CS-25 AMENDMENT 24 — CHANGE INFORMATION

EASA publishes amendments to certification specifications as consolidated documents. These documents are used for establishing the certification basis for applications made after the date of entry into force of the amendment.

Consequently, except for a note '[Amdt No: 25/24]' under the amended paragraph, the consolidated text of CS-25 does not allow readers to see the detailed changes introduced by the new amendment. To allow readers to see these detailed changes, this document has been created. The same format as for publication of Notices of Proposed Amendments (NPAs) has been used to show the changes:

(a) deleted text is ~~struck through~~;

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

(c) an ellipsis '[…]' indicates that the remaining text is unchanged.

BOOK 1

SUBPART D — DESIGN AND CONSTRUCTION

CS 25.629 Aeroelastic stability requirements

(...)

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

(...)

(9) The following flight control system failure combinations where aeroelastic stability relies on flight control system stiffness and/or damping:

(i) any dual hydraulic system failure;

(ii) any dual electrical system failure; and

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

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

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

(...)

CS 25.671 General

(See AMC 25.671)

(a) Each ~~control and~~ flight control system must operate with the ease, smoothness, and positiveness appropriate to its function. In addition, the flight control system shall be designed to continue to operate, respond appropriately to commands, and must not hinder aeroplane recovery, when the aeroplane is in any attitude or experiencing any flight dynamics parameter that could occur due to operating or environmental conditions. ~~(See AMC 25.671 (a).)~~

(b) Each element of each flight control system must be designed~~, or distinctively and permanently marked,~~ to minimise the probability of incorrect assembly that could result in the failure or malfunctioning of the system. Distinctive and permanent marking may be used where design means are impractical, taking into consideration the potential consequence of incorrect assembly. ~~(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 jams~~ming~~ 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~~. In addition, it must be shown that the pilot can readily counteract the effects of any probable failure.

(1) Any single failure, excluding failures of the type defined in CS 25.671(c)(3);

~~Any single failure not shown to be extremely improbable, excluding jamming, (for example, disconnection or failure of mechanical elements, or structural failure of hydraulic components, such as actuators, control spool housing, and valves). (See AMC 25.671(c)(1).)~~

(2) Any combination of failures not shown to be extremely improbable, excluding failures of the type defined in CS 25.671(c)(3); and

~~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 jam must be assumed to occur anywhere within the normal flight envelope and during any flight phase from take-off to landing; and

In the presence of a jam considered under this sub-paragraph, any additional failure conditions that could prevent continued safe flight and landing shall have a combined probability of 1/1 000 or less.

~~Any jam in a control position normally encountered during take-off, climb, cruise, normal turns, descent and landing unless the jam is shown to be extremely improbable, or can be alleviated. A runaway of a flight control to an adverse position and jam must be accounted for if such runaway and subsequent jamming is not extremely improbable.~~

(d) The aeroplane must be designed so that ~~it is controllable~~, if all engines fail at any time of the flight:

(1) it is controllable in flight;

(2) an approach can be made;

(3) a flare to a landing, and a flare to a ditching can be achieved; and

(4) during the ground phase, 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 aeroplane must be designed to indicate to the flight crew whenever the primary control means is near the limit of control authority.

(f) If the flight control system has multiple modes of operation, appropriate flight crew alerting must be provided 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

~~(See AMC 25.672)~~

(...)

(c) It must be shown that after any single failure of the stability augmentation system or any other automatic or power-operated system: –

(1) The aeroplane is safely controllable when the failure or malfunction occurs at any speed or altitude within the approved operating limitations that is critical for the type of failure being considered. ~~(See AMC 25.672 (c) (1).)~~

(...)

CS 25.705 Runway overrun awareness and alerting systems

(See AMC 25.705)

A runway overrun awareness and alerting system (ROAAS) must be installed. The ROAAS shall reduce the risk of a longitudinal runway excursion during landing by providing alert, in flight and on ground, to the flight crew when the aeroplane is at risk of not being able to stop within the available distance to the end of the runway.

(a) During approach (from a given height above the selected runway) and landing, the ROAAS shall perform real-time energy-based calculations of the predicted landing stopping point, compare that point with the location of the end of the runway, and provide the flight crew with:

(1) in-flight, timely, and unambiguous predictive alert(s) of a runway overrun risk, and

(2) on-ground, timely, and unambiguous predictive alert(s) of a runway overrun risk. At the option of the applicant, the ROAAS may also provide an automated means of deceleration control that prevents or minimises runway overrun during landing.

(b) The ROAAS shall at least accommodate dry and wet runway conditions for normal landing configurations.

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).

(See AMC 25.933(a)(1))

(...)

SUBPART F — EQUIPMENT

CS 25.1309 Equipment, systems and installations

(See AMC 25.1309)

The requirements of this paragraph, except as identified below, are applicable, in addition to specific design requirements of CS-25, to any equipment or system as installed in the aeroplane. Although this paragraph does not apply to the performance and flight characteristic requirements of Subpart B and the structural requirements of Subparts C and D, it does apply to any system on which compliance with any of those requirements is dependent. ~~Certain single failures or jams~~ Jams of flight control surfaces or pilot controls covered by ~~CS 25.671(c)(1) and~~ CS 25.671(c)(3) are excepted from the requirements of CS 25.1309(b)(1)(ii). Certain single failures covered by CS 25.735(b) are excepted from the requirements of CS 25.1309(b). The failure effects covered by CS 25.810(a)(1)(v) and CS 25.812 are excepted from the requirements of CS 25.1309(b). The requirements of CS 25.1309(b) apply to powerplant installations as specified in CS 25.901(c).

(...)

(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -

(1) Any catastrophic failure condition

(i) is extremely improbable; and

(ii) does not result from a single failure; and

(2) Any hazardous failure condition is extremely remote; and

(3) Any major failure condition is remote~~.~~; and

(4) Any significant latent failure is eliminated as far as practical, or, if not practical to eliminate, the latency of the significant latent failure is minimised; and

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

(i) it is impractical to provide additional redundancy; and

(ii) given that a single latent failure has occurred on a given flight, the failure condition is remote; and

(iii) the sum of the probabilities of the latent failures which are combined with each evident failure does not exceed 1/1 000.

(c) Information concerning unsafe system operating conditions must be provided to the flight crew to enable them to take appropriate corrective action in a timely manner. ~~A warning indication must be provided if immediate corrective action is required.~~ Installed ~~S~~systems and equipment for use by the flight crew, ~~controls,~~ including flight deck controls and information ~~indications and annunciations~~, must be designed to minimise flight crew errors~~,~~ which could create additional hazards.

(...)

BOOK 2

AMC — SUBPART D

AMC 25.629

Aeroelastic stability requirements

(…)

3.2. *Failures, Malfunctions~~,~~ and Adverse Conditions*. The following conditions should be investigated for aeroelastic instability within the fail-safe envelope defined in paragraph 2.3. above.

(…)

3.2.9. The following flight control system failure combinations where aeroelastic stability relies on flight control system stiffness and/or damping:

(i) any dual hydraulic system failure;

(ii) any dual electrical system failure; and

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

3.2.10 Any damage, failure or malfunction, considered under CS 25.631, CS 25.671, CS 25.672, and CS 25.1309. This includes the condition of two or more engines stopped or wind milling for the design range of fuel and payload combinations, including zero fuel.

3.2.~~10~~11. Any other combination of failures, malfunctions, or adverse conditions not shown to be extremely improbable.

(…)

4.3. Where aeroelastic stability relies on flight 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 disconnection 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.

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). However, ~~certain~~ some combinations of failures, such as dual ~~electric~~ electrical system or dual hydraulic system failures, or any single failure in combination with any probable ~~electric~~ electrical or hydraulic system failure ~~(CS 25.671)~~, are ~~not~~ normally not ~~considered~~ demonstrated as being 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*

This AMC provides an acceptable means, but not the only means, to demonstrate compliance with the control system requirements of CS 25.671.

2. *RELATED DOCUMENTS*

a. Advisory Circulars, Acceptable Means of Compliance.

(1) FAA Advisory Circular (AC) 25-7D, dated 4 May 2018, Flight Test Guide for Certification of Transport Category Airplanes.

(2) AMC 25.1309 System Design and Analysis.

b. Standards.

(1) EUROCAE document ED-79A, Guidelines for Development of Civil Aircraft and Systems, issued in December 2010, or the equivalent SAE Aerospace Recommended Practice (ARP) 4754A.

(2) SAE Aerospace Recommended Practice (ARP) 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, issued in December 1996.

3. *APPLICABILITY OF CS 25.671*

CS 25.671 applies to all flight control system installations (including primary, secondary, trim, lift, drag, feel, and stability augmentation systems (refer to CS 25.672)) regardless of implementation technique (manual, powered, fly-by-wire, or other means).

While CS 25.671 applies to flight control systems, CS 25.671(d) does apply to all control systems required to provide control, including deceleration, for the phases specified.

4. *DEFINITIONS*

The following definitions apply to CS 25.671 and this AMC. Unless otherwise stated, they should not be assumed to apply to the same or similar terms used in other rules or AMC.

a. *At-Risk Time.* The period of time during which an item must fail to cause the failure effect in question. This is usually associated with the final fault in a fault sequence leading to a specific failure condition. See also SAE ARP4761.

b. *Catastrophic Failure Condition.* Refer to AMC 25.1309 (Paragraph 7 FAILURE CONDITION CLASSIFICATIONS AND PROBABILITY TERMS).

c. *Continued Safe Flight and Landing.* The capability for continued controlled flight and landing at an aerodrome without requiring exceptional piloting skill or strength.

d. *Landing.* The phase following final approach and starting with the landing flare. It includes the ground phase on the runway and ends when the aeroplane comes to a complete stop on the runway.

e. *Latent Failure.* Refer to AMC 25.1309 (Paragraph 5 DEFINITIONS).

f. *Error.* Refer to AMC 25.1309 (Paragraph 5 DEFINITIONS).

g. *Event.* Refer to AMC 25.1309 (Paragraph 5 DEFINITIONS).

h. *Exposure Time.* The period of time between the time when an item was last known to be operating properly and the time when it will be known to be operating properly again. See also SAE ARP4761.

i. *Extremely Improbable.* Refer to AMC 25.1309 (Paragraph 7 FAILURE CONDITION CLASSIFICATIONS AND PROBABILITY TERMS).

j. *Failure.* Refer to AMC 25.1309 (Paragraph 5 DEFINITIONS).

The following types of failures should be considered when demonstrating compliance with CS 25.671(c). Since the type of failure and the effect of the failure depend on the system architecture, this list is not exhaustive, but serves as a general guideline.

(1) *Jam.* Refer to the definition provided below.

(2) *Loss of Control of Surface.* A failure that results in a surface not responding to commands. Failure sources can include mechanical disconnection, control cable disconnection, actuator disconnection, loss of hydraulic power, or loss of control commands due to computers, data path or actuator electronics failures. In these conditions, the position of the surface(s) or controls can be determined by analysing the system architecture and aeroplane aerodynamic characteristics; common positions include surface-centred (0°) or zero hinge-moment position (surface float).

(3) *Oscillatory Failure.* A failure that results in undue surface oscillation. Failure sources include control loop destabilisation, oscillatory sensor failure, oscillatory computer or actuator electronics failure. The duration of the oscillation, its frequency, and amplitude depend on the control loop, monitors, limiters, and other system features.

(4) *Restricted Control.* A failure that results in the achievable surface deflection being limited. Failure sources include foreign object interference, malfunction of a travel limiter, and malfunction of an envelope protection. This type of failure is considered under CS 25.671(c)(1) and CS 25.671(c)(2), as the system/surface can still be operated.

(5) *Runaway or Hardover.* A failure that results in uncommanded control surface movement. Failure sources include servo valve jams, computer or actuator electronics malfunctioning. The speed of the runaway, the duration of the runaway (permanent or transient), and the resulting surface position (full or partial deflection) depend on the available monitoring, limiters, and other system features. This type of failure is addressed under CS 25.671(c)(1) and (c)(2).

Runaways that are caused by external events, such as loose or foreign objects, control system icing, or any other environmental or external source are addressed in CS 25.671(c)(2).

(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 type of failure is considered under CS 25.671(c)(1) and CS 25.671(c)(2), as the system/surface can still be operated. In some architectures, higher friction may result in reduced centring of the controls.

k. *Failure Conditions.* As used in CS 25.671(c), this term refers to the sum of all failures and failure combinations contributing to a hazard, apart from the single failure (flight control system jam) being considered.

l. *Flight Control System.* Flight control system refers to the following: primary flight controls from the pilot's controllers to the primary control surfaces, trim systems from the pilot's trim input devices to the trim surfaces (including stabiliser trim), speed brake/spoiler systems from the pilot's control lever to the brake/spoiler panels or other drag/lift-dumping devices, high-lift systems from the pilot's controls to the high-lift surfaces, feel systems, and stability augmentation systems. Supporting systems

(i.e. hydraulic systems, electrical power systems, avionics, etc.) should also be included if failures in these systems have an impact on the function of the flight control system.

Examples of elements to be evaluated under CS 25.671 include, but are not limited to:

— linkages,

— hinges,

— cables,

— pulleys,

— quadrants,

— valves,

— actuators (including actuator components),

— flap/slat tracks (including track rollers and movable tracks),

— bearings, axles and pins,

— control surfaces (jam and runaway only),

— attachment fittings.

m. *In-flight* is the time period from the time when the aeroplane is at 10 m (35 ft) above aerodrome level (AAL) following a take-off, up to the time when the aeroplane reaches 15 m (50 ft) AAL prior to landing, including climb, cruise, normal turns, descent, and approach.

n. *Jam.* A failure or event that results in either a control surface, a pilot control, or a component being fixed in one position.

(i) Control surfaces and pilot controls fixed in one position due to a physical interference are 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 disconnection that results in a jam by creating interference. Normally encountered positions are defined in paragraph 7.b of this AMC.

(ii) All other failures or events that result in either a control surface, a pilot control, or a component being fixed in one position are addressed under CS 25.671(c)(1) and 25.671(c)(2) as appropriate. Depending on the system architecture and the location of the failure or the event, some failures or events that cause a jam may not always result in a fixed surface or pilot control; for example, a jammed valve could result in a surface runaway.

o. *Landing* is the time period from the time when the aeroplane is at 15 m (50 ft) AAL prior to landing, up to the complete stop of the aeroplane on the runway.

p. *Probability versus Failure Rate.* Failure rate is typically expressed in terms of average probability of occurrence per flight hour. In cases where the failure condition is associated with a certain flight condition that occurs only once per flight, the failure rate is typically expressed as average probability of occurrence per flight (or per take-off, or per landing). Failure rates are usually the 'root' numbers used in a fault tree analysis prior to factoring in latency periods, exposure time, or at-risk time. Probability is non-dimensional and expresses the likelihood of encountering or being in a failed state. Probability is obtained by multiplying a failure rate by the appropriate exposure time.

p. *Take-off* is the time period from the brake release up to the time when the aeroplane reaches 10 m (35 ft) AAL.

5. *EVALUATION OF FLIGHT CONTROL SYSTEM OPERATION — CS 25.671(a)*

a. *General.*

Flight control systems should be designed such that when a movement to one position has been selected, a different position can be selected without waiting for the completion of the initially selected movement, and the system should arrive at the finally selected position without further attention. The movements that follow and the time taken by the system to allow the required sequence of selection should not adversely affect the controllability of the aeroplane.

b. *Abnormal Attitude.*

Compliance should be demonstrated by evaluation of the closed-loop flight control system. This evaluation is intended to ensure that there are no features or unique characteristics (including numerical singularities) which would restrict the pilot's ability to recover from any attitude.

Open-loop flight control systems should also be evaluated, if applicable.

For aeroplanes that are equipped with a flight control envelope protection, the attitudes of the aeroplane to be considered should include cases outside the protected envelope.

c. *Parameters to be considered*

The following relevant flight dynamic parameters should be considered by the applicant (non-exhaustive list):

– Pitch, Roll or Yaw rate

– Vertical load factor

– Airspeed

– Angle of attack

d. *Operating and Environmental Conditions*

The parameters in paragraph 5.c. above should be considered within the limit flight envelope, which is the flight envelope that is associated with the aeroplane design limits or the flight control system protection limits.

6. *EVALUATION OF FLIGHT CONTROL SYSTEM ASSEMBLY — CS 25.671(b)*

The intent of CS 25.671(b) is to minimise the risk by design that the elements of the flight control system are incorrectly assembled, such that that this leads to significant safety effects. The intent is not to address configuration control (refer to CS 25.1301(a)(2)).

The applicant should take adequate precautions during the design process and provide adequate procedures in the instructions for continued airworthiness to minimise the risk of incorrect assembly (i.e. installation, connection, or adjustment) of elements of the flight control system during production and maintenance. The following steps should be used:

(1) assess the potential effects of potential incorrect assemblies of flight control systems elements and determine a classification of the severity of the associated failure conditions;

(2) when a failure condition is classified as catastrophic, hazardous, or major, EASA normally only accepts physical prevention means in the design of the elements to prevent an incorrect assembly. If, exceptionally, the applicant considers that providing such design prevention means is impractical, this should be presented to EASA. If agreed by EASA, the applicant may then use a distinctive and permanent marking of the involved elements.

(3) failure conditions that are classified either as minor or with no safety effect are not considered to have a significant safety effect.

Examples of significant safety effects:

(1) an out-of-phase action;

(2) reversal in the sense of the control;

(3) interconnection of the controls between two systems where this is not intended;

(4) loss of function.

7. EVALUATION OF FLIGHT CONTROL SYSTEM FAILURES — CS 25.671(c)

Development errors (e.g. mistakes in requirements, design, or implementation) should be considered when demonstrating compliance with CS 25.671(c). However, the guidance provided in this paragraph is not intended to address the means of compliance related to development errors. Development errors are managed through development assurance processes and system architecture. Some guidelines are provided in AMC 25.1309.

CS 25.671(c) requires that the aeroplane be shown by analysis, test, or both, to be capable of continued safe flight and landing following failures in the flight control system within the normal flight envelope.

CS 25.671(c)(1) requires the evaluation of any single failure, excluding the types of jams addressed in subparagraph CS 25.671(c)(3). CS 25.671(c)(1) requires to consider any single failure, suggesting that an alternative means of controlling the aeroplane or an alternative load path is provided in the case of a single failure. All single failures must be considered, even if they are 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).

Some combinations of failures, such as dual electrical system or dual hydraulic system failures, or any single failure in combination with any probable electrical or hydraulic system failure, are normally not demonstrated as being extremely improbable.

CS 25.671(c)(3) requires the evaluation of any failure or event that results in a jam of a flight control surface or pilot control. This subparagraph addresses failure modes that would result in the surface or pilot control being fixed in a position. It should be assumed that the fixed position is the position that is commanded at the time of the failure due to some physical interference. The position at the time of the jam should be at any control position normally encountered during take-off, climb, cruise, normal turn manoeuvres, descent, approach, and landing. In some architectures, component jams within the system may result in failure modes other than a fixed surface or pilot control; those types of jams (such as a jammed valve) are considered under subparagraphs CS 25.671(c)(1) and (c)(2). All single jams must be considered, even if they can be shown to be extremely improbable.

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.

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 which are not shown to be extremely improbable.

Some means to alleviate the runaway may be used to demonstrate compliance, such as by reconfiguring the control system, deactivating the system (or a failed portion of it), overriding the runaway by a movement of the flight controls in the normal sense, eliminating the consequences of a runaway to ensure continued safe flight and landing following a runaway. The consideration of a control runaway will be specific to each application and a general interpretation of an adverse position cannot be provided. Where applicable, the applicant is required to assess the resulting surface position after a runaway, if the failure condition is not extremely improbable or can occur due to a single failure.

It is acknowledged that determining a consistent and reasonable definition of normally encountered flight control positions can be difficult. Experience from in-service aeroplanes shows that the overall failure rate for a flight control surface jam is of an order of magnitude between 10^{-6} and 10^{-7} per flight hour. This failure rate may be used to justify a definition of 'normally encountered position' and is not intended to be used to support a probabilistic assessment. Considering this in-service aeroplane data, a reasonable definition of normally encountered positions represents the range of flight control surface deflections (from neutral to the largest deflection) expected to occur in 1 000 random operational flights, without considering other failures, for each of the flight phases addressed in this AMC.

One method of establishing acceptable flight control surface deflections is to use the performance-based criteria outlined in this AMC (see sub-paragraph 7.b. below) that were established to eliminate any differences between aeroplane types. The performance-based criteria prescribe environmental and operational manoeuvre conditions, and the resulting deflections may be considered as normally encountered positions for demonstrating compliance with CS 25.671(c)(3).

All approved aeroplane gross weights and centre-of-gravity locations should be considered. However, only critical combinations of gross weight and centre-of-gravity locations should be demonstrated.

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

When demonstrating compliance with the failure requirements of CS 25.671(c)(2), the following safety analysis/assessment should be considered.

A safety analysis/assessment according to AMC 25.1309 should be supplemented to demonstrate that the aeroplane is capable of continued safe flight and landing following any combination of failures not shown to be extremely improbable.

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

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

The following flight phases should be considered: 'take-off', 'in-flight' (climb, cruise, normal turn manoeuvres, descent, and approach), and 'landing' (refer to the definitions in paragraph 4. DEFINITIONS of this AMC).

CS 25.671(c)(3) requires that the aeroplane be capable of landing with a flight control or pilot control jam. The aeroplane should, therefore, be evaluated for jams in the landing configuration.

Only the aeroplane rigid body modes need to be considered when evaluating the aeroplane response to manoeuvres and continued safe flight and landing.

It should be assumed that, if the jam is detected prior to V_1, the take-off will be rejected.

Although 1 in 1 000 operational take-offs is expected to include crosswinds of 46 km/h (25 kt) or greater, the short exposure time associated with a flight control surface jam occurring between V_1 and V_{LOF} allows usage of a less conservative crosswind magnitude when determining normally encountered lateral and directional control positions. Given that lateral and directional flight controls are continuously used to maintain runway centre line in a crosswind take-off, and that flight control inputs greater than those necessary at V_1 occur at speeds below V_1, any jam in these flight control axes during a crosswind take-off is normally detected prior to V_1. Considering the flight control jam failure rate combined with the short exposure time between V_1 and V_{LOF}, a reasonable crosswind level for the determination of jammed lateral or directional flight control positions during take-off is 28 km/h (15 kt).

A similar reasoning applies for the approach and landing flight phases. It leads to consider that a reasonable crosswind level for the determination of jammed lateral or directional control positions during approach and landing is 28 km/h (15 kt).

The jam positions to be considered in demonstrating compliance should include any position up to the maximum position determined by the following manoeuvres. The manoeuvres and conditions described in this paragraph should only be used to determine the flight control surface and pilot control deflections to evaluate the continued safe flight and landing capability, and should not be used for the evaluation of flight test manoeuvres; see paragraph 7.e below.

(1) *Jammed Lateral Control Positions*

(i) Take-off: The lateral flight control position for wings level at V_1 in a steady crosswind of 28 km/h (15 kt) (at a height of 10 m (35 ft) above the take-off surface). Variations in wind speed from a 10-m (35-ft) height can be obtained using the following relationship:

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

where:

$V_{10metres}$ = wind speed in knots at 10 m (35 ft) above ground level (AGL)

V_{alt} = wind speed at desired altitude (kt)

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

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

(iii) Landing (including flare): The maximum lateral control position is the greater of:

(A) the peak lateral control position to maintain wings level in response to a steady crosswind of 28 km/h (15 kt), in manual or autopilot mode; or

(B) the peak lateral control position to maintain wings level in response to an atmospheric discrete lateral gust of 16 km/h (15 ft/s) from sea level to 6 096 m (20 000 ft).

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

(2) *Jammed Longitudinal Control Positions*

(i) Take-off: The following three longitudinal flight control positions should be considered:

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

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

(B) The longitudinal flight control position at V_1 based on the procedures recommended by the aeroplane manufacturer including the consideration for any runway condition for which the aeroplane is approved to operate.

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

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

(A) the longitudinal flight control position required to achieve steady state normal accelerations from 0.8 to 1.3 g at speeds from $1.23V_{SR1}$ to V_{MO}/M_{MO} or V_{FE}, as appropriate;

(B) the peak longitudinal flight control position commanded by the autopilot and/or stability augmentation system in response to atmospheric discrete vertical gust of 16 km/h (15 ft/s) from sea level to 6 096 m (20 000 ft).

(iii) Landing: Any longitudinal control position required, in manual or autopilot mode, for performing a flare and landing, using the procedures recommended by the aeroplane manufacturer.

(3) *Jammed Directional Control Positions*

(i) Take-off: The directional flight control position for take-off at V_1 in a steady crosswind of 28 km/h (15 kt) (at a height of 10 m (35 ft) above the take-off surface). Variations in wind speed from a height of 10 m (35 ft) can be obtained using the following relationship:

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

where:

$V_{10metres}$ = wind speed in knots at 10 m above ground level (AGL)

V_{alt} = wind speed at desired altitude

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

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

(A) the peak directional flight control position commanded by the autopilot and/or stability augmentation system in response to atmospheric discrete lateral gust of 16 km/h (15 ft/s) from sea level to 6 096 m (20 000 ft);

(B) maximum rudder angle required for lateral/directional trim from $1.23V_{SR1}$ to the maximum all-engines-operating airspeed in level flight with climb power, but not to exceed V_{MO}/M_{MO} or V_{FE} as appropriate. While more commonly a characteristic of propeller aeroplane, this addresses any lateral/directional asymmetry that can occur in flight with symmetric power; or

(C) for approach, the peak directional control position commanded by the pilot, autopilot and/or stability augmentation system in response to a steady crosswind of 28 km/h (15 kt).

(iii) Landing: The maximum directional control position is the greater of:

(A) the peak directional control position commanded by the pilot, autopilot and/or stability augmentation system in response to a steady crosswind of 28 km/h (15 kt); or

(B) the peak lateral control position to maintain wings level in response to an atmospheric discrete lateral gust of 16 km/h (15 ft/s) from sea level to 6 096 m (20 000 ft).

(4) *Control Tabs, Trim Tabs, and Trimming Stabilisers*

Any tabs installed on flight control surfaces are assumed jammed in the position that is 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 that are associated with the procedures recommended by the aeroplane manufacturer for take-off and that are normally used throughout the flight to trim the aeroplane from $1.23V_{SR1}$ 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 $1.23V_{SR1}$ to V_{MO}/M_{MO} or V_{FE}, as appropriate. Asymmetric extension and retraction of the speed brakes should be considered. Roll spoiler jam (asymmetric spoiler panel) is addressed in paragraph 7.b(1).

(6) *High-Lift Devices*

Leading edge and trailing edge high-lift devices are assumed to jam in any position for take-off, climb, cruise, approach, and landing. Skew of high-lift devices or asymmetric extension and retraction should be considered. CS 25.701 requires a mechanical interconnection (or equivalent means) between flaps or slats, unless the aeroplane has safe flight characteristics with the asymmetric flaps or slats positions.

(7) *Load Alleviation Systems*

(i) Gust Load Alleviation Systems: At any airspeed between $1.23V_{SR1}$ to V_{MO}/M_{MO} or V_{FE}, as appropriate, the flight control surfaces are assumed to jam in the maximum position commanded by the gust load alleviation system in response to an atmospheric discrete gust with the following reference velocities:

(A) 16 km/h (15 ft/s) equivalent airspeed (EAS) from sea level to 6 096 m (20 000 ft) (vertical gust);

(B) 16 km/h (15 ft/s) EAS from sea level to 6 096 m (20 000 ft) (lateral gust).

(ii) Manoeuvre Load Alleviation Systems: At any airspeed between $1.23V_{SR1}$ to V_{MO}/M_{MO} or V_{FE}, as appropriate, the flight control surfaces are assumed to jam in the maximum position commanded by the manoeuvre load alleviation system during a pull-up manoeuvre to 1.3 g or a push-over manoeuvre to 0.8 g.

c. *Considerations for jams just before landing — CS 25.671(c)(3)(i) and (ii)*

CS 25.671(c)(3)(ii) requires that failures (leading to a jam) must be assumed to occur anywhere within the normal flight envelope and during any flight phase from take-off to landing. This includes the flight phase just before landing and the landing itself. For the determination of the jam position per CS 25.671(c)(3)(i) and the assessment of continued safe flight and landing, guidance is provided in this AMC. However, there might be exceptional cases where it is not possible to demonstrate continued safe flight and landing. Even jam alleviation means (e.g., disconnection units) might not be efficient because of the necessary time for the transfer of pilot controls.

For these exceptional cases, the compliance to CS 25.671(c)(3)(ii) may be shown by demonstrating that the occurrence of a jam just before landing is extremely improbable.

Therefore, the overall compliance to CS 25.671(c)(3)(ii) for the flight phase just before landing may be performed as follows:

(1) Demonstrate continued safe flight and landing after a jam has occurred just before landing.

Note: The assessment of continued safe flight and landing in paragraph 7.e. below also applies to jams occurring just before landing;

(2) If continued safe flight and landing cannot be demonstrated, perform a qualitative assessment of the design, relative to jam prevention features and jam alleviation means, to show that all practical precautions have been taken; or

(3) As a last resort, after agreement by EASA, use data from in-service aeroplanes to support an extremely improbable argument (without use of at-risk time).

The typical means of jam prevention/alleviation include low-friction materials, dual-rotation bearings, clearances, jack catchers, priority switch on sidestick.

d. *Jam Combinations Failures — CS 25.671(c)(3)*

In addition to the demonstration of jams at 'normally encountered position', compliance with CS 25.671(c)(3) should include an analysis that shows that a minimum level of safety exists when a jam occurs. This additional analysis must show that in the presence of a jam considered under CS 25.671(c)(3), the failure conditions that could prevent continued safe flight and landing have a combined probability of 1/1 000 or less.

As a minimum, this analysis should include elements such as a jam breakout or override, disconnection means, alternate flight surface control, alternate electrical or hydraulic sources, or alternate cable paths. This analysis should help to determine the intervals for scheduled maintenance activity or the operational checks that ensure the availability of the alleviation or compensation means.

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

Following a flight control system failure of the types discussed in paragraphs 7.a., 7.b., 7.c. and 7.d. of this AMC, the manoeuvrability and structural strength criteria defined in the following paragraphs should be considered to determine the capability of continued safe flight and landing of the aeroplane. Additionally, a pilot assessment of the aeroplane handling qualities should be performed, although this does not supersede the criteria provided below.

A local structural failure (e.g. via a mechanical fuse or shear-out) that could lead to a surface departure from the aeroplane should not be used as a means of jam alleviation.

(1) *Flight Characteristics*

(i) *General.* Following a flight control system failure, appropriate procedures may be used including system reconfiguration, flight limitations, and flight crew resource management. The procedures for safe flight and landing should not require exceptional piloting skills or strengths.

Additional means of control, such as a trim system, may be used if it can be shown that the system is available and effective. Credit should not be given to the use of differential engine thrust to manoeuvre the aeroplane. However, differential thrust may be used after the recovery in order to maintain lateral/directional trim.

For the cases of longitudinal flight control surface and pilot control jams during take-off prior to rotation, it is necessary to show that the aeroplane can be safely rotated for lift-off without consideration of field length available.

(ii) *Transient Response.* There should be no unsafe conditions during the transient condition following a flight control system failure. The evaluation of failures or manoeuvres that lead to a jam is intended to be initiated from 1-g wings level flight conditions. For this purpose, continued safe flight and landing (within the transition phase) is generally defined as not exceeding any one of the following criteria:

(A) a load on any part of the primary structure sufficient to cause a catastrophic structural failure;

(B) catastrophic loss of flight path control;

(C) exceedance of V_{DF}/M_{DF};

(D) catastrophic flutter;

(E) excessive vibration or excessive buffeting conditions;

(F) bank angle in excess of 90 degrees.

In connection with the transient response, compliance with the requirements of CS 25.302 should be demonstrated. While V_F is normally an appropriate airspeed limit to be considered regarding continued safe flight and landing, temporary exceedance of V_F may be acceptable as long as the requirements of CS 25.302 are met.

Paragraph 7.b. of this AMC provides a means to determine flight control surface deflections for the evaluation of flight control jams. In some cases, aeroplane roll, pitch rate, or normal acceleration is used as a basis to determine these deflections. The roll or pitch rate and/or normal acceleration that is used to determine the flight control surface deflection need not be included in the evaluation of the transient condition. For example, the in-flight lateral flight control position determined in paragraph 7.b.(1)(ii) is based on a steady roll rate of 12°/s. When evaluating this condition, either by analysis, simulation, or in-flight demonstration, the resulting flight control surface deflection is simply input while the aeroplane is in wings level flight, at the appropriate speed, altitude, etc. During this evaluation, the actual roll or pitch rate of the aeroplane may or may not be the same as the roll or pitch rate used to determine the jammed flight control surface position.

(iii) *Delay Times.* Due consideration should be given to the delays involved in pilot recognition, reaction, and operation of any disconnection systems, if applicable.

Delay = Recognition + Reaction + Operation of Disconnection

Recognition is defined as the time from the failure condition to the point at which a pilot in service operation may be expected to recognise the need to take action. Recognition of the malfunction may be through the behaviour of the aeroplane or a reliable failure warning system, and the recognition point should be identified but should not normally be less than 1 second. For flight control system failures, except the types of jams addressed in CS 25.671(c)(3), control column or wheel movements alone should not be used for recognition.

The following reaction times should be used:

Flight condition	Reaction time
On ground	1 second*
In air (< 300 m (1 000 ft) above ground level (AGL))	1 second*
Manual flight (> 300 m (1 000 ft) AGL)	1 second*
Automatic flight (> 300 m (1 000 ft) AGL)	3 seconds

*3 seconds if the control must be transferred between the pilots.

The time required to operate any disconnection system should be measured either through ground test or flight test. This value should be used during all analysis efforts. However, flight test or manned simulation that requires the pilot to operate the disconnection includes this extra time, therefore, no additional delay time would be needed for these demonstrations.

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

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

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

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

(D) A wings level landing flare in a 90° crosswind of up to 18.5 km/h (10 kt) (measured at 10 m (33 ft) above the ground); and

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

Note: In the case of a lateral or directional flight control system jam during take-off as described in paragraph 7.b(1) or 7.b(3) of this AMC, it should be shown that the aeroplane can safely land on a suitable runway, without crosswind and with crosswind in the same direction as during take-off and at speeds up to the value at which the jam was established.

(v) *Control Forces.* The short- and long-term control forces should not be greater than 1.5 times the short- and long-term control forces allowed by CS 25.143(d) or CS 25.143(k) as applicable.

Short-term forces have typically been interpreted to mean the time required to accomplish a configuration or trim change. However, taking into account the capability of the crew to share the workload, the short-term forces provided in CS 25.143(d) or CS 25.143(k), as applicable, may be appropriate for a longer duration, such as the evaluation of a jam on take-off and return to landing.

During the recovery following the failure, transient control forces may exceed these criteria to a limited extent. Acceptability of any exceedance will be evaluated on a case-by-case basis.

(2) *Structural Strength for Flight Control System Failures.*

(i) *Failure Conditions per CS 25.671(c)(1) and (c)(2).* It should be shown that the aeroplane maintains structural integrity for continued safe flight and landing. This should be accomplished by demonstrating compliance with CS 25.302, where applicable, unless otherwise agreed with EASA.

(ii) *Jam Conditions per CS 25.671(c)(3).* It should be shown that the aeroplane 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 in this AMC, an acceptable means of compliance for structural substantiation of jam conditions is provided below in paragraph 7.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 and 1.75 g with high-lift devices fully retracted and in en-route configurations, and between 0.6 and 1.4 g with high-lift devices extended;

(B) Vertical and lateral discrete gusts corresponding to 40 % of the limit gust velocity specified at V_c in CS 25.341(a) with high-lift devices fully retracted, and a 5.2-m/s (17-ft/s) vertical and a 5.2-m/s (17-ft/s) head-on gust with high-lift devices extended. The vertical and lateral gusts should be considered separately.

A flexible aeroplane model should be used for load calculations, where the use of a flexible aeroplane model is significant for the loads being assessed.

8. *EVALUATION OF ALL-ENGINES-FAILED CONDITION — CS 25.671(d)*

a. *Explanation.*

The intent of CS 25.671(d) is to assure that in the event of failure of all engines, the aeroplane will be controllable, an approach and a flare to a landing and to a ditching is possible, and, assuming that a suitable runway is available, the aeroplane is controllable on ground and can be stopped.

In this context:

— 'flare to a landing/ditching' refers to the time until touchdown;

— 'suitable runway' is a hard-surface runway or equivalent for which the distance available following touchdown is consistent with the available aeroplane ground deceleration capability.

Although the rule refers to 'flare to a landing' with the implication that the aeroplane is on a runway, it is recognised that, with all engines inoperative, it may not be possible to reach a suitable runway or landing surface. In this case, the aeroplane must still be able to make a flare to a landing attitude.

Compliance with CS 25.671(d) effectively requires that the aeroplane is equipped with a source(s) of emergency power, such as an air-driven generator, windmilling engines, batteries, or other power source, capable of providing adequate power to the systems that are necessary to control the aeroplane.

Analysis, simulation, or a combination of analysis and simulation may be used to demonstrate compliance where the methods are shown to be reliable.

b. *Procedures.*

(1) The aeroplane should be evaluated to determine that it is possible, without requiring exceptional piloting skill or strength, to maintain control following the failure of all engines and attain the parameters provided in the operational procedure of the aeroplane flight manual (AFM), taking into account the time necessary to activate any backup systems. The aeroplane should also remain controllable during restart of the most critical engine, whilst following the AFM recommended engine restart procedures.

(2) The most critical flight phases, especially for aeroplanes with emergency power systems dependent on airspeed, are likely to be the take-off, the landing, and the ditching. Credit may be taken from the hydraulic pressure and/or the electrical power produced while the engines are spinning down and from any residual hydraulic pressure remaining in the system. Sufficient power must be available to complete a wings level approach and flare to a landing, and flare to a ditching.

Analyses or tests may be used to demonstrate the capability of the control systems to maintain adequate hydraulic pressure and/or electrical power during the time between the failure of the engines and the activation of any power backup systems. If any of the power backup systems rely on aerodynamic means to generate the power, then a flight test should be conducted to demonstrate that the power backup system can supply adequate electrical and/or hydraulic power to the control systems. The flight test should be conducted at the minimum practical airspeed required to perform an approach and flare to a safe landing and ditching attitude.

(3) The manoeuvre capability following the failure of all engines should be sufficient to complete an approach and flare to a landing, and flare to a ditching. Note that the aeroplane weight could be extremely low (e.g. the engine failures could be due to fuel exhaustion). The maximum speeds for approach and landing/ditching may be limited by other CS-25 specifications (e.g. tyre speeds, flap or landing gear speeds, etc.) or by an evaluation of the average pilot ability to conduct a safe landing/ditching. At an operational weight determined for this case and for any other critical weights and positions of the centre of gravity identified by the applicant, at speeds

down to the approach speeds appropriate to the aeroplane configuration, if the following manoeuvres can be performed, it will generally be considered that compliance has been shown:

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

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

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

(iv) a wings level landing flare in a 90° crosswind of up to 18.5 km/h (10 kt) (measured at 10 m (33 ft) above the ground).

Note: If the loss of all engines has no effect on the flight control authority of the aeroplane, then the results of the flight tests of the basic handling qualities with all engines operating may be used to demonstrate the satisfactory handling qualities of the aeroplane with all engines failed.

(4) It should be possible to perform a flare to a safe landing and ditching attitude, in the most critical configuration, from a stabilised approach using the recommended approach speeds, pitch angles, and the appropriate AFM procedures, without requiring exceptional piloting skills or strengths. For transient manoeuvres, forces are allowed up to 1.5 times those specified in CS 25.143(d) or CS 25.143(k) as applicable for temporary application with two hands available for control.

Similarly to paragraph 7.e.(1)(v) of this AMC, the acceptability of any exceedance will be evaluated on a case-by-case basis.

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

A suitable runway should have the lateral dimensions, length and load-bearing capability that meets the requirements defined in the emergency procedures of the AFM.

It is not necessary to consider adverse environmental conditions (e.g. wet or contaminated runway, tailwind) when demonstrating compliance for the on-ground phase.

9. *EVALUATION OF CONTROL AUTHORITY AWARENESS — CS 25.671(e)*

CS 25.671(e) requires an indication to the flight crew when a flight condition exists in which near-full-flight-control authority (whether or not it is pilot-commanded) is being used. Suitability of such an annunciation should take into account that some pilot-commanded manoeuvres (e.g. rapid roll) are necessarily associated with intended full performance, which may saturate the surface. Therefore, simple alerting systems, which should function in both intended and unexpected flight control-limiting situations, should be properly balanced between needed crew awareness and nuisance alerting. Nuisance alerting must be minimised per CS 25.1322 by correct setting of the alerting threshold.

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

When the aeroplane is equipped with an unpowered manual flight control system, the pilot may be de facto aware of the limit of control authority. In this case, no other means of indication may be required.

10. *EVALUATION OF FLIGHT CONTROL SYSTEM MODES OF OPERATION — CS 25.671(f)*

Some flight control systems, for instance, electronic flight control systems, may have multiple modes of operation not restricted to being either on or off. The applicant should evaluate the different modes of operation and the transition between them in order to establish if they are intuitive or not.

If these modes, or the transition between them, are not intuitive, an alert to the flight crew may be required. Any alert must comply with CS 25.1322. This includes the indication to the flight crew of the loss of protections.

11. *DEMONSTRATION OF ACCEPTABLE MEANS OF COMPLIANCE*

It is recognised that it may be neither practical nor appropriate to demonstrate compliance by flight test for all of the failure conditions noted herein. Compliance may be demonstrated by analysis, simulation, a piloted engineering simulator, flight test, or a combination of these methods, as agreed with EASA. Simulation methods should include an accurate representation of the aeroplane characteristics and of the pilot response, including time delays as specified in paragraph 7.e(1)(iii) of this AMC.

Compliance with CS 25.671 may result in AFM non-normal and emergency procedures. Verification of these procedures may be accomplished in flight, or, with the agreement of EASA, using a piloted simulator.

a. *Acceptable Use of Simulations.* It is generally difficult to define the types of simulations that might be acceptable in lieu of flight test without identifying specific conditions or issues. However, the following general principles can be used as guidance for making this kind of decision:

(1) In general, flight test is the preferred method to demonstrate compliance;

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

(i) a flight test would be too risky even after attempts to mitigate these risks (e.g. 'simulated' take-offs/landings at high altitude);

(ii) the required environmental conditions, or the representation of the failure conditions, are too difficult to attain (e.g. wind shear, high crosswinds, system failure configurations);

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

(iv) the simulation is used to demonstrate repeatability.

b. *Simulation Requirements.* In order to be acceptable for use in demonstrating compliance with the requirements for performance and handling qualities, a simulation method should:

(1) be suitably validated by flight test data for the conditions of interest; furthermore,:

(i) this does not mean that there must be flight test data at the exact conditions of interest; the reason why a simulation method is being used may be that it is too difficult or risky to obtain flight test data at the conditions of interest;

(ii) the level of substantiation of the simulator to flight correlation should be commensurate with the level of compliance (i.e. unless it is determined that the simulation is conservative, the closer the case is to being non-compliant, the higher the required quality of the simulation);

(2) be conducted in a manner appropriate to the case and conditions of interest:

(i) if closed-loop responses are important, the simulation should be piloted by a human pilot;

(ii) for piloted simulations, the controls/displays/cues should be substantially equivalent to what would be available in the real aeroplane (unless it is determined that not doing so would provide added conservatism).

12. *SPECIFICITIES OF AEROPLANES WITH FLY-BY-WIRE FLIGHT CONTROL SYSTEMS*

a. *Control Signal Integrity*.

If the aeroplane is equipped with a conventional flight control system, the transmission of command signals to the primary and secondary flight control surfaces is made through conventional mechanical and hydromechanical means.

The determination of the origin of perturbations to command transmissions is relatively straightforward since failure cases can usually be classified in a limited number of categories that include maintenance error, jamming, disconnection, runaway, failure of mechanical element, or structural failure of hydraulic components. Therefore, it is almost always possible to identify the most severe failure cases that would serve as an envelope to all other cases that have the same consequences.

However, when the aeroplane is equipped with flight control systems using the fly-by-wire technology, incorporating digital devices and software, experience from electronic digital transmission lines shows that the perturbation of signals from internal and external sources is not unlikely.

The perturbations are described as signals that result from any condition that is able to modify the command signal from its intended characteristics. They can be classified in two categories:

(1) Internal causes that could modify the command and control signals include, but are not limited to:

— loss of data bits, frozen or erroneous values;
— unwanted transients;
— computer capacity saturation;
— processing of signals by asynchronous microprocessors;
— adverse effects caused by transport lag;
— poor resolution of digital signals;
— sensor noise;
— corrupted sensor signals;
— aliasing effects;
— inappropriate sensor monitoring thresholds;
— structural interactions (such as control surface compliance or coupling of structural modes with control modes) that may adversely affect the system operation.

(2) External causes that could modify the command and control signals include but are not limited to:

— high-intensity radiated fields (HIRF);
— lightning;
— electromagnetic interference (EMI) effects (e.g. motor interference, aeroplane's own electrical power and power switching transients, smaller signals if they can affect flight control, transients due to electrical failures.)

Spurious signals and/or false data that are a consequence of perturbations in either of the two above categories may result in malfunctions that produce unacceptable system responses equivalent to those of conventional systems such as limit cycle/oscillatory failures, runaway/hardover conditions, disconnection, lockups and false indication/warning that consequently present a flight hazard. It is imperative that the command signals remain continuous and free from internal and external perturbations and common-cause failures. Therefore, special design measures should be employed to maintain system integrity at a level of safety at least equivalent to that which is achieved with traditional hydromechanical designs. These special

design measures can be monitored through the system safety assessment (SSA) process, provided specific care is directed to development methods and on quantitative and qualitative demonstrations of compliance.

The following should be considered when evaluating compliance with CS 25.671(c)(2):

(1) The flight control system should continue to provide its intended function, regardless of any malfunction from sources in the integrated systems environment of the aeroplane.

(2) Any malfunctioning system in the aerodynamic loop should not produce an unsafe level of uncommanded motion and should automatically recover its ability to perform critical functions upon removal of the effects of that malfunction.

(3) Systems in the aerodynamic loop should not be adversely affected during and/or after exposure to any sources of a malfunction.

(4) Any disruption to an individual unit or component as a consequence of a malfunction, and which requires annunciation and flight crew action, should be identified to and agreed by EASA to assure that:

a) the failure can be recognised by the flight crew, and

b) the flight crew action can be expected to result in continued safe flight and landing.

(5) An automatic change from a normal to a degraded mode that is caused by spurious signal(s) or malfunction(s) should meet the probability guidelines associated with the hazard assessment established in AMC 25.1309, e.g. for a condition assessed as 'major', the probability of occurrence should be no more than 'remote' ($Pc < 10^{-5}$ per flight hour).

(6) Exposure to a spurious signal or malfunction should not result in a hazard with a probability greater than that allowed by the criteria of AMC 25.1309. The impact on handling qualities should be evaluated.

The complexity and criticality of the fly-by-wire flight control system necessitates the additional laboratory testing beyond that required as part of individual equipment validation and software verification.

It should be shown that either the fly-by-wire flight control system signals cannot be altered unintentionally, or that altered signal characteristics would meet the following criteria:

(1) Stable gain and phase margins are maintained for all control surface closed-loop systems. Pilot control inputs (pilot in the loop) are excluded from this requirement;

(2) Sufficient pitch, roll, and yaw control power is available to provide control for continued safe flight and landing, considering all the fly-by-wire flight control system signal malfunctions that are not extremely improbable; and

(3) The effect of spurious signals on the systems that are included in the aerodynamic loop should not result in unacceptable transients or degradation of the performance of the aeroplane. Specifically, in case of signals that would cause a significant uncommanded motion of a control surface actuator, either the signal should be readily detected and deactivated or the surface motion should be arrested by other means in a satisfactory manner. Small amplitude residual system oscillations may be acceptable.

It should be demonstrated that the output from the control surface closed-loop system does not result in uncommanded, sustained oscillations of flight control surfaces. The effects of minor instabilities may be acceptable, provided that they are thoroughly investigated, documented, and understood. An example of an acceptable condition would be one where a computer input is perturbed by spurious signals, but the output signal remains within the design tolerances, and the system is able to continue to operate in its selected mode of operation and is not affected by this perturbation.

When demonstrating compliance with CS 25.671(c), these system characteristics should be demonstrated using the following means:

(1) Systematic laboratory validation that includes a realistic representation of all relevant interfacing systems, and associated software, including the control system components that are part of the pitch, roll, and yaw axis control. Closed-loop aeroplane simulation/testing is necessary in this laboratory validation;

(2) Laboratory or aeroplane testing to demonstrate unwanted coupling of electronic command signals and their effects on the mechanical actuators and interfacing structure over the spectrum of operating frequencies; and

(3) Analysis or inspection to substantiate that physical or mechanical separation and segregation of equipment or components are utilised to minimise any potential hazards.

A successful demonstration of signal integrity should include all the elements that contribute to the command and control signals to the 'aerodynamic closed loop' that actuates the aerodynamic control surfaces (e.g. rudder, elevator, stabiliser, flaps, and spoilers). The 'aerodynamic closed loop' should be evaluated for the normal and degraded modes. Elements of the integrated 'aerodynamic closed loop' may include, for example: digital or analogue flight control computers, power control units, control feedback, major data busses, and the sensor signals including: air data, acceleration, rate gyros, commands to the surface position, and respective power supply sources. Autopilot systems (including feedback functions) should be included in this demonstration if they are integrated with the fly-by-wire flight control system.

b. *Formalisation of Compliance Demonstration for Electronic Flight Control Laws*.

On fly-by-wire aeroplanes, flight controls are typically implemented according to complex control laws and logics.

The handling qualities certification tests, usually performed on conventional aeroplanes to demonstrate compliance with CS-25 Subpart B specifications, are not considered to be sufficient to demonstrate the behaviour of the flight control laws in all foreseeable situations that may be encountered in service.

In order to demonstrate compliance with an adequate level of formalisation, the following should be performed and captured within certification documents:

— Determination of the flight control characteristics that require detailed and specific test strategy; and

— Substantiation of the proposed validation strategy (flight tests, simulator tests, analyses, etc.) covering the characteristics and features determined above.

In particular, the following characteristics of flight control laws should be covered:

— discontinuities;

— robustness versus piloted manoeuvres and/or adverse weather conditions;

— protection priorities (entry/exit logic conditions not symmetrical);

— control law mode changes with and without failures; and

— determination of critical scenarios for multiple failures.

The validation strategy should include, but should not be limited to, operational scenarios. The determination that an adequate level of formalisation of validation strategy has been achieved should be based on engineering judgement.

~~**AMC 25.672(c)(1)**~~

~~**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 25.705 Runway overrun awareness and alerting systems

1. When demonstrating compliance with CS 25.705, the applicant should take account of EUROCAE Document ED-250, 'Minimum Operational Performance Standard for a Runway Overrun Awareness and Alerting System', dated December 2017.

2. When demonstrating compliance with CS 25.1581 and CS 25.1585, the applicant should include in the aeroplane flight manual the following elements:

(1) A description of the runway overrun awareness and alerting system (ROAAS) operational domain, including all conditions for which the ROAAS is expected to perform its intended function,

(2) Any operational limitations applicable to the ROAAS, and

(3) Operational procedures to be used by the flight crew when ROAAS alerts are triggered.

AMC — SUBPART E

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 to be practical and considered to be acceptable to EASA. ~~However, it also recognises that flexibility of design and maintenance are necessary for practical application.~~

(…)

8.b.(3) For configurations in which combinations of three or more failure situations result in in-flight thrust reversal, the following applies:

In order to limit the exposure to pre-existing failure situations, the maximum time each pre-existing failure situation is expected to be present should be related to the frequency with which the failure situation is anticipated to occur, such that their product is $1 \times$~~$\times$~~10^{-3}~~/fh~~ or less.

(...)

AMC — SUBPART F

AMC 25.1309

System Design and Analysis

Table of Contents

(...)

4. *APPLICABILITY OF CS 25.1309*.

(...)

b. ~~Certain single failures or jams~~ Jams of flight control surfaces or pilot controls that are covered by ~~CS 25.671(c)(1) and~~ CS 25.671(c)(3) are excepted from the requirements of CS 25.1309(b)(1)(ii). ~~FAR 25.671(c)(1) requires the consideration of single failures, regardless of the probability of the failure. CS 25.671(c)(1) does not consider the effects of single failures if their probability is shown to be extremely improbable and the failures also meet the requirements of CS 25.571(a) and (b).~~

(...)

d. The failure conditions covered by CS 25.810 and CS 25.812 are excepted from the requirements of CS 25.1309(b). These ~~F~~failure ~~C~~conditions related to loss of function are associated with varied evacuation scenarios for which the probability cannot be determined. (…)

f. Some systems and some functions already receive an evaluation to show compliance with specific requirements for specific ~~F~~failure ~~C~~conditions and, therefore, meet the intent of CS 25.1309 without the need for additional analysis for those specific ~~F~~failure ~~C~~conditions.

g. The safety assessment process should consider all phases during flight and on ground when the aeroplane is in service. While this includes the conditions associated with the pre-flight preparation, embarkation and disembarkation, taxi phase, etc., it, therefore, does not include periods of shop maintenance, storage, or other out-of-service activities.

Where relevant, the effects on persons other than the aeroplane occupants should be taken into account when assessing failure conditions in compliance with CS 25.1309.

5. *DEFINITIONS*.

(...)

c. *At-Risk Time.* The period of time during which an item must fail in order to cause the failure effect in question. This is usually associated with the final fault in a fault sequence leading to a specific failure condition.

d~~c~~. *Average Probability Per Flight Hour.* (…)

e~~d~~. *Candidate Certification Maintenance Requirements (CCMR).* A periodic maintenance or flight crew check may be used in a safety analysis to help demonstrate compliance with CS 25.1309(b) for ~~H~~hazardous and ~~C~~catastrophic ~~F~~failure ~~C~~conditions. (…)

f~~e~~. *Check*. (…)

g~~f~~. *Complex.* (…)

h. *Complexity*. An attribute of functions, systems or items, which makes their operation, failure modes, or failure effects difficult to comprehend without the aid of analytical methods.

i~~g~~. *Conventional*. (…)

j~~h~~. *Design Appraisal.* (…)

k~~i~~. *Development Assurance.* (…)

l~~j~~. *Development Error*. (…)

m~~k~~. *Error*. An omission or incorrect action by a crewmember or maintenance personnel, or a development error (e.g. mistake in requirements determination, design, or implementation).

n~~l~~. *Event*. (…)

o. *Exposure Time.* The period of time between the time when an item was last known to be operating properly and the time when it will be known to be operating properly again.

p~~m~~. *Failure.* (…)

q~~n~~. *Failure Condition*. (…)

r~~o~~. *Installation Appraisal*. (…)

s~~p~~. *Item*. (…)

t~~q~~. *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.~~

u~~r~~. *Qualitative.* (…)

v~~s~~. *Quantitative.* (…)

w~~t~~. *Redundancy.* (…)

x. *Significant Latent Failure.* A latent failure that would, in combination with one or more specific failure(s) or event(s), result in a hazardous or catastrophic failure condition.

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

6. *BACKGROUND*.

a. *General*.

For a number of years aeroplane systems were evaluated to specific requirements, to the "'single fault'" criterion, or to the fail-safe design concept. As later-generation aeroplanes developed, more safety-critical functions were required to be performed, which generally resulted in an increase in the complexity of the systems designed to perform these functions. The potential hazards to the aeroplane and its occupants which could arise in the event of loss of one or more functions provided by a system or that system's malfunction had to be considered, as also did the interaction between systems performing different functions. This has led to the general principle that an inverse relationship should exist between the probability of a ~~F~~failure ~~C~~condition and its effect on the aeroplane and/or its occupants (see Figure 1). In assessing the acceptability of a design it was recognised that rational probability values would have to be established. Historical evidence indicated that the probability of a serious accident due to operational and airframe-related causes was approximately one per million hours of flight. Furthermore, about 10 %~~percent~~ of the total were attributed to ~~F~~failure ~~C~~conditions caused by the aeroplane's systems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs. It is reasonable to expect that the probability of a serious accident from all such ~~F~~failure ~~C~~conditions be not greater than one per ten million flight hours or 1 ×~~x~~ 10^{-7} per flight hour for a newly designed aeroplane. The difficulty with this is that it is not possible to say whether the target has been met until all the systems on the aeroplane are collectively analysed numerically. For this reason it was assumed, arbitrarily, that there are about one hundred potential ~~F~~failure ~~C~~conditions in an aeroplane, which could be ~~C~~catastrophic. The target allowable ~~A~~average ~~P~~probability per ~~F~~flight ~~H~~hour of 1 ×~~x~~ 10^{-7} was thus apportioned equally among these ~~F~~failure ~~C~~conditions, resulting in an allocation of not greater than 1 ×~~x~~ 10^{-9} to each. The upper limit for the ~~A~~average ~~P~~probability per ~~F~~flight ~~H~~hour for ~~C~~catastrophic ~~F~~failure ~~C~~conditions would be 1 ×~~x~~ 10^{-9}, which establishes an approximate probability value for the term "'~~E~~extremely ~~I~~improbable'". Failure ~~C~~conditions having less severe effects could be relatively more likely to occur.

b. *Fail-Safe Design Concept.*

The CS-25 airworthiness standards are based on, and incorporate, the objectives and principles or techniques of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design.

(1) The following basic objectives pertaining to failures apply:

(i) In any system or subsystem, the failure of any single element, component, or connection during any one flight should be assumed, regardless of its probability. Such single failures should not be ~~C~~catastrophic.

(ii) Subsequent failures of related systems during the same flight, whether detected or latent, and combinations thereof, should also be considered. ~~assumed, unless their joint probability with the first failure is shown to be extremely improbable.~~

(2) The fail-safe design concept uses the following design principles or techniques in order to ensure a safe design. The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design; i.e. to ensure that ~~M~~major ~~F~~failure ~~C~~conditions are ~~R~~remote, ~~H~~hazardous ~~F~~failure ~~C~~conditions are ~~E~~extremely ~~R~~remote, and ~~C~~catastrophic ~~F~~failure ~~C~~conditions are ~~E~~extremely ~~I~~improbable:

(...)

c. ~~*Highly Integrated Systems.*~~ *Development of Aeroplane and System Functions.*

(1) A concern arose regarding the efficiency and coverage of the techniques used for assessing safety aspects of ~~highly integrated systems that perform complex and interrelated functions,~~ aeroplane and systems functions implemented~~, particularly~~ through the use of electronic technology and software-based techniques. The concern is that design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for these aeroplane and system functions ~~more complex systems.~~ Thus, other assurance techniques, such as development assurance utilising a combination of integral processes (e.g. process assurance, configuration management, requirement validation and implementation verification~~ coverage criteria~~), or structured analysis or assessment techniques applied at the aeroplane level~~, if necessary, or at least~~ and across integrated or interacting systems, have been requested~~ applied to these more complex systems.~~ Their systematic use increases confidence that development errors ~~in requirements or design,~~ and integration or interaction effects have been adequately identified and corrected.

(...)

7. FAILURE CONDITION CLASSIFICATIONS AND PROBABILITY TERMS

a. *Classifications*.

Failure ~~C~~conditions may be classified according to the severity of their effects as follows:

(1) *No Safety Effect*: Failure ~~C~~conditions that would have no effect on safety; for example, ~~F~~failure ~~C~~conditions that would not affect the operational capability of the aeroplane or increase crew workload.

(2) *Minor*: Failure ~~C~~conditions which would not significantly reduce aeroplane safety, and which involve crew actions that are well within their capabilities. Minor ~~F~~failure ~~C~~conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.

(3) *Major*: Failure ~~C~~conditions which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.

(4) *Hazardous*: Failure ~~C~~conditions~~,~~ which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating~~,~~ conditions to the extent that there would be:

(i) A large reduction in safety margins or functional capabilities;

(ii) Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or

(iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew.

(5) *Catastrophic*: Failure ~~C~~conditions~~,~~ which would result in multiple fatalities, usually with the loss of the aeroplane.

(Note: A ~~"Catastrophic"~~ ~~F~~failure ~~C~~condition ~~was defined in previous versions of the rule and the advisory material as a Failure Condition~~ which would prevent continued safe flight and landing should be classified catastrophic unless otherwise defined in other specific AMCs. For flight control systems, continued safe flight and landing is defined in AMC 25.671, paragraphs 4 and 7.)

b. *Qualitative Probability Terms*.

When using qualitative analyses to determine compliance with CS 25.1309(b), the following descriptions of the probability terms used in CS 25.1309 and this AMC have become commonly accepted as aids to engineering judgement:

(1) Probable ~~F~~failure ~~C~~conditions are those anticipated to occur one or more times during the entire operational life of each aeroplane.

(2) Remote ~~F~~failure ~~C~~conditions are those unlikely to occur to each aeroplane during its total life, but which may occur several times when considering the total operational life of a number of aeroplanes of the type.

(3) Extremely ~~R~~remote ~~F~~failure ~~C~~conditions are those not anticipated to occur to each aeroplane during its total life but which may occur a few times when considering the total operational life of all aeroplanes of the type.

(4) Extremely ~~I~~improbable ~~F~~failure ~~C~~conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type.

c. *Quantitative Probability Terms*.

When using quantitative analyses to help determine compliance with CS 25.1309(b), the following descriptions of the probability terms used in this requirement and this AMC have become commonly accepted as aids to engineering judgement. They are expressed in terms of acceptable ranges for the ~~A~~average ~~P~~probability ~~P~~per ~~F~~flight ~~H~~hour.

(1) Probability Ranges.

(i) Probable ~~F~~failure ~~C~~conditions are those having ~~A~~average ~~P~~probability ~~P~~per ~~F~~flight ~~H~~hour greater than of the order of 1 ~~×~~ 10^{-5}.

(ii) Remote ~~F~~failure ~~C~~conditions are those having an ~~A~~average ~~P~~probability ~~P~~per ~~F~~flight ~~H~~hour of the order of 1 ~~×~~ 10^{-5} or less, but greater than of the order of 1 ~~×~~ 10^{-7}.

(iii) Extremely ~~R~~remote ~~F~~failure ~~C~~conditions are those having an ~~A~~average ~~P~~probability ~~P~~per ~~F~~flight ~~H~~hour of the order of 1 ~~×~~ 10^{-7} or less, but greater than of the order of 1 ~~×~~ 10^{-9}.

(iv) Extremely ~~I~~improbable ~~F~~failure ~~C~~conditions are those having an ~~A~~average ~~P~~probability ~~P~~per ~~F~~flight ~~H~~hour of the order of 1 ~~×~~ 10^{-9} or less.

8. *SAFETY OBJECTIVE.*

a. The objective of CS 25.1309 is to ensure an acceptable safety level for equipment and systems as installed on the aeroplane. A logical and acceptable inverse relationship must exist between the ~~A~~average ~~P~~probability ~~P~~per ~~F~~flight ~~H~~hour and the severity of ~~F~~failure ~~C~~condition effects, as shown in Figure 1, such that:

(1) Failure ~~C~~conditions with ~~N~~no ~~S~~safety ~~E~~effect have no probability requirement.

(2) Minor ~~F~~failure ~~C~~conditions may be ~~P~~probable.

(3) Major ~~F~~failure ~~C~~conditions must be no more frequent than ~~R~~remote.

(4) Hazardous ~~F~~failure ~~C~~conditions must be no more frequent than ~~E~~extremely ~~R~~remote.

(5) Catastrophic ~~F~~failure ~~C~~conditions must be ~~E~~extremely ~~I~~improbable.

b. The classification of the ~~F~~failure ~~C~~conditions associated with the severity of their effects are described in Figure 2a.

The safety objectives associated with ~~F~~failure ~~C~~conditions are described in Figure 2b.

(...)

c. The safety objectives associated with ~~C~~catastrophic ~~F~~failure ~~C~~conditions~~, may~~ must be satisfied by demonstrating that:

(1) No single failure will result in a ~~C~~catastrophic ~~F~~failure ~~C~~condition; and

(2) Each ~~C~~catastrophic ~~F~~failure ~~C~~condition is ~~E~~extremely ~~I~~improbable; and

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

~~d. Exceptionally, for paragraph 8c(2) above of this AMC, if it is not technologically or economically practicable to meet the numerical criteria for a Catastrophic Failure Condition, the safety objective may be met by accomplishing all of the following:~~

~~(1) Utilising well proven methods for the design and construction of the system; and~~

~~(2) Determining the Average Probability Per Flight Hour of each Failure Condition using structured methods, such as Fault Tree Analysis, Markov Analysis, or Dependency Diagrams; and~~

~~(3) Demonstrating that the sum of the Average Probabilities per Flight Hour of all Catastrophic Failure Conditions caused by systems is of the order of 10^{-7} or less (See paragraph 6a for background).~~

9. *COMPLIANCE WITH CS 25.1309*.

(...)

a. *Compliance with CS 25.1309(a).*

(1) Equipment covered by CS 25.1309(a)(1) must be shown to function properly when installed. The aeroplane operating and environmental conditions over which proper functioning of the equipment, systems, and installation is required to be considered includes the full normal ~~operating~~ envelope of the aeroplane as defined by the Aeroplane Flight Manual operating limitations together with any modification to that envelope associated with abnormal or emergency procedures. Other external environmental conditions such as atmospheric turbulence, HIRF, lightning, and precipitation, which the aeroplane is reasonably expected to encounter, should also be considered. The severity of the external environmental conditions, which should be considered, are limited to those established by certification standards and precedence.

(...)

(4) The equipment, systems, and installations covered by CS 25.1309(a)(2) are typically those associated with amenities for passengers such as passenger entertainment systems, in-flight telephones, etc., whose failure or improper functioning in itself should not affect the safety of the aeroplane. Operational and environmental qualification requirements for those equipment, systems, and installations are reduced to the tests that are necessary to show that their normal or abnormal functioning does not adversely affect the proper functioning of the equipment, systems, or installations covered by CS 25.1309(a)(1) and does not otherwise adversely influence the safety of the aeroplane or its occupants. Examples of adverse influences are: fire, explosion, exposing passengers to high voltages, etc. Normal installation practices should result in sufficiently obvious isolation so that substantiation can be based on a relatively simple qualitative installation evaluation. If the possible impacts, including failure modes or effects, are questionable, or isolation between systems is provided by complex means, more formal structured evaluation methods may be necessary.

b. *Compliance with CS 25.1309(b)*.

Paragraph 25.1309(b) requires that the aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that any ~~C~~catastrophic ~~F~~failure ~~C~~condition is ~~E~~extremely ~~I~~improbable and does not result from a single failure. It also requires that any ~~H~~hazardous ~~F~~failure ~~C~~condition is extremely ~~R~~remote, and that any ~~M~~major ~~F~~failure ~~C~~condition is ~~R~~remote. An analysis should always consider the application of the ~~F~~fail-~~S~~safe design concept described in paragraph 6.b, and give special attention to ensuring the effective use of design techniques that would prevent single failures or other events from damaging or otherwise adversely affecting more than one redundant system channel or more than one system performing operationally similar functions.

(1) *General.* Compliance with the requirements of CS 25.1309(b) should be shown by analysis and, where necessary, by appropriate ground, flight, or simulator tests. Failure ~~C~~conditions should be identified and their effects assessed. The maximum allowable probability of the occurrence of each ~~F~~failure ~~C~~condition is determined from the ~~F~~failure ~~C~~condition's effects, and when assessing the probabilities of ~~F~~failure ~~C~~conditions, appropriate analysis considerations should be accounted for. Any analysis must consider:

(i) Possible ~~F~~failure ~~C~~conditions and their causes, modes of failure, and damage from sources external to the system.

(...)

(iv) The effect of reasonably anticipated crew errors after the occurrence of a failure or ~~F~~failure ~~C~~condition.

(...)

(vii) The resulting effects on the aeroplane and occupants, considering the stage of flight, the sequence of events/failures occurrence when relevant, and operating and environmental conditions.

(2) *Planning*.

(...)

(ii) Determination of detailed means of compliance, which ~~may~~ should include ~~the use of~~ ~~D~~development ~~A~~assurance ~~techniques~~ activities.

(...)

(3) *Availability of Industry Standards and Guidance Materials*. There are a variety of acceptable techniques currently being used in industry, which may or may not be reflected in the ~~D~~documents referenced in paragraphs 3.b(2) and 3.b(3). This AMC is not intended to compel the use of these documents during the definition of the particular method of satisfying the objectives of this AMC. However, these documents do contain material and methods of performing the ~~S~~system ~~S~~safety ~~A~~assessment. These methods, when correctly applied, are recognised by EASA as valid for showing compliance with CS 25.1309(b). In addition, the Document referenced in paragraph 3.b(3) contains tutorial information on applying specific engineering methods (e.g. Markov ~~A~~analysis, ~~F~~fault ~~T~~tree ~~A~~analysis) that may be utilised in whole or in part.

(4) *Acceptable Application of Development Assurance Methods*. Paragraph 9.b(1)(iii) above requires that any analysis necessary to demonstrate ~~show~~ compliance with CS 25.1309(b) must consider the possibility of development errors. Errors made during the design and development of systems have traditionally been detected and corrected by exhaustive tests conducted on the system and its components, by direct inspection, and by other direct verification methods capable of completely characterising the performance of the system. These direct techniques may still be appropriate for ~~simple~~ systems containing non-complex items (i.e. items that are fully assured by a combination of testing and analysis) ~~which~~that perform a limited number of functions and ~~which~~ that 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~~ that must be accomplished. For these types of systems, compliance may be demonstrated ~~shown~~ by the use of ~~D~~development ~~A~~assurance. The level of ~~D~~development ~~A~~assurance (function development assurance level (FDAL)/item development assurance level (IDAL)) should be commensurate with the severity of the ~~F~~failure ~~C~~conditions the system is contributing to.

Guidelines, which may be used for the assignment of development assurance levels to aeroplanes and system functions (FDAL) and to items (IDAL), are described in the ~~d~~Document referenced in 3.b(2) above. Through this ~~d~~Document, EASA recognises that credit can be taken from system architecture (e.g. functional or item development independence) for the FDAL/IDAL assignment process.

Guidelines, which may be used for providing ~~D~~development ~~A~~assurance, are described for aeroplane and system development in the ~~d~~Document referenced in 3.b(2), and for software in the ~~d~~Document referenced in 3.a(3) above. (There is currently no agreed development assurance standard for airborne electronic hardware.)

(...)

(5) *Crew and Maintenance Actions.*

(i) Where an analysis identifies some indication to, and/or action by, the flight crew, cabin crew, or maintenance personnel, the following activities should be accomplished:

1 Verify that any identified indications are actually provided by the system. This includes the verification that the elements that provide detection (e.g. sensors, logic) properly trigger the indication under the relevant situations considering various causes, flight phases, operating conditions, operational sequences, and environments.

(...)

(ii) These verification activities should be accomplished by consulting with engineers, pilots, flight attendants, maintenance personnel, and human factors specialists, as appropriate, taking due consideration of any relevant service experience and the consequences if the assumed action is not performed or ~~mis-performed~~ performed improperly.

(iii) In complex situations, the results of the review by specialists may need to be confirmed by simulator, ground tests, or flight tests. However, quantitative assessments of the probabilities of crew or maintenance errors are not currently considered feasible. If the failure indications are considered to be recognisable and the required actions do not cause an excessive workload, then for the purposes of the analysis, such corrective actions can be considered to be satisfactorily accomplished. ~~the probability that the corrective action will be accomplished, can be considered to be one~~. If the necessary actions cannot be satisfactorily accomplished, the tasks and/or the systems need to be modified.

(6) *Significant Latent Failures.*

(i) Compliance with CS 25.1309(b)(4)

For compliance with CS 25.1309(b)(4), the hereafter systematic approach should be followed:

1. The applicant must first eliminate significant latent failures to the maximum practical extent utilising the current state-of-the-art technology, e.g. implement practical and reliable failure monitoring and flight crew indication systems to detect failures that would otherwise be latent for more than one flight. Additional guidance is provided in AMC 25-19 Section 8, Design Considerations Related to Significant Latent Failures.

2. For each significant latent failure which cannot reasonably be eliminated, the applicant must minimise the exposure time by design utilising current state-of-the-art technology rather than relying on scheduled maintenance tasks at lengthy intervals, i.e. implementing pilot-initiated checks, or self-initiated checks (e.g. first flight of the day check, power-up built-in tests, other system automated checks).

3. When relying on scheduled maintenance tasks, quantitative as well as qualitative aspects need to be addressed when limiting the latency. Additional guidance is provided in AMC 25-19 Section 10, Identification of Candidate CMRs (CCMRs).

Note: For turbojet thrust reversing systems, the design configurations in paragraphs 8.b(2) and 8.b(3) of AMC 25.933(a)(1) have traditionally been considered to be acceptable to EASA for compliance with CS 25.1309(b)(4).

(ii) Compliance with CS 25.1309(b)(5)

When a catastrophic failure condition involves two failures, either one of which is latent for more than one flight, and cannot reasonably be eliminated, compliance with CS 25.1309(b)(5) is required. Following the proper application of CS 25.1309(b)(4), the 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 EASA 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 the proposed design being state-of-the-art, past experience, sound engineering judgment, or other arguments, which led to the decision not to implement other potential means of avoidance (e.g. eliminating the significant latent failure or adding redundancy).

Two criteria are implemented in CS 25.1309(b)(5): limit latency and limit residual probability.

Limit latency is intended to limit the time of operating with one evident failure away from a catastrophic failure condition. This is achieved by requiring that the sum of the probabilities of the latent failures, which are combined with each evident failure, does not exceed 1/1 000. Taking one catastrophic failure condition at a time,

– in case an evident failure is combined only once in a dual failure combination of concern, the probability of the individual latent failure needs to comply with the 1/1 000 criterion;

– in case an evident failure is combined in multiple dual failure combinations of concern, the combined probabilities of the latent failures need to comply with the 1/1 000 criterion.

Limit residual probability is intended to limit the average probability per flight hour of the failure condition given the presence of a single latent failure. This is achieved by defining the residual probability to be ‘remote’. Residual probability is the combined average probability per flight hour of all the single active failures that result in the catastrophic failure condition assuming one single latent failure has occurred.

These requirements are applied in addition to CS 25.1309(b)(1), which requires that catastrophic failure conditions be shown to be extremely improbable and do not result from a single failure.

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

For compliance with the 1/1 000 criterion, the probability of the latent failures of concern should be derived from the probability of the worst-case flight, i.e. the probability where the evident failure occurs in the last flight before the scheduled maintenance inspection, while the latent failure may have occurred in any flight between two consecutive scheduled maintenance inspections. When dealing with constant failure rates, the probability of the latent failure should be computed as the product of the maximum time during which the failure may be present (i.e. exposure time) and its failure rate, if this probability is less than or equal to 0.1.

c. *Compliance with CS 25.1309(c)*.

CS 25.1309(c) requires that information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action in a timely manner, thereby mitigating the effects to an acceptable level. Any system operating condition that, if not detected and properly accommodated by flight crew action, would contribute to or cause a hazardous or catastrophic failure condition should be considered to be an 'unsafe system operating condition'. Compliance with this requirement is usually demonstrated by the analysis identified in paragraph 9.b(1) above, which also includes consideration of crew alerting cues, corrective action required, and the capability of detecting faults. The required information may be provided by dedicated indication and/or annunciation or made apparent to the flight crew by the inherent aeroplane/systems responses. ~~CS 25.1309(c) requires that~~When flight crew alerting is required, it must be provided in compliance with CS 25.1322. ~~a warning indication must be provided if immediate corrective action is required. Paragraph~~ CS 25.1309(c) also requires that installed systems and ~~controls~~ equipment for use by the flight crew, including ~~indications and annunciations~~ flight deck controls and information, ~~must~~ be designed to minimise flight crew errors ~~which~~ that could create additional hazards (in compliance 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 system failure and not annunciating that system failure are ~~C~~catastrophic, the combination of the system failure with the failure of its annunciation must be ~~E~~extremely ~~I~~improbable. The loss of annunciation itself should be considered a failure condition, and particular attention should be paid to the impact on the ability of the flight crew to cope with the subject system failure. In addition, unwanted operation (e.g.~~,~~ nuisance warnings) should be assessed. The failure monitoring and indication should be reliable, technologically feasible, and economically practical~~practicable~~. Reliable failure monitoring and indication should utilise current state-of-the-art technology to maximise the probability of detecting and indicating genuine failures while minimising the probability of falsely detecting and indicating non-existent failures. Any indication should be timely, obvious, clear, and unambiguous.

(...)

(5) Even if operation or performance is unaffected or insignificantly affected at the time of failure, information to the crew is required if it is considered necessary for the crew to take any action or observe any precautions. Some examples include reconfiguring a system, being aware of a reduction in safety margins, changing the flight plan or regime, or making an unscheduled landing to reduce exposure to a more severe ~~F~~failure ~~C~~condition that would result from subsequent failures or operational or environmental conditions. Information is also required if a failure must be corrected before a subsequent flight. If operation or performance is unaffected or insignificantly affected, information and alerting indications may be inhibited during specific phases of flight where corrective action by the crew is considered more hazardous than no action.

(6) The use of periodic maintenance or flight crew checks to detect significant latent failures when they occur is undesirable and should not be used in lieu of practical and reliable failure monitoring and indications. When this is not accomplished, refer to paragraph 9.b(6) for guidance.

Paragraph 12 provides further guidance on the use of periodic maintenance or flight crew checks. Comparison with similar, previously approved systems is sometimes helpful. However,

if a new technical solution allows practical and reliable failure monitoring and indications, this should be preferred in lieu of periodic maintenance or flight crew checks.

(...)

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

a. *Identification of Failure Conditions.*

Failure ~~C~~conditions should be identified by considering the potential effects of failures on the aeroplane and occupants. These should be considered from two perspectives:

(1) by considering failures of aeroplane-level functions -— ~~F~~failure ~~C~~conditions identified at this level are not dependent on the way the functions are implemented and the systems' architecture.

(2) by considering failures of functions at the system level -— these ~~F~~failure ~~C~~conditions are identified through examination of the way that functions are implemented and the systems' architectures. It should be noted that a ~~F~~failure ~~C~~condition might result from a combination of lower-level ~~F~~failure ~~C~~conditions. This requires that the analysis of complex, highly integrated systems, in particular, should be conducted in a highly methodical and structured manner to ensure that all significant ~~F~~failure ~~C~~conditions, ~~which~~ that arise from multiple failures and combinations of lower-level ~~F~~failure ~~C~~conditions, are properly identified and accounted for. The relevant combinations of failures and ~~F~~failure ~~C~~conditions should be determined by the whole safety assessment process that encompasses the aeroplane and system level functional hazard assessments and common-cause analyses. The overall effect on the aeroplane of a combination of individual system ~~F~~failure ~~C~~conditions occurring as a result of a common or cascade failure, may be more severe than the individual system effect. For example, ~~F~~failure ~~C~~conditions classified as ~~M~~minor or ~~M~~major by themselves may have ~~H~~hazardous effects at an aeroplane level, when considered in combination.

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

(1) Before a detailed safety assessment is proceeded with, a ~~F~~functional ~~H~~hazard ~~A~~assessment (FHA) of the aeroplane and system functions to determine the need for and scope of subsequent analysis should be prepared. This assessment may be conducted using service experience, engineering and operational judgement, and/or a top-down deductive qualitative examination of each function. An FHA ~~Functional Hazard Assessment~~ is a systematic, comprehensive examination of aeroplane and system functions to identify potential ~~M~~minor, ~~M~~major, ~~H~~hazardous, and ~~C~~catastrophic ~~F~~failure ~~C~~conditions ~~which~~ that may arise, not only as a result of malfunctions or failure to function, but also as a result of normal responses to unusual or abnormal external factors. It is concerned with the operational vulnerabilities of systems rather than with a detailed analysis of the actual implementation.

(...)

(3) The ~~Functional Hazard Assessment~~ FHA is an engineering tool, which should be performed early in the design and updated as necessary. It is used to define the high-level aeroplane or system safety objectives that must be considered in the proposed system architectures. It should also be used to assist in determining the development assurance levels for the systems. Many systems may need only a simple review of the system design by the applicant to determine the hazard classification. An FHA ~~Functional Hazard Assessment~~ requires experienced engineering judgement and early co-ordination between the applicant and the certification authority.

(4) Depending on the extent of functions to be examined and the relationship between functions and systems, different approaches to FHA ~~Functional Hazard Assessment~~ may be taken. Where there is a clear correlation between functions and systems, and where system, and hence function, interrelationships are relatively simple, it may be feasible to conduct separate FHAs ~~Functional Hazard Assessment~~ for each system, providing any interface aspects are properly considered and are easily understood. ~~However, w~~Where system and function interrelationships are more complex, a top-down approach, from an aeroplane-level perspective, should be taken in planning and conducting FHAs~~Functional Hazard Assessments~~. However, with the increasing integrated system architectures, this traditional top-down approach should be performed in

conjunction with common-cause considerations (e.g. common resources) in order to properly address the cases where one system contributes to several aeroplane-level functions.

c. *Considerations When Assessing Failure Condition Effects*.

(...)

In assessing the effects of a ~~F~~failure ~~C~~condition, factors~~,~~ which might alleviate or intensify the direct effects of the initial ~~F~~failure ~~C~~condition should be considered. Some of these factors include consequent or related conditions existing within the aeroplane ~~which~~ that may affect the ability of the crew to deal with direct effects, such as the presence of smoke, acceleration effects, interruption of communication, interference with cabin pressurisation, etc. When assessing the consequences of a given ~~F~~failure ~~C~~condition, account should be taken of the failure information provided, the complexity of the crew action, and the relevant crew training. The number of overall ~~F~~failure ~~C~~conditions involving other than instinctive crew actions may influence the flight crew performance that can be expected. Training recommendations may need to be identified in some cases.

(1) The severity of ~~F~~failure ~~C~~conditions should be evaluated according to the following:

(i) Effects on the aeroplane, such as reductions in safety margins, degradation in performance, loss of capability to conduct certain flight operations, reduction in environmental protection, or potential or consequential effects on structural integrity. When the effects of a failure condition are difficult to assess, the hazard classification may need to be validated by tests, simulation, or other appropriate analytical techniques.

(...)

(2) For convenience in conducting design assessments, ~~F~~failure ~~C~~conditions may be classified according to the severity of their effects as '~~N~~no ~~S~~safety ~~E~~effect', '~~M~~minor', '~~M~~major', '~~H~~hazardous', or '~~C~~catastrophic'. Paragraph 7.a above provides accepted definitions of these terms.

~~(i)~~(i) The classification of ~~F~~failure ~~C~~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 ~~M~~minor ~~F~~failure ~~C~~conditions. Conversely, other systems which are not ~~"~~'required'~~"~~, such as auto-flight systems, may have the potential for '~~M~~major', '~~H~~hazardous', or '~~C~~catastrophic ~~F~~failure ~~C~~conditions'.

(ii) Regardless of the types of assessment used, the classification of ~~F~~failure ~~C~~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 ~~F~~failure ~~C~~condition. When flight duration, flight phase, or diversion time can adversely affect the classification of failure conditions, they must be considered to be intensifying factors. Other intensifying factors include conditions that are not related to the failure (such as weather or adverse operational or environmental conditions), and which reduce the ability of the flight crew to cope with a failure condition. An example of an alleviating factor would be the continued performance of identical or operationally similar functions by other systems not affected by the ~~F~~failure ~~C~~condition. Another example of an alleviating factor is the ability of the flight crew to recognise the failure condition and take action to mitigate its effects. Whenever this is taken into account, particular attention should be paid to the detection means to ensure that the ability of the flight crew (including physical ability and timeliness of the response) to detect the failure condition and take the necessary corrective action(s) is sufficient. Refer to

CS 25.1309(c) and paragraph 9.c of this AMC for more detailed guidance on crew annunciations and crew response evaluation. ~~Examples of intensifying factors would include unrelated conditions that would reduce the ability of the crew to cope with a Failure Condition, such as weather or other adverse operational or environmental conditions.~~ Combinations of intensifying or alleviating factors need to be considered only if they are anticipated to occur together.

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

After the ~~F~~failure ~~C~~conditions have been identified and the severity of the effects of the ~~F~~failure ~~C~~conditions have been assessed, there is a responsibility to determine how to show compliance with the requirement and obtain the concurrence of EASA. Design and installation reviews, analyses, flight tests, ground tests, simulator tests, or other approved means may be used.

a. *Assessment of Failure Condition Probabilities.*

(1) The probability that a ~~F~~failure ~~C~~condition would occur may be assessed as ~~P~~probable, ~~R~~remote, ~~E~~extremely ~~R~~remote, or ~~E~~extremely ~~I~~improbable. These terms are defined in paragraph 7. Each ~~F~~failure ~~C~~condition should have a probability that is inversely related to the severity of its effects as described in paragraph 8.

(2) When a system provides protection from events (e.g.~~,~~ cargo compartment fire, gusts), its reliability should be compatible with the safety objectives necessary for the ~~F~~failure ~~C~~condition associated with the failure of the protection system and the probability of such events. (See paragraph 11g of this AMC and Appendix 4.)

(3) An assessment to identify and classify ~~F~~failure ~~C~~conditions is necessarily qualitative. On the other hand, an assessment of the probability of a ~~F~~failure ~~C~~condition may be either qualitative or quantitative. An analysis may range from a simple report that interprets test results or compares two similar systems to a detailed analysis that may or may not include estimated numerical probabilities. The depth and scope of an analysis depends on the types of functions performed by the system, the severity of ~~F~~failure ~~C~~conditions, and whether or not the system is complex.

(4) Experienced engineering and operational judgement should be applied when determining whether or not a system is complex. Comparison with similar, previously approved systems is sometimes helpful. All relevant systems' attributes should be considered; however, the complexity of the software and hardware item need not be a dominant factor in the determination of complexity at the system level~~, e.g., the design may be very complex, such as a satellite communication system, but its function may be fairly simple~~.

b. *Single Failure Considerations.*

(1) According to the requirements of CS 25.1309(b)(1)(ii), a ~~C~~catastrophic ~~F~~failure ~~C~~condition must not result from the failure of a single component, part, or element of a system. Failure containment should be provided by the system design to limit the propagation of the effects of any single failure to preclude ~~C~~catastrophic ~~F~~failure ~~C~~conditions. In addition, there must be no common-cause failure, which could affect both the single component, part, or element, and its failure containment provisions. A single failure includes any set of failures, which cannot be shown to be independent from each other. Common-cause failures (including common mode failures) and cascading failures should be evaluated as dependent failures from the point of the root cause or the initiator. Errors in development, manufacturing, installation, and maintenance can result in common-cause failures (including common mode failures) and cascading failures. They should, therefore, be assessed and mitigated in the frame of the common-cause and cascading failures consideration. Appendix 1 and the Document referenced in paragraph 3.b(3) describe types of common-cause analyses~~,~~ ~~which~~ that may be conducted~~,~~ to assure that independence is maintained. Failure containment techniques available to establish independence may include partitioning, separation, and isolation.

(2) While single failures must normally be assumed to occur, there are cases where it is obvious that, from a realistic and practical viewpoint, any knowledgeable, experienced person would unequivocally conclude that

a failure mode simply would not occur, unless it is associated with a wholly unrelated ~~F~~failure ~~C~~condition that would itself be ~~C~~catastrophic. (…)

(...)

d. *Depth of Analysis*. The following identifies the depth of analysis expected based on the classification of a ~~F~~failure ~~C~~condition.

(1) *No Safety Effect Failure Conditions*. An FHA ~~Functional Hazard Assessment~~, with a design and installation appraisal, to establish independence from other functions is necessary for the safety assessment of these ~~F~~failure ~~C~~conditions. If it is chosen not to do an FHA, the safety effects may be derived from the design and installation appraisal.

(2) *Minor Failure Conditions*. An FHA ~~Functional Hazard Assessment~~, with a design and installation appraisal, to establish independence from other functions is necessary for the safety assessment of these ~~F~~failure ~~C~~conditions. Combinations of ~~F~~failure ~~C~~condition effects, as noted in paragraph 10 above, must also be considered. If it is chosen not to do an FHA, the safety effects may be derived from the design and installation appraisal.

(3) *Major Failure Conditions*. Major ~~F~~failure ~~C~~conditions must be ~~R~~remote:

(…)

(ii) For systems that are not complex, where similarity cannot be used as the basis for compliance, then compliance may be shown by means of a qualitative assessment ~~which~~ that shows that the system-level ~~M~~major ~~F~~failure ~~C~~conditions, of the system as installed, are consistent with the FHA and are ~~R~~remote, e.g.~~,~~ redundant systems.

(iii) For complex systems without redundancy, compliance may be shown as in paragraph 11.d(3)(ii) of this AMC. To show that malfunctions are indeed ~~R~~remote in systems of high complexity without redundancy (for example, a system with a self-monitoring microprocessor), it is sometimes necessary to conduct a qualitative functional ~~F~~failure ~~M~~modes and ~~E~~effects ~~A~~analysis (FMEA) supported by failure rate data and fault detection coverage analysis.

(…)

(4) *Hazardous and Catastrophic Failure Conditions*. Hazardous ~~F~~failure ~~C~~conditions must be ~~E~~extremely ~~R~~remote, and ~~C~~catastrophic ~~F~~failure ~~C~~conditions must be ~~E~~extremely ~~I~~improbable:

(i) Except as specified in paragraph 11.d(4)(ii) below, a detailed safety analysis will be necessary for each ~~H~~hazardous and ~~C~~catastrophic ~~F~~failure ~~C~~condition identified by the FHA~~functional hazard assessment~~. The analysis will usually be a combination of qualitative and quantitative assessment of the design.

(ii) For very simple and conventional installations, i.e. low complexity and similarity in relevant attributes, it may be possible to assess a ~~H~~hazardous or ~~C~~catastrophic ~~F~~failure ~~C~~condition as being ~~E~~extremely ~~R~~remote or ~~E~~extremely ~~I~~improbable, respectively, on the basis of experienced engineering judgement, using only qualitative analysis. (…)

(iii) For complex systems where true similarity in all relevant attributes, including installation attributes, can be rigorously established, it may be also possible to assess a ~~H~~hazardous or ~~C~~catastrophic ~~F~~failure ~~C~~condition as being ~~E~~extremely ~~R~~remote or ~~E~~extremely ~~I~~improbable, respectively, on the basis of experienced engineering judgement, using only qualitative analysis. A high degree of similarity in both design and application is required to be substantiated.

e. *Calculation of Average Probability per Flight Hour (Quantitative Analysis).*

(1) The ~~A~~average ~~P~~probability per ~~F~~flight ~~H~~hour is the probability of occurrence, normalised by the flight time, of a ~~F~~failure ~~C~~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 ~~A~~average ~~P~~probability per ~~F~~flight ~~H~~hour for a ~~F~~failure ~~C~~condition should consider:

(…)

(ii) all combinations of failures and events that contribute to the ~~F~~failure ~~C~~condition,

(iii) the conditional probability if a sequence of events is necessary to produce the ~~F~~failure ~~C~~condition,

(iv) the relevant ~~"~~'at risk'~~"~~ time if an event is only relevant during certain flight phases, and

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

(2) The details how to calculate the ~~A~~average ~~P~~probability per ~~F~~flight ~~H~~hour for a ~~F~~failure ~~C~~condition are given in Appendix 3 of this AMC.

(3) If the probability of a subject ~~F~~failure ~~C~~condition occurring during a typical flight of mean duration for the aeroplane type divided by the flight's mean duration in hours is likely to be significantly different from the predicted average rate of occurrence of that ~~F~~failure ~~C~~condition during the entire operational life of all aeroplanes of that type, then a risk model that better reflects the ~~F~~failure ~~C~~condition should be used.

(4) It is recognised that, for various reasons, component failure rate data are not precise enough to enable accurate estimates of the probabilities of ~~F~~failure ~~C~~conditions. This results in some degree of uncertainty, as indicated by the wide line in Figure 1, and the expression ~~"~~'on the order of'~~"~~ in the descriptions of the quantitative probability terms that are provided above. When calculating the estimated probability of each ~~F~~failure ~~C~~condition, this uncertainty should be accounted for in a way that does not compromise safety.

f. *Integrated Systems.* Interconnections between systems have been a feature of aeroplane design for many years and CS 25.1309(b) recognises this in requiring systems to be considered in relation to other systems. Providing the interfaces between systems are relatively few and simple, and hence readily understandable, compliance may often be demonstrated~~shown~~ through a series of system safety assessments, each of which deals with a particular ~~F~~failure ~~C~~condition (or more likely a group of ~~F~~failure ~~C~~conditions) associated with a system and, where necessary, takes account of failures arising at the interface with other systems. This procedure has been found to be acceptable in many past certification programmes. However, where the systems and their interfaces become more complex and extensive, the task of demonstrating compliance may become more complex. It is therefore essential that the means of compliance ~~are~~be considered early in the design phase to ensure that the design can be supported by a viable safety assessment strategy. Aspects of the guidance material covered elsewhere in this AMC and which should be given particular consideration are as follows:

(1) planning the proposed means of compliance; this should include development assurance activities to mitigate the occurrence of errors in the design,

(…)

(3) the potential for common-cause failures and cascade effects and the possible need to assess combinations of multiple lower-level (e.g. ~~M~~major) ~~F~~failure ~~C~~conditions,

(4) the importance of ~~multi-disciplinary~~ multidisciplinary teams in identifying and classifying significant ~~F~~failure ~~C~~conditions,

(...)

g. *Operational or Environmental Conditions*. A probability of one should usually be used for encountering a discrete condition for which the aeroplane is designed, such as instrument meteorological conditions

or Category III weather operations. However, Appendix 4 contains allowable probabilities, which may be assigned to various operational and environmental conditions for use in computing the average probability per flight hour of ~~F~~failure ~~C~~conditions ~~resulting from multiple independent failures,~~ without further justification. Single failures, which, in combination with operational or environmental conditions, lead to catastrophic failure conditions, are, in general, not acceptable.

Limited cases that are properly justified may be considered on a case-by-case basis (e.g. operational events or environmental conditions that are extremely remote).

Appendix 4 is provided for guidance and is not intended to be exhaustive or prescriptive. At this time, a number of items have no accepted standard statistical data from which to derive a probability figure. However, these items are included for either future consideration or as items for which the applicant may propose a probability figure supported by statistically valid data or supporting service experience. The applicant may propose additional conditions or different probabilities from those in Appendix 4 provided they are based on statistically valid data or supporting service experience. The applicant should obtain early concurrence of ~~the Agency~~ EASA 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 ~~c~~Crew Action.*

When assessing the ability of the flight crew to cope with a ~~F~~failure ~~C~~condition, the information provided to the crew and the complexity of the required action should be considered. When considering the information provided to the flight crew, refer also to paragraph 9.c (compliance with CS 25.1309(c)). Credit for flight crew actions, and considerations of flight crew errors, should be consistent with relevant service experience and acceptable human factors evaluations. If the evaluation indicates that a potential ~~F~~failure ~~C~~condition can be alleviated or overcome without jeopardising other safety-related flight crew tasks and without requiring exceptional pilot skill or strength, credit may be taken for both qualitative and quantitative assessments. Similarly, credit may be taken for correct flight crew performance of the periodic checks required to demonstrate compliance with CS 25.1309(b) provided overall flight crew workload during the time available to perform them is not excessive and they do not require exceptional pilot skill or strength. Unless flight crew actions are accepted as normal airmanship, they should be described in the approved Aeroplane Flight Manual in compliance with CS 25.1585. The applicant should provide a means to ensure that the AFM will contain the required flight crew actions that have been used as mitigation factors in the hazard classification or that have been taken as assumptions to limit the exposure time of failures.

b. *Maintenance Action*.

Credit may be taken for the correct accomplishment of reasonable maintenance tasks, for both qualitative and quantitative assessments. The maintenance tasks needed to demonstrate ~~show~~ compliance with CS 25.1309(b) should be established. In doing this, the following maintenance scenarios can be used:

(1) For failures known to the flight crew, refer to paragraph 12.d.~~Annunciated failures will be corrected before the next flight, or a maximum time period will be established before a maintenance action is required. If the latter is acceptable, the analysis should establish the maximum allowable interval before the maintenance action is required. These maximum allowable intervals should be reflected in either the MMEL or the type certificate.~~

(2) Latent failures will be identified by a scheduled maintenance task. If this approach is taken, and the ~~F~~failure ~~C~~condition is ~~H~~hazardous or ~~C~~catastrophic, then a CCMR maintenance task should be established. Some ~~L~~latent ~~F~~failures can be assumed to be identified based upon return to service test on the LRU following its removal and repair (component ~~M~~mean ~~T~~time ~~B~~between ~~F~~failures (MTBF) should be the basis for the check interval time).

c. *Candidate Certification Maintenance Requirements*.

(1) By detecting the presence of, and thereby limiting the exposure time to significant latent failures that would, in combination with one or more other specific failures or events identified by safety analysis, result in a ~~H~~hazardous or ~~C~~catastrophic ~~F~~failure ~~C~~condition, periodic maintenance or flight crew checks may be used to help show compliance with CS 25.1309(b). Where such checks cannot be accepted as basic servicing or airmanship they become CCMRs. AMC 25.19 details the handling of CCMRs.

(...)

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

An applicant may elect to develop ~~A~~ a list ~~may be developed~~ of equipment and functions ~~which~~ that need not be operative for flight, based on stated compensating precautions that should be taken, e.g.~~,~~ operational or time limitations, flight crew procedures, or ground crew checks. The documents used to demonstrate ~~show~~ compliance with CS 25.1309, together with any other relevant information, should be considered in the development of this list~~, which then becomes the basis for a Master Minimum Equipment List (MMEL)~~. Experienced engineering and operational judgement should be applied during the development of ~~the MMEL~~this list. When operation is envisaged with equipment that is known to be inoperative, and this equipment affects the probabilities associated with hazardous and/or catastrophic failure conditions, limitations may be needed on the number of flights and/or the allowed operation time with such inoperative equipment. These limitations should be established in accordance with the recommendations contained in CS-MMEL.

(...)

APPENDIX 1. ASSESSMENT METHODS.

Various methods for assessing the causes, severity, and probability of ~~F~~failure ~~C~~conditions are available to support experienced engineering and operational judgement.

(...)

c. *Failure Modes and Effects Analysis*.

(…)

-- assuming all failure modes result in the ~~F~~failure ~~C~~conditions of interest,

(…)

d. *Fault Tree or Dependence Diagram Analysis*. Structured, deductive, top-down analyses that are used to identify the conditions, failures, and events that would cause each defined ~~F~~failure ~~C~~condition. They are graphical methods of identifying the logical relationship between each particular ~~F~~failure ~~C~~condition and the primary element or component failures, other events, or combinations thereof that can cause it. A failure modes and effects analysis may be used as the source document for those primary failures or other events.

(…)

f. *Common-Cause Analysis.* The acceptance of adequate probability of ~~F~~failure ~~C~~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~~considered to be acceptable. These studies may also identify a combination of failures and effects that would otherwise not have been foreseen by FMEA or fault tree analysis.

The ~~C~~common ~~C~~cause ~~A~~analysis is ~~sub-divided~~ subdivided into three areas of study:

(…)

(3) *Common Mode Analysis*. This analysis is performed to confirm the assumed independence of the events, which were considered in combination for a given ~~F~~failure ~~C~~condition.

(...)

g. *Safety Assessment Process*. Appendix 2 provides an overview of the ~~S~~safety ~~A~~assessment ~~P~~process.

APPENDIX 2. SAFETY ASSESSMENT PROCESS OVERVIEW.

(...)

a. Define the system and its interfaces, and identify the functions that the system is to perform. Some functions are intended to be protective, i.e. functions preventing the failures in system X from adversely affecting system Y. As the implementation of the functional requirements becomes more developed, care should be taken to identify all protective functions upon which airworthiness will depend. Determine whether or not the system is complex, similar to systems used on other aeroplanes, or conventional. When ~~re~~ multiple systems and functions are to be evaluated, consider the relationships between multiple safety assessments.

b. Identify and classify ~~F~~failure ~~C~~conditions. All relevant engineering organisations, such as systems, structures, propulsion, and flight test, should be involved in this process. This identification and classification may be done by conducting an FHA~~Functional Hazard Assessment,~~ which is usually based on one of the following methods, as appropriate:

(...)

c. Choose the means to be used to determine compliance with CS 25.1309. The depth and scope of the analysis depends on the types of functions performed by the system, the severity of system ~~F~~failure ~~C~~conditions, and whether or not the system is complex (see Figure A2-2). For ~~M~~major ~~F~~failure ~~C~~conditions, experienced engineering and operational judgement, design and installation appraisals and comparative service experience data on similar systems may be acceptable, either on their own or in conjunction with qualitative analyses or selectively used quantitative analyses. For ~~H~~hazardous or ~~C~~catastrophic ~~F~~failure ~~C~~conditions, a very thorough safety assessment is necessary. The early concurrence of ~~the Agency~~ EASA on the choice of an acceptable means of compliance should be obtained.

d. Conduct the analysis and produce the data, which are agreed with the certification authority as being acceptable to show compliance. A typical analysis should include the following information to the extent necessary to show compliance:

(…)

(3) The conclusions, including a statement of the ~~F~~failure ~~C~~conditions and their classifications and probabilities (expressed qualitatively or quantitatively, as appropriate) that show compliance with the requirements of CS 25.1309.

(4) A description that establishes correctness and completeness and traces the work leading to the conclusions. This description should include the basis for the classification of each ~~F~~failure ~~C~~condition (e.g.~~,~~ analysis or ground, flight, or simulator tests). It should also include a description of precautions taken against common-cause failures, provide any data such as component failure rates and their sources and applicability, support any assumptions made, and identify any required flight crew or ground crew actions, including any CCMRs.

e. Assess the analyses and conclusions of multiple safety assessments to ensure compliance with the requirements for all aeroplane-level ~~F~~failure ~~C~~conditions.

(…)

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

The purpose of this material is to provide guidance for calculating the "'Average Probability per Flight Hour'" for a Ffailure Ccondition so that it can be compared with the quantitative criteria of the AMC.

The process of calculating the "'Average Probability per Flight Hour'" for a Ffailure Ccondition will be described as a four-step process and is based on the assumption that the life of an aeroplane is a sequence of "'Average Flights'".

Step 1: Determination of the "'Average Flight'"

Step 2: Calculation of the probability of a Ffailure Ccondition for a certain "'Average Flight'"

Step 3: Calculation of the "'Average Probability per Flight'" of a Ffailure Ccondition

Step 4: Calculation of the "'Average Probability Per Flight Hour'" of a Ffailure Ccondition

(...)

b. *Calculation of the Probability of a Failure Condition for a certain "'Average Flight'"*. The probability of a Ffailure Ccondition occurring on an "'Average Flight'" P_{Flight}(Ffailure Ccondition) should be determined by structured methods (see Document referenced in paragraph 3.b(3) for example methods) and should consider all significant elements (e.g. combinations of failures and events) that contribute to the Ffailure Ccondition. The following should be considered:

(1) The ~~individual part,~~ component~~, and assembly~~ failure rates utilised in calculating the "'Average Probability per Flight Hour'" should be estimates of the mature constant failure rates after infant mortality and prior to wear-out. For components whose probability of failure may be associated with non-constant failure rates within the operational life of the aeroplane, a reliability analysis may be used to determine component replacement times (e.g. Weibull analysis). ~~and~~ In either case, the failure rate should be based on all causes of failure (operational, environmental, etc.). ~~Where~~ If available, service history of same or similar components in the same or similar environment should be used.

Ageing and wear of similarly constructed and similarly loaded redundant components, whose failure could lead directly, or in combination with one other failure, to a catastrophic or hazardous failure condition, should be assessed when determining scheduled maintenance tasks for such components.

The replacement times, necessary to mitigate the risk due to ageing and wear of such components within the operational life of the aeroplane, should be assessed through the same methodology like other scheduled maintenance tasks that are required to comply with CS 25.1309 (refer to AMC 25-19 for guidance) and documented in the Airworthiness Limitations Section of the Instructions for Continued Airworthiness, as appropriate.

(...)

(4) If the failure rate of one element varies during different flight phases, the calculation should consider the failure rate and related time increments in such a manner as to establish the probability of the Ffailure Ccondition occurring on an "'Average Flight'":

(…)

(5) If there is only an effect when failures occur in a certain order, the calculation should account for the conditional probability that the failures occur in the sequence necessary to produce the Ffailure Ccondition.

c. *Calculation of the Average Probability per Flight of a Failure Condition*. The next step is to calculate the "'Average Probability per Flight'" for the Ffailure Ccondition~~,~~ ~~i~~.e. the probability of the Ffailure Ccondition for each flight (which might be different although all flights are "'Average Flights'") during the relevant time

(e.g. the least common multiple of the exposure times or the aeroplane life) should be calculated, summed up and divided by the number of flights during that period. The principles of calculating are described below and also in more detail in the Document referenced in paragraph 3.b(3).

APPENDIX 4. ALLOWABLE PROBABILITIES.

The following probabilities may be used for environmental conditions and operational factors (not caused by aeroplane failures) in quantitative safety analyses:

Environmental Factors

Condition	Model or other Justification	Probability
~~Normal icing (trace, light, moderate icing)~~ CS-25 Appendix C icing conditions		1
CS-25 Appendix O icing conditions		10^{-2} per flight hour
Icing conditions beyond certified conditions (considered as 'Severe icing')		No accepted standard data
Headwind >25 kt~~s~~ during take-off and landing	AC 120-28 CS-AWO	10^{-2} per flight
Tailwind >10 kt~~s~~ during take-off and landing	AC 120-28 CS-AWO	10^{-2} per flight
Crosswind >20 kt~~s~~ during take-off and landing	AC 120-28 CS-AWO	10^{-2} per flight
Limit design gust and turbulence	CS 25.341	10^{-5} per flight hour
Air temperature < -70°C		No accepted standard data
~~Lightning strike~~		~~No accepted standard data~~
~~HIRF conditions~~		~~No accepted standard data~~

(...)

Other Events

Event	Model or other Justification	Probability
Fire in a lavatory not caused by aeroplane failures		No accepted standard data
Fire in a cargo compartment not caused by aeroplane failures		No accepted standard data
~~Fire in APU compartment~~		~~No accepted standard data~~

Event	Model or other Justification	Probability
~~Engine fire~~		~~No accepted standard data~~
~~Cabin high altitude requiring passenger oxygen~~		~~No accepted standard data~~

(...)

***APPENDIX 5. EXAMPLE OF LIMIT LATENCY AND RESIDUAL PROBABILITY ANALYSIS*.**

The following example illustrates how the quantitative criteria of CS 25.1309(b)(5) are to be implemented together with CS 25.1309(b)(1). The methodology used is based on the identification of the minimal cut sets associated with the catastrophic top event of the generic system level fault tree provided in Figure A5-1.

The term 'minimal cut set' refers to the smallest set of primary events whose occurrence is sufficient to cause a system failure or, in this case, the failure condition of concern.

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

(2) The dual-order minimal cut sets that contain a primary event that is latent for more than one flight are then identified from the list in Table A5-1.

(3) Then group those dual-order minimal cut sets:

(3.1) that contain the same active primary event. For each group, sum the remaining latent failure probabilities. For each group, the sum of the latent primary events should be less than 1/1 000.

(3.2) that contain the same latent primary event. For each group, assume that the latent primary event has failed and sum the remaining active primary event probabilities. For each group, the sum of the primary event probabilities should be less than 1×10^{-5}/FH.

(4) The sum of all minimal cut sets should be in the order of 1×10^{-9}/FH.

An alternative method to perform step (3.2) would be to rerun the fault-tree-probability calculation assuming for each model rerun that a different latent primary event has occurred and then verify that the average probability per flight hour of the top event is of the order of 1×10^{-5}/FH or less.

The results of the limit latency and residual probability analysis are provided in Table A5-1.

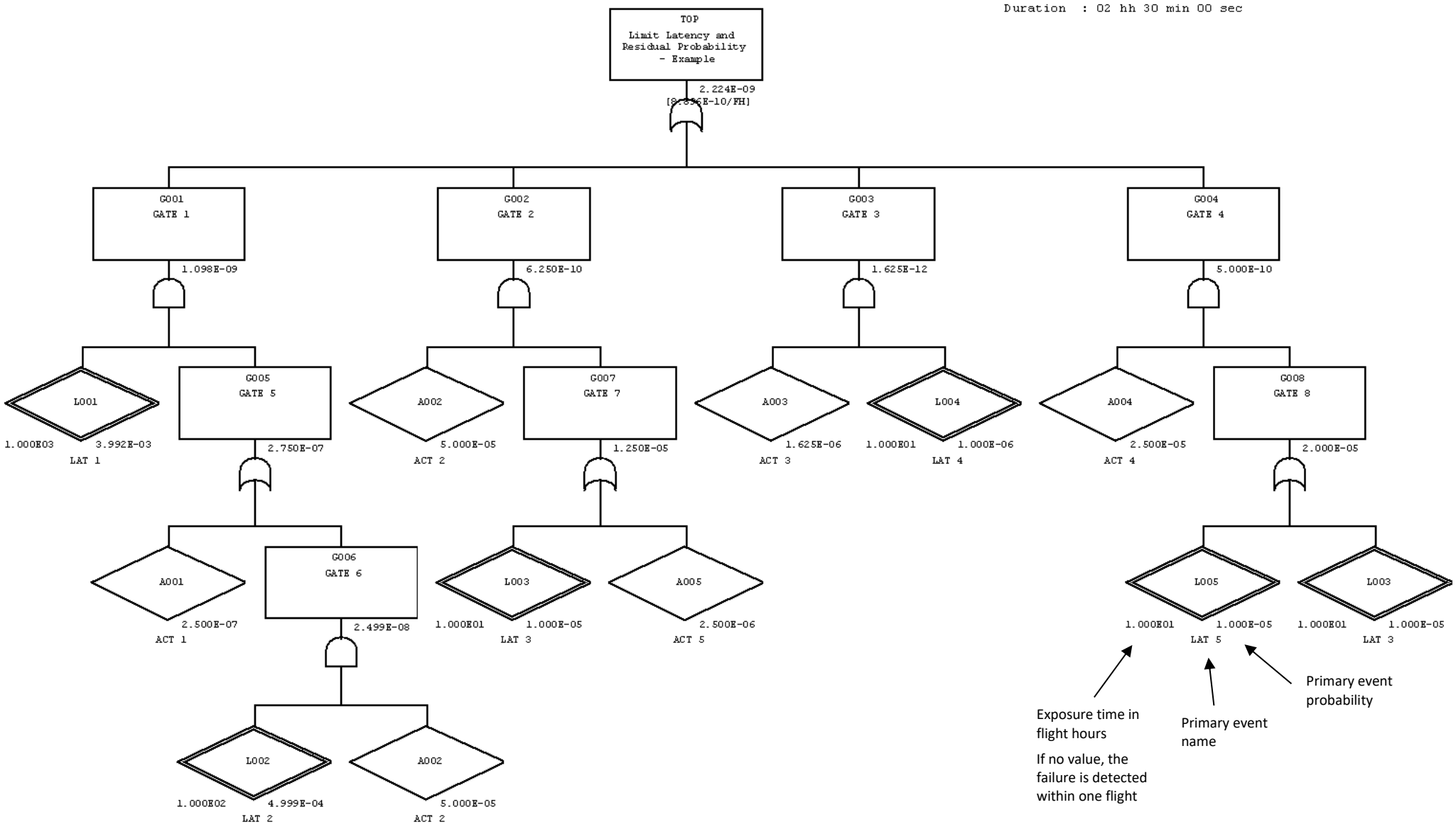

Figure A5-1: Fault Tree

#	Probability (per flight hour)	Event name	Event description	Failure rate (constant, unless noted)	Exposure time	Event probability (per flight)	CS 25.1309(b)(5) Applicability/ compliance
1	3.992E-10	A001	ACT 1	1.000E-07	2.5 h	2.500E-07	Not compliant with the limit latency criterion [L001 probability is more frequent than 1.000E-03].
		L001	LAT 1	4.000E-06	1 000.0 h	3.992E-03	
2	2.000E-10	A002	ACT 2	2.000E-05	2.5 h	5.000E-05	Not compliant with the residual probability criterion [A002 probability per flight hour (2.000E-05/FH) is more frequent than 1.000E-05/FH].
		L003	LAT 3	1.000E-06	10.0 h	1.000E-05	
3	1.000E-10	A004	ACT 4	1.000E-05	2.5 h	2.500E-05	Not compliant with the residual probability criterion [while A004 probability per flight hour is equal to 1.000E-05/FH, the combined probability per flight hour of A004 and A002 (1.000E-05/FH + 2.000E-05/FH) is more frequent than 1.000E-05/FH. *Note: Dual-order minimal cut sets #2 and #3 are grouped due to same event L003 appearing under G002 and G004.*
		L003	LAT 3	1.000E-06	10.0 h	1.000E-05	
4	1.000E-10	A004	ACT 4	1.000E-05	2.5 h	2.500E-05	Compliant with both limit latency and residual probability criteria [A004 probability per flight hour is equal to 1.000E-05/FH and combined probability of L005 and L003 (1.000E-05 + 1.000E-05) is less frequent than 1.000E-03].
		L005	LAT 5	1.000E-06	10.0 h	1.000E-05	
5	2.000E-11	A002	ACT 2	2.000E-05	2.5 h	5.000E-05	This dual-order minimal cut set does not contain any basic event being latent for more than one flight. Therefore, CS 25.1309(b)(5) is not applicable to this minimal cut set.
		A005	ACT 5	1.000E-06	2.5 h	2.500E-06	
6	6.500E-13	A003	ACT 3	6.500E-07	2.5 h	1.625E-06	Compliant with both limit latency and residual probability criteria [A003 probability per flight hour (6.500E-07/FH) is less frequent than 1.000E-05/FH and L004 probability is less frequent than 1.000E-03]
		L004	LAT 4	1.000E-07	10.0 h	1.000E-06	
7	3.991E-11	A002	ACT 2	2.000E-05	2.5 h	5.000E-05	This minimal cut set is more than a dual failure combination. Therefore, CS 25.1309(b)(5) is not applicable to this minimal cut set.
		L001	LAT 1	4.000E-06	1 000.0 h	3.992E-03	
		L002	LAT 2	5.000E-06	100.0 h	4.999E-04	
Flight time = 2.5 hours P[LAT i] ~ FR * T							

Table A5-1: Minimal Cut Sets