latent failure that would, in combination with one or more specific failures or events, results in a Hazardous or Catastrophic Failure</p>	comment by: <i>Rockwell Collins, Inc.</i>

	<p>Condition.”, EASA should remove the phrase ‘a Hazardous or’ in order to be consistent with the ASAWG Latent Failure Subteam conclusion that only Catastrophic Failure Conditions need to be assessed AND to be consistent with the NPA’s proposed verbiage for CS 25.1309 (b).(5). Please consider revising the text to align with the ASAWG conclusion.</p>
response	Please refer to the response to comment #239.
comment	<p>303 comment by: <i>Rockwell Collins, Inc.</i></p> <p>10.b.(4) Last sentence For the statement, “With the increasing integrated system architectures, this traditional top down approach should also be complemented with a bottom up approach in order to properly address where one system contributes to several aeroplane level functions.”, will EASA work with SAE S-18 Committee to include this NEW concept of FHA “bottom-up” approach in ARP4761 Rev A? Otherwise, will EASA further define/discuss this NEW concept within AMC 25.1309? Please provide information on how EASA intends to inject this “bottom up” approach within the industry as a best practice.</p>
response	Please refer to the response to comment #143.
comment	<p>306 comment by: <i>AIRBUS</i></p> <p>PARAGRAPH / SECTION THE COMMENT IS RELATED TO: AMC 25.1309 9 b 6 i PROPOSED TEXT / COMMENT: This AMC needs further explanation to be clearly understood regarding the EASA objectives, below: (A) Significant latent failures should be eliminated to the extent practical, (B) For each significant latent failure which cannot be practically eliminated, the latency should be limited to a probability of 1/1000, and (C) For each remaining significant latent failure where the 1/1000 criterion cannot be practically met, the latency should be minimised. RATIONALE / REASON / JUSTIFICATION The NPA changes related to AMC 25.1309, Section 9.b.(6) are related to several aspects not in line with ASAWG recommendation. Having qualitative criteria in CS 25.1309 was not agreed by ASAWG. Appreciation of pass-fail criteria seems to be let under the Agency control, whereas it should be under applicant control.</p>
response	<p>Noted.</p> <p>The approach proposed in the NPA (introducing CS 25.1309(b)(4) and CS 25.1309(b)(5)(i)) addresses the EASA dissenting opinion and the FAA dissenting opinion #2, submitted to the ASAWG and recorded in the report.</p> <p>The aim of AMC 25.1309 section 9.b.(6) is to provide acceptable means of compliance to CS 25.1309(b)(4) and CS 25.1309(b)(5)(i). When a catastrophic failure condition involves two failures, either of which is latent for more than one flight, and that cannot reasonably be eliminated, EASA requests to be informed as early as possible, and that the applicant provides a supporting rationale.</p>

comment	<p data-bbox="359 235 406 280">307</p> <p data-bbox="1173 235 1498 280" style="text-align: right;">comment by: <i>Rolls-Royce</i></p> <p data-bbox="359 291 1498 369">Page 40 item (B), Latency is a measure of time, not probability. So a little rewording is required.</p> <p data-bbox="359 369 845 403">Suggestion to Change the wording from:</p> <p data-bbox="359 436 1498 515">"For each significant latent failure which cannot be practically eliminated, the latency should be limited to a probability of 1/1000,"</p> <p data-bbox="359 548 391 582">to</p> <p data-bbox="359 616 1498 683">"For each significant latent failure which cannot be practically eliminated, the probability of the latent failure should be limited to a value of 1/1000".</p> <p data-bbox="359 683 941 728">Submitted on behalf of Andy Ward (Rolls-Royce)</p>
response	<p data-bbox="359 739 582 772">Partially accepted.</p> <p data-bbox="359 772 1498 884">The use of the term 'latency' will be corrected and made consistent throughout the document. The term is used to describe the exposure time of the latent failure. Section 9.b.(6) is updated accordingly.</p>
comment	<p data-bbox="359 907 406 952">308</p> <p data-bbox="1173 907 1498 952" style="text-align: right;">comment by: <i>Rolls-Royce</i></p> <p data-bbox="359 963 1498 1176">Page 43 item e.(1) (v), The calculation of the average probability should be based on the average exposure time if the failure can persist for multiple flights. But the NPA is proposing to change the words "average exposure time" to "maximum exposure time". This does not provide the average probability, it provides the probability in the very last flight prior to the check/repair of the failed part. It therefore provides the maximum probability.</p> <p data-bbox="359 1176 758 1209">Suggestion to change the words:</p> <p data-bbox="359 1243 686 1276">"maximum exposure time"</p> <p data-bbox="359 1310 454 1344">back to</p> <p data-bbox="359 1377 670 1411">"average exposure time".</p> <p data-bbox="359 1411 941 1456">Submitted on behalf of Andy Ward (Rolls-Royce)</p>
response	<p data-bbox="359 1489 917 1523">Please refer to the response to comment #61.</p>
comment	<p data-bbox="359 1534 406 1579">332</p> <p data-bbox="893 1534 1498 1579" style="text-align: right;">comment by: <i>Gulfstream Aerospace Corporation</i></p> <p data-bbox="359 1590 798 1624">4. APPLICABILITY OF CS 25.1309. (g)</p> <p data-bbox="359 1624 1498 1892"><i>"CS 25.1309 is always applicable to flight conditions, but only applicable to ground conditions when the airplane is in service (that is, from the time the airplane arrives at a gate or other location for pre-flight preparations, until it is removed from service for shop maintenance, storage, etc.). While this does include conditions associated with line maintenance, dispatch determinations, embarkation and disembarkation, taxi, or the like, it does not include periods of shop maintenance, storage, or other out of service activities."</i></p> <ul data-bbox="406 1892 638 1926" style="list-style-type: none"> • GAC Response: <p data-bbox="359 1926 1498 2004">Originally flight was defined as being initiated with throttle advance on takeoff to achievement of taxi speed on landing. Flight safety regulation applied within this scope.</p> <p data-bbox="359 2004 1498 2038">This scope has been significantly expanded by interpretation (not rulemaking). The proposed</p>

	<p>guidance here expands the definition of flight even further beyond what has recently been practiced.</p> <p>Gulfstream proposes that the ICAO definition of an accident should be a widely acceptable basis for defining what a "flight" is.</p> <p>"Accident. An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which (...)" - ICAO Annex 13.</p> <p>CS 25.1309 would, therefore, be applicable between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked.</p>
response	Accepted.
comment	<p>333 comment by: <i>Gulfstream Aerospace Corporation</i></p> <p>4. APPLICABILITY OF CS 25.1309. (h)</p> <p><i>"Risks to persons other than airplane occupants should be taken into account when assessing failure conditions in compliance with CS 25.1309. Such risks include threats to people on the ground or adjacent to the airplane during ground operations, electric shock threats to mechanics, and other similar situations. Because such risks are usually less significant in comparison with the risk to the airplane and its occupants, applicants have not typically addressed these risks in demonstrating compliance with CS 25.1309. However, designs may be considered non-compliant due to an unacceptable potential threat to persons outside the airplane or to line mechanics."</i></p> <ul style="list-style-type: none"> • GAC Response: <i>"...shock threats to mechanics, "</i> <p>Gulfstream disagrees that these issues are subject to CS 25.1309. Specific regulation exists for workplace safety, which applies when the aircraft is static, on the ground, and not in use with the intent of flight.</p> <p>The proposed definition of flight operation based on the ICAO annex would not include maintenance operations conducted when the aircraft is not actively in a flight operation.</p>
response	<p>Noted.</p> <p>The aim of paragraph 4.h is to ensure that the applicant will not disregard on a systematic basis the effects on persons other than aeroplane occupants during ground operations, when assessing failure conditions.</p>
comment	<p>334 comment by: <i>Gulfstream Aerospace Corporation</i></p> <p>5. DEFINITION. (o)</p> <p><i>"(1) A concept that minimises the likelihood of common mode errors and cascade failures between aircraft/system functions or items; "</i></p> <p><i>"(2) Separation of responsibilities that assures the accomplishment of objective evaluation, e.g. validation activities not performed solely by the developer of the requirement of a system or item."</i></p> <ul style="list-style-type: none"> • GAC Response: The following definition is proposed: <i>Independence. The absence of common sources of error or failure between systems, functions, or items.</i>
response	<p>Partially accepted.</p> <p>The definition of 'independence' is no longer retained in the resulting text.</p>

Paragraph 11.b.(1) is amended to reflect that errors need to be considered when assessing independence. A new sentence is inserted to state that common-cause failures (incl. common mode failures) and cascading failures should be considered as single failure from the perspective of the root cause or initiator. Errors in development, manufacturing, installation, and maintenance can result in common-cause failures (incl. common mode failures) and cascading failures. Errors should therefore be assessed in the frame of the single failure consideration.

comment	335	comment by: <i>Gulfstream Aerospace Corporation</i>
	<p>5. DEFINITION. (v) “Significant Latent Failure. A latent failure that would, in combination with one or more specific failures or events, results in a Hazardous or Catastrophic Failure Condition.”</p> <ul style="list-style-type: none"> • GAC Response: By this definition, a latent failure which combined with three remote non-latent failures results in a Hazardous or Catastrophic condition would be considered significant, even though the active failures alone render the scenario extremely improbable (and the specific risk when the latent failure is present remains <<1E-9). The following definition is proposed: Significant Latent Failure. A latent failure that would: (1) In combination with a single non-latent failure or event, and any number of additional latent events, result in a Hazardous or Catastrophic failure condition; or (2) When present, cause the average probability per flight hour of a Hazardous or Catastrophic failure condition to exceed its quantitative requirement by one or more orders of magnitude. 	
response	Please refer to the response to comment #239.	

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: § AMC 25.1309 Section 5v

Comment: NPA AMC 25.1309 Section 5v (and NPA CS 25.1309(b) (4)) introduces the concept of a “Significant Latent Failure” as a latent failure which would, in combination with one or more specific failures or events result in a Hazardous or Catastrophic Failure Condition. While the concept of a “Significant Latent Failure” may be understood to mean a latent failure which carries more importance because it may be the last remaining part of a fault tree guarding against HAZ or CAT failures, as worded this is unclear. Many HAZ/CAT fault trees contain latent failures requiring inspection intervals. As defined in NPA AMC 25.1309 Section 5v, ALL of the latent failures in ANY fault tree leading to HAZ/CAT top event are “Significant Latent Failures” because they, in combination with one or more failures or events, results in HAZ/CAT. If “or more failures” were struck from the definition, the increased importance of the Significant Latent Failure would be justified as that latency, coupled with one other failure, could result in HAZ/CAT, and hence deserves potential additional scrutiny. Is the intent to have ALL latent failures in ANY fault tree leading to HAZ/CAT being considered “Significant,”?

Suggested change: Propose striking “or more failures”.

EASA response: Please refer to the response to comment #239.



Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC Subpart F – Equipment, AMC 25.1309

Comment: “Significant Latent Failure. A latent failure that would in combination with one or more specific failures or events, results in a Hazardous or Catastrophic Failure Condition.” Cessna objects because the problem is not bounded by probability or cutsets. So any latent, even one in a 4th order cutset with a probability of 1e-13 when all the other failures are active becomes a significant latent failure. Cessna is not convinced that the modern tools can generate an exhaustive cutset listing, and, therefore, is not clear how to show compliance to this requirement.

Suggested change: Recommends that this be struck or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Please refer to the response to comment #239.

comment	336	comment by: <i>Gulfstream Aerospace Corporation</i>
	<p>6. BACKGROUND. (b)(1)(ii) <i>“Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless and their joint probability with the first failure is shown to be extremely improbable. The effect of combinations of failures that are not extremely improbable should not be catastrophic.”</i></p> <ul style="list-style-type: none"> GAC Response: <i>“...also be assumed...”</i> <p>As worded, the text seems to imply that subsequent failures should be assumed to occur (which contradicts the determination of probability). Recommended: “... also be considered...”</p>	
response	Accepted.	
comment	337	comment by: <i>Gulfstream Aerospace Corporation</i>
	<p>6. BACKGROUND. (b)(1)(ii) <i>“Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless and their joint probability with the first failure is shown to be extremely improbable. The effect of combinations of failures that are not extremely improbable should not be catastrophic.”</i></p> <ul style="list-style-type: none"> GAC Response: <i>“...failure is shown...”</i> <p>Delete.</p>	
response	Noted. The commented text has been deleted.	



Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC 25.1309 Section 6bii

Comment: NPA AMC 25.1309 Section 6bii adds “effect of combinations of failures that are not extremely improbable should not be catastrophic” is redundant as that concept is already covered in the concept of severity vs. frequency of occurrence in the broader existing CS 25.1309 and guidance material

Suggested change: Propose deleting the last sentence of AMC 25.1309 Section 6bii “The effect of combinations of failures...not extremely improbable...not be catastrophic.” as it is redundant with the concept of severity vs. frequency of occurrence already part of CS 25.1309 and related guidance.

EASA response: Not accepted.

For consistency in the approach, the proposed change should be performed along with the deletion of the ‘no single failure’ criterion from paragraph 6.b.(1)(i). No adverse comment was received regarding paragraph 6.b.(1)(i), therefore the decision was made to retain the occurrence probability in paragraph 6.b.(1)(ii).

comment	<p>338</p> <p style="text-align: right;"><i>comment by: Gulfstream Aerospace Corporation</i></p> <p>9. COMPLIANCE WITH CS 25.1309. (b)(5)(i)(1) “...system. This includes verification that the sensor coverage and logic that detects the situations and triggers the indicator is sufficient to always detect the situations considering various causes, flight phases, operating conditions, operational sequences, and environments.”</p> <ul style="list-style-type: none"> • GAC Response: All items are subject to failure, therefore this standard (“always”) cannot be met. It is sufficient that the indication function correctly in all foreseeable operating conditions (per CS 25.1301). Recommended: "This includes verification that the method of detection and indication is capable of detecting the condition in all environmental and operational conditions per CS 25.1309(a)(1)."
response	<p>Please refer to the response to comment #248.</p>

comment	<p>339</p> <p style="text-align: right;"><i>comment by: Gulfstream Aerospace Corporation</i></p> <p>10. IDENTIFICATION OF FAILURE CONDITIONS AND CONSIDERATIONS WHEN ASSESSING THEIR EFFECTS. (b, 4) “...and conducting Functional Hazard Assessments. With the increasing integrated system architectures, this traditional top down approach should also be complemented with a bottom up approach in order to properly address where one system contributes to several aeroplane level functions.”</p> <ul style="list-style-type: none"> • GAC Response: The need for performing these bottom-up activities is indeed (as noted) due to the limitations of the FHA methodology, however these methods cannot produce the same type of output as the FHA. All bottom-up analysis methods are design dependent verification methods (FMEA, cascading failure analysis, etc.). These are fundamentally different from the FHA, which is a design independent assessment which generates requirements. Adding this text at this location will generate confusion, as it seems to imply that bottom-up
---------	--

	<p>methods should be used to identify functional failure conditions (in addition to the FHA). No such bottom-up methods exist, or can exist.</p> <p>This content is best added where discussing verification activities (system safety assessment, aircraft safety assessment).</p> <p>Recommended: Delete from this section. This content may be added to a section discussing system or aircraft level safety assessment.</p>
response	Please refer to the response to comment #143.
comment	<p>340 comment by: Gulfstream Aerospace Corporation</p> <p>11. ASSESSMENT OF FAILURE CONDITION PROBABILITIES AND ANALYSIS CONSIDERATIONS. (e, 1, iv)</p> <p><i>“This should be based on the probability per flight, rather than per flight hour, for failure conditions that have a very short exposure window.”</i></p> <ul style="list-style-type: none"> • GAC Response: <p>Disagree with this stipulation. When a condition is limited to a short exposure on each flight, the exposure will occur much less frequently on aircraft that have long average flights than on aircraft with short average flights - over the same amount of flight hours.</p> <p>This stipulation unnecessarily increases the strictness of quantitative requirements for long range aircraft, by preventing the limited exposure from being computed against the total flight time. There is no regulatory basis for this. Quantitative safety requirements are "per flight hour" average probability requirements.</p> <p>When considering a hazard that only occurs on takeoff, an aircraft that performs one takeoff every 10 flight hours is objectively safer than an aircraft that performs 10 takeoffs every 10 flight hours.</p> <p>The existing "no single failure" and the added specific risk requirements are sufficient to ensure that conditions caused by high failure rate failures would not be found compliant on the basis of limited exposure alone.</p>
response	Please refer to the response to comment #58.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: AMC Subpart F – Equipment, AMC 25.1309 (e)

Comment: Do not support the proposal in (1)(iv) “This should be based on the probability per flight, rather than per flight hour, for failure conditions that have a very short exposure window”, this should be based on the published methods in SAE ARP 4761, and not changed at the whim of the regulators without explanation or rationale. At the very least, they should define what the intent of the phrase “very short exposure window” means. When we compare our part 25 non ETOPs aircraft that have average flight duration of 1.5 hours, and carry 10 people, is that a “very short exposure window” compared to a 12 hour mission on an ETOPS that carries several hundred people? Cessna believes that it is.

Suggested change: Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11

EASA response: Please refer to the response to comment #58.



comment	345	comment by: <i>Universal Avionics Systems Corporation</i>
	Page 43, section 11e(1)(v). Clarify definition of "maximum". We assume the intent is for the maximum exposure time to be representative across the target fleet, not the maximum possible exposure time that could occur in any one instance.	
response	Noted. The maximum exposure time is the period of time between the time when an item was last known to be operating properly and the time when it will be known to be operating properly again, as used in the system safety assessment for demonstrating compliance with the safety objectives.	
comment	347	comment by: <i>Universal Avionics Systems Corporation</i>
	Page 36, section 5(q). The term "item" should include aeronautical and other non-DO-178B databases, because a system is composed of hardware items, software items, and database items, any combination of which may cause failure conditions. The importance of considering databases in the context of system safety is already recognized for aeronautical databases (DO-200A) and airborne system databases (DO-178B). Include database in the definition of "item".	
response	Not accepted. While the importance of considering databases in the context of system safety assessment is recognised, the long-debated definition of the term 'item' is not changed in order to keep consistency with ED79A/ARP4754A. Please note that the definition of the term 'item' was introduced in AMC 25.1309 at Amendment 19 of CS-25, dated 15 May 2017.	
comment	348	comment by: <i>GE Aviation</i>
	The AMC introduces consideration of risks to persons other than airplane occupants such as people on the ground or adjacent to the airplane. Because the locations of these people are not part of the airplane design, analysis of risk to persons with an unknown location is not practicable. The most conservative assumption, that the airplane is entirely surrounded by people, is highly unrealistic and will distort the results of the analysis done for compliance with 25.1309. If EASA wishes to regulate the risks posed by the airplane to persons on the ground, this should be done as a separate rule, to enable consideration of appropriate tools, metrics and pass/fail criteria.	
response	Noted. Paragraph 4.h aims to ensure that the applicant does not disregard on a systematic basis the effects on persons other than aeroplane occupants during ground operations, when assessing failure conditions.	
comment	349	comment by: <i>GE Aviation</i>
	The phrase "operational sequences" referred to in 9b(1) is not understood	
response	Please refer to the response to comment #136.	
comment	350	comment by: <i>GE Aviation</i>

	<p>Introduction of Development Assurance levels (9b(4)) should be reconsidered. The concept of Development Assurance Levels was intended to safeguard designs which were complex and for which failure modes and propagations could not be deterministically analyzed. Simple mechanical systems can be thoroughly tested and analyzed and their failure modes understood. It is not necessary to introduce Development Assurance processes for such systems. For instance, engines are relatively isolated from the rest of the aeroplane so that their integration is limited and readily understood. They have well-known failure modes, simple architecture, established type design standards, and their reliability and safety is currently the best in history. There is no rationale to justify imposition of the DAL concept on a system like this.</p>
response	<p>Noted. Paragraph 9.b.(4) of AMC 25.1309 has been changed at Amendment 19 of CS-25, dated 15 May 2017, thereby introducing references to development errors and FDAL/IDAL.</p>
comment	<p>351 comment by: <i>Universal Avionics Systems Corporation</i></p> <p>Page 38, section 9(b)(4) and throughout the document. Clarify definition of "system with non-complex item" and "integrated system". We assume that the intent is to provide a definition consistent with 6.c(1). Based on the current definition there's a gap between a system containing a non-complex item and an integrated system. Make change consistent with definition on page 37, para 6.c(1).</p>
response	<p>Partially accepted. An item is considered to be non-complex when fully assured by a combination of testing and analysis. The text is amended with this clarification, in accordance with the notion of non-complex item in ED79A/ARP4754A.</p>
comment	<p>352 comment by: <i>Universal Avionics Systems Corporation</i></p> <p>Page 39, section 9.b(4). It is unclear which document "Section 3.b(2)" refers to. Clarify intended reference.</p>
response	<p>Noted. Paragraph 3.b(2) refers to Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A/EUROCAE ED-79A, Guidelines for Development of Civil Aircraft and Systems.</p>
comment	<p>353 comment by: <i>GE Aviation</i></p> <p>The AMC refers to ARP4754A. This is not an Industry Standard, as stated in the NPA, it is a Recommended Practice. It is not intended to be imposed as a standard; the ARP itself states: <i>"This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary"</i> <i>"The contents are recommended practices and should not be construed to be regulatory requirements. For this reason, the use of words such as "shall" and "must" is avoided except if used in the context of an example. It is recognized that alternative methods to the processes described or referenced in this document may be available to an organization desiring to obtain certification.</i> <i>This document provides neither guidelines concerning the structure of an individual organization nor how the responsibilities for certification activities are divided. No such</i></p>

	<p><i>guidance should be inferred from the descriptions provided."</i> and also <i>"Components that can be fully assured by a combination of testing and analysis, relative to their requirements and identified Failure Conditions may be considered to provide a level of confidence equivalent to IDAL A, provided the design has been validated and verified. This can be useful when considering their role in relation to other items or functions in a system to assign the FDALs and IDALs for the functions and items within that system. Examples include mechanical components, electro-mechanical devices, electro valves, or servo valves."</i></p> <p>The ARP clearly was not intended to be mandated. Incorporation of this material into rule is inappropriate and will greatly reduce industry support for the development of ARPs.</p>
response	<p>Noted.</p> <p>ARP4754A/ED79A is actually referenced in the AMC as an industry document providing guidelines for development assurance activities. This standard is not considered to have been incorporated in the rule as suggested in the comment. Furthermore, this is not a new topic brought by the NPA.</p> <p>The whole AMC 25.1309 will be reviewed to ensure consistency.</p>
comment	<p>354 comment by: GE Aviation</p> <p>9b(5) requires for any indications to flight crew or maintenance crew... "verification that the sensor coverage and logic that detects the situations...is sufficient to always detect the situations considering various causes, flight phases, operating conditions, operational sequences and environments". It is not possible to meet this "always" requirement. Failure propagations vary considerably from one event to another, depending on initiating conditions, and so the physical parameters being sensed will vary considerably. It is not possible to rule out a potential, for very unusual conditions, of delayed sensor activation, except by making the sensor so reactive that it created large numbers of false warnings, which introduce their own safety issues. It is not clear that this guidance is driven by an observed problem in service where safety has been compromised by sensor limitations The requirement should be reconsidered, to establish whether it provides sufficient safety benefit to justify it. Retaining this requirement will likely result in initiatives to remove sensors and helpful crew responses from the safety analysis, as driving disproportionate sensor resources.</p>
response	<p>Please refer to the response to comment #248.</p>
comment	<p>355 comment by: GE Aviation</p> <p>9c(2) requires that loss of annunciation of a potentially Catastrophic failure be considered Major. This is not consistent with other conditions considered Major, since the flight crew 's ability to manage the aeroplane and the aeroplane capabilities are both unaffected. The loss of safety margin is negligible, unless the actual failure occurs.</p>
response	<p>Please refer to the response to comment #54.</p>
comment	<p>356 comment by: GE Aviation</p> <p>Introduction of Development Assurance levels (9b(4) should be reconsidered. The concept of Development Assurance Levels was intended to safeguard designs which were complex and for which failure modes and propagations could not be deterministically analyzed. Simple</p>

mechanical systems can be thoroughly tested and analyzed and their failure modes understood. It is not necessary to introduce Development Assurance processes for such systems. For instance, engines are relatively isolated from the rest of the aeroplane so that their integration is limited and readily understood. They have well-known failure modes, simple architecture, established type design standards, and their reliability and safety is currently the best in history. There is no rationale to justify imposition of the DAL concept on a system like this, as acknowledged within ARP 4754A.

response Please refer to the response to comment #350.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: Appendix 1. Assessment Methods

Comment: Do not agree with the statement that “These analyses may also identify a combination of failures and effects that would otherwise not have been foreseen by FMEA or FTA.” If the analysis is properly done top down and developed from a functional perspective, these common mode items will be identified by the FMEA, FTA or by both. If problems are showing up in the field because the analysis that the regulators are requiring are not identifying these issues, then maybe the regulators should step back, form a problem statement, and address this issue through the S-18 group and change the emphasis described in SAE ARP 4761.

Suggested change: Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Not accepted.

A pure functional top-down approach is not sufficient to assess aircraft and systems architecture within the frame of the overall aircraft and system safety assessment process. The consideration of common causes is already included in AMC 25.1309 and SAE ARP4761.

3. Proposed amendments - CS-25 - Book 2 - AMC 25.1309 - new Appendix 5

p. 47-50

comment	5	comment by: <i>Duane Kritzinger</i>
	Page 50 of 60: Table A5-2: I am not sure I follow the logic in #2 and #3 . More explanation is needed.	
response	Accepted. CS 25.1309(b)(5)(ii) and the column ‘CS 25.1309(b)(5) Applicability / Compliance’ for items #2 and #3 have been clarified.	
comment	79	comment by: <i>Thales Avionics- JD Chauvet</i>
	Table A5-2 and Figure A5-1: The accuracy of provided numbers (time and probability) is ambitious but unrealistic ==> remove the decimal of the numbers	
response	Not accepted. While EASA agrees with the comment, the sole purpose of Figure A5-1 and Table A5-2 is to illustrate the applicability and compliance criteria of CS 25.1309(b)(5).	



comment	149	comment by: <i>Garmin International</i>
	<p>AMC 25.1309, Appendix 5</p> <p>The model shown in AMC 25.1309 Appendix 5 is different than the one provided by ASAWG. The Fault tree model top event probability does not represent average probability per flight hour. This is a change to the standard method of calculation used to address the probability safety objectives of 10-9, 10-7, etc. This modification to the ASAWG proposal is not recommended.</p>	
response	<p>Partially accepted.</p> <p>The ASAWG proposal does not reflect the case where a single latent failure contributes to more than one minimal cut set in the fault tree. Therefore, the example has been improved to reflect such a case.</p> <p>The average flight time is 1 hour in the example, therefore the absolute probability and the probability per flight hour of the top-level event are identical. For latent failures, the formula of the worst-case probability has been used.</p> <p>Notwithstanding the above, considering Garmin International feedback and comment #259, the example will be recomputed with an average flight duration greater than 1 hour.</p>	
comment	150	comment by: <i>Garmin International</i>
	<p>AMC 25.1309 Appendix 5</p> <p>One of the column titles is "Law". What does this acronym or abbreviation mean? It is recommended that the more familiar "failure rate" term be used.</p>	
response	Please refer to the response to comment #258.	
comment	165	comment by: <i>Dassault Aviation</i>
	<p>Dassault-Aviation comment page #47</p> <p>Extract: AMC 25.1309(appendix 5) The following example illustrates how the quantitative criteria of CS 25.1309(b)(5) are to be implemented. The methodology used is based (...).</p> <p>Comment: This appendix may be misleading. It may be understood that a combination of a 1E-05/FH evident failure with a 1E-03/FH latent failure is acceptable for a catastrophic top event, without consideration of the extremely remote criteria (1E-09/FH).</p> <p>Requested Change: Precise that the given example illustrates how the quantitative criteria of CS 25.1309(b)(5) are to be implemented together with CS 25.1309(b)(1).</p>	
response	<p>Partially accepted.</p> <p>It is agreed to clarify that CS 25.1309(b)(4) and (b)(5) are to be implemented in addition to CS 25.1309(b)(1).</p> <p>New text has been added in paragraph 9.b(6) and Appendix 5.</p>	
comment	166	comment by: <i>Dassault Aviation</i>



Dassault-Aviation comment page #50

Extract:

AMC 25.1309(appendix 5)(Table A5-2)

$P[\text{LAT } i] \sim \text{FR} * T$

Comment:

Dassault-Aviation position for computing the occurrence probabilities of latent failures is to use the average probability, that is to say the product of the average time (and not the maximum time) the latent failure is expected and its failure rate.

A different approach would be not consistent with ARP 4761, ARAC ASAWG and more particularly with the 25.1309 probability criteria that are defined as average probabilities per flight hour. It may also lead to unjustified constraints on maintenance (economic impact).

Requested Change:"

Change " $P[\text{LAT } i] \sim \text{FR} * T$ " by " $P[\text{LAT } i] \sim \text{FR} * T/2$ ". Adapt Table A5-2 and Figure A5-1 consequently.

response

Not accepted.
Please refer to the response to comment #61.

comment

258

comment by: *Boeing*

Page: 50

Paragraph: *APPENDIX 5*

*Table A5-2: Example of CS 25.1309(b)(5) Minimal Cut Set
5TH Column header*

The header of the 5th column is titled "Law".

REQUESTED CHANGE:

- Change the header title to "**Failure rate**" (**constant unless noted**).
- Remove the exponential notation from each row under it.

JUSTIFICATION: This is not a regulation or a "law" per se. If the intent is to somehow indicate a probability calculation method or principle, then the text should specifically indicate this. The language in the row cells in the column is unclear, e.g. "*exponential X.000E-0Y*"; to clarify this, we suggest inserting "*constant unless noted*" in the column header and remove the exponential notation from each row.

response

Accepted.

comment

259

comment by: *Boeing*

Page: 50

Paragraph: *APPENDIX 5*

*Table A5-2: Example of CS 25.1309(b)(5) Minimal Cut Set
Cut sets 2 and 3*

The proposed text states:

The proposed table is using a "1-hour" flight length.

REQUESTED CHANGE:

Redo this table with a longer flight length of 2-4 hours.



JUSTIFICATION: The 1.0 hour flight used in the example in Figure A5-1 and Table A5-2 results in the following issues:

1. Cut set #3 having a latent event with 10-hour exposure time appears unacceptable when some airplane models typically have flights that long; thus implying that an exposure time of one flight is unacceptable.
2. More importantly it makes it difficult to distinguish failure probability units between “No Units” and “Per Flight Hour” – It is important to quickly see the difference, as the limit latency requirement is in “Probability Units” and the residual risk requirement is in “Per Flight Hour Units,” as specified on page 40 of the NPA: *“Two criteria are implemented in the CS, limit latency and residual risk. Limit latency is intended to limit the time of operating with a latent failure present. This is achieved by requiring the product of the maximum time the latent failure is expected to be present and its failure rate to not exceed 1/1000. Residual risk is intended to limit the average probability per flight hour of the failure condition given the presence of a single latent failure.”*
Using a flight length of more than 1.0 hour will help the user see the application of the two requirements more clearly.

response

Partially accepted.

1. The Minimal Cut Set #3 is actually not compliant with the residual probability (i.e. active part). The latent failure and its related exposure time are not of concern in this minimal cut set.
2. Agreed with the recommendation. The example will be recomputed with an average flight duration greater than 1 hour.

comment

304

comment by: Rockwell Collins, Inc.

APPENDIX 5 Table A5-2

Per the table title, i.e., **“Example of CS 25.1309(b)(5) Minimal Cut Set”**, the title implies that the whole table represents the Minimal Cut Set. This interpretation of the title would be consistent with the ‘Fault Tree Minimal Cut Set’ definition found in ARP4761Appendix D, Section D.10.1.

Please consider removing the phrase ‘minimal cut set’ from the individual cells found in the table column “CS 25.1309 (b)(5) Applicability/ Compliance” so that readers of the AMC are not confused by EASA’s apparent multiple definitions of the term ‘minimal cut set’.

response

Partially accepted.

The resulting text reads: ‘Table A5-1: Fault Tree’ and ‘Table A5-2: Minimal Cut Sets’



Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: Appendix 1. Assessment Methods

Comment: Do not agree with the statement that “These analyses may also identify a combination of failures and effects that would otherwise not have been foreseen by FMEA or FTA.” If the analysis is properly done top down and developed from a functional perspective, these common mode items will be identified by the FMEA, FTA or by both. If problems are showing up in the field because the analysis that the regulators are requiring are not identifying these issues, then maybe the regulators should step back, form a problem statement, and address this issue through the S-18 group and change the emphasis described in SAE ARP 4761.

Suggested change: Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Not accepted.

A pure functional top-down approach is not sufficient to assess aircraft and systems architecture within the frame of the overall aircraft and system safety assessment process. The consideration of common causes is already included in AMC 25.1309 and SAE ARP4761.

Comment from Textron Aviation (extracted from the letter attached to comment #289):

Page/Paragraph: Appendix 5

Comment: Cessna objects to the simplistic example that requests that EASA use a representative example from a recent part 25 certification effort. For our small part 25 business jet, these examples involve functionally constructed fault trees that span hundreds of pages and involve thousands of gates and basic events. One can only assume that the size and complexity of the tree would scale with the aircraft, and that an example from the Airbus 380 or Boeing 787 would be, say, 10 times as large. How this concept can be explained using a one page fault tree is not clear, but it is clear that the example presented in this appendix is made up of a reduced tree based on the members of the cutsets and not the logical flow of design details as the tree is constructed. This approach re-enforces the notion presented in the paragraph above that “These analyses may also identify a combination of failures and effects that would otherwise not have been foreseen by FMEA or FTA.” So EASA has stated that there is a problem with the analysis, and then presented a simplified example to make their case. Again, Cessna cannot support a methodology along the lines of “An alternative but more conservative method would be to rerun the fault tree probability calculation assuming for each model rerun that a different latent primary event had failed.” As described in the ASAWG minority position presented to TAEIG on this subject, the estimated cost for a new program to do this exercise is someplace between 3 and 4 million dollars without any safety benefit.

Suggested change: Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.

EASA response: Not accepted.

The purpose of Figure A5-1 and Table A5-2 is to illustrate in a simpler manner the applicability and compliance criteria of CS 25.1309(b)(5).

4. Regulatory Impact Assessment (RIA) - 4.1 - 4.5

p. 51-58

comment 70 ❖

comment by: *Laurent Lalaque***Proposed change**

At the bottom of page 43, paragraph e. (1) (v) Calculation of average probability per flight



hour (Quantitative Analysis), we strongly disagree and we propose to leave "average" instead of "maximum" in the sentence "the maximum exposure time if the failure can persist for multiple flights."

In the page 56, in the paragraph 4.5.4, the assessment of the economic impact for options 1, 2 and 3 does not reflect the very significant additional costs of dividing by 2 the periodicity of preventive maintenance inspections, induced by replacing "average" by "maximum" (see the justification hereafter).

Justification.

1 - As mentioned in another Turbomeca comment on pages 39, 40 and 41, the number of latent failures is significant, and the dormancies are not all the same due to different kind and different periodicity of preventive maintenance actions that are requested to limit at a certain level the non-availability of the maximum rating power when requested. It is not realistic to consider that, simultaneously on the same engine, all latent failures are in the same engine, the same flight, at their maximum of dormancy, that is to say just the flight before the maintenance action.

2 - Even for just one order two minimum cut set leading to a CAT FC, using the "maximum exposure time" is not consistent with the spirit of computing an "average probability".

3 - With this new practice, taking into account the maximum exposure time into the SSA would lead to divide by 2 the periodicity of most of the periodic preventive maintenance inspections. This would lead to a serious impact at operators level, organizations, maintenance costs ...and then a significant economic impact has to be taken into account in the paragraph 4.5.4 economic impact.

response Partially accepted.
Please refer to the response to comment #61.

comment 357 comment by: GE Aviation

The Regulatory Impact Assessment acknowledges that there is no evidence that the (listed) safety concerns have ever led to catastrophic accidents. We believe the stated concerns to be hypothetical, and that attempting to expand the regulation to encompass these issues will have a negative effect on safety, by distracting attention and resources from higher risk areas. Specifically, we believe that safety assessments can best be improved by careful consideration of the validity of underlying assumptions, rather than by expanding the number of scenarios to be addressed. It has frequently been noted in forums of industry safety experts that the design-related accidents in the last 20 years are associated with misunderstanding of the physics of the failure progression, rather than insufficient statistical or "systems safety" analysis. In that context, we consider the proposed rule and advisory material to be safety-negative.

response Not accepted.
EASA does not agree that the proposed change will divert attention or resources from high-risk areas. The standardisation and clarification of safety assessments is expected to be beneficial in terms of safety level and also in terms of workload and resources for both the applicants and EASA.

comment 358 comment by: GE Aviation

The Regulatory Impact Assessment acknowledges that there is no evidence that the (listed) safety concerns have ever led to catastrophic accidents. We believe the stated concerns to be hypothetical, and that attempting to expand the regulation to encompass these issues will



have a negative effect on safety, by distracting attention and resources from higher risk areas. Specifically, we believe that safety assessments can best be improved by careful consideration of the validity of underlying assumptions, rather than by expanding the number of scenarios to be addressed. It has frequently been noted in forums of industry safety experts that the design-related accidents in the last 20 years are associated with misunderstanding of the physics of the failure progression, rather than insufficient statistical or "systems safety" analysis. In that context, we consider the proposed rule and advisory material to be safety-negative.

response Please refer to the response to comment #358.

comment 359 comment by: GE Aviation

The economic impact aspect of the RIA should be revised to reflect the additional cost of introducing monitoring systems on a large number of airplane structures and systems, and of upgrading all sensors to avoid any potential for non-indication or delayed indication, driven by the proposed rule/ advisory material. This will be far greater than the certification cost savings suggested. The additional time required to execute specific risk analyses has not been taken into account. The additional cost of maintenance interventions for physical inspection of possible these failures is not taken into account. The proposed rule and policy will significantly increase certification and operational costs.

response Not accepted.
Various changes have been made to the proposed regulatory text based on the comments received. The economic impact assessment of the RIA is deemed to be still valid.

comment 360 comment by: GE Aviation

The Regulatory Impact Assessment should be revised. It states in paragraph 4.5.6 that option 0, doing nothing, "will lead to a loss of harmonization with the FAA , since that authority...**is also drafting a Notice of Proposed Rulemaking...**".The assessment should be based on the current FAA regulations, not on potential regulations which have not yet been proposed and which may not go forward. The table should show that option 0 is the most beneficial for harmonization, and that option 1 decreases harmonization.

response Noted.
The assessment in section 4.5.6 was performed based on the assumption that the FAA would pursue their project and publish an NPRM in cooperation with EASA. EASA has therefore been waiting for the FAA NPRM after the publication of NPA 2014-02.
Based on the information available to EASA at the time of preparing this CRD, the FAA still intend to pursue a rulemaking action, however the associated schedule appears to be uncertain.
EASA has therefore decided to continue its rulemaking project and publish this CRD. EASA will continue to seek harmonisation with the FAA in the future.

comment 361 comment by: GE Aviation

The focus on latent failures does not account for the impracticability of monitoring all simple mechanical systems and structures. These simple mechanical systems with time-proven robust and rugged designs have shown over the last billion flight hours that they do not form a significant risk to the airplane. Addition of monitoring means to address the effects of a



response

hypothetical latent failure, or series of failures, does not provide a safety benefit, and adds significant cost and complexity to the design.


Not accepted.

EASA has carefully considered all the comments received and revised the regulatory text to ensure clarity and avoid misinterpretations.

EASA does not intend to impose impractical or disproportionate monitoring systems. The goal is to better identify and manage the potential latent failures during the design development phase. The design should be developed in a way to avoid the need to put in place heavy monitoring systems.



4. Appendix A — Attachments

 [EASA NPA- 2014-02.pdf](#)

Attachment #1 to comment [#289](#)

 [A&C-14-070 Gulfstream response to EASA NPA 2014-02.pdf](#)

Attachment #2 to comment [#311](#)



5. Appendix B — Resulting text

The resulting text shows the changes relative to CS-25 Amendment 21.

The text of the amendment is arranged to show deleted text, new or amended text as follows:

- (1) deleted text is ~~struck through~~;
- (2) new or amended text is highlighted in grey;
- (3) an ellipsis '(...)' indicates that the remaining text is unchanged.

BOOK 1

SUBPART D — DESIGN AND CONSTRUCTION

GENERAL

CS 25.629 is amended as follows:

CS 25.629 Aeroelastic stability requirements

(...)

- (d) Failures, malfunctions, and adverse conditions. The failures, malfunctions, and adverse conditions which must be considered in showing compliance with this paragraph are:

(...)

- (9) Any of the following failure combinations:

(i) any dual hydraulic system failure;

(ii) any dual electrical system failure; and

(iii) any single failure in combination with any probable hydraulic or electrical system failure.

~~(9)~~(10) Any damage, failure or malfunction, considered under CS 25.631, CS 25.671, CS 25.672, and CS 25.1309.

~~(10)~~(11) Any other combination of failures, malfunctions, or adverse conditions not shown to be extremely improbable.

(...)



CONTROL SYSTEMS

CS 25.671 is amended as follows:

CS 25.671 General

(See AMC 25.671)

- (a) Each flight control and flight control system must operate with the ease, smoothness, and positiveness appropriate to its function. In addition, the flight control system shall be designed to continue to operate in any attitude and must not hinder aeroplane recovery from any attitude. ~~(See AMC 25.671 (a).)~~
- (b) Each element of each flight control system must be designed, ~~or distinctively and permanently marked,~~ to minimise the probability of incorrect assembly that could result in the failure or malfunctioning of the system. Distinctive and permanent marking may be used where design means are impractical, or for elements whose failure cannot lead to a safety effect. ~~(See AMC 25.671 (b).)~~
- (c) The aeroplane must be shown by analysis, test, or both, to be capable of continued safe flight and landing after any of the following failures ~~or, including jamming,~~ in the flight control system ~~and surfaces (including trim, lift, drag, and feel systems)~~ within the normal flight envelope, ~~without requiring exceptional piloting skill or strength. Probable malfunctions must have only minor effects on control system operation and must be capable of being readily counteracted by the pilot.~~
- (1) Any single failure, excluding failures of the type defined in CS 25.671(c)(3).
~~Any single failure not shown to be extremely improbable, excluding jamming, (for example, disconnection or failure of mechanical elements, or structural failure of hydraulic components, such as actuators, control spool housing, and valves). (See AMC 25.671(c)(1).)~~
- (2) For combinations of failures, excluding failures of the type defined in CS 25.671(c)(3):
- (i) Any combination of failures not shown to be extremely improbable; and
- (ii) Given any single latent failure has occurred, the average probability per flight hour of any failure condition preventing continued safe flight and landing, due to the sum of the probabilities of all subsequent single failures, must be less than 10^{-5} . For combinations of failures involving a single active failure and latent failures preventing continued safe flight and landing, the combined probability of the latent failures must be 1/1000 or less.
~~Any combination of failures not shown to be extremely improbable, excluding jamming (for example, dual electrical or hydraulic system failures, or any single failure in combination with any probable hydraulic or electrical failure).~~
- (3) Any failure or event that results in a jam of a flight control surface or pilot control that is fixed in position due to a physical interference. The jam must be evaluated as follows:
- (i) The jam must be considered at any normally encountered position of the control surface, or pilot controls;
- (ii) The causal failure or failures must be assumed to occur anywhere within the normal flight envelope; and
- (iii) In the presence of a jam considered under this subparagraph, any additional failure states that could prevent continued safe flight and landing shall have a combined probability of 1/1000 or less.

~~Any jam in a control position normally encountered during take off, climb, cruise, normal turns, descent and landing unless the jam is shown to be extremely improbable, or can be~~



alleviated. A runaway of a flight control to an adverse position and jam must be accounted for if such runaway and subsequent jamming is not extremely improbable.

- (4) Any runaway of a flight control system or surface to an adverse position that results from a single particular risk occurrence, maintenance error, or other foreseeable external event.

In addition, it must be shown that the pilot can readily counteract the effects of any probable failure.

- (d) The aeroplane must be designed so that, if all engines fail at any time of the flight, then the aeroplane is controllable:

(1) in flight;

(2) on approach;

(3) during the flare to a landing, and the flare to a ditching; and

(4) during the ground phase, and the aeroplane can be stopped, assuming that a suitable runway is available for a landing.

Compliance with this requirement may be shown by analysis where that method has been shown to be reliable.

- (e) The flight control system must be designed to ensure that the flight crew is aware whenever the primary control means approaches the limit of control authority.

- (f) If the flight control system has multiple modes of operation, appropriate flight crew alerting must be provided to ensure the pilot is aware whenever the aeroplane enters any mode that significantly changes or degrades the normal handling or operational characteristics of the aeroplane.

CS 25.672 is amended as follows:

CS 25.672 Stability augmentation and automatic and power-operated systems

~~(See AMC 25.672)~~

(...)

- (c) It must be shown that after any single failure of the stability augmentation system or any other automatic or power-operated system –

- (1) The aeroplane is safely controllable when the failure or malfunction occurs at any speed or altitude within the approved operating limitations that is critical for the type of failure being considered. ~~(See AMC 25.672 (c) (1).)~~

(...)



SUBPART E — POWERPLANT

CS 25.933 is amended as follows:

CS 25.933 Reversing systems

(a) For turbojet reversing systems:

(1) Each system intended for ground operation only must be designed so that either:

- (i) The aeroplane can be shown to be capable of continued safe flight and landing during and after any thrust reversal in flight; or
- (ii) It can be demonstrated that any in-flight thrust reversal is extremely improbable and does not result from a single failure or malfunction complies with CS 25.1309(b).

(See AMC 25.933(a)(1))

(...)



SUBPART F — EQUIPMENT

CS 25.1309 is amended as follows:

CS 25.1309 Equipment, systems and installations

(See AMC 25.1309)

The requirements of this paragraph, except as identified below, are applicable, in addition to specific design requirements of CS-25, to any equipment or system as installed in the aeroplane. Although this paragraph does not apply to the performance and flight characteristic requirements of Subpart B and the structural requirements of Subparts C and D, it does apply to any system on which compliance with any of those requirements is dependent. ~~Certain single failures or jams~~ Certain jams of flight control surfaces or pilot controls and flight control system/surface runaways covered by ~~CS 25.671(c)(1) and CS 25.671(c)(3) and CS 25.671(c)(4)~~ are excepted from the requirements of CS 25.1309(b)(1)(ii). Certain single failures covered by CS 25.735(b) are excepted from the requirements of CS 25.1309(b). The failure effects covered by CS 25.810(a)(1)(v) and CS 25.812 are excepted from the requirements of CS 25.1309(b). The requirements of CS 25.1309(b) apply to powerplant installations as specified in CS 25.901(c).

(...)

- (b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -
- (1) Any catastrophic failure condition
 - (i) is extremely improbable; and
 - (ii) does not result from a single failure; and
 - (2) Any hazardous failure condition is extremely remote; and
 - (3) Any major failure condition is remote; and
 - (4) Any significant latent failure is either eliminated or, if impracticable, its latency is minimised; and
 - (5) For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, it must be shown that:
 - (i) it is impracticable to provide additional redundancy; and
 - (ii) given that a single latent failure has occurred on a given flight, the catastrophic failure condition is remote; and
 - (iii) the occurrence probability of the latent failure does not exceed 1/1000.
- (c) Information concerning unsafe system operating conditions must be provided to the flight crew to enable them to take appropriate corrective action in a timely manner. ~~A warning indication must be provided if immediate corrective action is required.~~ When flight crew alerting is required, this must be provided in compliance with CS 25.1322. Installed systems and equipment for use by the flight crew controls, including flight deck controls and information indications and annunciations, must be designed in compliance with CS 25.1302 to minimise flight crew errors, which could create additional hazards.

(...)

BOOK 2

AMC — SUBPART D

AMC 25.671(a) is deleted:

AMC 25.671(a)**Control Systems — General**

~~Control systems for essential services should be so designed that when a movement to one position has been selected, a different position can be selected without waiting for the completion of the initially selected movement, and the system should arrive at the finally selected position without further attention. The movements which follow and the time taken by the system to allow the required sequence of selection should not be such as to adversely affect the airworthiness of the aeroplane.~~

AMC 25.671(b) is deleted:

AMC 25.671(b)**Control Systems — General**

~~For control systems which, if incorrectly assembled, would hazard the aeroplane, the design should be such that at all reasonably possible break-down points it is mechanically impossible to assemble elements of the system to give —~~

- ~~a. — An out-of-phase action,~~
- ~~b. — An assembly which would reverse the sense of the control, and~~
- ~~c. — Interconnection of the controls between two systems where this is not intended.~~

~~Only in exceptional circumstances should distinctive marking of control systems be used to comply with the above.~~

AMC 25.671(c)(1) is deleted:

AMC 25.671(c)(1)**Control Systems — General**

~~To comply with CS 25.671(c)(1) there should normally be —~~

- ~~a. — An alternative means of controlling the aeroplane in case of a single failure, or~~
- ~~b. — An alternative load path.~~

~~However, where a single component is used on the basis that its failure is extremely improbable, it should comply with CS 25.571(a) and (b).~~



New AMC 25.671 is inserted as follows:

AMC 25.671

Control Systems — General

1. PURPOSE.

This AMC provides an acceptable means, but not the only means, to demonstrate compliance with the control system requirements of CS 25.671.

2. RELATED DOCUMENTS.

a. Advisory Circulars, Acceptable Means of Compliance.

- (1) AC 25-7C, Flight Test Guide for Certification of Transport Category Airplanes.
- (2) AMC 25.1309 System Design and Analysis
- (3) AMC 20-115, Software Considerations for Airborne Systems and Equipment Certification

b. Standards.

- (1) Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A/EUROCAE ED-79A, Guidelines for Development of Civil Aircraft and Systems.
- (2) Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

3. APPLICABILITY OF CS 25.671.

CS 25.671 applies to all flight control system installations (including primary, secondary, trim, lift, drag, feel, and stability augmentation systems) regardless of implementation technique (manual, powered, fly-by-wire, or other means).

While CS 25.671 applies to flight control systems, CS 25.671(d) does apply to all control systems required to provide control, including deceleration, for the phases specified.

4. DEFINITIONS.

The following definitions apply to CS 25.671 and this AMC. Unless otherwise stated, they should not be assumed to apply to the same or similar terms used in other rules or AMCs.

- a. *At-Risk Time.* The period of time during which an item must fail to cause the failure effect in question. This is usually associated with the final fault in a fault sequence leading to a specific failure condition. See also SAE ARP4761.
- b. *Catastrophic Failure Condition.* Refer to AMC 25.1309 (chapter 7).
- c. *Continued Safe Flight and Landing.* The capability for continued controlled flight and landing at an aerodrome without requiring exceptional piloting skill or strength.
- d. *Landing.* The phase following final approach and starting with the landing flare. It includes the ground phase on the runway and ends when the aeroplane comes to a complete stop on the runway.



- e. *Latent Failure*. Refer to AMC 25.1309 (§ 5).
- f. *Error*. Refer to AMC 25.1309 (§ 5).
- g. *Event*. Refer to AMC 25.1309 (§ 5).
- h. *Exposure Time*. The period of time between the time when an item was last known to be operating properly and the time when it will be known to be operating properly again. See also SAE ARP4761.
- i. *Extremely Improbable*. Refer to AMC 25.1309 (§7).
- j. *Failure*. Refer to AMC 25.1309 (§ 5).

The following are some of the types of failures to be considered when demonstrating compliance with CS 25.671(c). Since the type of failure and the effect of the failure depend on the system architecture, this list is not exhaustive, but serves as a general guideline.

- (1) *Jam*. A failure or event such that a control surface, pilot control, or component is fixed in one position.
 - (i) If the control surface or pilot control is fixed in position due to physical interference, it is addressed under CS 25.671(c)(3). Causes may include corroded bearings, interference with a foreign or loose object, control system icing, seizure of an actuator, or disconnect that results in a jam by creating interference. Normally encountered positions are defined in paragraph 7.b of this AMC.
 - (ii) All other failures that result in a fixed control surface, pilot control, or component are addressed under CS 25.671(c)(1) and 25.671(c)(2) as appropriate. Depending on system architecture and the location of the failure, some jam failures may not always result in a fixed surface or pilot control; for example, a jammed valve could result in a surface runaway.
- (2) *Loss of Control of Surface*. A failure such that a surface does not respond to commands. Failure sources can include mechanical disconnection, control cable disconnection, actuator disconnection, loss of hydraulic power, or loss of control commands due to computers, data path or actuator electronics failures. In these conditions, the position of the surface(s) or controls can be determined by analysing the system architecture and aeroplane aerodynamic characteristics; common positions include surface-centred (0°) or zero hinge-moment position (surface float).
- (3) *Oscillatory Failure*. A failure that results in undue surface oscillation. Failure sources include control loop destabilisation, oscillatory sensor failure, oscillatory computer or actuator electronics failure. The duration of the oscillation, its frequency, and amplitude depend on the control loop, monitors, limiters, and other system features.
- (4) *Restricted Control*. A failure that results in the achievable surface deflection being limited. Failure sources include foreign object interference or travel limiter malfunctioning. This failure is considered under CS 25.671(c)(1) and CS 25.671(c)(2), as the system/surface can still be operated.
- (5) *Runaway or Hardover*. A failure that results in uncommanded control surface movement. Failure sources include servo valve jams, computer or actuator electronics malfunctioning. The speed of the runaway, the duration of the runaway (permanent or transient) and the resulting surface position (full or partial deflection) depend on the available monitoring, limiters and other system features. This type of failure is addressed under CS 25.671(c)(1) and (c)(2).

Runaways that are caused by external events, such as loose or foreign objects, control system icing, or any other environmental or external source are addressed in CS 25.671(c)(4).



(6) *Stiff or Binding Controls.* A failure that results in a significant increase in control forces. Failure sources include failures of artificial feel systems, corroded bearings, jammed pulleys, and failures causing high friction. This failure is considered under CS 25.671(c)(1) and CS 25.671(c)(2), as the system/surface can still be operated. In some architectures, higher friction may result in reduced centring of the controls.

k. *Failure States.* As used in CS 25.671(c), this term refers to the sum of all failures and failure combinations contributing to a hazard, apart from the single failure (flight control system jam) being considered.

l. *Flight Control System.* Flight control system refers to the following: primary flight controls from the pilot's controllers to the primary control surfaces, trim systems from the pilot's trim input devices to the trim surfaces (including stabiliser trim), speed brake/spoiler systems from the pilot's control lever to the brake/spoiler panels or other drag/lift-dumping devices, high-lift systems from the pilot's controls to the high-lift surfaces, feel systems, and stability augmentation systems. Supporting systems (i.e. hydraulic systems, electrical power systems, avionics, etc.) should also be included if failures in these systems have an impact on the function of the flight control system.

Examples of elements to be evaluated under CS 25.671 include but are not limited to:

- linkages,
- hinges,
- cables,
- pulleys,
- quadrants,
- valves,
- actuators (including actuator components),
- flap/slat tracks (including track rollers and movable tracks),
- bearings, axles and pins,
- control surfaces (jam and runaway only),
- attachment fittings.

m. *In-flight* is the time period from the time when the aeroplane is at 10 m (35 ft) above aerodrome level (AAL) following a take-off, up to the time when the aeroplane reaches 15 m (50 ft) AAL prior to landing, including climb, cruise, normal turns, descent, and approach.

n. *Landing* is the time period from the time when the aeroplane is at 15 m (50 ft) AAL prior to landing, up to the complete stop of the aeroplane on the runway.

o. *Probability versus Failure Rate.* Failure rate is typically expressed in terms of average probability of occurrence per flight hour. In cases where the failure condition is associated with a certain flight condition that occurs only once per flight, the failure rate is typically expressed as average probability of occurrence per flight (or per take-off, or per landing). Failure rates are usually the 'root' numbers used in a fault tree analysis prior to factoring in latency periods, exposure time, or at-risk time. Probability is non-dimensional and expresses the likelihood of encountering or being in a failed state. Probability is obtained by multiplying a failure rate by the appropriate exposure time.

p. *Take-off* is the time period from brake release up to the time when the aeroplane reaches 10 m (35 ft) AAL.



5. EVALUATION OF FLIGHT CONTROL SYSTEM OPERATION — CS 25.671(a).**a. General.**

Flight control systems for essential services should be designed such that when a movement to one position has been selected, a different position can be selected without waiting for the completion of the initially selected movement, and the system should arrive at the finally selected position without further attention. The movements that follow and the time taken by the system to allow the required sequence of selection should not adversely affect the controllability of the aeroplane.

b. Abnormal Attitude.

Compliance should be demonstrated by evaluation of the closed-loop flight control system. This evaluation is intended to ensure that there are no features or unique characteristics (including numerical singularities) which would restrict the pilot's ability to recover from any attitude. CS 25.671(a) does not intend to limit the use of envelope protection features or other systems that augment the control characteristics of the aeroplane.

Open-loop flight control systems should also be evaluated.

CS 25.671(a) is intended to include cases outside the protected envelope (for aeroplanes with flight control envelope protection).

6. EVALUATION OF FLIGHT CONTROL SYSTEM ASSEMBLY — CS 25.671(b).

This rule is intended to ensure that the parts applicable to the type design are correctly assembled, and is not intended to address configuration control (refer to CS 25.1301(a)(2)).

- a. For flight control systems, the design should ensure that it is impossible to assemble elements of the system in a way that prevents its intended function.

Examples of unacceptable consequences of incorrect assembly:

- (1) an out-of-phase action;
- (2) reversal in the sense of the control;
- (3) interconnection of the controls between two systems where this is not intended;
- (4) loss of function.

- b. Adequate precautions should be taken in the design process and adequate procedures should be specified in the instructions for continued airworthiness to prevent the incorrect installation, connection, or adjustment of parts of the flight control system.

The applicant should:

- (1) analyse the assembly and maintenance of the system to assess the classification of potential incorrect assembly;
- (2) for catastrophic and hazardous failures, introduce physical prevention means against mis-assembly or discuss with the Agency whether physical prevention means is (are) not possible.

7. EVALUATION OF FLIGHT CONTROL SYSTEM FAILURES — CS 25.671(c).

Development errors (i.e. mistake in requirement, design, or implementation) should be considered when demonstrating compliance with CS 25.671(c). However, the guidance provided in this paragraph is not intended to address the means of compliance related to development errors. Development errors are

managed through development assurance processes and system architecture, and are addressed by SAE ARP4754A/EUROCAE ED-79A, AMC 20-115 and AMC 25.1309 with additional Agency guidance.

CS 25.671(c) requires that the aeroplane be shown by analysis, test, or both, to be capable of continued safe flight and landing following failures in the flight control system within the normal flight envelope.

CS 25.671(c)(1) requires the evaluation of any single failure, excluding the types of jams addressed in subparagraph CS 25.671(c)(3). CS 25.671(c)(1) requires that any single failure be considered, suggesting that an alternative means of controlling the aeroplane or an alternative load path be provided in the case of a single failure. All single failures must be considered, even if they can be shown to be extremely improbable.

CS 25.671(c)(2) requires the evaluation of any combination of failures not shown to be extremely improbable, excluding the types of jams addressed in CS 25.671(c)(3).

CS 25.671(c)(3) requires the evaluation of any failure or event that results in a jam of a flight control surface or pilot control. This subparagraph addresses failure modes that would result in the surface or pilot's control being fixed at the position commanded at the time of the failure due to some physical interference. The position at the time of the jam should be at any control position normally encountered during take-off, climb, cruise, normal turns, descent, and landing. In some architectures, component jams within the system may result in failure modes other than a fixed surface or pilot control; those types of jams (such as a jammed valve) are considered under subparagraphs CS 25.671(c)(1) and (c)(2). All single jams must be considered, even if they can be shown to be extremely improbable.

As such, any runaway of a flight control to an adverse position must be accounted for, as per CS 25.671(c)(1) and (c)(2), if such a runaway is due to:

- a single failure; or
- a combination of failures not shown to be extremely improbable.

Some means to alleviate the runaway may be used to demonstrate compliance, such as by reconfiguring the control system, deactivating the system (or a failed portion of it), overriding the runaway by movement of the flight controls in the normal sense, eliminating the consequences of a runaway in order to ensure continued safe flight and landing following a runaway. The consideration of a control runaway will be specific to each application and a general interpretation of an adverse position cannot be given. Where applicable, the applicant is required to assess the resulting surface position after a runaway, if the failure condition is not extremely improbable or can occur due to a single failure.

Additionally, runaways that are caused by external sources, such as a foreign or loose object, control system icing, or any other environmental or external source, are addressed by CS 25.671(c)(4).

It is acknowledged that determining a consistent and reasonable definition of normally encountered flight control positions can be difficult. Experience from in-service aeroplanes shows that the overall failure rate for a flight control surface jam is approximately 10^{-6} to 10^{-7} per flight hour. This probability may be used to justify a definition of 'normally encountered position' and is not intended to be used to support a probabilistic assessment. Considering this in-service aeroplane data, a reasonable definition of normally encountered positions represents the range of flight control surface deflections (from neutral to the largest deflection) expected to occur in 1 000 random operational flights, without considering other failures, for each of the flight segments addressed in this AMC.

One method of establishing acceptable flight control surface deflections is the performance-based criteria outlined in this AMC (see subparagraph b below) which were established to eliminate any differences between aeroplane types. The performance-based criteria prescribe environmental and operational manoeuvre conditions, and the resulting deflections may be considered to be normally encountered positions for compliance with CS 25.671(c)(3).



All approved aeroplane gross weights and centre-of-gravity locations should be considered. However, only critical combinations of gross weight and centre-of-gravity locations should be demonstrated.

a. *Compliance with CS 25.671(c)(2).*

In demonstrating compliance with the failure requirements of CS 25.671(c)(2), the following safety analysis/assessment should be considered.

The safety analysis/assessment requires that the aeroplane be capable of continued safe flight and landing following any combination of failures not shown to be extremely improbable. To satisfy this requirement, a safety analysis/assessment according to AMC 25.1309 should be used.

The aeroelastic stability (flutter) requirements of CS 25.629 should also be considered.

b. *Determination of Flight Control System Jam Positions — CS 25.671(c)(3).*

The following time periods should be considered: ‘take-off’, ‘in-flight’ (climb, cruise, normal turns, descent, and approach), and ‘landing’ (refer to the definitions in paragraph 4 of this AMC).

CS 25.671(c)(3) requires that the aeroplane be capable of landing with a flight control or pilot control jam and that the aeroplane be evaluated for jams in the landing configuration.

Only the aeroplane rigid body modes need to be considered when evaluating the aeroplane response to manoeuvres and continued safe flight and landing.

It should be assumed that, if the jam is detected prior to V_1 , the take-off will be rejected.

Although 1 in 1 000 operational take-offs is expected to include crosswinds of 46 km/h (25 kt) or greater, the short exposure time associated with a flight control surface jam occurring between V_1 and V_{LOF} allows usage of a less conservative crosswind magnitude when determining normally encountered lateral and directional control positions. Given that lateral and directional flight controls are continuously used to maintain runway centre line in a crosswind take-off, and that flight control inputs greater than those necessary at V_1 occur at speeds below V_1 , any jam in these flight control axes during a crosswind take-off is normally detected prior to V_1 . Considering the flight control jam failure rate combined with the short exposure time between V_1 and V_{LOF} , a reasonable crosswind level for the determination of jammed lateral or directional flight control positions during take-off is 28 km/h (15 kt).

A similar reasoning applies for the approach and landing flight phases. It leads to consider that a reasonable crosswind level for the determination of jammed lateral or directional control positions during approach and landing is 28 km/h (15 kt).

The jam positions to be considered in demonstrating compliance should include any position up to the maximum position determined by the following manoeuvres. The manoeuvres and conditions described in this paragraph should only be used to determine the flight control surface and pilot control deflections to evaluate the continued safe flight and landing capability, and should not be used for the evaluation of flight test manoeuvres; see paragraph 7.e below.

(1) *Jammed Lateral Control Positions.*

- (i) Take-off: The lateral flight control position for wings-level at V_1 in a steady crosswind of 28 km/h (15 kt) (at a height of 10 m (35 ft) above the take-off surface). Variations in wind speed from a 10-m (35-ft) height can be obtained using the following relationship:

$$V_{alt} = V_{10metres} * (H_{desired}/10.0)^{1/7}$$

where:

$V_{10metres}$ = wind speed in knots at 10 m (35 ft) above ground level (AGL)

V_{alt} = wind speed at desired altitude (kt)



H_{desired} = desired altitude for which wind speed is sought (AGL), but not lower than 1.5 m (5 ft)

- (ii) In-flight: The lateral flight control position to sustain a 12-degree/second steady roll rate from $1.23V_{\text{SR1}}$ ($1.3V_S$) to $V_{\text{MO}}/M_{\text{MO}}$ or V_{FE} , as appropriate, but not greater than 50 % of the control input.
- (iii) Landing (including flare): The maximum lateral control position is the greater of:
 - (A) the peak lateral control position to maintain wings-level in response to a steady crosswind of 28 km/h (15 kt), in manual or autopilot mode; or
 - (B) the peak lateral control position to maintain wings-level in response to an atmospheric discrete lateral gust of 16 km/h (15 ft/s) from sea level to 6 096 m (20 000 ft).

Note: If the flight control system augments the pilot's input, then the maximum surface deflection to achieve the above manoeuvres should be considered.

(2) *Jammed Longitudinal Control Positions.*

- (i) Take-off: Three longitudinal flight control positions should be considered:
 - (A) Any flight control position from that which the flight controls naturally assume without pilot input at the start of the take-off roll to that which occurs at V_1 using the procedures recommended by the aeroplane manufacturer.
 Note: It may not be necessary to consider this case if it can be demonstrated that the pilot is aware of the jam before reaching V_1 (for example, through a manufacturer's recommended AFM procedure).
 - (B) The longitudinal flight control position at V_1 based on the procedures recommended by the aeroplane manufacturer including the consideration for any runway condition for which the aeroplane is approved to operate.
 - (C) Using the procedures recommended by the aeroplane manufacturer, the peak longitudinal flight control position to achieve a steady aeroplane pitch rate of the lesser of $5^\circ/\text{s}$ or the pitch rate necessary to achieve the speed used for all-engines-operating initial climb procedures (V_2+XX) at 35 ft.
- (ii) In-flight: The maximum longitudinal flight control position is the greater of:
 - (A) the longitudinal flight control position required to achieve steady state normal accelerations from 0.8 to 1.3g at speeds from $1.23V_{\text{SR1}}$ ($1.3V_S$) to $V_{\text{MO}}/M_{\text{MO}}$ or V_{FE} , as appropriate;
 - (B) the peak longitudinal flight control position commanded by the autopilot and/or stability augmentation system in response to atmospheric discrete vertical gust of 16 km/h (15 ft/s) from sea level to 6 096 m (20 000 ft).
- (iii) Landing: Any longitudinal control position required, in manual or autopilot mode, for performing a flare and landing, using the procedures recommended by the aeroplane manufacturer.

(3) *Jammed Directional Control Positions.*

- (i) Take-off: The directional flight control position for take-off at V_1 in a steady crosswind of 28 km/h (15 kt) (at a height of 10 m (35 ft) above the take-off surface). Variations in

wind speed from a height of 10 m (35 ft) can be obtained using the following relationship:

$$V_{\text{alt}} = V_{10\text{metres}} * (H_{\text{desired}}/10.0)^{1/7}$$

where:

$V_{10\text{metres}}$ = wind speed in knots at 10 m above ground level (AGL)

V_{alt} = wind speed at desired altitude

H_{desired} = desired altitude for which wind speed is sought (AGL), but not lower than 1.5 m (5 ft)

- (ii) In-flight: The directional flight control position is the greater of:
- (A) the peak directional flight control position commanded by the autopilot and/or stability augmentation system in response to atmospheric discrete lateral gust of 16 km/h (15 ft/s) from sea level to 6 096 m (20 000 ft);
 - (B) maximum rudder angle required for lateral/directional trim from $1.23V_{SR1}$ ($1.3V_S$) to the maximum all-engines-operating airspeed in level flight with climb power, but not to exceed V_{MO}/M_{MO} or V_{FE} as appropriate. While more commonly a characteristic of propeller aeroplane, this addresses any lateral/directional asymmetry that can occur in flight with symmetric power; or
 - (C) for approach, the peak directional control position commanded by the pilot, autopilot and/or stability augmentation system in response to a steady crosswind of 28 km/h (15 kt).
- (iii) Landing: The maximum directional control position is the greater of:
- (A) the peak directional control position commanded by the pilot, autopilot and/or stability augmentation system in response to a steady crosswind of 28 km/h (15 kt); or
 - (B) the peak directional control position commanded by the pilot, autopilot and/or stability augmentation system in response to an atmospheric discrete lateral gust of 16 km/h (15 ft/s) from sea level to 6096 m (20 000 ft).

(4) Control Tabs, Trim Tabs, and Trimming Stabilisers.

Any tabs installed on flight control surfaces are assumed jammed in the position associated with the normal deflection of the flight control surface on which they are installed.

Trim tabs and trimming stabilisers are assumed jammed in the positions associated with the procedures recommended by the aeroplane manufacturer for take-off and that are normally used throughout the flight to trim the aeroplane from $1.23V_{SR1}$ ($1.3V_S$) to V_{MO}/M_{MO} or V_{FE} , as appropriate.

(5) Speed Brakes.

Speed brakes are assumed jammed in any position for which they are approved to operate during flight at any speed from $1.23V_{SR1}$ ($1.3V_S$) to V_{MO}/M_{MO} or V_{FE} , as appropriate. Asymmetric extension and retraction of the speed brakes should be considered. Roll spoiler jam (asymmetric spoiler panel) is addressed in paragraph 7.b(1).

(6) High-Lift Devices.

Leading edge and trailing edge high-lift devices are assumed to jam in any position for take-off, climb, cruise, approach, and landing. Skew of high-lift devices or asymmetric extension and retraction should be considered; CS 25.701 contains a requirement for flap mechanical interconnection unless the aeroplane has safe flight characteristics with the asymmetric flap positions.

(7) *Load Alleviation Systems.*

- (i) Gust Load Alleviation Systems: At any airspeed between $1.23V_{SR1}$ ($1.3V_S$) to V_{MO}/M_{MO} or V_{FE} , as appropriate, the flight control surfaces are assumed to jam in the maximum position commanded by the gust load alleviation system in response to an atmospheric discrete gust with the following reference velocities:
 - (A) 16 km/h (15 ft/s) equivalent airspeed (EAS) from sea level to 6 096 m (20 000 ft) (vertical gust);
 - (B) 16 km/h (15 ft/s) EAS from sea level to 6096 m (20 000 ft) (lateral gust).
- (ii) Manoeuvre Load Alleviation Systems: At any airspeed between $1.23V_{SR1}$ ($1.3V_S$) to V_{MO}/M_{MO} or V_{FE} , as appropriate, the flight control surfaces are assumed to jam in the maximum position commanded by the manoeuvre load alleviation system during a pull-up manoeuvre to 1.3 g or a push-over manoeuvre to 0.8 g.

c. *Considerations for jams just before landing — CS 25.671(c)(3)(i) and (ii).*

CS 25.671(c)(3)(ii) requires that failures (leading to a jam) must be assumed to occur anywhere within the normal flight envelope. This includes the flight phase just before landing and the landing itself. For the determination of the jam position per CS 25.671(c)(3)(i) and the assessment of continued safe flight and landing, guidance is provided in this AMC. However, there might be exceptional cases where it is not possible to demonstrate continued safe flight and landing. Even jam alleviation means (for example, disconnect units) might not be efficient because of the necessary time for the transfer of pilot controls.

For these exceptional cases the jam should be shown to be extremely improbable. This may be performed as follows:

- (1) Demonstrate continued safe flight and landing after a jam has occurred just before landing;
- (2) If continued safe flight and landing cannot be demonstrated, perform a qualitative assessment of the design, relative to jam prevention features and jam alleviation means; or
- (3) As a last resort, after agreement by the Agency, use data from in-service aeroplanes to support an extremely improbable argument (without use of at-risk time).

If the extremely improbable demonstration (using either method (1), (2) or (3)) is accepted by the Agency, the design would be considered to be compliant with the intent of CS 25.671(c)(3)(i) and (ii).

The typical means of jam prevention/alleviation include low-friction materials, dual-rotation bearings, clearances, jack catchers.

The assessment of continued safe flight and landing in paragraph 7.e below also applies to jams occurring just before landing.

d. *Jam Combinations Failures — CS 25.671(c)(3)(iii).*

In addition to the demonstration of jams at 'normally encountered position', compliance with CS 25.671(c)(3) should include an analysis that shows that a minimum level of safety exists when a jam occurs. This additional analysis must show that in the presence of a jam considered under CS 25.671(c)(3), the failure states that could prevent continued safe flight and landing have a combined probability of 1/1000 or less.

As a minimum, this analysis should include elements such as a jam breakout or override, disconnect means, alternate flight surface control, alternate electrical or hydraulic sources, or alternate cable paths. This analysis should help to determine the intervals for scheduled maintenance activity or the operational checks that ensure the availability of the alleviation or compensation means.



e. *Assessment of Continued Safe Flight and Landing — CS 25.671(c).*

Following a flight control system failure of the types discussed in paragraphs 7.a, 7.b, 7.c and 7.d of this AMC, the manoeuvrability and structural strength criteria defined in the following paragraphs should be considered to determine the capability of continued safe flight and landing of the aeroplane.

A local structural failure (e.g. via a mechanical fuse or shear-out) that could lead to a surface departure from the aeroplane should not be used as a means of jam alleviation.

(1) *Flight Characteristics.*

(i) *General.* Following a flight control system failure, appropriate procedures may be used including system reconfiguration, flight limitations, and flight crew resource management. The procedures for safe flight and landing should not require exceptional piloting skill or strength.

Additional means of control, such as trim system, may be used if it can be shown that the systems are available and effective. Credit should not be given to the use of differential engine thrust to manoeuvre the aeroplane. However, differential thrust may be used after the recovery in order to maintain lateral/directional trim.

For the longitudinal flight control surface jam during take-off prior to rotation, it is necessary to show that the aeroplane can be safely rotated for lift-off without consideration of field length available.

(ii) *Transient Response.* There should be no unsafe conditions during the transient condition following a flight control system failure. The evaluation of failures, or manoeuvres, leading to a jam, is intended to be initiated at 1-g wings-level flight. For this purpose, continued safe flight and landing (within the transition phase) is generally defined as not exceeding any one of the following criteria:

- (A) a load on any part of the primary structure sufficient to cause a catastrophic structural failure;
- (B) catastrophic loss of flight path control;
- (C) exceedance of V_{DF}/M_{DF} ;
- (D) catastrophic flutter;
- (E) vibration and buffeting conditions;
- (F) bank angle in excess of 90 degrees.

In connection with the transient response, compliance with the requirements of CS 25.302 should be demonstrated. While V_F is normally an appropriate airspeed limit to be considered regarding continued safe flight and landing, temporary exceedance of V_F may be acceptable as long as the requirements of CS 25.302 are met.

Paragraph 7.b. of this AMC provides a means to determine flight control surface deflections for the evaluation of flight control jams. In some cases, aeroplane roll, or pitch rate, or normal acceleration is used as a basis to determine these deflections. The roll or pitch rate and/or normal acceleration used to determine the flight control surface deflection need not be included in the evaluation of the transient condition. For example, the in-flight lateral flight control position determined in paragraph 7.b.(1)(ii) is based on a steady roll rate of 12°/s. When evaluating this condition, either by analysis, simulation or in-flight demonstration, the resulting flight control surface deflection is simply input while the aeroplane is in wings-level flight, at the appropriate speed, altitude, etc. During this evaluation, the actual roll or pitch rate of the aeroplane may or may not be the same as the roll or pitch rate used to determine the jammed flight control surface position.



(iii) *Delay Times*. Due consideration should be given to the delays involved in pilot recognition, reaction, and operation of any disconnect systems, if applicable.

Delay = Recognition + Reaction + Operation of Disconnect

Recognition is defined as the time from the failure condition to the point at which a pilot in service operation may be expected to recognise the need to take action. Recognition of the malfunction may be through the behaviour of the aeroplane or a reliable failure warning system, and the recognition point should be identified but should not normally be less than 1 second. For flight control system failures, except the types of jams addressed in CS 25.671(c)(3), control column or wheel movements alone should not be used for recognition.

The following reaction times should be used:

Flight condition	Reaction time
On ground	1 second*
In air (< 300 m (1 000 ft) above ground level (AGL))	1 second*
Manual flight (> 300 m (1 000 ft) AGL)	1 second*
Automatic flight (> 300 m (1 000 ft) AGL)	3 seconds

*3 seconds if control must be transferred between pilots.

The time required to operate any disconnect system should be measured either through ground test or flight test. This value should be used during all analysis efforts. However, flight test or manned simulation that requires the pilot to operate the disconnect includes this extra time; therefore, no additional delay time would be needed for these demonstrations.

(iv) *Manoeuvre Capability for Continued Safe Flight and Landing*. If, using the procedures recommended by the aeroplane manufacturer, the following manoeuvres can be performed following the failure, it will generally be considered that continued safe flight and landing has been shown:

- (A) A steady 30° banked turn to the left or right;
- (B) A roll from a steady 30° banked turn through an angle of 60° so as to reverse the direction of the turn in not more than 11 seconds (in this manoeuvre, the rudder may be used to the extent necessary to minimise side-slip, and the manoeuvre may be unchecked);
- (C) A push-over manoeuvre to 0.8 g, and a pull-up manoeuvre to 1.3 g;
- (D) A wings-level landing flare in a 90° crosswind of up to 18.5 km/h (10 kt) (measured at 10 m (33 ft) above the ground); and
- (E) The aeroplane remains on the paved runway surface during the landing roll, until reaching a complete stop.

Note: In the case of a lateral or directional flight control system jam during take-off as described in paragraph 7.b(1) or 7.b(3) of this AMC, it should be shown that the aeroplane can safely land on a suitable runway, without crosswind and with crosswind speeds up to the value at which the jam was established.

(v) *Control Forces*. The short- and long-term control forces should not be greater than 1.5 times the short- and long-term control forces allowed by CS 25.143(d).

Short-term forces have typically been interpreted to mean the time required to accomplish a configuration or trim change. However, taking into account the capability of the crew to share the workload, the short-term forces provided in CS 25.143(d) may be appropriate for a longer duration, such as the evaluation of a jam on take-off and return to landing.

During the recovery following the failure, transient control forces may exceed these criteria to a limited extent. Acceptability of any exceedance will be evaluated on a case-by-case basis.

(2) *Structural Strength for Flight Control System Failures*.

(i) *Failure Conditions per CS 25.671(c)(1) and (c)(2)*. It should be shown that the aeroplane maintains structural integrity for continued safe flight and landing. This should be accomplished by demonstrating compliance with CS 25.302, unless otherwise agreed with the Agency.

(ii) *Jam Conditions per CS 25.671(c)(3) and Runaways of Flight Control System or Surface per CS 25.671(c)(4)*. It should be shown that the aeroplane maintains structural integrity for continued safe flight and landing. Recognising that jams and runaways are infrequent occurrences and that margins have been taken in the definition of normally encountered positions in this AMC, criteria other than those specified in CS 25.302 and Appendix K, K25.2(c), may be used for the structural substantiation to show continued safe flight and landing.

The structure must be designed such that continued safe flight and landing is ensured after any single jam in a normally encountered position or after a runaway.

Attention should be paid to the detectability of the jam or the runaway and the risk for the jam or the runaway, and/or its consequences, to remain hidden for more than one flight.

This structural substantiation should take into account paragraph 7.e.(2)(iii) of this AMC.

(iii) *Structural Substantiation*. The loads considered as ultimate should be derived from the following conditions at speeds up to the maximum speed allowed for the jammed position or for the failure condition:

- (A) Balanced manoeuvre of the aeroplane between 0.25 and 1.75 g with high-lift devices fully retracted and in en-route configurations, and between 0.6 and 1.4 g with high-lift devices extended;
- (B) Vertical and lateral discrete gusts corresponding to 40 % of the limit gust velocity specified at V_c in CS 25.341(a) with high-lift devices fully retracted, and a 5.2-m/s (17-ft/s) vertical and 5.2-m/s (17-ft/s) head-on gust with high-lift devices extended. The vertical and lateral gusts should be considered separately.

A flexible aeroplane model should be used for load calculations, where the use of a flexible aeroplane model is significant for the loads being assessed.

8. EVALUATION OF ALL-ENGINES-FAILED CONDITION — CS 25.671(d).

a. *Explanation*.

The intent of CS 25.671(d) is to assure that in the event of failure of all engines, the aeroplane will be controllable, an approach and a flare to a landing and to a ditching is possible and, assuming that a suitable runway is available, the aeroplane is controllable on ground and can be stopped.

In this context:

- ‘flare to a landing/ditching’ refers to the time until touchdown;
- ‘suitable runway’ is a hard-surface runway or equivalent for which the distance available following touchdown is consistent with the available aeroplane ground deceleration capability.

Although the rule refers to ‘flare to a landing’ with the implication of being on a runway, it is recognised that with all engines inoperative it may not be possible to reach a suitable runway or landing surface; in this case, the aeroplane must still be able to make a flare to landing attitude.

Compliance with CS 25.671(d) effectively requires that the aeroplane is equipped with a source(s) of emergency power, such as an air-driven generator, windmilling engines, batteries, or other power source, capable of providing adequate power to the systems that are necessary to control the aeroplane.

Analysis, simulation, or a combination of analysis and simulation may be used to demonstrate compliance where the methods are shown to be reliable.

b. *Procedures.*

(1) The aeroplane should be evaluated to determine that it is possible, without requiring exceptional piloting skill or strength, to maintain control following the failure of all engines and attain the parameters provided in the operational procedure of the aeroplane flight manual (AFM), taking into account the time necessary to activate any backup systems. The aeroplane should also remain controllable during restart of the most critical engine, whilst following the AFM recommended engine restart procedures.

(2) The most critical flight phases, especially for aeroplanes with emergency power systems dependent on airspeed, are likely to be the take-off and the landing. Credit may be taken from the hydraulic pressure and/or the electrical power produced while the engines are spinning down and from any residual hydraulic pressure remaining in the system. Sufficient power must be available to complete a wings-level approach and flare to a landing, and flare to a ditching.

Analyses or tests may be used to demonstrate the capability of the control systems to maintain adequate hydraulic pressure and/or electrical power during the time between the failure of the engines and the activation of any power backup systems. If any of the power backup systems rely on aerodynamic means to generate the power, then a flight test should be conducted to demonstrate that the power backup system can supply adequate electrical and/or hydraulic power to the control systems. The flight test should be conducted at the minimum practical airspeed required to perform an approach and flare to a safe landing and ditching attitude.

(3) The manoeuvre capability following the failure of all engines should be sufficient to complete an approach and flare to a landing, and flare to a ditching. Note that the aeroplane weight could be extremely low (e.g. the engine failures could be due to fuel exhaustion). The maximum speeds for approach and landing/ditching may be limited by other CS-25 specifications (e.g. tyre speeds, flap or landing gear speeds, etc.) or by an evaluation of the average pilot ability to conduct a safe landing/ditching. At an operational weight determined for this case and for any other critical weights and positions of the centre of gravity identified by the applicant, at speeds down to the approach speeds appropriate to the aeroplane configuration, the aeroplane should be capable of performing the following:

- (i) a steady 30° banked turn to the left or right;
- (ii) a roll from a steady 30° banked turn through an angle of 60° so as to reverse the direction of the turn in not more than 11 s (in this manoeuvre, the rudder may be used to the extent necessary to minimise side-slip, and the manoeuvre may be unchecked);
- (iii) a push-over manoeuvre to 0.8 g, and a pull-up manoeuvre to 1.3 g;



- (iv) a wings-level landing flare in a 90° crosswind of up to 18.5 km/h (10 kt) (measured at 10 m (33 ft) above the ground).

Note: If the loss of all engines has no effect on the flight control authority of the aeroplane, then the results of the flight tests of the basic handling qualities with all engines operating may be used to demonstrate the satisfactory handling qualities of the aeroplane with all engines failed.

- (4) It should be possible to perform a flare to a safe landing and ditching attitude, in the most critical configuration, from a stabilised approach using the recommended approach speeds, pitch angles, and the appropriate AFM procedures, without requiring exceptional piloting skill or strength. For transient manoeuvres, forces are allowed up to 1.5 times those specified in CS 25.143(d) for temporary application with two hands available for control.
- (5) Finally, assuming that a suitable runway is available, it should be possible to control the aeroplane until it comes to a complete stop on the runway. A means of positive deceleration should be provided.

A suitable runway should have the lateral dimensions, length and load-bearing capability which meets the requirements defined in the emergency procedures of the AFM.

It is not necessary to consider adverse environmental conditions (e.g. wet or contaminated runway, tailwind) when demonstrating compliance for the on-ground phase.

9. EVALUATION OF CONTROL AUTHORITY AWARENESS — CS 25.671(e).

CS 25.671(e) requires ‘suitable’ annunciation to the flight crew when a flight condition exists in which near full-flight control authority (whether or not it is pilot-commanded) is being used. Suitability of such an annunciation should take into account that some pilot-commanded manoeuvres (e.g. rapid roll) are necessarily associated with intended full performance, which may saturate the surface. Therefore, simple alerting systems, which should function in both intended and unexpected flight control-limiting situations, should be properly balanced between needed crew awareness and nuisance alerting. Nuisance alerting must be minimised per CS 25.1322 by correct setting of the alerting threshold. The term ‘suitable’ indicates an appropriate balance between nuisance and necessary operation.

Depending on the application, suitable annunciations may include cockpit flight control position, annunciator light, or surface position indicators. Furthermore, this requirement applies to the limits of flight control authority, not necessarily to the limits of any individual surface travel.

When the aeroplane is equipped with an unpowered manual flight control system, the pilot may be de facto aware of the limit of control authority. In this case, no other means of annunciation should be required.

10. EVALUATION OF FLIGHT CONTROL SYSTEM MODES OF OPERATION — CS 25.671(f).

Some flight control systems, for instance, electronic flight control systems, may have multiple modes of operation not restricted to being either on or off. The applicant should evaluate the different modes of operation and the transition between them in order to establish if they are intuitive or not.

If these modes, or the transition between them, are not intuitive, an alert to the flight crew may be required. Any alert must comply with CS 25.1322. This includes the indication to the flight crew of the loss of protections.



11. DEMONSTRATION OF ACCEPTABLE MEANS OF COMPLIANCE.

It is recognised that it may be neither practical nor appropriate to demonstrate compliance by flight test for all of the failure conditions noted herein. Compliance may be demonstrated by analysis, simulation, a piloted engineering simulator, flight test, or combination of these methods as agreed with the Agency. Simulation methods should include an accurate representation of the aeroplane characteristics and of the pilot response, including time delays as specified in paragraph 7.e(1)(iii) of this AMC.

Compliance with CS 25.671 may result in AFM non-normal procedures. Verification of these procedures may be accomplished in flight or, with the agreement of the Agency, using a piloted simulator.

a. *Acceptable Use of Simulations.* It is generally difficult to define the types of simulations that might be acceptable in lieu of flight test without identifying specific conditions or issues. However, the following general principles can be used as guidance for making this kind of decision:

- (1) In general, flight test is the preferred method to demonstrate compliance;
- (2) Simulation may be an acceptable alternative to flight test, especially when:
 - (i) a flight test would be too risky even after attempts to mitigate these risks (e.g. 'simulated' take-offs/landings at high altitude);
 - (ii) the required environmental conditions, or the representation of the failure states, are too difficult to attain (e.g. wind shear, high crosswinds, system failure configurations);
 - (iii) the simulation is used to augment a reasonably broad flight test programme;
 - (iv) the simulation is used to demonstrate repeatability.

b. *Simulation Requirements.* In order to be acceptable for use in demonstrating compliance with the requirements for performance and handling qualities, a simulation method should:

- (1) be suitably validated by flight test data for the conditions of interest; furthermore:
 - (i) this does not mean that there must be flight test data at the exact conditions of interest; the reason why a simulation method is being used may be that it is too difficult or risky to obtain flight test data at the conditions of interest;
 - (ii) the level of substantiation of the simulator to flight correlation should be commensurate with the level of compliance (i.e. unless it is determined that the simulation is conservative, the closer the case is to being non-compliant, the higher the required quality of the simulation);
- (2) be conducted in a manner appropriate to the case and conditions of interest:
 - (i) if closed-loop responses are important, the simulation should be piloted by a human pilot;
 - (ii) for piloted simulations, the controls/displays/cues should be substantially equivalent to what would be available in the real aeroplane (unless it is determined that not doing so would provide added conservatism).

12. SPECIFICITIES OF AEROPLANES WITH FLY-BY-WIRE FLIGHT CONTROL SYSTEMS.

a. *Control Signal Integrity.*

If the aeroplane is equipped with a conventional flight control system, the transmission of command signals to the primary and secondary flight control surfaces is made through conventional mechanical and hydromechanical means.

The determination of the origin of perturbations to command transmissions is relatively straightforward since failure cases can usually be classified in a limited number of categories that include maintenance

error, jamming, disconnection, runaway, failure of mechanical element, or structural failure of hydraulic components. Therefore, it is almost always possible to identify the most severe failure cases that would serve as an envelope to all other cases that have the same consequences.

However, when the aeroplane is equipped with flight control systems using the fly-by-wire technology, incorporating digital devices and software, experience from electronic digital transmission lines shows that the perturbation of signals from internal and external sources is not unlikely.

The perturbations are described as signals that result from any condition that is able to modify the command signal from its intended characteristics. They can be classified in two categories:

- (1) Internal causes that could modify the command and control signals include but are not limited to:
 - loss of data bits, frozen or erroneous values;
 - unwanted transients;
 - computer capacity saturation;
 - processing of signals by asynchronous microprocessors;
 - adverse effects caused by transport lag;
 - poor resolution of digital signals;
 - sensor noise;
 - corrupted sensor signals;
 - aliasing effects;
 - inappropriate sensor monitoring thresholds;
 - structural interactions (such as control surface compliance or coupling of structural modes with control modes) that may adversely affect the system operation.
- (2) External causes that could modify the command and control signals include but are not limited to:
 - high-intensity radiated fields (HIRF);
 - lightning;
 - electromagnetic interference (EMI) effects (e.g. motor interference, aeroplane's own electrical power and power switching transients, smaller signals if they can affect flight control, transients due to electrical failures.)

Spurious signals and/or false data that are a consequence of perturbations in either of the two above categories may result in malfunctions that produce unacceptable system responses equivalent to those of conventional systems such as limit cycle/oscillatory failures, runaway/hardover conditions, disconnection, lockups and false indication/warning that consequently present a flight hazard. It is imperative that the command signals remain continuous and free from internal and external perturbations and common-cause failures. Therefore, special design measures should be employed to maintain system integrity at a level of safety at least equivalent to that which is achieved with traditional hydromechanical designs. These special design measures can be monitored through the system safety assessment (SSA) process, provided specific care is directed to development methods and on quantitative and qualitative demonstrations of compliance.

The following should be considered when evaluating compliance with CS 25.671(c)(2):

- (1) The flight control system should continue to provide its intended function, regardless of any malfunction from sources in the integrated systems environment of the aeroplane.



(2) Any malfunctioning system in the aerodynamic loop should not produce an unsafe level of uncommanded motion and should automatically recover its ability to perform critical functions upon removal of the effects of that malfunction.

(3) Systems in the aerodynamic loop should not be adversely affected during and/or after exposure to any sources of a malfunction.

(4) Any disruption to an individual unit or component as a consequence of a malfunction, and which requires annunciation and flight crew action, should be identified to and approved by the Agency to assure that: a) the failure can be recognised by the flight crew, and b) the flight crew action can be expected to result in continued safe flight and landing.

(5) An automatic change from a normal to a degraded mode that is caused by spurious signal(s) or malfunction(s) should meet the probability guidelines associated with the hazard assessment established in AMC 25.1309, e.g. for a condition assessed as 'major', the probability of occurrence should be no more than 'remote' ($P_c < 10^{-5}$ per flight hour).

(6) Exposure to a spurious signal or malfunction should not result in a hazard with a probability greater than that allowed by the criteria of AMC 25.1309. The impact on handling qualities should be evaluated.

The complexity and criticality of the fly-by-wire flight control system necessitates the additional laboratory testing beyond that required as part of individual equipment validation and software verification.

It should be shown that either the fly-by-wire flight control system signals cannot be altered unintentionally, or that altered signal characteristics would meet the following criteria:

(1) Stable gain and phase margins are maintained for all control surface closed-loop systems. Pilot control inputs (pilot in the loop) are excluded from this requirement;

(2) Sufficient pitch, roll, and yaw control power is available to provide control for continued safe flight and landing, considering all the fly-by-wire flight control system signal malfunctions that are not extremely improbable; and

(3) The effect of spurious signals on the systems which are included in the aerodynamic loop should not result in unacceptable transients or degradation of the performance of the aeroplane. Specifically, in case of signals that would cause a significant uncommanded motion of a control surface actuator, either the signal should be readily detected and deactivated or the surface motion should be arrested by other means in a satisfactory manner. Small amplitude residual system oscillations may be acceptable.

It should be demonstrated that the output from the control surface closed-loop system does not result in uncommanded, sustained oscillations of flight control surfaces. The effects of minor instabilities may be acceptable, provided that they are thoroughly investigated, documented, and understood. An example of an acceptable condition would be one where a computer input is perturbed by spurious signals, but the output signal remains within the design tolerances, and the system is able to continue to operate in its selected mode of operation and is not affected by this perturbation.

When demonstrating compliance with CS 25.671(c), these system characteristics should be demonstrated using the following means:



(1) Systematic laboratory validation which includes a realistic representation of all relevant interfacing systems, and associated software, including the control system components which are part of the pitch, roll and yaw axis control. Closed-loop aeroplane simulation/testing is necessary in this laboratory validation;

(2) Laboratory or aeroplane testing to demonstrate unwanted coupling of electronic command signals and their effects on the mechanical actuators and interfacing structure over the spectrum of operating frequencies; and

(3) Analysis or inspection to substantiate that physical or mechanical separation and segregation of equipment or components are utilised to minimise any potential hazards.

A successful demonstration of signal integrity should include all the elements which contribute to the command and control signals to the 'aerodynamic closed loop' that actuates the aerodynamic control surfaces (e.g. rudder, elevator, stabiliser, flaps, and spoilers). The 'aerodynamic closed loop' should be evaluated for the normal and degraded modes. Elements of the integrated 'aerodynamic closed loop' may include, for example: digital or analogue flight control computers, power control units, control feedback, major data busses, and the sensor signals including: air data, acceleration, rate gyros, commands to the surface position, and respective power supply sources. Autopilot systems (including feedback functions) should be included in this demonstration if they are integrated with the fly-by-wire flight control system.

b. *Formalisation of Compliance Demonstration for Electronic Flight Control Laws.*

On fly-by-wire aeroplanes, flight controls are implemented according to complex control laws and logics.

The handling qualities certification tests, usually performed on conventional aeroplanes to demonstrate compliance with CS-25 Subpart B specifications, are not considered to be sufficient to demonstrate the behaviour of the flight control laws in all foreseeable situations that may be encountered in service.

In order to demonstrate compliance with an adequate level of formalisation, the following should be performed and captured within certification documents:

- Determination of the flight control characteristics that require detailed and specific test strategy; and
- Substantiation of the proposed validation strategy (flight tests, simulator tests, analyses, etc.) covering the characteristics and features determined above.

In particular, the following characteristics of flight control laws should be covered:

- discontinuities;
- robustness versus piloted manoeuvres and/or adverse weather conditions;
- protections priorities (entry/exit logic conditions not symmetrical);
- control law mode changes with and without failures; and
- determination of critical scenario for multiple failures.

The validation strategy should include, but should not be limited to, operational scenarios. The determination that an adequate level of formalisation of validation strategy has been achieved should be based on engineering judgement.



AMC 25.672(c)(1) is deleted:

~~AMC 25.672(c)(1)~~

~~Stability Augmentation and Automatic and Power-operated Systems~~

~~The severity of the flying quality requirement should be related to the probability of the occurrence in a progressive manner such that probable occurrences have not more than minor effects and improbable occurrences have not more than major effects.~~

AMC — SUBPART E

AMC 25.933(a)(1) is amended as follows:

AMC 25.933(a)(1)

Unwanted in-flight thrust reversal of turbojet thrust reversers

...

8. “RELIABILITY OPTION”: PROVIDE CONTINUED SAFE FLIGHT AND LANDING BY PREVENTING ANY IN-FLIGHT THRUST REVERSAL

...

8.b. System Safety Assessment (SSA): (...)

The primary intent of this approach to compliance is to improve safety by promoting more reliable designs and better maintenance, including minimising pre-existing faults. Latent failures involved in unwanted in-flight thrust reversal should be avoided whenever practicable. The design configurations in paragraphs 8.b.(2) and 8.b.(3) have traditionally been considered to be practicable and deemed to be acceptable to the Agency. ~~However, it also recognises that flexibility of design and maintenance are necessary for practical application.~~

(...)

8.b.(3) For configurations in which combinations of three or more failure situations result in in-flight thrust reversal, the following applies:

In order to limit the exposure to pre-existing failure situations, the maximum time each pre-existing failure situation is expected to be present should be related to the frequency with which the failure situation is anticipated to occur, such that their product is 1×10^{-3} /h or less.

(...)



AMC — SUBPART F

AMC 25.1309 is amended as follows:

AMC 25.1309**System Design and Analysis****Table of Contents**

1. **PURPOSE**
2. **RESERVED**
3. **RELATED DOCUMENTS**
 - a. *Advisory Circulars, Acceptable Means of Compliance*
 - b. *Industry Documents*
4. **APPLICABILITY OF CS 25.1309**
5. **DEFINITIONS**
6. **BACKGROUND**
 - a. *General*
 - b. *Fail-Safe Design Concept*
 - c. *Development of Aeroplane and System Functions*
7. **FAILURE CONDITION CLASSIFICATIONS AND PROBABILITY TERMS**
 - a. *Classifications*
 - b. *Qualitative Probability Terms*
 - c. *Quantitative Probability Terms*
8. **SAFETY OBJECTIVE**
9. **COMPLIANCE WITH CS 25.1309**
 - a. *Compliance with CS 25.1309(a)*
 - b. *Compliance with CS 25.1309(b)*
 - (1) *General*
 - (2) *Planning*
 - (3) *Availability of Industry Standards and Guidance Materials*
 - (4) *Acceptable Application of Development Assurance Methods*
 - (5) *Crew and Maintenance Actions*
 - (6) *Significant Latent Failures*
 - c. *Compliance with CS 25.1309(c)*
10. **IDENTIFICATION OF FAILURE CONDITIONS AND CONSIDERATIONS WHEN ASSESSING THEIR EFFECTS**
 - a. *Identification of Failure Conditions*



b. Identification of Failure Conditions Using a Functional Hazard Assessment

c. Considerations When Assessing Failure Condition Effects

11. ASSESSMENT OF FAILURE CONDITION PROBABILITIES AND ANALYSIS CONSIDERATIONS

a. Assessment of Failure Condition Probabilities

b. Single Failure Considerations

c. Common-Cause Failure Considerations

d. Depth of Analysis

e. Calculation of Average Probability per Flight Hour (Quantitative Analysis)

f. Integrated Systems

g. Operational or Environmental Conditions

h. Justification of Assumptions, Data Sources and Analytical Techniques

12. OPERATIONAL AND MAINTENANCE CONSIDERATIONS

a. Flight Crew Action

b. Maintenance Action

c. Candidate Certification Maintenance Requirements

d. Flight with Equipment or Functions known to be Inoperative

13. ASSESSMENT OF MODIFICATIONS TO PREVIOUSLY CERTIFIED AEROPLANES

APPENDIX 1. ASSESSMENT METHODS

APPENDIX 2. SAFETY ASSESSMENT PROCESS OVERVIEW

APPENDIX 3. CALCULATION OF THE AVERAGE PROBABILITY PER FLIGHT HOUR

APPENDIX 4. ALLOWABLE PROBABILITIES

APPENDIX 5. EXAMPLE OF LIMIT LATENCY AND RESIDUAL PROBABILITY ANALYSIS

(...)

4. APPLICABILITY OF CS 25.1309.

(...)

b. ~~Certain single failures or jams~~ Certain jams of flight control surfaces or pilot controls and flight control system/surface runaways covered by ~~CS 25.671(c)(1) and CS 25.671(c)(3) and CS 25.671(c)(4)~~ are excepted from the requirements of CS 25.1309(b)(1)(ii). ~~CS 25.671(c)(1) requires the consideration of single failures, regardless of the probability of the failure. CS 25.671(c)(1) does not consider the effects of single failures if their probability is shown to be extremely improbable and the failures also meet the requirements of CS 25.571(a) and (b).~~

(...)

d. The failure conditions covered by CS 25.810 and CS 25.812 are excepted from the requirements of CS 25.1309(b). These ~~F~~ failure ~~C~~ conditions related to loss of function are associated with varied evacuation scenarios for which the probability cannot be determined. (...)

f. Some systems and some functions already receive an evaluation to show compliance with specific requirements for specific ~~F~~ failure ~~C~~ conditions and therefore meet the intent of CS 25.1309 without the need for additional analysis for those specific ~~F~~ failure ~~C~~ conditions.



- g. The functional hazard assessment should consider the effects of failure conditions during flight and on ground from the time when any person boards the aeroplane with the intention of flight until such time when all these persons have disembarked. While this does include the conditions associated with the preflight preparation, embarkation and disembarkation, taxi phase and the like, it therefore does not include periods of shop maintenance, storage, or other out-of-service activities.
- h. Effects on persons other than the aeroplane occupants should be taken into account when assessing failure conditions in compliance with CS 25.1309. Such effects may result from threats to people on the ground or adjacent to the aeroplane during ground operations, electric shock threats to mechanics, and other similar situations.

5. DEFINITIONS.

(...)

- c. *At-Risk Time*. The period of time during which an item must fail in order to cause the failure effect in question. This is usually associated with the final fault in a fault sequence leading to a specific failure condition.
- dē. *Average Probability Per Flight Hour*. (...)
- ēē. *Candidate Certification Maintenance Requirements (CCMR)*. A periodic maintenance or flight crew check may be used in a safety analysis to help demonstrate compliance with CS 25.1309(b) for Hazardous and Catastrophic Failure Conditions. (...)
- fe. *Check*. (...)
- gf. *Complex*. (...)
- h. *Complexity*. An attribute of functions, systems or items, which makes their operation, failure modes, or failure effects difficult to comprehend without the aid of analytical methods.
- ig. *Conventional*. (...)
- jh. *Design Appraisal*. (...)
- ki. *Development Assurance*. (...)
- lj. *Development Error*. (...)
- mk. *Error*. An omission or incorrect action by a crewmember or maintenance personnel, or a development error (i.e. mistake in requirements determination, design, or implementation).
- nł. *Event*. (...)
- o. *Exposure Time*. The period of time between the time when an item was last known to be operating properly and the time when it will be known to be operating properly again.
- pā. *Failure*. (...)
- qā. *Failure Condition*. (...)
- rē. *Installation Appraisal*. (...)
- sp. *Item*. (...)
- te. *Latent Failure*. A failure is latent until it is made known to the flight crew or maintenance personnel. A significant latent failure is one, which would in combination with one or more specific failures, or events result in a Hazardous or Catastrophic Failure Condition.
- uf. *Qualitative*. (...)
- vs. *Quantitative*. (...)



wł. *Redundancy.* (...)

x. *Significant Latent Failure.* A latent failure that would, in combination with one or more specific failure(s) or event(s), result in a hazardous or catastrophic failure condition.

ys. *System.* A combination of interrelated items arranged components, parts, and elements, which are inter-connected to perform one or more specific functions.

6. BACKGROUND.

a. *General.*

For a number of years aeroplane systems were evaluated to specific requirements, to the "single fault" criterion, or to the fail-safe design concept. As later-generation aeroplanes developed, more safety-critical functions were required to be performed, which generally resulted in an increase in the complexity of the systems designed to perform these functions. The potential hazards to the aeroplane and its occupants which could arise in the event of loss of one or more functions provided by a system or that system's malfunction had to be considered, as also did the interaction between systems performing different functions. This has led to the general principle that an inverse relationship should exist between the probability of a failure condition and its effect on the aeroplane and/or its occupants (see Figure 1). In assessing the acceptability of a design it was recognised that rational probability values would have to be established. Historical evidence indicated that the probability of a serious accident due to operational and airframe-related causes was approximately one per million hours of flight. Furthermore, about 10 per cent percent of the total were attributed to failure conditions caused by the aeroplane's systems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs. It is reasonable to expect that the probability of a serious accident from all such failure conditions be not greater than one per ten million flight hours or 1×10^{-7} per flight hour for a newly designed aeroplane. The difficulty with this is that it is not possible to say whether the target has been met until all the systems on the aeroplane are collectively analysed numerically. For this reason it was assumed, arbitrarily, that there are about one hundred potential failure conditions in an aeroplane, which could be catastrophic. The target allowable average probability per flight hour of 1×10^{-7} was thus apportioned equally among these failure conditions, resulting in an allocation of not greater than 1×10^{-9} to each. The upper limit for the average probability per flight hour for catastrophic failure conditions would be 1×10^{-9} , which establishes an approximate probability value for the term "Extremely improbable". Failure conditions having less severe effects could be relatively more likely to occur.

b. *Fail-Safe Design Concept.*

The CS-25 airworthiness standards are based on, and incorporate, the objectives and principles or techniques of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design.

(1) The following basic objectives pertaining to failures apply:

- (i) In any system or subsystem, the failure of any single element, component, or connection during any one flight should be assumed, regardless of its probability. Such single failures should not be catastrophic.
- (ii) Subsequent failures of related systems during the same flight, whether detected or latent, and combinations thereof, should also be considered assumed, unless their joint probability with the first failure is shown to be extremely improbable.

(2) The fail-safe design concept uses the following design principles or techniques in order to ensure a safe design. The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design; i.e. to ensure that



Major Failure Conditions are Remote, Hazardous Failure Conditions are Extremely Remote, and Catastrophic Failure Conditions are Extremely Improbable:

(...)

c. ~~Highly Integrated Systems.~~ *Development of Aeroplane and System Functions.*

- (1) A concern arose regarding the efficiency and coverage of the techniques used for assessing safety aspects of ~~highly integrated systems that perform complex and interrelated functions,~~ aeroplane and systems functions implemented, particularly through the use of electronic technology and software-based techniques. The concern is that design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for these aeroplane and system functions ~~more complex systems.~~ Thus, other assurance techniques, such as development assurance utilising a combination of integral processes (e.g. process assurance, configuration management, requirement validation and implementation verification ~~coverage criteria~~), or structured analysis or assessment techniques applied at the aeroplane level, ~~if necessary, or at least~~ and across integrated or interacting systems, have been ~~requested applied to these more complex systems.~~ Their systematic use increases confidence that ~~development errors in requirements or design,~~ and integration or interaction effects have been adequately identified and corrected.

(...)

7. FAILURE CONDITION CLASSIFICATIONS AND PROBABILITY TERMS

a. Classifications.

Failure Conditions may be classified according to the severity of their effects as follows:

- (1) *No Safety Effect*: Failure Conditions that would have no effect on safety; for example, Failure Conditions that would not affect the operational capability of the aeroplane or increase crew workload.
- (2) *Minor*: Failure Conditions which would not significantly reduce aeroplane safety, and which involve crew actions that are well within their capabilities. Minor Failure Conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.
- (3) *Major*: Failure Conditions which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.
- (4) *Hazardous*: Failure Conditions, which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating, conditions to the extent that there would be:
- (i) A large reduction in safety margins or functional capabilities;
 - (ii) Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or
 - (iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew.
- (5) *Catastrophic*: Failure Conditions, which would result in multiple fatalities, usually with the loss of the aeroplane. (Note: A “Catastrophic” Failure Condition was defined in previous versions of the rule and the advisory material as a Failure Condition which would prevent continued safe flight and landing.)

b. Qualitative Probability Terms.



When using qualitative analyses to determine compliance with CS 25.1309(b), the following descriptions of the probability terms used in CS 25.1309 and this AMC have become commonly accepted as aids to engineering judgement:

- (1) Probable Failure Conditions are those anticipated to occur one or more times during the entire operational life of each aeroplane.
- (2) Remote Failure Conditions are those unlikely to occur to each aeroplane during its total life, but which may occur several times when considering the total operational life of a number of aeroplanes of the type.
- (3) Extremely Remote Failure Conditions are those not anticipated to occur to each aeroplane during its total life but which may occur a few times when considering the total operational life of all aeroplanes of the type.
- (4) Extremely Improbable Failure Conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type.

c. Quantitative Probability Terms.

When using quantitative analyses to help determine compliance with CS 25.1309(b), the following descriptions of the probability terms used in this requirement and this AMC have become commonly accepted as aids to engineering judgement. They are expressed in terms of acceptable ranges for the Average Probability per Flight Hour.

(1) Probability Ranges.

- (i) Probable Failure Conditions are those having an Average Probability per Flight Hour greater than of the order of 1×10^{-5} .
- (ii) Remote Failure Conditions are those having an Average Probability per Flight Hour of the order of 1×10^{-5} or less, but greater than of the order of 1×10^{-7} .
- (iii) Extremely Remote Failure Conditions are those having an Average Probability per Flight Hour of the order of 1×10^{-7} or less, but greater than of the order of 1×10^{-9} .
- (iv) Extremely Improbable Failure Conditions are those having an Average Probability per Flight Hour of the order of 1×10^{-9} or less.

8. SAFETY OBJECTIVE.

a. The objective of CS 25.1309 is to ensure an acceptable safety level for equipment and systems as installed on the aeroplane. A logical and acceptable inverse relationship must exist between the Average Probability per Flight Hour and the severity of Failure Condition effects, as shown in Figure 1, such that:

- (1) Failure Conditions with No Safety Effect have no probability requirement.
- (2) Minor Failure Conditions may be Probable.
- (3) Major Failure Conditions must be no more frequent than Remote.
- (4) Hazardous Failure Conditions must be no more frequent than Extremely Remote.
- (5) Catastrophic Failure Conditions must be Extremely Improbable.

b. The classification of the Failure Conditions associated with the severity of their effects are described in Figure 2a.



The safety objectives associated with failure conditions are described in Figure 2b.

(...)

c. The safety objectives associated with catastrophic failure conditions, ~~may~~ **must** be satisfied by demonstrating that:

- (1) No single failure will result in a catastrophic failure condition; and
- (2) Each catastrophic failure condition is extremely improbable; and
- (3) Given that a single latent failure has occurred on a given flight, each catastrophic failure condition, resulting from two failures, either of which is latent for more than one flight, is remote.

d. Exceptionally, for paragraph 8.c(2) above of this AMC, if it is not technologically or economically practicable to meet the numerical criteria for a catastrophic failure condition, the safety objective may be met by accomplishing all of the following:

- (1) Utilising well-proven methods for the design and construction of the system; and
- (2) Determining the average probability per flight hour of each failure condition using structured methods, such as fault tree analysis, Markov analysis, or dependency diagrams; and
- (3) Demonstrating that the sum of the average probabilities per flight hour of all catastrophic failure conditions caused by systems is of the order of 10^{-7} or less (see paragraph 6.a for background).

9. COMPLIANCE WITH CS 25.1309.

(...)

a. *Compliance with CS 25.1309(a).*

(...)

- (4) The equipment, systems, and installations covered by CS 25.1309(a)(2) are typically those associated with amenities for passengers such as passenger entertainment systems, in-flight telephones, etc., whose failure or improper functioning in itself should not affect the safety of the aeroplane. Operational and environmental qualification requirements for those equipment, systems, and installations are reduced to the tests that are necessary to show that their normal or abnormal functioning does not adversely affect the proper functioning of the equipment, systems, or installations covered by CS 25.1309(a)(1) and does not otherwise adversely influence the safety of the aeroplane or its occupants. Examples of adverse influences are: fire, explosion, exposing passengers to high voltages, etc. Normal installation practices should result in sufficiently obvious isolation so that substantiation can be based on a relatively simple qualitative installation evaluation. If the possible impacts, including failure modes or effects, are questionable, or isolation between systems is provided by complex means, more formal structured evaluation methods may be necessary.

b. *Compliance with CS 25.1309(b).*

Paragraph 25.1309(b) requires that the aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that any catastrophic failure condition is extremely improbable and does not result from a single failure. It also requires that any hazardous failure condition is extremely remote, and that any major failure condition is remote. An analysis should always consider the application of the fail-safe design concept described in paragraph 6.b, and give special attention to ensuring the effective use of design techniques that would prevent single failures

or other events from damaging or otherwise adversely affecting more than one redundant system channel or more than one system performing operationally similar functions.

(1) *General.* Compliance with the requirements of CS 25.1309(b) should be shown by analysis and, where necessary, by appropriate ground, flight, or simulator tests. Failure conditions should be identified and their effects assessed. The maximum allowable probability of the occurrence of each failure condition is determined from the failure condition's effects, and when assessing the probabilities of failure conditions, appropriate analysis considerations should be accounted for. Any analysis must consider:

(i) Possible failure conditions and their causes, modes of failure, and damage from sources external to the system.

(...)

(iv) The effect of reasonably anticipated crew errors after the occurrence of a failure or failure condition.

(...)

(vii) The resulting effects on the aeroplane and occupants, considering the stage of flight, the operational sequences, and operating and environmental conditions.

(2) *Planning.*

(...)

(ii) Determination of detailed means of compliance, which may should include the use of development assurance techniques activities.

(...)

(3) *Availability of Industry Standards and Guidance Materials.* There are a variety of acceptable techniques currently being used in industry, which may or may not be reflected in the documents referenced in paragraphs 3.b(2) and 3.b(3). This AMC is not intended to compel the use of these documents during the definition of the particular method of satisfying the objectives of this AMC. However, these documents do contain material and methods of performing the system safety assessment. These methods, when correctly applied, are recognised by the Agency as valid for showing compliance with CS 25.1309(b). In addition, the Document referenced in paragraph 3.b(3) contains tutorial information on applying specific engineering methods (e.g. Markov analysis, fault tree analysis) that may be utilised in whole or in part.

(4) *Acceptable Application of Development Assurance Methods.* Paragraph 9.b(1)(iii) above requires that any analysis necessary to demonstrate show compliance with CS 25.1309(b) must consider the possibility of development errors. Errors made during the design and development of systems have traditionally been detected and corrected by exhaustive tests conducted on the system and its components, by direct inspection, and by other direct verification methods capable of completely characterising the performance of the system. These direct techniques may still be appropriate for simple systems containing non-complex items (i.e. items that are fully assured by a combination of testing and analysis) which perform a limited number of functions and which are not highly integrated with other aeroplane systems. For more complex or integrated systems, exhaustive testing may either be impossible because all of the system states cannot be determined or impractical because of the number of tests which must be accomplished. For these types of systems, compliance may be demonstrated shown by the use of development assurance. The level of development assurance (function development assurance level (FDAL)/item development assurance level



(IDAL)) should be commensurate with the severity of the failure conditions the system is contributing to.

Guidelines, which may be used for the assignment of development assurance levels to aeroplanes and system functions (FDAL) and to items (IDAL), are described in the document referenced in 3.b(2) above. Through this document, EASA the Agency recognises that credit can be taken from system architecture (e.g. functional or item development independence) for the FDAL/IDAL assignment process.

Guidelines, which may be used for providing development assurance, are described for aeroplane and system development in the document referenced in 3.b(2), and for software in the document referenced in 3.a(3) above. (There is currently no agreed development assurance standard for airborne electronic hardware.)

(...)

(5) *Crew and Maintenance Actions.*

(i) Where an analysis identifies some indication to, and/or action by, the flight crew, cabin crew, or maintenance personnel, the following activities should be accomplished:

- 1 Verify that any identified indications are actually provided by the system. This includes the verification that the elements that provide detection (e.g. sensors, logic) properly trigger the indication under the relevant situations considering various causes, flight phases, operating conditions, operational sequences, and environments.

(...)

(ii) These verification activities should be accomplished by consulting with engineers, pilots, flight attendants, maintenance personnel, and human factors specialists, as appropriate, taking due consideration of any relevant service experience and the consequences if the assumed action is not performed or mis-performed performed improperly.

(iii) In complex situations, the results of the review by specialists may need to be confirmed by simulator, ground tests, or flight tests. However, quantitative assessments of the probabilities of crew or maintenance errors are not currently considered feasible. If the failure indications are considered to be recognisable and the required actions do not cause an excessive workload, then for the purposes of the analysis, such corrective actions can be considered to be satisfactorily accomplished ~~the probability that the corrective action will be accomplished, can be considered to be one.~~ If the necessary actions cannot be satisfactorily accomplished, the tasks and/or the systems need to be modified.

(6) *Significant Latent Failures.*

(i) Compliance with CS 25.1309(b)(4)

For compliance with CS 25.1309(b)(4), the applicant should establish design practices for reasonably managing exposure to significant latent failures.

These design practices should drive the applicant to first eliminate significant latent failures to the extent practicable. Additional guidance is provided in AMC 25-19 section 8, Design Considerations Related to Significant Latent Failures.

Then, for each significant latent failure which cannot be reasonably eliminated, the applicant should limit the latency so that compliance with the safety objectives is ensured. Quantitative as well as qualitative aspects need to be addressed when limiting



the latency. Additional guidance is provided in AMC 25-19 section 10, Identification of Candidate CMRs (CCMRs).

(ii) Compliance with CS 25.1309(b)(5)

When a catastrophic failure condition involves two failures, either of which is latent for more than one flight, and cannot reasonably be eliminated, compliance with CS 25.1309(b)(5) is required. Following the proper integration of the safety objectives minimising the significant latent failures into the design process (in accordance with CS 25.1309(b)(4)), failure conditions involving multiple significant latent failures are expected to be sufficiently unlikely such that the dual-failure situations addressed in CS 25.1309(b)(5) are the only remaining significant latent failures of concern.

These significant latent failures of concern should be highlighted to the Agency as early as possible. The system safety assessment should explain why avoidance is not practicable, and provide supporting rationale for the acceptability. Rationale should be based on past experience, sound engineering judgment or other arguments, which led to the decision not to implement other potential means of avoidance (e.g. eliminating the significant latent failure or adding redundancy). For turbojet reversing systems, the design configurations in paragraphs 8.b(2) and 8.b(3) of AMC 25.933(a)(1) have traditionally been considered to be practicable and deemed to be acceptable to the Agency for compliance with CS 25.1309(b)(5).

Two criteria are implemented in CS 25.1309(b)(5): limit latency and limit residual probability. Limit latency is intended to limit the time of operating with a latent failure present. This is achieved by requiring that the occurrence probability of the latent failure does not exceed 1/1000. Limit residual probability is intended to limit the average probability per flight hour of the failure condition given the presence of a single latent failure. This is achieved by defining the residual probability to be 'remote'. Residual probability is the combined average probability per flight hour of all the single active failures that result in the catastrophic failure condition assuming one single latent failure has occurred.

These requirements are applied in addition to CS 25.1309(b)(1) which requires that catastrophic failure conditions be shown to be extremely improbable and do not result from a single failure.

In numerical terms, compliance with CS 25.1309(b)(1) and CS 25.1309(b)(5) together means that the residual probability, i.e. the sum of all subsequent single active failures, must be in the order of 1×10^{-6} per flight hour when the occurrence probability of the significant latent failure is limited to 1/1000 to satisfy the extremely improbable safety objective. Conversely, if the residual probability is 1×10^{-5} per flight hour, then the occurrence probability of the significant latent failure is limited to a maximum of 1×10^{-4} .

Appendix 5 provides simplified examples explaining how the limit latency and limit residual probability analysis might be applied.

When applying the 1/1000 criterion, the occurrence probability of the significant latent failure may be computed as the worst-case flight probability or the average probability per flight. The applicant is not expected to run two different types of computation for compliance within CS 25.1309(b).



c. Compliance with CS 25.1309(c).

CS 25.1309(c) requires that information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action in a timely manner, thereby mitigating the effects to an acceptable level. Any system operating condition which, if not detected and properly accommodated by flight crew action, would contribute to or cause a hazardous or catastrophic failure condition should be considered to be an 'unsafe system operating condition'. Compliance with this requirement is usually demonstrated by the analysis identified in paragraph 9.b(1) above, which also includes consideration of crew alerting cues, corrective action required, and the capability of detecting faults. The required information may be provided by dedicated indication and/or annunciation or made apparent to the flight crew by the inherent aeroplane/systems responses. ~~CS 25.1309(c) requires that~~ When flight crew alerting is required, it must be provided in compliance with CS 25.1322. ~~a warning indication must be provided if immediate corrective action is required.~~ Paragraph CS 25.1309(c) also requires that installed systems and controls equipment for use by the flight crew, including indications and annunciations flight deck controls and information, must be designed in compliance with CS 25.1302 to minimise flight crew errors which could create additional hazards.

(...)

- (2) When failure monitoring and indication are provided by a system, its reliability should be compatible with the safety objectives associated with the system function for which it provides that indication. For example, if the effects of having a system failure and not annunciating that system failure are catastrophic, the combination of the system failure with the failure of its annunciation must be extremely improbable. The loss of annunciation should itself be considered to be a failure condition, and particular attention should be paid to the impact on the ability of the flight crew to cope with the subject system failure. In addition, unwanted operation (e.g., nuisance warnings) should be assessed. The failure monitoring and indication should be reliable, technologically feasible and economically practicable. Reliable failure monitoring and indication should utilise current state-of-the-art technology to maximise the probability of detecting and indicating genuine failures while minimising the probability of falsely detecting and indicating non-existent failures. Any indication should be timely, obvious, clear, and unambiguous.

(...)

- (5) Even if operation or performance is unaffected or insignificantly affected at the time of failure, information to the crew is required if it is considered necessary for the crew to take any action or observe any precautions. Some examples include reconfiguring a system, being aware of a reduction in safety margins, changing the flight plan or regime, or making an unscheduled landing to reduce exposure to a more severe failure condition that would result from subsequent failures or operational or environmental conditions. Information is also required if a failure must be corrected before a subsequent flight. If operation or performance is unaffected or insignificantly affected, information and alerting indications may be inhibited during specific phases of flight where corrective action by the crew is considered more hazardous than no action.
- (6) The use of periodic maintenance or flight crew checks to detect significant latent failures when they occur is undesirable and should not be used in lieu of practical and reliable failure monitoring and indications. When this is not accomplished, refer to paragraph 9.b(6) for guidance.

Paragraph 12 provides further guidance on the use of periodic maintenance or flight crew checks. Comparison with similar, previously approved systems is sometimes helpful. However,

if a new technical solution allows practicable and reliable failure monitoring and indications, this should be preferred in lieu of periodic maintenance or flight crew checks.

(...)

10. IDENTIFICATION OF FAILURE CONDITIONS AND CONSIDERATIONS WHEN ASSESSING THEIR EFFECTS.

a. Identification of Failure Conditions.

Failure conditions should be identified by considering the potential effects of failures on the aeroplane and occupants. These should be considered from two perspectives:

(1) by considering failures of aeroplane-level functions — Failure conditions identified at this level are not dependent on the way the functions are implemented and the systems' architecture.

(2) by considering failures of functions at the system level — these failure conditions are identified through examination of the way that functions are implemented and the systems' architectures. It should be noted that a failure condition might result from a combination of lower-level failure conditions. This requires that the analysis of complex, highly integrated systems, in particular, should be conducted in a highly methodical and structured manner to ensure that all significant failure conditions, which arise from multiple failures and combinations of lower-level failure conditions, are properly identified and accounted for. The relevant combinations of failures and failure conditions should be determined by the whole safety assessment process that encompasses the aeroplane and system level functional hazard assessments and common-cause analyses. The overall effect on the aeroplane of a combination of individual system failure conditions occurring as a result of a common or cascade failure, may be more severe than the individual system effect. For example, failure conditions classified as minor or major by themselves may have hazardous effects at an aeroplane level, when considered in combination.

b. Identification of Failure Conditions Using a Functional Hazard Assessment.

(1) Before a detailed safety assessment is proceeded with, a functional hazard assessment (FHA) of the aeroplane and system functions to determine the need for and scope of subsequent analysis should be prepared. This assessment may be conducted using service experience, engineering and operational judgement, and/or a top-down deductive qualitative examination of each function. An ~~Functional Hazard Assessment~~ is a systematic, comprehensive examination of aeroplane and system functions to identify potential minor, major, hazardous, and catastrophic failure conditions which may arise, not only as a result of malfunctions or failure to function, but also as a result of normal responses to unusual or abnormal external factors. It is concerned with the operational vulnerabilities of systems rather than with a detailed analysis of the actual implementation.

(...)

(3) The ~~Functional Hazard Assessment~~ ~~FHA~~ is an engineering tool, which should be performed early in the design and updated as necessary. It is used to define the high-level aeroplane or system safety objectives that must be considered in the proposed system architectures. It should also be used to assist in determining the development assurance levels for the systems. Many systems may need only a simple review of the system design by the applicant to determine the hazard classification. An ~~FHA~~ ~~Functional Hazard Assessment~~ requires experienced engineering judgement and early co-ordination between the applicant and the certification authority.

(4) Depending on the extent of functions to be examined and the relationship between functions and systems, different approaches to ~~FHA~~ ~~Functional Hazard Assessment~~ may be taken. Where there is a clear correlation between functions and systems, and where system, and hence function, interrelationships are relatively simple, it may be feasible to conduct separate ~~FHAs~~ ~~Functional Hazard Assessments~~ for each system, providing any interface aspects are properly considered and are easily understood. However, where system and function interrelationships are more complex, a top-down approach, from an aeroplane-level perspective, should be taken in planning and conducting ~~FHAs~~ ~~Functional Hazard Assessments~~.



However, with the increasing integrated system architectures, this traditional top-down approach should be performed in conjunction with common-cause considerations (e.g. common resources) in order to properly address the cases where one system contributes to several aeroplane-level functions.

c. *Considerations When Assessing Failure Condition Effects.*

(...)

In assessing the effects of a Failure Condition, factors, which might alleviate or intensify the direct effects of the initial Failure Condition should be considered. Some of these factors include consequent or related conditions existing within the aeroplane which may affect the ability of the crew to deal with direct effects, such as the presence of smoke, acceleration effects, interruption of communication, interference with cabin pressurisation, etc. When assessing the consequences of a given Failure Condition, account should be taken of the failure information provided, the complexity of the crew action, and the relevant crew training. The number of overall Failure Conditions involving other than instinctive crew actions may influence the flight crew performance that can be expected. Training recommendations may need to be identified in some cases.

(1) The severity of Failure Conditions should be evaluated according to the following:

- (i) Effects on the aeroplane, such as reductions in safety margins, degradation in performance, loss of capability to conduct certain flight operations, reduction in environmental protection, or potential or consequential effects on structural integrity. When the effects of a failure condition are difficult to assess, the hazard classification may need to be validated by tests, simulation, or other appropriate analytical techniques.

(...)

(2) For convenience in conducting design assessments, Failure Conditions may be classified according to the severity of their effects as 'No Safety Effect', 'Minor', 'Major', 'Hazardous', or 'Catastrophic'. Paragraph 7.a above provides accepted definitions of these terms.

- (i) The classification of Failure Conditions does not depend on whether or not a system or function is the subject of a specific requirement or regulation. Some "required" systems, such as transponders, position lights, and public address systems, may have the potential for only Minor Failure Conditions. Conversely, other systems which are not "required", such as auto-flight systems, may have the potential for 'Major', 'Hazardous', or 'Catastrophic Failure Conditions'.

- (ii) Regardless of the types of assessment used, the classification of Failure Conditions should always be accomplished with consideration of all relevant factors; e.g., system, crew, performance, operational, external. Examples of factors include the nature of the failure modes, any effects or limitations on performance, and any required or likely crew action. It is particularly important to consider factors that would alleviate or intensify the severity of a Failure Condition. When flight duration, flight phase, or diversion time can adversely affect the classification of failure conditions, they must be considered to be intensifying factors. Other intensifying factors include conditions which are not related to the failure (such as weather or adverse operational or environmental conditions), and which reduce the ability of the flight crew to cope with a failure condition. An example of an alleviating factor would be the continued performance of identical or operationally similar functions by other systems not affected by the Failure Condition. Another example of an alleviating factor is the ability of the flight crew to recognise the failure condition and take action to mitigate its effects. Whenever this is



taken into account, particular attention should be paid to the detection means to ensure that the ability of the flight crew (including physical ability and timeliness of the response) to detect the failure condition and take the necessary corrective action(s) is sufficient. Refer to CS 25.1309(c) and paragraph 9.c of this AMC for more detailed guidance on crew annunciations and crew response evaluation. ~~Examples of intensifying factors would include unrelated conditions that would reduce the ability of the crew to cope with a Failure Condition, such as weather or other adverse operational or environmental conditions. Combinations of intensifying or alleviating factors need to be considered only if they are anticipated to occur together.~~

11. ASSESSMENT OF FAILURE CONDITION PROBABILITIES AND ANALYSIS CONSIDERATIONS.

After the Failure Conditions have been identified and the severity of the effects of the Failure Conditions have been assessed, there is a responsibility to determine how to show compliance with the requirement and obtain the concurrence of the Agency EASA. Design and installation reviews, analyses, flight tests, ground tests, simulator tests, or other approved means may be used.

a. Assessment of Failure Condition Probabilities.

(1) The probability that a Failure Condition would occur may be assessed as Probable, Remote, Extremely Remote, or Extremely Improbable. These terms are defined in paragraph 7. Each Failure Condition should have a probability that is inversely related to the severity of its effects as described in paragraph 8.

(2) When a system provides protection from events (e.g., cargo compartment fire, gusts), its reliability should be compatible with the safety objectives necessary for the Failure Condition associated with the failure of the protection system and the probability of such events. (See paragraph 11g of this AMC and Appendix 4.)

(3) An assessment to identify and classify Failure Conditions is necessarily qualitative. On the other hand, an assessment of the probability of a Failure Condition may be either qualitative or quantitative. An analysis may range from a simple report that interprets test results or compares two similar systems to a detailed analysis that may or may not include estimated numerical probabilities. The depth and scope of an analysis depends on the types of functions performed by the system, the severity of Failure Conditions, and whether or not the system is complex.

(4) Experienced engineering and operational judgement should be applied when determining whether or not a system is complex. Comparison with similar, previously approved systems is sometimes helpful. All relevant systems' attributes should be considered; however, the complexity of the software and hardware item need not be a dominant factor in the determination of complexity at the system level, e.g., the design may be very complex, such as a satellite communication system, but its function may be fairly simple.

b. Single Failure Considerations.

(1) According to the requirements of CS 25.1309(b)(1)(ii), a Catastrophic Failure Condition must not result from the failure of a single component, part, or element of a system. Failure containment should be provided by the system design to limit the propagation of the effects of any single failure to preclude Catastrophic Failure Conditions. In addition, there must be no common-cause failure, which could affect both the single component, part, or element, and its failure containment provisions. A single failure includes any set of failures, which cannot be shown to be independent from each other. Common-cause failures (including common mode failures) and cascading failures should be considered as single failures from the perspective of the root cause or the initiator. Errors in development, manufacturing, installation, and maintenance can result in common-cause failures (including common mode failures) and cascading failures. Errors should therefore be assessed in the frame of the single failure consideration. Appendix 1 and the Document referenced in paragraph 3.b(3) describe types of common-cause analyses, which may be



conducted, to assure that independence is maintained. Failure containment techniques available to establish independence may include partitioning, separation, and isolation.

(2) While single failures must normally be assumed to occur, there are cases where it is obvious that, from a realistic and practical viewpoint, any knowledgeable, experienced person would unequivocally conclude that a failure mode simply would not occur, unless it is associated with a wholly unrelated failure condition that would itself be catastrophic. (...)

(...)

d. *Depth of Analysis.* The following identifies the depth of analysis expected based on the classification of a failure condition.

(1) *No Safety Effect Failure Conditions.* An ~~FHA Functional Hazard Assessment~~, with a design and installation appraisal, to establish independence from other functions is necessary for the safety assessment of these failure conditions. If it is chosen not to do an FHA, the safety effects may be derived from the design and installation appraisal.

(2) *Minor Failure Conditions.* An ~~FHA Functional Hazard Assessment~~, with a design and installation appraisal, to establish independence from other functions is necessary for the safety assessment of these failure conditions. Combinations of failure condition effects, as noted in paragraph 10 above, must also be considered. If it is chosen not to do an FHA, the safety effects may be derived from the design and installation appraisal.

(3) *Major Failure Conditions.* Major failure conditions must be remote:

(...)

(ii) For systems that are not complex, where similarity cannot be used as the basis for compliance, then compliance may be shown by means of a qualitative assessment which shows that the system-level major failure conditions, of the system as installed, are consistent with the FHA and are remote, e.g., redundant systems.

(iii) For complex systems without redundancy, compliance may be shown as in paragraph 11.d(3)(ii) of this AMC. To show that malfunctions are indeed remote in systems of high complexity without redundancy (for example, a system with a self-monitoring microprocessor), it is sometimes necessary to conduct a qualitative functional modes and effects analysis (FMEA) supported by failure rate data and fault detection coverage analysis.

(...)

(4) *Hazardous and Catastrophic Failure Conditions.* Hazardous failure conditions must be extremely remote, and catastrophic failure conditions must be extremely improbable:

(i) Except as specified in paragraph 11.d(4)(ii) below, a detailed safety analysis will be necessary for each hazardous and catastrophic failure condition identified by the ~~FHA functional hazard assessment~~. The analysis will usually be a combination of qualitative and quantitative assessment of the design.

(ii) For very simple and conventional installations, i.e. low complexity and similarity in relevant attributes, it may be possible to assess a hazardous or catastrophic failure condition as being extremely remote or extremely improbable, respectively, on the basis of experienced engineering judgement, using only qualitative analysis. (...)

(iii) For complex systems where true similarity in all relevant attributes, including installation attributes, can be rigorously established, it may be also possible to assess a hazardous or catastrophic failure condition as being extremely remote or extremely improbable, respectively, on the basis of experienced engineering judgement, using only qualitative analysis. A high degree of similarity in both design and application is required to be substantiated.

e. *Calculation of Average Probability per Flight Hour (Quantitative Analysis).*



(1) The Average Probability per Flight Hour is the probability of occurrence, normalised by the flight time, of a Failure Condition during a flight, which can be seen as an average over all possible flights of the fleet of aeroplane to be certified. The calculation of the Average Probability per Flight Hour for a Failure Condition should consider:

(...)

(ii) all combinations of failures and events that contribute to the Failure Condition,

(iii) the conditional probability if a sequence of events is necessary to produce the Failure Condition,

(iv) the relevant "at risk" time if an event is only relevant during certain flight phases, and

(v) the average exposure time if the failure can persist for multiple flights.

(2) The details how to calculate the Average Probability per Flight Hour for a Failure Condition are given in Appendix 3 of this AMC.

(3) If the probability of a subject Failure Condition occurring during a typical flight of mean duration for the aeroplane type divided by the flight's mean duration in hours is likely to be significantly different from the predicted average rate of occurrence of that Failure Condition during the entire operational life of all aeroplanes of that type, then a risk model that better reflects the Failure Condition should be used.

(4) It is recognised that, for various reasons, component failure rate data are not precise enough to enable accurate estimates of the probabilities of Failure Conditions. This results in some degree of uncertainty, as indicated by the wide line in Figure 1, and the expression "on the order of" in the descriptions of the quantitative probability terms that are provided above. When calculating the estimated probability of each Failure Condition, this uncertainty should be accounted for in a way that does not compromise safety.

f. *Integrated Systems.* Interconnections between systems have been a feature of aeroplane design for many years and CS 25.1309(b) recognises this in requiring systems to be considered in relation to other systems. Providing the interfaces between systems are relatively few and simple, and hence readily understandable, compliance may often be demonstrated through a series of system safety assessments, each of which deals with a particular Failure Condition (or more likely a group of Failure Conditions) associated with a system and, where necessary, takes account of failures arising at the interface with other systems. This procedure has been found to be acceptable in many past certification programmes. However, where the systems and their interfaces become more complex and extensive, the task of demonstrating compliance may become more complex. It is therefore essential that the means of compliance are considered early in the design phase to ensure that the design can be supported by a viable safety assessment strategy. Aspects of the guidance material covered elsewhere in this AMC and which should be given particular consideration are as follows:

(1) planning the proposed means of compliance; this should include development assurance activities to mitigate the occurrence of errors in the design,

(...)

(3) the potential for common-cause failures and cascade effects and the possible need to assess combinations of multiple lower-level (e.g. Major) Failure Conditions,



- (4) the importance of ~~multi-disciplinary~~ multidisciplinary teams in identifying and classifying significant Failure Conditions,

(...)

- g. *Operational or Environmental Conditions.* A probability of one should usually be used for encountering a discrete condition for which the aeroplane is designed, such as instrument meteorological conditions or Category III weather operations. However, Appendix 4 contains allowable probabilities, which may be assigned to various operational and environmental conditions for use in computing the average probability per flight hour of Failure Conditions ~~resulting from multiple independent failures~~, without further justification. Single failures which, in combination with operational or environmental conditions, lead to catastrophic failure conditions are, in general, not acceptable.

Limited cases that are properly justified may be considered on a case-by-case basis (e.g. operational events or environmental conditions that are extremely remote).

Appendix 4 is provided for guidance and is not intended to be exhaustive or prescriptive. At this time, a number of items have no accepted standard statistical data from which to derive a probability figure. However, these items are included for either future consideration or as items for which the applicant may propose a probability figure supported by statistically valid data or supporting service experience. The applicant may propose additional conditions or different probabilities from those in Appendix 4 provided they are based on statistically valid data or supporting service experience. The applicant should obtain early concurrence of the Agency when such conditions are to be included in an analysis. When combining the probability of such a random condition with that of a system failure, care should be taken to ensure that the condition and the system failure are independent of one another, or that any dependencies are properly accounted for.

(...)

12. OPERATIONAL AND MAINTENANCE CONSIDERATIONS.

...

- a. *Flight Crew Action.*

When assessing the ability of the flight crew to cope with a Failure Condition, the information provided to the crew and the complexity of the required action should be considered. When considering the information provided to the flight crew, refer also to paragraph 9.c (compliance with CS 25.1309(c)). Credit for flight crew actions, and considerations of flight crew errors, should be consistent with relevant service experience and acceptable human factors evaluations. If the evaluation indicates that a potential Failure Condition can be alleviated or overcome without jeopardising other safety-related flight crew tasks and without requiring exceptional pilot skill or strength, credit may be taken for both qualitative and quantitative assessments. Similarly, credit may be taken for correct flight crew performance of the periodic checks required to demonstrate compliance with CS 25.1309(b) provided overall flight crew workload during the time available to perform them is not excessive and they do not require exceptional pilot skill or strength. Unless flight crew actions are accepted as normal airmanship, they should be described in the approved Aeroplane Flight Manual in compliance with CS 25.1585. The applicant should provide a means to ensure that the AFM will contain the required flight crew actions that have been used as mitigation factors in the hazard classification or that have been taken as assumptions to limit the exposure time of failures.

- b. *Maintenance Action.*

Credit may be taken for the correct accomplishment of reasonable maintenance tasks, for both qualitative and quantitative assessments. The maintenance tasks needed to demonstrate show



compliance with CS 25.1309(b) should be established. In doing this, the following maintenance scenarios can be used:

- (1) ~~For failures known to the flight crew, refer to paragraph 12.d. Annunciated failures will be corrected before the next flight, or a maximum time period will be established before a maintenance action is required. If the latter is acceptable, the analysis should establish the maximum allowable interval before the maintenance action is required. These maximum allowable intervals should be reflected in either the MMEL or the type certificate.~~
- (2) Latent failures will be identified by a scheduled maintenance task. If this approach is taken, and the failure condition is hazardous or catastrophic, then a CCMR maintenance task should be established. Some latent failures can be assumed to be identified based upon return to service test on the LRU following its removal and repair (component Mean Time Between Failures (MTBF) should be the basis for the check interval time).

c. *Candidate Certification Maintenance Requirements.*

- (1) By detecting the presence of, and thereby limiting the exposure time to significant latent failures that would, in combination with one or more other specific failures or events identified by safety analysis, result in a hazardous or catastrophic failure condition, periodic maintenance or flight crew checks may be used to help show compliance with CS 25.1309(b). Where such checks cannot be accepted as basic servicing or airmanship they become CCMRs. AMC 25.19 details the handling of CCMRs.

(...)

d. *Flight with Equipment or Functions known to be Inoperative.*

~~An applicant may elect to develop a list may be developed of equipment and functions which need not be operative for flight, based on stated compensating precautions that should be taken, e.g., operational or time limitations, flight crew procedures, or ground crew checks. The documents used to demonstrate show compliance with CS 25.1309, together with any other relevant information, should be considered in the development of this list, which then becomes the basis for a Master Minimum Equipment List (MMEL). Experienced engineering and operational judgement should be applied during the development of the MMEL this list. When operation is envisaged with equipment that is known to be inoperative, and this equipment affects the probabilities associated with hazardous and/or catastrophic failure conditions, limitations may be needed on the number of flights and/or the allowed operation time with such inoperative equipment. These limitations should be established in accordance with the recommendations contained in CS-MMEL.~~

(...)

APPENDIX 1. ASSESSMENT METHODS.

Various methods for assessing the causes, severity, and probability of failure conditions are available to support experienced engineering and operational judgement.

(...)

c. *Failure Modes and Effects Analysis.*

(...)

-- assuming all failure modes result in the failure conditions of interest,

(...)



d. *Fault Tree or Dependence Diagram Analysis*. Structured, deductive, top-down analyses that are used to identify the conditions, failures, and events that would cause each defined Failure Condition. They are graphical methods of identifying the logical relationship between each particular Failure Condition and the primary element or component failures, other events, or combinations thereof that can cause it. A failure modes and effects analysis may be used as the source document for those primary failures or other events.

(...)

f. *Common-Cause Analysis*. The acceptance of adequate probability of Failure Conditions is often derived from the assessment of multiple systems based on the assumption that failures are independent. Therefore, it is necessary to recognise that such independence may not exist in the practical sense and specific studies are necessary to ensure that independence can either be assured or deemed to be acceptable. These studies may also identify a combination of failures and effects that would otherwise not have been foreseen by FMEA or fault tree analysis.

The Common Cause Analysis is subdivided into three areas of study:

(...)

(3) *Common Mode Analysis*. This analysis is performed to confirm the assumed independence of the events, which were considered in combination for a given Failure Condition.

(...)

g. *Safety Assessment Process*. Appendix 2 provides an overview of the Safety Assessment Process.

APPENDIX 2. SAFETY ASSESSMENT PROCESS OVERVIEW.

(...)

a. Define the system and its interfaces, and identify the functions that the system is to perform. Some functions are intended to be protective, i.e. functions preventing the failures in system X from adversely affecting system Y. As the implementation of the functional requirements becomes more developed, care should be taken to identify all protective functions upon which airworthiness will depend. Determine whether or not the system is complex, similar to systems used on other aeroplanes, or conventional. Where multiple systems and functions are to be evaluated, consider the relationships between multiple safety assessments.

b. Identify and classify Failure Conditions. All relevant engineering organisations, such as systems, structures, propulsion, and flight test, should be involved in this process. This identification and classification may be done by conducting an FHA Functional Hazard Assessment, which is usually based on one of the following methods, as appropriate:

(...)

c. Choose the means to be used to determine compliance with CS 25.1309. The depth and scope of the analysis depends on the types of functions performed by the system, the severity of system Failure Conditions, and whether or not the system is complex (see Figure A2-2). For Major Failure Conditions, experienced engineering and operational judgement, design and installation appraisals and comparative service experience data on similar systems may be acceptable, either on their own or in conjunction with qualitative analyses or selectively used quantitative analyses. For Hazardous or Catastrophic Failure Conditions, a very thorough safety assessment is necessary. The early concurrence of the Agency on the choice of an acceptable means of compliance should be obtained.



d. Conduct the analysis and produce the data, which are agreed with the certification authority as being acceptable to show compliance. A typical analysis should include the following information to the extent necessary to show compliance:

(...)

(3) The conclusions, including a statement of the Failure Conditions and their classifications and probabilities (expressed qualitatively or quantitatively, as appropriate) that show compliance with the requirements of CS 25.1309.

(4) A description that establishes correctness and completeness and traces the work leading to the conclusions. This description should include the basis for the classification of each Failure Condition (e.g., analysis or ground, flight, or simulator tests). It should also include a description of precautions taken against common-cause failures, provide any data such as component failure rates and their sources and applicability, support any assumptions made, and identify any required flight crew or ground crew actions, including any CCMRs.

e. Assess the analyses and conclusions of multiple safety assessments to ensure compliance with the requirements for all aeroplane-level Failure Conditions.

(...)

APPENDIX 3. CALCULATION OF THE AVERAGE PROBABILITY PER FLIGHT HOUR.

The purpose of this material is to provide guidance for calculating the "Average Probability per Flight Hour" for a Failure Condition so that it can be compared with the quantitative criteria of the AMC.

The process of calculating the "Average Probability per Flight Hour" for a Failure Condition will be described as a four-step process and is based on the assumption that the life of an aeroplane is a sequence of "Average Flights".

Step 1: Determination of the "Average Flight"

Step 2: Calculation of the probability of a Failure Condition for a certain "Average Flight"

Step 3: Calculation of the "Average Probability per Flight" of a Failure Condition

Step 4: Calculation of the "Average Probability Per Flight Hour" of a Failure Condition

(...)

b. *Calculation of the Probability of a Failure Condition for a certain "Average Flight"*. The probability of a Failure Condition occurring on an "Average Flight" $P_{\text{Flight}}(\text{Failure Condition})$ should be determined by structured methods (see Document referenced in paragraph 3.b(3) for example methods) and should consider all significant elements (e.g. combinations of failures and events) that contribute to the Failure Condition. The following should be considered:

(1) ~~The individual part, component, and assembly~~ failure rates utilised in calculating the "Average Probability per Flight Hour" should be estimates of the mature constant failure rates after infant mortality and prior to wear-out. For components whose probability of failure may be associated with non-constant failure rates within the operational life of the aeroplane, a reliability analysis may be used to determine component replacement times (e.g. Weibull analysis). ~~and~~ In either case, the failure rate should be based on all causes of failure (operational, environmental, etc.). ~~Where~~ If available, service history of same or similar components in the same or similar environment should be used.

Ageing and wear of similarly constructed and similarly loaded redundant components, whose failure could lead directly, or in combination with one other failure, to a catastrophic or hazardous failure condition, should be assessed when determining scheduled maintenance tasks for such components.

Replacement times, necessary to mitigate the risk due to ageing and wear of such components within the operational life of the aeroplane, should be assessed through the same methodology like other scheduled



maintenance tasks which are required to satisfy CS 25.1309 (refer to AMC 25-19 for guidance) and documented in the Airworthiness Limitations Section of the Instructions for Continued Airworthiness, as appropriate.

(...)

(4) If the failure rate of one element varies during different flight phases, the calculation should consider the failure rate and related time increments in such a manner as to establish the probability of the Failure Condition occurring on an "Average Flight":

(...)

(5) If there is only an effect when failures occur in a certain order, the calculation should account for the conditional probability that the failures occur in the sequence necessary to produce the Failure Condition.

c. Calculation of the Average Probability per Flight of a Failure Condition. The next step is to calculate the "Average Probability per Flight" for the Failure Condition, i.e. the probability of the Failure Condition for each flight (which might be different although all flights are "Average Flights") during the relevant time (e.g. the least common multiple of the exposure times or the aeroplane life) should be calculated, summed up and divided by the number of flights during that period. The principles of calculating are described below and also in more detail in the Document referenced in paragraph 3.b(3).



APPENDIX 4. ALLOWABLE PROBABILITIES.

The following probabilities may be used for environmental conditions and operational factors (not caused by aeroplane failures) in quantitative safety analyses:

Environmental Factors

Condition	Model or other Justification	Probability
Normal icing (trace, light, moderate icing) CS-25 Appendix C icing conditions		1
CS-25 Appendix O icing conditions		10 ⁻² per flight hour
Icing conditions beyond certified conditions (considered as 'Severe icing')		No accepted standard data
Headwind >25 kts during take-off and landing	AC 120-28 CS-AWO	10 ⁻² per flight
Tailwind >10 kts during take-off and landing	AC 120-28 CS-AWO	10 ⁻² per flight
Crosswind >20 kts during take-off and landing	AC 120-28 CS-AWO	10 ⁻² per flight
Limit design gust and turbulence	CS 25.341	10 ⁻⁵ per flight hour
Air temperature < -70°C		No accepted standard data
Lightning strike		No accepted standard data
HIRF conditions		No accepted standard data

(...)

Other Events

Event	Model or other Justification	Probability
Fire in a lavatory not caused by aeroplane failures		No accepted standard data
Fire in a cargo compartment not caused by aeroplane failures		No accepted standard data
Fire in APU compartment		No accepted standard data
Engine fire		No accepted standard data
Cabin high altitude requiring passenger oxygen		No accepted standard data

(...)



APPENDIX 5. EXAMPLE OF LIMIT LATENCY AND RESIDUAL PROBABILITY ANALYSIS.

The following example illustrates how the quantitative criteria of CS 25.1309(b)(5) are to be implemented together with CS 25.1309(b)(1). The methodology used is based on the identification of the minimal cut sets associated with the catastrophic top event of the generic system level fault tree provided in Figure A5-1.

The term 'minimal cut set' refers to the smallest set of primary events whose occurrence is sufficient to cause a system failure or, in this case, the failure condition of concern.

- (1) The list of minimal cut sets should be produced by cut set order. This will group all dual-order cut sets or failure combinations. The entire list of minimal cut sets of the fault tree in Figure A5-1 is provided in Table A5-1.
- (2) The dual-order minimal cut sets that contain a primary event that is latent for more than one flight are then identified from the list in Table A5-1. The probability of each of these latent events should be less than 1×10^{-3} .
- (3) Then group those dual-order minimal cut sets that contain the same latent primary event. For each group, assume that the latent primary event has failed and sum the remaining active failure probabilities. For each group, the sum of the active failures should be less than $1 \times 10^{-5}/FH$.
- (4) The sum of all minimal cut sets should be in the order of $1 \times 10^{-9}/FH$.

An alternative method would be to rerun the fault tree probability calculation assuming for each model rerun that a different latent primary event has occurred.

The results of the limit latency and residual probability analysis are provided in Table A5-1.



Duration : 02 hh 30 min 00 sec

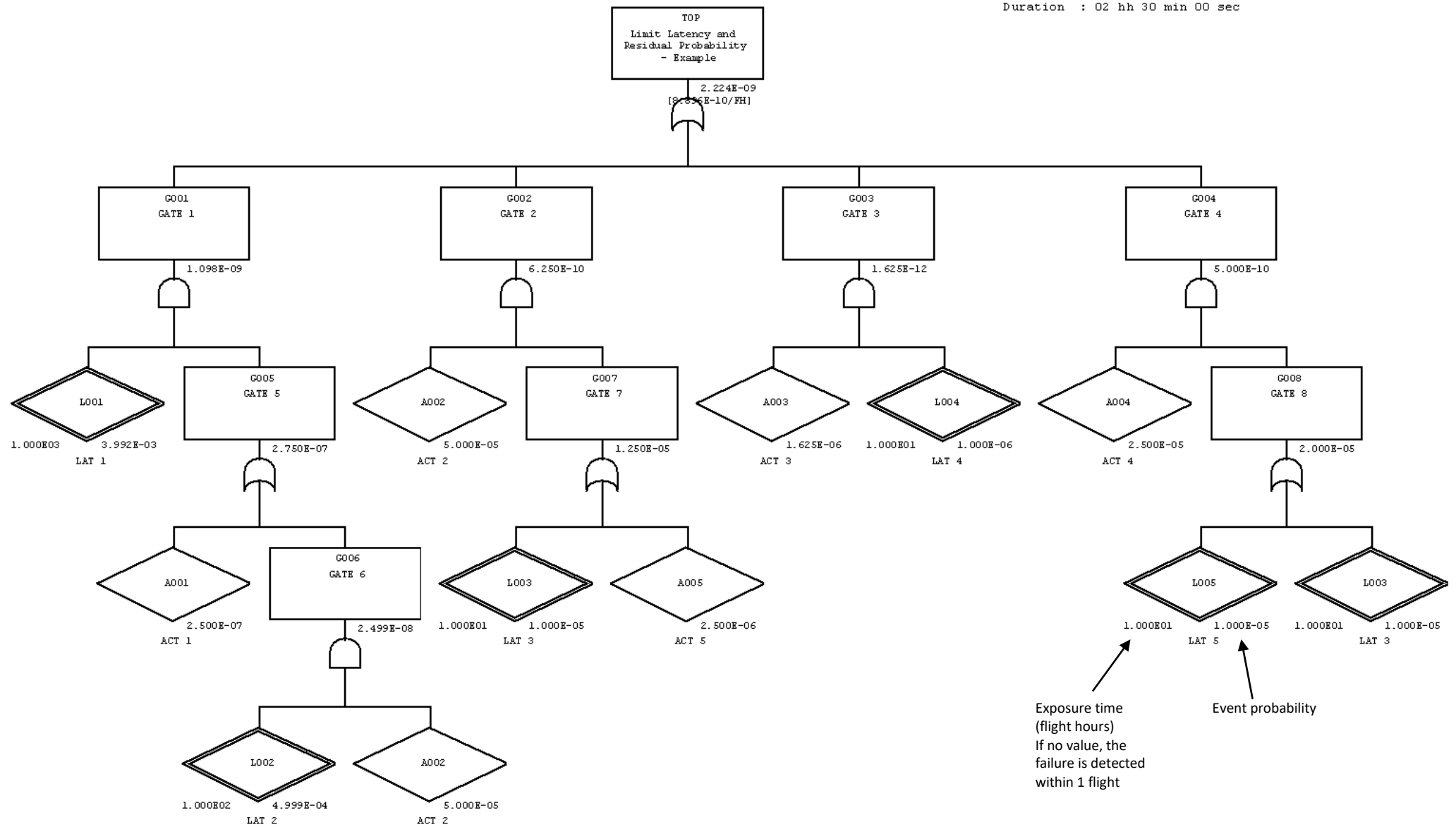


Figure A5-1: Fault Tree

#	Probability (per flight hour)	Event name	Event description	Failure rate (constant, unless noted)	Exposure time	Event probability (per flight)	CS 25.1309 (b)(5) Applicability/compliance
1	3.992E-10	A001	ACT 1	1.000E-07	2.5 h	2.500E-07	Not compliant with the limit latency criterion [L001 probability is more frequent than 1.000E-03].
		L001	LAT 1	4.000E-06	1000.0 h	3.992E-03	
2	2.000E-10	A002	ACT 2	2.000E-05	2.5 h	5.000E-05	Not compliant with the residual probability criterion [A002 probability per flight hour (2.000E-05/FH) is more frequent than 1.000E-05/FH].
		L003	LAT 3	1.000E-06	10.0 h	1.000E-05	
3	1.000E-10	A004	ACT 4	1.000E-05	2.5 h	2.500E-05	Not compliant with the residual probability criterion [while A004 probability per flight hour is equal to 1.000E-05/FH, the combined probability per flight hour of A004 and A002 (1.000E-05/FH + 2.000E-05/FH) is more frequent than 1.000E-05/FH. <i>Note: Dual-order minimal cut sets #2 and #3 are grouped due to same event L003 appearing under G002 and G004.</i>
		L003	LAT 3	1.000E-06	10.0 h	1.000E-05	
4	1.000E-10	A004	ACT 4	1.000E-05	2.5 h	2.500E-05	Compliant with both limit latency and residual probability criteria [A004 probability per flight hour is equal to 1.000E-05/FH and L005 probability is less frequent than 1.000E-03].
		L005	LAT 5	1.000E-06	10.0 h	1.000E-05	
5	2.000E-11	A002	ACT 2	2.000E-05	2.5 h	5.000E-05	This dual-order minimal cut set does not contain any basic event being latent for more than one flight. Therefore, CS 25.1309(b)(5) is not applicable to this minimal cut set.
		A005	ACT 5	1.000E-06	2.5 h	2.500E-06	
6	6.500E-13	A003	ACT 3	6.500E-07	2.5 h	1.625E-06	Compliant with both limit latency and residual
		L004	LAT 4	1.000E-07	10.0 h	1.000E-06	



							probability criteria [A003 probability per flight hour (6.500E-07/FH) is less frequent than 1.000E-05/FH and L004 probability is less frequent than 1.000E-03]
7	3.991E-11	A002	ACT 2	2.000E-05	2.5 h	5.000E-05	This minimal cut set is more than a dual failure combination. Therefore, CS 25.1309(b)(5) is not applicable to this minimal cut set.
		L001	LAT 1	4.000E-06	1000.0 h	3.992E-03	
		L002	LAT 2	5.000E-06	100.0 h	4.999E-04	
Flight time = 2.5 hours $P[\text{LAT } i] \sim \text{FR} * T$							

Table A5-1: Minimal Cut Sets

