European Aviation Safety Agency — Rulemaking Directorate

Notice of Proposed Amendment 2014-02

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

RMT.0049 (25.029) — 27/01/2014

EXECUTIVE SUMMARY

This Notice of Proposed Amendment (NPA) addresses a safety issue, as well as a regulatory coordination issue related to safety assessment of critical systems at aircraft level.

The specific objectives are to maintain high safety and regulatory harmonisation through:

- definition of a standardised criterion for conducting aeroplane-level safety assessment of specific risks that encompasses all critical aeroplane systems on large aeroplanes (i.e. in particular update AMC to CS 25.1309), based on the results of the ARAC ASAWG;
- amendment of AMC 25.1309 to take into account of the latest updates of industry documents, such as ED79A/ARP4754A; and
- updating CS 25.671 on safety assessment of flight control systems, based on the results of the ARAC FCHWG.

In general terms, the approach proposed in the present NPA is based on the results of the FCHWG (Flight Controls Harmonisation Working Group) on the subsequent results of the ASAWG (Airplane-level Safety Analysis Working Group) report (together with the dissenting opinions expressed) to which the Agency and the FAA participated.

Through this NPA the Agency is seeking to acquire the views of the stakeholders on the proposed amendments to CS-25 (Book 1 and Book 2), before amending Decision No 2003/02/RM of the Executive Director of the European Aviation Safety Agency of 17 October 2003 on certification specifications, including acceptable means of compliance, for large aeroplanes ('CS-25').

Applicability		Process map	
Affected regulations and decisions:	CS-25 (Certification Specification for large aeroplanes)	Terms of Reference (issue 2):	18 March 2013
Affected stakeholders:	Manufacturers of Large Aeroplanes and related airborne equipment	Concept Paper:	No
Driver/origin:	Safety, level playing field	Rulemaking group:	No
Reference:	Recommendations produced by the Airplane-level Safety Analysis Working Group (ASAWG), and the Flight Controls Harmonisation Working Group (FCHWG) established by the FAA ARAC	RIA type:	Light
		Technical consultation during NPA drafting:	Yes (with FAA)
		Duration of NPA consultation:	3 months
		Review group:	No
		Focussed consultation:	No
		Publication date of the Opinion:	Not applicable
		Publication date of the Decision:	2015/Q2

Table of contents

1. Procedural information

1.1. The rule development procedure

The European Aviation Safety Agency (hereinafter referred to as the 'Agency') developed this Notice of Proposed Amendment (NPA) in line with Regulation (EC) No 216/2008[1] (hereinafter referred to as the 'Basic Regulation') and the Rulemaking Procedure[2].

This rulemaking activity is included in the Agency's 4-year Rulemaking Programme. It implements the rulemaking task RMT.0049 (25.029) 'Specific risk and standardised criteria for conducting aeroplane-level safety assessments of critical systems'.

The text of this NPA has been developed mainly based on the recommendations produced by the Airplane-level Safety Analysis Working Group (ASAWG), and the Flight Controls Harmonisation Working Group (FCHWG) established by the FAA ARAC[3]. The Agency participated to both working groups.

The text of this NPA has been drafted by the Agency based on the resuts of the two mentioned groups and further bi-lateral coordination with the FAA experts. The results of the two groups, in particular of the FCHWG, whose recommendations had been presented in September 2002, were for some aspects aligned with the evolution of the 'state of the art' in particular in relation to flight controls.

The text of the rules proposed by this NPA is hereby submitted for consultation of all interested parties[4].

The process map on the title page contains the major milestones of this rulemaking activity to date and provides an outlook of the timescale of the next steps.

1.2. The structure of this NPA and related documents

Chapter 1 of this NPA contains the procedural information related to this task. Chapter 2 (Explanatory Note) explains the core technical content. Chapter 3 contains the proposed text for the new requirements. Chapter 4 contains the Regulatory Impact Assessment showing which options were considered and what impacts were identified, thereby providing the detailed justification for this NPA.

1.3. How to comment on this NPA

Please submit your comments using the automated **Comment-Response Tool (CRT)** available at **http://hub.easa.europa.eu/crt/**[5].

The deadline for submission of comments is **27 April 2014.**

---

[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), as last amended by Commission Regulation (EU) No 6/2013 of 8 January 2013 (OJ L 4, 9.1.2013, p. 34).

[2] The Agency is bound to follow a structured rulemaking process as required by Article 52(1) of the Basic Regulation. Such process has been adopted by the Agency's Management Board and is referred to as the 'Rulemaking Procedure'. See Management Board Decision concerning the procedure to be applied by the Agency for the issuing of Opinions, Certification Specifications and Guidance Material (Rulemaking Procedure), EASA MB Decision No 01-2012 of 13 March 2012.

[3] The Aviation Rulemaking Advisory Committee (ARAC) is a formal standing committee, comprised of representatives from aviation associations and industry. Established by the Federal Aviation Administration (FAA) 15 February 1991, ARAC provides industry input in the form of information, advice and recommendations to be considered in the full range of FAA rulemaking activities.

[4] In accordance with Article 52 of the Basic Regulation and Articles 5(3) and 6 of the Rulemaking Procedure.

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

1.4. The next steps in the procedure

Following the closing of the NPA public consultation period, the Agency will review all comments.

The outcome of the NPA public consultation will be reflected in the respective Comment-Response Document (CRD).

The Agency will publish the CRD simultaneously with the Decision amending Certification Specification CS-25 (Book 1) and related Acceptable Means of Compliance (AMC) and Guidance Material (GM) (Book 2).

2. Explanatory Note

2.1. Overview of the issues to be addressed

The purpose of this Notice of Proposed Amendment (NPA) is to amend Decision No 2003/002/RM of the Executive Director of the European Aviation Safety Agency of 17 October 2003 on Certification Specifications, including Acceptable Means of Compliance, for Large Aeroplanes ('CS-25')[6]. The scope of this rulemaking activity is outlined in the Terms of Reference (ToR) RMT.0049 (25.029) issue 2, dated 18 March 2013 and is described in more detail below.

Different ARAC Harmonisation Working Groups (HWG) (Flight Controls, Power Plant Installations, and Systems Design and Analysis) have produced, during the last decade, various recommendations regarding the safety assessment of critical systems at aeroplane level.

The Agency has already adopted part of these recommendations. However, it has neither yet adopted the recommendations from the Flight Controls Harmonisation Working Group (FCHWG), nor from the Phase 2 recommendations from the Systems Design and Analysis Harmonisation Working Group (SDAHWG).

Although the subject of specific risk analysis was addressed in both working groups, the respective recommendations have not always been mutually consistent. Direct application of these recommendations could, therefore, result in non-standardised system safety assessments across various critical systems. This could also cause conflicting interpretations when conducting system safety assessments in future certification programmes.

The suboptimal situation generated by mutually inconsistent requirements is expected, if nothing is done, to progressively become even worse, due to the industry trend towards highly integrated systems

2.2. Objectives

The overall objectives of the EASA system are defined in Article 2 of the Basic Regulation. This proposal will contribute to the achievement of the overall objectives by addressing the issues outlined in Chapter 2 of this NPA.

The specific objectives of this proposal are to:

- define a standardised criterion for conducting aeroplane-level safety assessment of specific risks that encompasses all critical aeroplane systems on large aeroplanes (i.e. in particular update AMC to CS 25.1309), based on the results of the ARAC ASAWG;
- amend AMC 25.1309 to take into account of the latest updates of industry documents, such as ED79A/ARP4754A; and
- update CS 25.671 on safety assessment of flight control systems, based on the results of the ARAC FCHWG.

[6] Decision as last amended by Decision No 2013/033/R of 19 December 2013 ('CS-25' Amendment 14).

2.3. Summary of the Regulatory Impact Assessment (RIA)

To pursue the specific objectives identified in the paragraph above, four options have been identified:

No.	Identification	Description
0	**Do nothing**	Do not amend CS-25 and associated AMC's to address recommendations from ARAC FCHWG and ASAWG reports.
1	**Amend CS-25**	Amend CS-25 and associated AMC's to address recommendations from ARAC FCHWG and ASAWG reports, with the objective to harmonise the specific risk consideration within the systems.
2	**Publish AMC 20-1309**	Delete AMC XX.1309 from all aircraft CSs and replace them by a single AMC 20-1309 to make the specific risk consideration applicable to any aircraft and not only to large aeroplanes.
3	**Publish generic AMC**	Issue generic rules for risk assessment in the total aviation system (recital 1 of Regulation 1109/2009) applicable to any aviation domain (e.g. ATM).

The identified options have been compared from the safety, social, environmental, economic, proportionality and regulatory harmon,isation perspectives. All the considerations have been expressed in non-dimensional coefficientss according to the Multi-Criteria Analysis (MCA) methodology, with higher 'weighted' scores assigned to safety (3) and environment (2).

Option 0 ('do nothing') is globally negative and, although neutral in terms of safety (no pressing safety issue has been identified), it is highly negative in terms of regulatory harmonisation between America and Europe, which would cause problems to manufacturers of large aeroplanes.

Option 1 (i.e. amend CS-25 Book 1 and 2 in a similar timeframe and harmonise with FAA) is the only option significantly positive, including in terms of safety, economic impact, proportionality and regulatory harmonisation. It is neutral for the social and environmental impacts.

Option 2 (i.e. impose the same rigour of safety assessment to manufacturers of any aircraft, beyond large aeroplanes) is the most positive in safety terms, but extremely negative in terms of economic, proportionality and harmonisation

Option 3 (i.e. generic AMC covering not only initial airworthiness, but safety assessments also in other aviation domains, like ATM and airports) is in summary the most negative option. It is negative also in terms of safety impact.

Therefore, Option 1 (i.e. amend CS-25) is the preferred one.

2.4. Overview of the proposed amendments

2.4.1. General approach

After reviewing the existing regulations and the recommendations from various harmonisation working groups, the Agency, together with the FAA, has identified the need to clarify and standardise safety assessment criteria. This activity was performed under an

ARAC task, open to other aviation rulemakers in addition to the US FAA, to integrate the safety assessment criteria from various system disciplines.

In particular CS-25.671 (control systems) and associated AMC requires an amendment based on recommendation from the Flight Controls Harmonisation Working Group (FCHWG).

Other amendments, in particular to AMC CS-25.1309, stem from the Airplane-level Safety Analysis Working Group (ASAWG), which completed its task and produced its final report.

For the purpose of this NPA, the definition of 'Specific Risk', developed by the above-mentioned ASAWG, is:

'The risk on a given flight due to a particular condition'

The Specific Risks of Concern (SRC) are those when the aeroplane is one failure away from a catastrophe, or when the risk is greater than the average probability criteria provided in AMC 25.1309 for hazardous and catastrophic failure conditions on a given flight due to a particular condition.

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.

In conclusion, based on recommendations from both groups, and bi-lateral coordination with FAA (from which the corresponding NPRM is expected in the first half of 2014), the following topics are covered by this NPA:

- Control systems;
- Latent failure;
- Aging and wear;
- Master Minimum Equipment List (MMEL); and
- Flight and diversion time.

2.4.2. Control systems

The following paragraphs detail the rationale supporting the draft Decision proposing changes to CS 25-671, 25-629 and associated AMC:

(a) It is recommended that CS 25.671(a) should include material from fly-by-wire certification programmes requiring consideration of aircraft operation in any attitude.

(b) CS 25.671(b) is proposed to be revised by discouraging marking alone as a desired means of ensuring correct assembly.

(c) CS 25.671(c)(1) is recommended to be changed by removing 'extremely improbable' as a means of compliance and to clarify which jamming is to be excluded from 'any single failure' but addressed under CS 25.671(c)(3).

(d) CS 25.671(c)(2) is proposed to be changed by adding the latent failure-specific risk and exposure time limitation criteria similar to that defined in CS 25.1309(b)(5) and to clarify which jamming is to be excluded but addressed under CS 25.671(c)(3).

(e) CS 25.671(c)(3) is proposed to be changed by providing a definition for a (c)(3) jam and to add the exposure time limitation criterion similar to that from 25.1309(b)(5) on additional failure 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.

(g) CS 25.671(e) is proposed to be reviesed by adding a requirement for recognition of control means at the limits of authority from fly-by-wire certifications.

(h) CS 25.671(f) is proposed to be revised by adding a requirement for mode annunciation from fly-by-wire certifications.

(i) AMC 25.671(a), AMC 25.671(b), and AMC 25.671(c)(1) are proposed to be replaced by AMC 25.671.

(j) AMC 25.671(c) is recommended to be changed by proposing a definition and assessment for Continued Safe Flight and Landing.

(k) AMC 25.672(c)(1) is proposed to be deleted as it is being completely covered by CS 25.1309 and associated AMC. Systems showing compliance with CS 25.672 must also show compliance with CS 25.1309.

(l) Furthermore, the current CS 25.629 requires the aeroplane to be free from aeroelastic instability (including flutter) under normal conditions and, separately, under failures, malfunctions, and adverse conditions. The latter conditions include any damage, failure or malfunction, considered under CS 25.671 and CS 25.1309, and any other combination of failures, malfunctions, or adverse conditions, which are not shown to be extremely improbable. Due to the amended CS 25.671(c)(2), in turn, based on the FCHWG report, the failure combinations such as dual hydraulic system failure, dual electrical system failure and single failure in combination with any probable hydraulic or electrical failure are proposed to be added to CS 25.629(d). As reflected in AMC 25.629, certain combinations of failures are not normally considered extremely improbable regardless of probability calculations.

(m) It is acknowledged that the current text of AMC 25.629 (paragraph 4.3.)[7] is not completely unambiguous in addressing the failure combinations mentioned in the paragraph above. However, for aircraft where reliance is placed on restraint stiffness and/or damping of the flight controls to prevent flutter, it has been standard practice to consider these failure combinations regardless of probability. In many cases this has been explicitly enforced by FAA Issue Papers on this subject, reflecting the philosophy supported by the Agency that the level of safety for these aircraft equipped with two actuators per control surface should not be degraded compared with earlier designs of flight controls, or compared with mass balanced control surfaces.

(n) AMC 25.629 paragraph 4.3 is hence proposed to be revised by deleting the sentence related to reliability assessment since the failure combinations under concern (ref. above) need to be considered regardless of probability calculations.

(o) Amendments to Appendix K in CS-25 are proposed to be revised by aligning the overall approach on the proposed CS 25.671 and CS 25.1309.

2.4.3. Latent Failure

CS 25.1309 in Book 1 of CS-25 was considered as the natural candidate to host the standardised approach for the latent specific risk across all systems also having in mind that the tasking boundaries of ASAWG excluded specific risk associated with airframe structures and methodologies not covering aeroplane certification.

This standardised approach for the latent specific risk took into account the following aspects:

- To give special consideration to the avoidance of significant latent failures, whenever practical, while preventing negative consequences for maintenance.

[7] I.e. Amendment 14 of CS-25.

- To establish screening criteria (or filters) to determine which failure conditions will have additional specific risk criteria applied.
- To concentrate on the specific risk of concern when the aeroplane is one failure away from a catastrophe on a given flight due to latent failures.
- To establish a single consistent objective quantitative criterion and methodology to limit the worst anticipated residual risk for catastrophic failure conditions given that any single latent failure has occurred.
- To establish a single consistent objective quantitative criteria and methodology to limit the worst anticipated latency for catastrophic failure conditions.
- To avoid imposing unnecessary additional redundancy which would result in average risk significantly less frequent than 10-9/FH.

After reviewing the existing regulations and the recommendations from various harmonisation working groups, the ASAWG established a recommendation for amending CS 25.1309(b) and AMC 25.1309, sections 9.b.(6) & 9.c.(6).

The purpose of this recommendation was to ensure a standardised consideration of the latent specific risk across all systems. Consequently, other material in FAR/CS and related AC/AMC, requires amendment, since, as highlighted by the ARAC recommendations, they still consider latent specific risk using different approaches. Amendments are hence proposed to refer to the revised CS 25.1309(b) and AMC 25.1309, sections 9.b.(6) & 9.c.(6) from other paragraphs of CS-25.

The industry was concerned about the proliferation and use of the qualitative statements in FAR/CS (e.g. 'whenever practical', these 'latent failures should be avoided', etc.). Such statements were considered in fact too open to different practices, although recognised as good design practices and widely implemented by industry. Therefore, ASAWG recommended to only introduce into the requirement CS 25.1309(b) quantitative objectives applicable to catastrophic failure conditions resulting from two failures, either of which is latent for more than one flight. These quantitative objectives provided the ultimate mitigation when latent failures have proven over time to be impractical to design around or eliminate in aircraft systems.

When developing new requirement CS 25.1309(b)(4), as proposed in this NPA, there was a desire to enforce the first intended objective 'significant latent failure minimisation', while considering industry's concerns by providing clear means to address compliance with this objective in the AMC (see AMC 25.1309 section 9.b.(6)). The Agency's concern, along with the FAA's, was that not introducing this qualitative objective in the requirement in Book 1 can be considered as 'rulemaking by AMC'. On the other side the Agency accepts that maximum clarity on the acceptable methods should be achieved, indeed, at the level of AMC.

When developing new requirement CS 25.1309(b)(5), there was a desire to keep the acceptance criteria for both limit latency criteria and limit residual risk in the qualitative terms currently used by the industry. The term '… on the order of 1/1000 or less' in the ASAWG recommendation was first selected over a qualitative term such as probable, because the historical use of this term in the current regulations and Guidance Material is not consistent. Later on, however, the Agency, as well as the FAA, deemed it more appropriate to remove the terms 'on the order of' which preceded '1/1000'. Since a qualitative term could not be agreed on, and a specific quantitative threshold was defined as ultimate mitigation, there was no point in keeping such terms any longer.

Based on the same rationale as above related to 'significant latent failure minimisation', a sub-provison has been introduced into CS 25.1309(b)(5) in addition to the ASAWG recommendation. Without this hook in the requirement, the compliance with CS 25.933(a)(1)(ii) referring to CS 25.1309(b) would have then allowed design configurations with pre-existing failures which are traditionally avoided per current practices, refer to AMC 25.933(a)(1).

The Decision to limit CS 25.1309(b)(5) to only two order cut sets was made after an extensive review by the industry conducted on several certified aircraft. The average risk analysis, along with the qualitative approach of minimising the significant latent failures, adequately protect the three or more failure combinations.

The last sentence of the ASAWG recommendation for AMC 25.1309 Section 9.b.(6) 'Residual risk is the sum of single active component(s) that have to be combined with the single latent failure to result in the Catastrophe.' was considered difficult to comprehend. An example of limit latency and residual risk analysis is then provided in a new Appendix to AMC 25.1309, accommodating ANAC additional recommendation.

A change to CS 25.933(a)(1)(ii) is proposed since the rule, combined with recent policy, implies that latent specific-risk criteria should be applied to thrust reversers. This policy, based on earlier ARAC recommendations and currently also used by the Agency, requires the review of latent related specific risk. Deletion of Sections 8.b.2 and 8.b.3 from the current AMC 25.933(a)(1) is recommended by ASAWG to ensure consistency across the industry and systems. As explained above, the Agency considered that the proposed change would allow design configurations with pre-existing failures which are traditionally avoided per current practices. Paragraph 8.b. of AMC 25.933(a)(1) was only updated to highlight design configurations detailed in subparagraphs 8.b.(2) and 8.b.(3), which traditionally have been deemed practical.

As stated in the ASAWG report, the group did not have experience and adequate knowledge to recommend changes to AMC 25.981(a). The Agency has then considered that any change to CS 25.981(a)(3) and associated AMC should not be handled as part of this rulemaking task RMT.0049.

2.4.4. Ageing and Wear

Appendix 3 - b.(1) of AMC 25.1309 was proposed by ASAWG to be changed fpr clarifying the consideration of ageing & wear aspects of system components. It was in fact recognised by the ASAWG, that replacement times, associated with system components whose probability of failure may be associated with non-constant failure rates during the operational life of the aircraft, have not been treated in the same manner by different applicants and across various systems by a single applicant.

The change that is recommended by this NPA aims at ensuring consistent documentation of system component replacement times, as necessary to protect system components against ageing and wear out. The following aspects are taken into account by the recommended change:

By referencing 'the operational life of the aircraft' the change highlights that it is not necessary to consider increased failure rate of components when this increase is exhibited beyond the operational life of the aircraft,

- by referencing '… same methodology as other scheduled maintenance tasks required to satisfy 25.1309 (e.g. AMC 25-19) and documented in the Airworthiness Limitation Section…' the recommended change mentions the appropriate place for documenting the replacement times;
- by referencing '...those components whose failures could lead directly or in combination with one other to a catastrophic or hazardous failure conditions...' the recommended change avoids that items which have to fail in combination with many others to cause a catastrophic or hazardous functional failure condition have to be documented in the Airworthiness Limitation Section.

2.4.5. Master Minimum Equipment List (MMEL)

AMC 25.1309 Sections 12.b.(1) and 12.d are proposed to be changed for allowing better harmonisation and improved clarity between this AMC 25.1309 and the MMEL development process introduced in CS-MMEL.

2.4.6. Flight and Diversion Time

AMC 25.1309 paragraph 10.c.(2)(ii) is proposed for change to clarify the consideration of intensifying and alleviating factors, particularly with respect to flight duration, flight phase, and diversion time. While this is not strictly a specific risk concept, it is considered essential that the Functional Hazard Assessment (FHA) defines the hazard classification for a given failure condition correctly. Without properly accounting for intensifying factors in the FHA, specific risk concerns, worthy of being addressed, may be missed while still in this criteria setting activity.

Specific changes include deleting the second sentence in the paragraph based on the rationale that this sentence does not provide any useful guidance and adds confusion by mixing up relevant factors with effects of failure. A new sentence is proposed to be added to specifically address flight duration, flight phase and diversion time as relevant factors.

Subsequent minor changes are proposed in sentence following in the same paragraph, to make the text more logically flowing and not to lose the existing examples of intensifying factors.

A final sentence of the paragraph is also proposed to address confusion with respect to the compounding nature of factors in defining the hazard classifications in an FHA. Obviously, compounding factors which are in themselves extremely improbable, need not be considered; but the question of what must be considered is a constant source of confusion both for the regulatory experts and for the applicants.

The sentence proposed by this NPA aims at best capturing both historical concepts and the concern that the FHA is a qualitative assessment and, therefore, it avoids terms that would be interpreted as requiring a probabilistic assessment. For instance, the words 'Combinations of Factors need only be considered if they are anticipated to occur together' can lead to different interpretations. While it is unavoidable that certain probabilistic aspects are considered, the intent of the proposed modification is to make clear that a quantitative probabilistic assessment of what to consider as 'relevant factors' is not necessarily required, while a qualitative consideration regarding the likelihood of factors and their independence should always be part of the assumptions documented with functional failures described in the FHA.

AMC 25.1309 Section 11.g is proposed for change to address unclear guidance in the first paragraph on how environmental or operational factors are considered in safety assessments. For this purpose, the second sentence of the first paragraph is modified and a new third and fourth sentence are added.

Furthermore, AMC 25.1309 Appendix 4 is proposed for change to clearly focus on environmental conditions and operational factors. Some of the items listed as 'Other Events' in the table in Appendix 4 are system failures, not environmental or operational conditions. These failures were removed from the table and remaining items were revised for clarity. Reference to HIRF and Lightning were removed from the table to avoid confusion that numerical analyses are always required for compliance with CS 25.1309 when effects of HIRF and lightning are considered. No attempt was made to modify the table for completeness or to re-justify the probability values.

2.4.7. Aeroplane and Systems Development Assurance

Finally, AMC 25.1309 Sections 5, Section 6.c, and Section 9.b.(4) are also proposed for change to take into account the latest update of Industry Standard ED-79A/ARP 4754A 'Guidelines for Development of Civil Aircraft and Systems'.

3. Proposed amendments

The text of the amendment is arranged to show deleted text, new or amended text as shown below:

(a) deleted text is marked with ~~strike through~~;

(b) new or amended text is highlighted in grey;

(c) an ellipsis (…) indicates that the remaining text is unchanged in front of or following the reflected amendment.

3.1. Draft Certification Specification CS-25 Book 1 (Draft EASA Decision)

SUBPART D–DESIGN AND CONSTRUCTION

GENERAL

CS 25.629 Aeroelastic stability requirements

...

(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:

...

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

...

(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, malfunctions, or adverse conditions not shown to be extremely improbable.

...

CONTROL SYSTEMS

CS 25.671 General

(See AMC 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.

(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).)~~

(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) For single failures:

Any single failure, excluding failures of the type defined in (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 (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.

~~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.

(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.

~~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 to an adverse position that is caused by an external source.

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

(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 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.

~~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 is approaching 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 Stability augmentation and automatic and power-operated systems

...

(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 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).

...

SUBPART F - EQUIPMENT

CS 25.1309 Equipment, systems and installations

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 power plant 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 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.

(c) Information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action. ~~A warning indication must be provided if immediate corrective action is required.~~ 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.

...

APPENDIX K

Interactions of Systems and Structure

K25.1 *General.*

The following criteria must be used for showing compliance with CS 25.302 for aeroplanes equipped with systems that affect the structural performance of the aeroplanes (e.g. systems that either directly or as a result of a failure or malfunction induce loads, change the response of the aeroplane to inputs such as gusts or pilot actions, or lower flutter margins). Examples of such systems are: automatic or electronic flight control systems, autopilots, stability augmentation systems, load alleviation systems, flutter control systems, and fuel management systems. These criteria also apply to hydraulic systems, electrical systems and mechanical systems. If this appendix is used for other systems, it may be necessary to adapt the criteria to the specific system.

...

(c) The following definitions are applicable to this appendix.

...

Failure condition: The term failure condition is the same as that used in CS 25.671 and CS 25.1309~~, however this appendix applies only to system failure conditions that affect the structural performance of the aeroplane (e.g., system failure conditions that induce loads, change the response of the aeroplane to inputs such as gusts or pilot actions, or lower flutter margins)~~.

...

K25.2 *Effects of Systems on Structures.*

...

(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:

...

(d) Failure indications. For system failure detection and indication, the following apply:

(1) The system must be checked for failure conditions, not extremely improbable or resulting from a single failure, that degrade the structural capability below the level required by CS-25 or significantly reduce the reliability of the remaining system. As far as reasonably practicable, the flight crew must be made aware of these failures before flight. Certain elements of the control system, such as mechanical and hydraulic components, may use special periodic inspections, and electronic components may use daily checks, in lieu of detection and indication systems to achieve the objective of this requirement. These certification maintenance requirements must be limited to components that are not readily detectable by normal detection and indication systems and where service history shows that inspections will provide an adequate level of safety.

(2) The existence of any failure condition, not extremely improbable or resulting from a single failure, during flight that could significantly affect the structural capability of the aeroplane and for which the associated reduction in airworthiness can be minimised by suitable flight limitations, must be signalled to the flight crew. For example, failure conditions that result in a factor of safety between the aeroplane strength and the loads of Subpart C below 1.25, or flutter margins below V", must be signalled to the crew during flight.

...

3.2. Draft Acceptable Means of Compliance and Guidance Material (Draft EASA Decision CS-25 Book 2)

AMC - SUBPART D –DESIGN AND CONSTRUCTION

AMC 25.629 - Aeroelastic stability requirements

...

4. *Detail Design Requirements.*

...

4.3. Where aeroelastic stability relies on control system stiffness and/or damping, additional conditions should be considered. The actuation system should continuously provide, at least, the minimum stiffness or damping required for showing aeroelastic stability without regard to probability of occurrence for:

(i) more than one engine stopped or wind milling,

(ii) any discrete single failure resulting in a change of the structural modes of vibration (for example; a disconnect or failure of a mechanical element, or a structural failure of a hydraulic element, such as a hydraulic line, an actuator, a spool housing or a valve);

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

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. ~~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.~~(CS 25.671), are not normally considered extremely improbable regardless of probability calculations. The reliability assessment should be part of the substantiation documentation.~~ In practice, meeting the above conditions may involve design concepts such as the use of check valves and accumulators, computerised pre-flight system checks and shortened inspection intervals to protect against undetected failures.

...

~~**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)**~~

~~**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)**~~

~~**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).~~

AMC 25.671

Control Systems – General

1. *PURPOSE.*

a. This AMC provides an acceptable means, but not the only means, of showing compliance with the control system requirements of CS 25.671. These means are intended to provide guidance to supplement the engineering and operational judgment that must form the basis of any compliance demonstration.

b. The means described in this AMC are neither mandatory nor regulatory by nature and do not constitute a regulation. These means are issued, in the interest of standardisation, for guidance purposes and to outline a method that has been found acceptable in showing compliance with the standards set forth in the rule. As this AMC is not mandatory, terms 'shall' and 'must' used in this AMC only apply to those applicants who choose to demonstrate compliance using this particular method.

c. Other alternative means of compliance that an applicant may propose should be given due consideration, provided they meet the intent of the regulation. In the absence of a rational analysis substantiated by data supporting alternative criteria, the criteria listed in this AMC may be used to show compliance with CS 25.671.

2*. RESERVED.*

3. *RELATED DOCUMENTS.*

The following guidance and advisory materials are referenced herein:

a. Advisory Circulars, Acceptable Means of Compliance.

(1) AC 25-7B, Flight Test Guide for Certification of Transport Category Airplanes.

(2) AMC 25.1309 System Design and Analysis

b. Industry documents.

(1) RTCA, Inc., Document No. DO-178()/EUROCAE ED-12(), Software Considerations in Airborne Systems and Equipment Certification, as recognised by AMC 20-115().

(2) Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A/EUROCAE ED-79A, Guidelines for development of civil aircraft and systems.

(3) Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4761/EUROCAE ED-135, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

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'.

5. *DEFINITIONS.*

The following definitions apply to the requirements of CS 25.671 and the Guidance Material provided in this AMC. Unless otherwise stated, they should not be assumed to apply to the same or similar terms used in other regulations or AMCs. Terms for which standard dictionary definitions apply are not defined herein.

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.

b. *Catastrophic Failure Condition.* As used in AMC 25.1309 (reference 3.a.2).

c. *Continued Safe Flight and Landing.* The capability for continued controlled flight and landing at an airport without requiring exceptional pilot 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 aircraft comes to a complete stop on the runway.

e. *Latent Failure.* As used in AMC 25.1309 (reference 3.a.2).

f. *Latency Period.* 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."

g. *Error.* As used in AMC 25.1309 (reference 3.a.2).

h. *Event.* As used in AMC 25.1309 (reference 3.a.2).

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.

j. *Extremely Improbable.* As used in AMC 25.1309 (reference 3.a.2).

k. *Failure.* As used in AMC 25.1309 (reference 3.a.2).

The following are some of the types of failures to be considered in showing compliance with CS 25.671(c). Since the type of failure and the failure's effect depends on system architecture, this list is not all-inclusive, 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. 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.

(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, or loss of hydraulic power. 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 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 jamming, 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 to be 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 CS25.671(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, the higher friction may result in reduced centring of the controls.

l. *Failure States.* As used in CS25.671(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.

m. *Flight Control System.* Flight control system refers to the following: primary flight controls from the pilots' controllers to the primary control surfaces, trim systems from the pilots' trim input devices to the trim surfaces (incl. stabiliser trim), speed brake/spoiler (drag devices) systems from the pilots' control lever to the spoiler panels or other drag/lift-dumping devices, high-lift systems from the pilots' 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
- Control Surfaces
- Attachment Fittings

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.

o. *Take-off* is considered to be the time period between brake release and 35 ft. *In-flight* is considered to be from 35 ft following a take-off to 50 ft prior to landing including climb, cruise, normal turns, descent, and approach.

6. *BACKGROUND.*

a. This AMC was developed based on recommendations from several working groups under the FAA Aviation Rulemaking Advisory Committee.

b. In 2001, the Flight Controls Harmonization Working Group (FCHWG) provided recommendations for changes to FAR/JAR 25.671 and the corresponding advisory material used to develop this AMC. These recommendations included a unique criterion to address latent failures in flight control systems.

c. In addition to the FCHWG, several other working groups separately developed different criteria for latent failures in system designs. In 2010, the Airplane Level Safety Analysis Working Group reviewed all of the previous recommendations and developed a common approach to addressing latent failures. As a result, the FCHWG recommendations were modified, and the requirements specified in CS 25.671(c) are now intended to be identical with the corresponding requirements in CS 25.1309 and rely on the same methods of compliance.

d. Some additional aspects have been included, based on in-service experience.

7. EVALUATION OF CONTROL SYSTEM OPERATION – CS 25.671(a).

a. *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 that 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.

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).

8. *EVALUATION OF 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 parts control (ref. CS 25.1301(a)(2)).

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.

b. Adequate precautions should be taken in the design process and adequate procedures should be specified in the maintenance manual to prevent the incorrect installation, connection, or adjustment of parts of the control system.

The applicant should:

(i) Analyse the assembly and maintenance of the system to assess the classification of potential failures.

(ii) For Cat/Haz/Maj failures: Introduce Physical Prevention against mis-assembly or discuss with the Authority if Physical Prevention is not possible.

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

9. *EVALUATION OF CONTROL SYSTEM FAILURES – CS 25.671(c).*

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.

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,.

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). For this application, extremely improbable is defined based on the criteria established in AMC 25.1309.

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 is intended to address 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 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 pilot control; those types of jams (such as a jammed valve) are considered under subparagraphs CS 25.671(c)(1) and (c)(2).

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.

Means to alleviate the runaway may be used to show compliance by reconfiguring the control system, deactivating the system (or a failed portion thereof), 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, or using a means of preventing a runaway. Without a suitable means to alleviate or prevent the runaway, an adverse position would represent any position for which they are approved to operate.

Additionally, runaways that are caused by external sources, such as a foreign or loose objects, control system icing or any other environmental or external source are addressed in CS25.671(c)(4)

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. This probability is used to justify the definition of 'normally encountered position' and is not intended to be used to support a probabilistic assessment. 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.

One method of establishing acceptable flight control surface deflections is the performance-based criteria outlined in this AMC which were established to eliminate any differences between aircraft types. The performance-based criteria prescribe environmental and operational manoeuvre conditions, and the resulting deflections may be considered normally encountered positions for compliance with CS 25.671(c)(3).

Alleviation means may be used to show compliance with CS 25.671(c)(3). For this purpose, alleviation means include system reconfigurations or any other features that eliminate or reduce the consequences of a jam or permit continued safe flight and landing.

All approved aircraft gross weights and cg locations should be considered. However, only critical combinations of gross weight and cg need to be demonstrated.

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

In showing compliance with the failure requirements of CS 25.671(c)(2), the following analysis/assessment is necessary.

The 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 these requirements, a safety analysis/assessment according to the techniques of AMC 25.1309 should be used.

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.

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

The flight phases required by CS 25.671 can be encompassed by three flight phases: take-off, in-flight (climb, cruise, normal turns, descent, and approach), and landing.

CS 25.671(c)(3) requires that the aeroplane be capable of landing with a flight 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 aircraft response to manoeuvres and continued safe flight to landing.

It is 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 25 knots 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 flight control inputs greater than that necessary at V_1 will occur at speeds below V1, any jam in these flight control axes during a crosswind take-off will normally be 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 determination of jammed lateral or directional flight control positions during take-off is 15 knots.

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.

The jam positions to be considered in showing compliance include any position up to the maximum position determined by the following manoeuvres. 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, and are not to represent flight test manoeuvres for such an evaluation; see section 9.e.

(1) *Jammed Lateral Control Positions.*

(i) Take-off: The lateral flight control position for wings-level at V_1 in a steady crosswind of 15 knots (at a height of 10 meters above the take-off surface). Variations in wind speed from a 10 meter height can be obtained using the following relationship:

$$V_{alt} = V_{10meters} * (H_{desired}/10.0)^{1/7}$$

Where:

$V_{10meters}$ = Wind speed in knots at 10 meters above ground level (AGL)

V_{alt} = Wind speed at desired altitude (knots)

$H_{desired}$ = Desired altitude for which wind speed is sought (meters AGL), but not lower than 1.5 meters (5 feet)

(ii) In-flight: The lateral flight control position to sustain a 12 degree/second steady roll rate from $1.23V_{SR1}(1.3V_S)$ to V_{MO}/M_{MO} or V_{fe}, as appropriate, but not greater than 50 % of the control input.

Note: If the flight control system augments the pilot's input, then the maximum surface deflection to achieve the above manoeuvres should be considered.

(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.

(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 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.

(ii) In-flight: The maximum longitudinal flight control position is the greater of:

(1) The longitudinal flight control position required to achieve steady state normal accelerations from 0.8g to 1.3g at speeds from $1.23V_{SR1}$($1.3V_S$) to V_{MO}/M_{MO} or V_{fe}, as appropriate.

(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.

(iii) Flare/landing: any longitudinal control position required, in manual or autopilot mode, for performing a flare and landing, using the manufacturer recommended procedures.

(3) *Jammed Directional Control Positions.*

(i) Take-off: The directional flight control position for take-off at V_1 in a steady crosswind of 15 knots (at a height of 10 meters above the take-off surface). Variations in wind speed from a height of 10 meters can be obtained using the following relationship:

$$V_{alt} = V_{10meters} * (H_{desired}/10.0)^{1/7}$$

Where:

$V_{10meters}$ = Wind speed in knots at 10 meters above ground level (AGL)

V_{alt} = Wind speed at desired altitude (knots)

$H_{desired}$ = Desired altitude for which wind speed is sought (meters AGL), but not lower than 1.5 meters (5 feet)

(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 defined by 15 fps from sea level to 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

aircraft, this addresses any lateral/directional asymmetry that can occur in flight with symmetric power.

(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.

(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.

(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 manufacturer's recommended procedures for take-off and that are normally used throughout the flight to trim the aircraft 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 jamming (asymmetric spoiler panel) is addressed in Section 9.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 aircraft has safe flight characteristics with the asymmetric flap positions not shown to be extremely improbable.

(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 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).

(ii) Manoeuvre Load Alleviation Systems: At any airspeed between $1.23V_{SR1}(1.3V_S)$ to V_{MO}/M_{MO} or Vfe, 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)/(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 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 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

(2) A qualitative analysis. This should be used only for root causes where no in-service data are available. This qualitative analysis should include

(i) a description of the design features that are intended to prevent a jam from occurring, due to physical interference (jam prevention means), and

(ii) a description of the means by which a jam could be alleviated (jam alleviation).

If the extremely improbable demonstration (using either method (1) or (2)) is accepted by the agency the design would be considered as compliant with the intent of CS 25.671(c)(3)(i)/(ii).

d. Jam Combinations Failures – CS 25.671(c)(3)(iii)

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.

As a minimum, this analysis should include such elements 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 determine intervals for scheduled maintenance activity or operational checks that ensure the availability of 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 Sections 9.a, 9.b, 9.c and 9.d, the manoeuvrability and structural strength criteria defined in the following sections should be considered to determine the aeroplane's capability for continued safe flight and landing.

(1) *Flight Characteristics.*

(i) *General.* Following flight control system failure, appropriate procedures may be used including system reconfiguration, flight limitations, and 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 for use of differential engine thrust to manoeuvre the aircraft. However, differential thrust may be used following the recovery to maintain lateral/directional trim following the flight control system failure.

For the longitudinal flight control surface jam during take-off prior to rotation, it is necessary to show that the aircraft 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 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:

(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 or vibration;
(E) Bank angle in excess of 90 degrees.

In connection with the transient response, compliance with the requirements of CS 25.302 should be shown. 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 9.b. provides a means of determining flight control surface deflections for the evaluation of flight control jams. In some cases, aircraft 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 9.b.(1)(ii) is based on a steady roll rate of 12 degrees per second. When evaluating this condition, whether 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 aeroplane's actual roll or pitch rate 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 type 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 (<1,000 feet AGL)	1 second*
Manual flight (>1,000 feet AGL)	1 second*
Automatic flight (>1,000 feet 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 tests or during flight testing. This value should be used during all analysis efforts. However, flight testing 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 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.

Note: For the case of a lateral or directional flight control system jam during take-off that is described in Section 9(b)(1) or 9(b)(3), it should be shown that the aircraft can safely land on a suitable runway with any crosswind from 0 kt to the crosswind level and direction 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(c).

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 of CS 25.143(c) 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 exceedances 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 aircraft maintains structural integrity for continued safe flight and landing. This should be accomplished by showing compliance with CS 25.302.

(ii) *Jam Conditions per CS 25.671(c)(3).* It should be shown that the aircraft maintains structural integrity for continued safe flight and landing. Recognising that jams are infrequent occurrences and that margins have been taken in the definition of normally encountered positions of this AMC, criteria other than those specified in CS 25.302 Appendix K25.2(c) may be used for structural substantiation to show continued safe flight and landing.

Structure is to be designed such that Continued Safe Flight & Landing is ensured after any single jam in a normally encountered position.

Attention should be paid to the detectability of the jam and risk for the jam and/or its consequences to remain hidden for more than one flight.

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.

This structural substantiation should be per Section 9.e.2.(iii).

(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 g and 1.75 g with high-lift devices fully retracted and in en-route configurations, and between 0.6 g 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 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.

A flexible aircraft model should be used for loads calculations.

10. *EVALUATION OF ALL ENGINES FAILED CONDITION – CS 25.671(d).*

a. *Explanation.*

CS 25.671(d) states that,

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:

(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. '

The intent of CS 25.671(d) is to assure that in the event of failure of all engines and given the availability of an adequate runway, the aeroplane will be controllable, an approach and flare to a landing 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.*

(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, including the time it takes for activating 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 take-off and landing. Credit may be taken for hydraulic pressure/electrical power produced while the engines are spinning down and any residual hydraulic pressure is remaining in the system. Sufficient power must be available to complete a wings-level approach and flare to a landing.

Analyses or tests may be used to demonstrate the capability of the control systems to maintain adequate hydraulic pressure/electrical power during the time between the failure of the engines and the activation of any backup systems. If any of the

backup systems rely on aerodynamic means to generate power, then a flight test demonstration should be performed to demonstrate that the backup system could supply adequate electrical and hydraulic power to the flight control systems. The flight test should be conducted at the minimum practical airspeed required to perform an approach and flare to a safe landing attitude.

(3) The manoeuvre capability following the failure of all engines should be sufficient to complete an approach and flare to a landing. Note that the aircraft weight could be extremely low (e.g., the engine failures could be due to fuel exhaustion). The maximum speeds for approach and landing may be limited by other Part-25 requirements (e.g., ditching, tire speeds, flap or landing gear speeds, etc.) or by an evaluation of the average pilot's ability to conduct a safe landing. 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 aircraft configuration, the aircraft should be capable of:

(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 seconds (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 10 knots (measured at 10 meters above the ground);

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.

(4) It should be possible to perform a flare to a safe landing attitude, in the most critical configuration, from a stabilised approach using the recommended approach speeds 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.

11. *EVALUATION OF CONTROL AUTHORITHY AWARENESS – CS 25.671(e).*

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 must take into account that some pilot-demanded manoeuvres (e.g., rapid roll) are necessarily associated with intended full performance, which may saturate the surface. Therefore, simple alerting systems, which would function in both intended and unexpected flight control-limiting situations, must be properly balanced between needed crew-awareness and nuisance alerting. Nuisance alerting should be minimised. The term suitable indicates an appropriate balance between nuisance and necessary operation.

b. Depending on the application, suitable annunciations may include cockpit flight control position, annunciator light, or surface position indicators. Furthermore, this requirement applies at limits of flight control authority, not necessarily at limits of any individual surface travel.

12. *EVALUATION OF FLIGHT CONTROL SYSTEM SUBMODES – CS 25.671(f).*

Some systems, Electrical Flight Control Systems in particular, may have multiple modes of operation not restricted to being either on or off. The means provided to the crew to indicate the current mode of operation should be in accordance with CS 25.1322. This includes the indication to the crew of the loss of protections.

13. *ACCEPTABLE MEANS OF COMPLIANCE DEMONSTRATION.*

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 shown by analysis, simulation, a piloted engineering simulator, flight test, or combination of these methods as agreed with the certification authority. 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).

Efforts to show compliance with this Regulation may result in flight manual abnormal procedures. Verification of these procedures may be accomplished in flight or, with the agreement of the certification authority, 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 testing 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 demonstrations are the preferred method to show compliance.

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

      (i) A flight demonstration 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 are too difficult to attain (e.g., wind shear, high crosswinds);

      (iii) The simulation is used to augment a reasonably broad flight test programme;

      (iv) The simulation is used to demonstrate repeatability.

b. *Simulation Requirements.* Where it is agreed that a simulation will be used to establish compliance, to be acceptable for use in showing compliance with the performance and handling qualities requirements, the simulation should:

   (1) Be suitably validated by flight test data for the conditions of interest.

      (i) This does not mean that there must be flight test data at the exact conditions of interest; the reason simulation 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).

~~**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 - POWERPLANT

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 practical. The design configurations in paragraphs 8.b.(2) and 8.b.(3) have traditionally been considered practical and deemed acceptable to the Agency. ~~However, it also recognises that flexibility of design and maintenance are necessary for practical application.~~

8.b.(1) The thrust reverser system should be designed so that any in-flight thrust reversal that is not shown to be controllable in accordance with Section 7,above, is extremely improbable (i.e., average probability per hour of flight of the order of 1x10-9/fh. or less) and does not result from a single failure or malfunction. And

8.b.(2) For configurations in which combinations of two-failure situations (ref. Section 5, above) result in in-flight thrust reversal, the following apply:

Neither failure may be pre-existing (i.e., neither failure situation can be undetected or exist for more than one flight); the means of failure detection must be appropriate in consideration of the monitoring device reliability, inspection intervals, and procedures.

The occurrence of either failure should result in appropriate cockpit indication or be self-evident to the crew to enable the crew to take necessary actions such as discontinuing a take-off, going to a controllable flight envelope en-route, diverting to a suitable airport, or reconfiguring the system in order to recover single failure tolerance, etc. And

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 $1x10^{-3}$~~/fh~~ or less.

...

AMC - SUBPART F - EQUIPMENT

AMC 25.1309

System Design and Analysis

Table of Content

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 CERTIFICATED 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 RISK 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). ~~FAR~~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).~~

...

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.

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.

5. *DEFINITIONS*.

...

~~f. *Complex.* A system is Complex when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods.~~

f. *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.

...

j. *Development Error*. A mistake in requirements determination, design or implementation.

~~j.~~k. *Error*. An omission or incorrect action by a crewmember or maintenance personnel, or a mistake in requirements, design, or implementation.

~~k.~~l. *Event*. An occurrence which has its origin distinct from the aeroplane, such as atmospheric conditions (e.g. gusts, temperature variations, icing and lightning strikes), runway conditions, conditions of communication, navigation, and surveillance services, bird-strike, cabin and baggage fires. The term is not intended to cover sabotage.

~~l.~~m. *Failure.* An occurrence, which affects the operation of a component, part, or element such that it can no longer function as intended, (this includes both loss of function and malfunction). Note: Errors may cause Failures, but are not considered to be Failures.

~~m.~~n. *Failure Condition*. A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.

o. *Independence*.

(1) A concept that minimises the likelihood of common mode errors and cascade failures between aircraft/system functions or items;

(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.

~~n.~~p. *Installation Appraisal*. This is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry-accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service.

q. *Item*. A hardware or software element having bounded and well-defined interfaces.

~~o.~~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.~~

~~p.~~s. *Qualitative.* Those analytical processes that assess system and aeroplane safety in an objective, non-numerical manner.

~~q.~~t. *Quantitative.* Those analytical processes that apply mathematical methods to assess system and aeroplane safety.

~~r.~~u. *Redundancy.* The presence of more than one independent means for accomplishing a given function or flight operation.

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.

~~s. *System*. A combination of components, parts, and elements, which are inter-connected to perform one or more functions.~~

w. *System*. A combination of interrelated items arranged to perform a specific function(s).

...

6. *BACKGROUND*.

...

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 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.

...

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,~~ 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 ~~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 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.

...

8. *SAFETY OBJECTIVE.*

...

c. The safety objectives associated with Catastrophic Failure Conditions, may 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) 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.

...

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 of the impacts of such equipment on safety 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)*.

...

(1) *General.*

...

(vii) The resulting effects on the airplane 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.

...

(4) *Acceptable Application of Development Assurance Methods*. Paragraph 9b(1)(iii) above requires that any analysis necessary to show compliance with CS 25.1309(b) must consider the possibility of ~~requirement, design, and implementation~~ 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 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 shown by the use of Development Assurance. The level of Development Assurance should be determined by the severity of the failure conditions ~~potential effects on the aeroplane in case of system malfunctions or loss of functions~~.

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.

Guidelines, which may be used for providing Development Assurance, are described for ~~aircraft~~ aeroplane and systems development in the ~~D~~document referenced in paragraph 3b(~~3~~2), and for software in the ~~D~~document~~s~~ referenced in paragraph~~s~~ 3a(3) ~~and 3b(2)~~. ~~(~~There is currently no agreed Development Assurance standard for airborne electronic hardware.~~) Because these documents were not developed simultaneously, there are differences in the guidelines and terminology that they contain. A significant difference is the guidance provided on the use of system architecture for determination of the appropriate development assurance level for hardware and software. EASA recognises that consideration of system architecture for this purpose is appropriate. If the criteria of Document referenced in paragraph 3b(3) are not satisfied by a particular development assurance process the development assurance levels may have to be increased using the guidance of Document referenced in paragraph 3b(2).~~

...

(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 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.

...

(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)

It may not be possible to completely eliminate latent failures due to practical limitations in the ability to detect every failure during flight. CS 25.1309(b)(4) therefore requires significant latent failures be minimised to the extent practical.

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.

The probability value 1/1000 is the product of the maximum time the failure is allowed to be present and its failure rate.

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 and associated cost, it may be found not in the public interest to rigidly apply the criterion. In such situations, safety is better served when the latent failure is serviced at a suitable maintenance facility, even though a longer inspection interval means the probability of the latent failure existing would exceed 1/1000.

The Agency does not expect a dedicated demonstration of compliance with CS 25.1309(b)(4). The minimisation 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.

(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 that cannot practically 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 practical, 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 latency or adding redundancy).

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 $1x10^{-6}$ 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 $1x10^{-5}$ per flight hour, then latency is limited to a maximum probability of $1x10^{-4}$.

Appendix 5 gives simplified examples explaining how the limit latency and residual risk analysis might be applied.

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, thereby mitigating the effects to an acceptable level. 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'. Compliance with this requirement is usually demonstrated by the analysis identified in paragraph 9b(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 by the inherent airplane responses. CS 25.1309(c) requires that crew alerting must be provided in accordance with CS 25.1322. ~~a warning indication must be provided if immediate corrective action is required.~~ Paragraph 25.1309(c) also requires that systems and controls, including indications and annunciations, must be designed to minimise crew errors which could create additional hazards, consistent with CS 25.1302.

...

(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 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. 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.

...

(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. Where this is not accomplished, see 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, what is feasible and practical can change with time and circumstances.

...

10. *IDENTIFICATION OF FAILURE CONDITIONS AND CONSIDERATIONS WHEN ASSESSING THEIR EFFECTS*.

...

b. *Identification of Failure Conditions Using a Functional Hazard Assessment.*

...

(4) Depending on the extent of functions to be examined and the relationship between functions and systems, different approaches to 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 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 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.

...

c. *Considerations When Assessing Failure Condition Effects*.

...

(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.

...

(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 7a 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. Where flight duration, flight phase, or diversion time can adversely affect the FHA outcome, they must be considered as intensifying factors. Other intensifying factors include conditions (not related to the failure, such as weather or adverse operational or environmental conditions), which reduce the ability of the 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 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. ~~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 only be considered if they are anticipated to occur together.

...

11. *ASSESSMENT OF FAILURE CONDITION PROBABILITIES AND ANALYSIS CONSIDERATIONS.*

...

a. *Assessment of Failure Condition Probabilities.*

...

(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~~.

...

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:

(i) the average flight duration and the average flight profile for the aeroplane type to be certified;

(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;

This should be based on the probability per flight, rather than per flight hour, for failure conditions that have a very short exposure window.

(v) the ~~average~~ maximum exposure time if the failure can persist for multiple flights.

...

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 shown 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 programs. 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.

(2) considering the importance of architectural design in limiting the impact and propagation of failures,

...

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 in combination with operational or environmental conditions leading 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). 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.

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 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. 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. The applicant should provide a means to ensure the AFM will contain all the expected crew actions.

b. *Maintenance Action*.

Credit may be taken for correct accomplishment of reasonable maintenance tasks, for both qualitative and quantitative assessments. The maintenance tasks needed to 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, see 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.~~

...

d. *Flight with Equipment or Functions known to be Inoperative*.

An applicant may elect to develop~~A~~ 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 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 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.

...

APPENDIX 1. *ASSESSMENT METHODS.*

...

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 acceptable. These analyses may also identify a combination of failures and effects that would otherwise not have been foreseen by FMEA or FTA.

...

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, such as 'the purpose of function P is to prevent failures in X from adversely affecting Y'. As the implementations of the functional requirements become 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.

...

APPENDIX 3. *CALCULATION OF THE AVERAGE PROBABILITY PER FLIGHT HOUR*.

...

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_{Flight}(Failure Condition) should be determined by structured methods (see Document referenced in paragraph 3b(4) 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 aircraft, reliability analysis may be used to determine component replacement times. ~~and~~ In either case, the failure rate should be based on all causes of failure (operational, environmental, etc.). Where 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 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.

Replacement times, necessary to mitigate the risk due to ageing and wear of those components whose failures could lead directly or in combination with one other failure to a catastrophic or hazardous failure conditions within the operational life of the aircraft, should be assessed through the same methodology as other scheduled maintenance tasks required to satisfy 25.1309 (e.g. AMC 25-19) and documented in the Airworthiness Limitation Section as appropriate.

(2) If the failure is only relevant during certain flight phases, the calculation should be based on the probability of failure during the relevant 'at risk' time for the 'Average Flight'.

...

APPENDIX 4. *ALLOWABLE PROBABILITIES*.

The following probabilities may be used for environmental conditions and operational factors not due to aeroplane failure causes in quantitative safety analyses:

Environmental Factors

Condition	Model or other Justification	Probability

Condition	Model or other Justification	Probability
Normal icing (trace, light, moderate icing)		1
Severe icing		No accepted standard data
Head wind >25 kts during take-off and landing	AC 120-28 CS-AWO	10^{-2} per flight
Tail wind >10 kts during take-off and landing	AC 120-28 CS-AWO	10^{-2} per flight
Cross wind >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 due to airplane failure causes		No accepted standard data
Fire in a cargo compartment not due to aeroplane failure causes		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 RISK ANALYSIS*.

The following example illustrates how the quantitative criteria of CS 25.1309(b)(5) are to be implemented. 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 system failure or in this case the failure condition of concern.

1) The list of cut sets should be produced by cut set order. This will group all dual order cut sets or failure combinations. The entire list of cut sets of the fault tree in Figure A5-1 is provided in Table A5-2.

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 1×10^{-3}.

3) Then group those dual order cut sets that contain the same latent primary event. For each group assume that 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 x 10^{-5}/FH.

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.

The results of the limit latency and residual risk analysis are provided in Table A5-2.

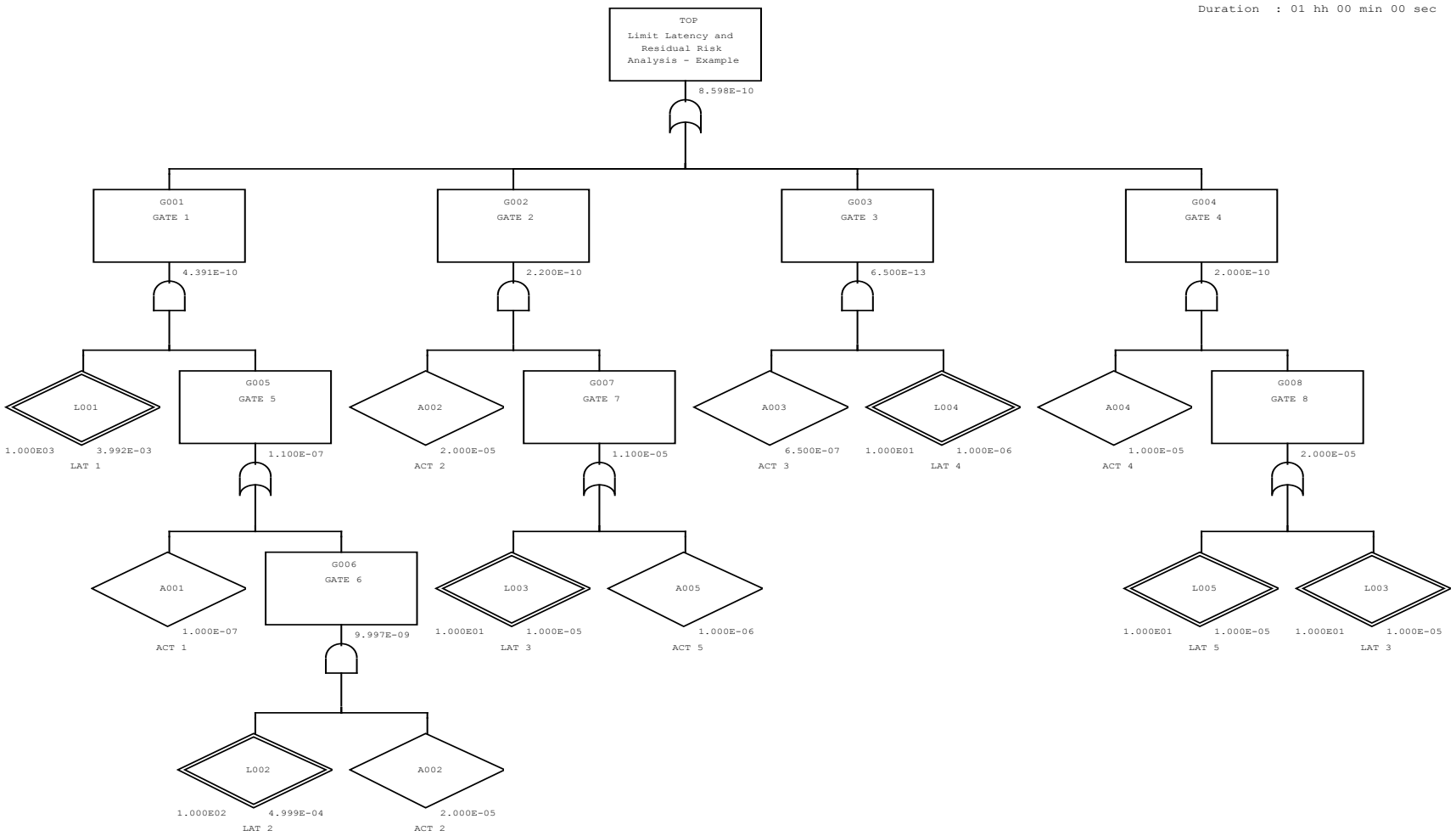

Figure A5-1: Example of CS 25.1309(b)(5) Fault Tree

#	Probability	Event Name	Event Description	Law	Exposure	Event Probability	CS 25.1309 (b)(5) Applicability/ Compliance
1	3.992E-10	A001	ACT 1	exponential 1.000E-07	1.0 h	1.000E-07	Not compliant with limit latency criterion since L001 probability is more frequent than 1.000E-03.
		L001	LAT 1	exponential 4.000E-06	1000.0 h	3.992E-03	
2	2.000E-10	A002	ACT 2	exponential 2.000E-05	1.0 h	2.000E-05	Not compliant with residual risk criterion since A002 probability is more frequent than 1.000E-05.
		L003	LAT 3	exponential 1.000E-06	10.0 h	1.000E-05	
3	1.000E-10	A004	ACT 4	exponential 1.000E-05	1.0 h	1.000E-05	Although A004 probability is equal to 1.000E-05, not compliant with residual risk criterion since the combined probability of A004 and A002 (1.000E-05 + 2.000E-05) is more frequent than 1.000E-05. *Note: Dual order minimal cut sets #2 and #3 are grouped due to L003.*
		L003	LAT 3	exponential 1.000E-06	10.0 h	1.000E-05	
4	1.000E-10	A004	ACT 4	exponential 1.000E-05	1.0 h	1.000E-05	Compliant with both limit latency and residual risk criteria.
		L005	LAT 5	exponential 1.000E-06	10.0 h	1.000E-05	
5	2.000E-11	A002	ACT 2	exponential 2.000E-05	1.0 h	2.000E-05	CS 25.1309(b)(5) does not apply since this dual order minimal cut set does not contain any basic event latent for more than one flight.
		A005	ACT 5	exponential 1.000E-06	1.0 h	1.000E-06	
6	6.500E-13	A003	ACT 3	exponential 6.500E-07	1.0 h	6.500E-07	Compliant with both limit latency and residual risk criteria.
		L004	LAT 4	exponential 1.000E-07	10.0 h	1.000E-06	
7	3.991E-11	A002	ACT 2	exponential 2.000E-05	1.0 h	2.000E-05	CS 25.1309(b)(5) does not apply since this minimal cut set is more than a dual failure combination.
		L001	LAT 1	exponential 4.000E-06	1000.0 h	3.992E-03	
		L002	LAT 2	exponential 5.000E-06	100.0 h	4.999E-04	
Flight time = considering 1hr of flight P[LAT i] ~ FR * T							

Table A5-2: Example of CS 25.1309(b)(5) Minimal Cut Set

4. Regulatory Impact Assessment (RIA)

4.1. Issues to be addressed

4.1.1. Specifc risk assessment

Different FAA ARAC Harmonisation Working Groups (HWGs), such as Flight Controls, Power Plant Installations, and Systems Design and Analysis, have produced various recommendations regarding the safety of critical aeroplane systems. Although the subject of specific risk analysis was addressed in those Working Groups, the recommendations were not mutually consistent, which is not surprising, since they had been developed independently by different groups of experts..

The Agency has already adopted part of these recommendations, but has not yet adopted the ones coming from the Flight Controls Harmonisation Working Group (FCHWG) and the Phase 2 recommendations from the Systems Design and Analysis HWG.

This could result in non-standardised system safety assessments across various critical airborne systems. This could also cause conflicting interpretations for conducting system safety assessments in future certification programmes, specifically taking into account the trend for highly integrated systems on board large aeroplanes.

After reviewing the existing regulations and the recommendations from various harmonisation Working Groups, the Agency, together with the FAA, indeed identified the need to clarify and standardise safety assessment criteria across various system disciplines.

FAA therefore issued a Draft Tasking Statement in October 2005 entitled 'Airplane-Level Safety – Specific Risk Analysis' proposing to address the safety assessment criteria by establishing a new 'airplane-level safety analysis working group' (ASAWG). This Group was in particular charged to tackle the following four main issues:

- Definition of 'specific risk' to aid the correct understanding of the term;
- Review of the approaches to assessment and management of specific risks, both in rulemaking and in actual certification practice;
- Confirmation of the need for a possible amendment of the airworthiness Certification Specifications applicable to safety analysis at (large)-aeroplane level;
- Development of recommendations for rulemaking containing also the rationale and safety benefits for each proposed change, and a standardised approach for applying specific risk.

The absence of harmonised safety assessment criteria across the various domains and the non-uniform interpretation of some rules in CS-25 of course lead to more hours spent during the certification processes, by both the Agency and the applicants for TC, changes to TC or STC.

In 10 years the Agency has issued about 280 TCs to aircraft, of which about 220 TCs to aeroplanes and among the latter about 50 to large aeroplanes (= 20% of 280). Therefore, on average the Agency has issued 5 TCs to large aeroplanes per year. The additional hours of labour required to compensate the regulatory shortcomings mentioned above can be estimated in 100 h per project for the Agency and 200 h for the applicant. This means about 300 hours 'wasted' per project x 5 projects = 1 500 hours per year.

Furthermore, in about 10 years of its existence, the Agency has issued about 5 000 Supplemental Type Certificates (STCs), i.e. about 500 STCs per year. More than 20 % are related to large aeroplanes, but not all of them require system safety analysis. In summary, it is estimated that about 10 % of these 500 STC projects per year required system safety analysis as per 25.1309 = 50 STC projects/year of interest in this RIA.

For each STC project, it is estimated that the 'wasted' hours could have been in total 100 encompassing both the Agency and the applicant. This means 5 000 hours per year.

In total (for TCs and STCs) this represent a 'waste' of around 6 500 working hours per year.

The labour cost is estimated starting from the 55 €/hour for aviation engineers, based on the salary figures of ERI Economic Research Institute for France, Germany, Italy, Spain and the United Kingdom (these five countries together account for 83.5 % of all employment in the manufacture of aircraft and spacecraft sector in EASA countries) in 2007. Estimates for ERI salary are derived from employer information, national statistics offices and employee-provided data. These value of 55 €/hour has been increased by 3 % per year until 2012 and then further increased to take into account that the cost of labour in the Agency is above industry average.

In conclusion, a labour cost of 100 €/hour is estimated, leading to a diseconomy (100 x 6 500 hours) of about 650 k€/year due to the mentioned regulatory shortcomings.

Accordingly this NPA tackles the issue of 'specific risks' and their harmonised assessment and mitigation, across different technical disciplines, to avoid non uniform safety across various systems, but also disproportionate burden for both Agency and applicants during certification projects.

4.1.2. Safety risk assessment

Under the current rules, the following safety issues may emerge:

- Non-uniform safety assessment of the 'specific risk' across various applicants, or even across various disciplines in the same certification project;
- concerns regarding the adequacy of current regulations in ensuring that compliance with 25.1309 requirements encompass the analysis of common mode and single points of failure from development errors in hardware and/or software;
- concerns that safety analyses carried out to demonstrate compliance with CS 25.1309 may not adequately address failure modes arising during the aircraft's operational life.

No evidence is however available to state the above concerns have ever led to catastrophic accidents.

4.1.3. Who is affected?

The sectors of the civil aviation community concerned by this NPA are aircraft manufacturers, equipment manufacturers, aircraft operators and competent authorities, including the Agency.

In particular, a significant impact is expected on Aircraft and Equipment Manufacturers, since certification activities relating to compliance with FAR/CS 25.1309 will need to be expanded to address specific risk issues in a deeper way.

Operators may be affected by increased maintenance.

Finally, there will also be an impact on competent authorities in relation to proof of compliance.

4.1.4. How could the issue/problem evolve?

As stated in 4.1.2, there is no evidence that the regulatory shortcomings mentioned above have led to non-tolerable safety risks during the initial airworthiness processes.

However, most experts concur that regulatory guidance for safety assessment, in particular for complex systems installed on large aeroplanes, could still be improved, at least in terms of clarity and unambiguity. If nothing were done, the risk coud increase due to:

- Ever growing complexity and interdependence of aircraft systems;
- Limitation of public resources which imposes not to waste time of staff inside regulatory authorities;
- Commercial pressures on industry, which also require to focus resources in the optimum way, to avoid wasting resources on inconsti=encies and so having less time to tackle safety issues.

4.2. Objectives

The overall objectives of the EASA system are defined in Article 2 of the Basic Regulation. This proposal will contribute to the achievement of the overall objectives by addressing the issues outlined in Chapter 2 of this NPA.

The specific objectives of this proposal are to:

- Define a standardised criterion for conducting aeroplane-level safety assessment of specific risks that encompasses all critical aeroplane systems on large aeroplanes (i.e. in particular update AMC to CS 25.1309), based on the results of the ARAC ASAWG;
- in addition, amend AMC 25.1309 to take into account of the latest updates of industry documents, such as ED79A/ARP4754A.
- Update CS 25.671 on safety assessment of flight control systems, based on the results of the ARAC FCHWG.

4.3. Policy options

Four options have been identified:

No.	Identification	Description
0	**Do nothing**	Do not amend CS-25 and associated AMC's to address recommendations from ARAC FCHWG and ASAWG reports.
1	**Amend CS-25**	Amend CS-25 and associated AMC's to address recommendations from ARAC FCHWG and ASAWG reports, with the objective to harmonise the specific risk consideration within the systems.
2	**Publish AMC 20-1309**	Delete AMC XX.1309 from all aircraft CSs and replace them by a single AMC 20-1309 to make the specific risk consideration applicable to any aircraft and not only to large aeroplanes.
3	**Publish generic AMC**	Issue generic rules for risk assessment in the total aviation system (recital 1 of Regulation 1109/2009) applicable to any aviation domain (e.g. ATM).

4.4. Methodology and data (only for a full RIA)

4.4.1. Applied methodology

The identified options are comparatively assessed using the Multi-Criteria Analysis (MCA), which allows to translate any assessment (qualitative or quantitative but not in the same units of measurement) into a non-dimensional numerical weighted scores.

These options are compared in terms of safety, environmental, social and economic impacts, as well as proportionality and harmonisation.

All identified impacts are qualitatively assessed (RIA light) and expressed as a score, which is a numerical single digit:

Scale for assessment of impacts	Score
Highly positive (High)	+5
Significantly positive (Medium)	+3
Slightly positive (Low)	+1
Neutral	0
Slightly negative (Low)	-1
Significantly negative (Medium)	-3
Highly negative (High)	-5

Safety scores, since safety is the primary objective of the Agency as per Article 2 of the Basic Regulation, are assigned a weight of 3. Environmental scores, based on the same article, have a weight of 2. Other scores' weight is 1.

Finally, all these scores are algebraically summed.

Differences in the order of magnitude of these final scores support the decision on the option to be preferred.

4.5. Analysis of impacts

4.5.1. Safety impact

The option 'do nothing', is considered neutral in terms of safety (= no change in respect of the current situation), since there is no evidence that it is unsafe.

However, the concerns that safety analyses carried out to demonstrate compliance with CS 25.1309 may not adequately address failure modes arising during the aircraft's operational life could be mitigated by Options 1, 2 or 3.

If regulatory action is taken by the Agency, then it is evident that improving the quality of the certification processes would contribute to further improvement of the safety levels.

The four Options can, hence, be compared from the safety perspective in the table below:

Options	**0**	**1**	**2**	**3**
	Do nothing	**Amend CS-25**	**AMC 20.1309**	**Generic AMC**
Assessment	Safety will remain at the current level	Quality of certification processes for large aeroplanes improved	Quality of certification processes for all aircraft improved, although aircraft other than large aeroplanes are usually not fitted with so many interconnected complex systems	As in Option 2, it might take several years to agree on rules, since the safety assessment culture in ATL is slightly different, while the concept of safety assessment is not yet spread across the aerodrome community. This means that for a number of years unsatisfactory rules for large aeroplanes would apply.
Score (un-weighted)	0	3	5	-1
Weight	Multiply the un-weighted score by: 3			
Score (weighted)	**0**	**9**	**15**	**-3**

4.5.2. Environmental impact

All the four identified Options are neutral from the environmental perspective.

4.5.3. Social impact

All the four identified Options are neutral from the social perspective.

4.5.4. Economic impact

The four Options can be compared from the economic perspective in the table below:

Options	**0**	**1**	**2**	**3**
	Do nothing	**Amend CS-25**	**AMC 20.1309**	**Generic AMC**
Assessment	650 k€ per year of burden in the certification processes for large aeroplanes remain.	Cost-efficiency of regulatory processes improved for both the Agency and the applicants for design approvals related top large aeroplanes.	Beneficial for design approvals of large aeroplanes (as in Option 1), but imposing additional work (and hence cost) on applicants for design approvals for other categories of aircraft.	Not worse than Option 2, since ANS providers and aerodrome operators will anyway have to carry out respective safety assessments.
Score (unweighted)	-1	3	-5	-5
Weight	Multiply the unweighted score by: 1			
Score (weighted)	**-1**	**3**	**-5**	**-5**

4.5.5. General aviation and proportionality issues

The four Options can be compared from the proportionality perspective in the table below:

Options	**0**	**1**	**2**	**3**
	Do nothing	**Amend CS-25**	**AMC 20.1309**	**Generic AMC**
Assessment	Neutral. Situation remains unchanged.	Uniform criteria across various disciplines for large aeroplanes. Applicants for other aircraft categories not affected. Amendments targeted on products having a high number of complex interconnected systems	Manufacturers of aircraft other than large aeroplanes significantly and possibly disproportionately affected. These manufacturers are normally companies smaller than manufacturers of large aeroplanes	As in Option 2.
Score (un-weighted)	0	3	-5	-5
Weight	Multiply the unweighted score by: 1			
Score (weighted)	**0**	**3**	**-5**	**-5**

4.5.6. Impact on 'Better Regulation' and harmonisation

'Do nothing' would lead to loss of harmonisation with FAA, since that authority, based on the work of the same expert groups mentioned above, is also drafting a Notice of Proposed Rulemaking (NPRM) to amend FAR-25 in the same direction as proposed in this NPA.

The four Options can be compared from the proportionality perspective in the table below:

Options	**0**	**1**	**2**	**3**
	Do nothing	**Amend CS-25**	**AMC 20.1309**	**Generic AMC**
Assessment	Loss of harmonisation with other regulators, including FAA, which will cause problems to manufacturers of large aeroplanes, seeking validation of respective TCs	Maximum possible harmonisation with FAA. More consistent cross-discipline applroach	More complex rules for EU manufacturers of simpler aircraft, compared with world-wide competition	Scope of the rules much beyond the recommendations of the ARAC WGs
Score (unweighted)	-5	5	-5	-3
Weight	Multiply the unweighted score by: 1			
Score (weighted)	**-5**	**5**	**-5**	**-3**

4.6. Comparison and conclusion

4.6.1. Comparison of options

The above considerations can be presented also using the Multi-Criteria Analysis (MCA) methodology, according to which the 'weighted' scores assigned above are algebraically summed:

Options	0	1	2	3
	Do nothing	**Amend CS-25**	**AMC 20.1309**	**Generic AMC**
	Weighted score			
Safety	0	9	15	-3
Environment	0	0	0	0
Social impact	0	0	0	0
Economic impact	-1	3	-5	-5
Proportionality	0	3	-5	-5
Regulatory harmonisation	-5	5	-5	-3
TOTAL	**-6**	**20**	**0**	**-15**

Option 0 ('do nothing') is globally negative and, although neutral in terms of safety (no pressing safety issue has been identified), is highly negative in terms of regulatory harmonisation between America and Europe, which would cause problems to manufacturers of large aeroplanes.

Option 1 (i.e. amend CS-25 Book 1 and 2 in a similar timeframe and harmonised with FAA) is the only option significantly positive, including in terms of safety, economic impact, proportionality and regulatory harmonisation. It is neutral for the social and environmental impacts.

Option 2 (i.e. impose the same rigour of safety assessment to ma nufacturers of any aircraft, beyond large aeroplanes) is the most positive in safety terms, but extremely negative from for economy, proportionality and harmonisation.

Option 3 (i.e. generic AMC covering not only initial airworthiness, but safety assessments also in otger aviation domains, like e.g. ATM and airports) is in summary the most negative. It is negative also for safety impact.

Therefore, Option 1 (i.e. amend CS-25) is the preferred one.

5. References

5.1. Affected CS, AMC and GM

Decision No. 2003/002/RM of the Executive Director of the European Aviation Safety Agency of 17 October 2003 on Certification Specifications, including Acceptable Means of Compliance, for Large Aeroplanes ('CS-25'), as last amended (Amendment 14) by Executive Director Decision 2013/033/R of 19 December 2013.