Process Support
Rulemaking Directorate
EASA
Postfach 101253
50452 Cologne
Germany

Subject: Gulfstream Aerospace Corporation response to EASA Proposed Amendments to CS-25 (Certification Specification for large aeroplanes)

Enclosures: 1) Draft CS-25 (Certification Specification for large aeroplanes) Comments

Gulfstream appreciates the opportunity to review this Notice of Proposed Amendment concerning certification specifications of large aircraft. EASA has encouraged comments to improve and support this NPA. Gulfstream is pleased to support EASA in this effort and offers the following specific comments and recommendations:

CS 25.671 (a)

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

- GAC Response:

  The added text constitutes a new and unrelated requirement.

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

  Recommended:

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

CS 25.671 (b)

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

- GAC Response:

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

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

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

CS 25.671 (c)

"The aeroplane must be shown by analysis, test, or both, to be capable of continued safe flight and landing after any of the following failures ~~or~~, including jamming, in the.."

- GAC Response:

  The wording "including jamming" is superfluous, recommend deletion.

CS 25.671 (c)(2)(ii)

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

~~*Any combination of failures not shown to be extremely improbable, excluding jamming (for example, dual electrical or hydraulic system failures, or any single failure in combination with any probable hydraulic or electrical failure).*~~*"*

- GAC Response:

  The wording of this item does not fit the paragraph.

  Also, the text does not make sense. The 1/1000 condition does not relate to "given any single latent failure has occurred".

CS 25.671 (c)(4)

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

- GAC Response:

  "Adverse position" and "external source" are vague.

  Recommended:

  (c)(4) Any flight control system condition resulting from a single particular risk occurrence, maintenance error, or other foreseeable external event.

CS 25.671 (c)(5)

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

- GAC Response:

  The wording of this item does not fit the paragraph.

CS 25.671 (c)

To make 25.671(c) clear and to resolve all the individual issues noted, the following rewording is proposed:

- CS 25.671(c) The aeroplane must be shown by analysis, test, or both, to meet the following conditions:

  (1) To be capable of continued safe flight and landing after any of the following failures in the flight control system within the normal flight envelope:

  (i) Any single failure, excluding failures of the type defined in (c)(1)(iii).

  (ii) Any combination of failures not shown to be extremely improbable, excluding failures of the type defined in (c)(1)(iii).

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

  (iv) Any flight control system condition resulting from a single particular risk occurrence, maintenance error, or other foreseeable external event.

  (2) Given any single failure, including failures of the type defined in (c)(1)(iii), the combined probability of all the subsequent failure states that could prevent continued safe flight and landing must be less than 1/1000.

  (3) Given any single latent failure has occurred, the combined average probability of all the subsequent single failures preventing continued safe flight and landing must be less than 1E-5 per flight hour.

  (4) The jam defined in (c)(1)(iii) must be evaluated as follows:

  (i) The jam must be considered at any normally encountered position of the control surface, or pilot controls.

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

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

CS 25.671 (d)

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

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

- GAC Response:

  The last item does not fit the paragraph.

  Recommended:

  (d) The aeroplane must be designed so that, if all engines fail at any point of the flight and a suitable runway is available, then:

  (1) It is controllable:

  (i) In flight;

  (ii) On approach;

  (iii) During the flare to a landing;

  (iv) During the ground phase

  (2) The aeroplane can be stopped.

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

"(5) For each catastrophic failure condition that results from two failures, either of which is latent for more than one flight, it must be shown that:
(i) it is impractical to provide additional fault tolerance; and
(ii) given any single latent failure has occurred, the catastrophic failure condition due to the sum of all subsequent single failures is remote; and

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

- GAC Response:

  Recommended:

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

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

AMC 25.629 (4.3)(iii)

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

- GAC Response:

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

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

  Recommended:
  Delete highlighted text from (iii) and add:

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

AMC 25.629 (4.3)(iii)

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

- GAC Response:

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

AMC 25.629 (4.3)(iii)

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

- GAC Response:

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

AMC 25.629 (4.3)(iii)

"…probable electric or hydraulic system failure (including loss of hydraulic fluid), are assumed to occur regardless of probability calculations and must be evaluated.(CS 25.671), are not normally considered extremely improbable regardless of probability calculations. The reliability… "

- GAC Response:

  Dual failures such as the ones mentioned here are not assumed to occur regardless of probability in complying with any other regulations.

  Since this is not a general practice, this text should be reworded accordingly.

  Recommended:

  "When complying with CS 25.629, the conditions described in (d)(10) should be assumed to occur regardless of probability."

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

"(…)a. For control systems, the design intent should be such that it is impossible to assemble elements of the system so as to prevent its intended function. Examples of the consequences of incorrect assembly include the following:
(1) an out-of-phase action, or
(2) reversal in the sense of the control, or
(3) interconnection of the controls between two systems where this is not intended, or
(4) loss of function."

- GAC Response:

CS 25.671(b) applies to flight control systems, the same scope should be preserved here.

This section should clarify that the intent of the rule is to prevent mis-assembly from affecting the safety of flight. It may be possible to incorrectly assemble a system in such a way that the resulting installation is evidently non-functional. Aircraft with such conditions would never plausibly be dispatched.

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

Recommended:

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

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

(1) an out-of-phase action, or

(2) reversal in the sense of the control, or

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

(4) uncommanded motion, or

(5) loss of function or redundancy.

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

d. Examples of unmistakably evident effects include the following:

(1) Jammed cockpit controls,

(2) Severely off center cockpit controls,

(3) Conditions resulting in caution or warning alerts that cannot be circumvented by normal operating procedures.

CS 25.671 (b)

"b. (…) The applicant should:
(i) Analyse the assembly and maintenance of the system to assess the classification of potential failures.

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

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

- GAC Response:

The current text equivocates between the assembly or maintenance error and the failure condition resulting from the error.

Recommended:

The applicant should:

(i) Analyze the system to assess the failure conditions that could be caused by incorrect assembly or maintenance.

(ii) For assembly or maintenance errors resulting in Cat/Haz/Maj failures, introduce physical prevention against mis-assembly, or an indication to the flight crew capable of preventing dispatch with the condition. Discuss with the Authority if neither of these solutions is possible.

(iii) For assembly or maintenance errors resulting in Minor or No Safety Effect failure conditions marking alone is generally considered sufficient to prevent incorrect assembly.

CS 25.671 (c)

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

- GAC Response:

Typo

"…flight envelope,."

10. EVALUATION OF ALL ENGINES FAILED CONDITION – CS 25.671 (d)(b)(3)(iv)

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

- GAC Response:

Note: Loss of engines can have an effect on control authority for manually controlled propeller driven aircraft.

4. APPLICABILITY OF CS 25.1309. (g)

"CS 25.1309 is always applicable to flight conditions, but only applicable to ground conditions when the airplane is in service (that is, from the time the airplane arrives at a gate or other location for pre-flight preparations, until it is removed from service for shop maintenance, storage, etc.). While this does include conditions associated with line maintenance, dispatch determinations, embarkation and disembarkation, taxi, or the like, it does not include periods of shop maintenance, storage, or other out of service activities."

- GAC Response:

Originally flight was defined as being initiated with throttle advance on takeoff to achievement of taxi speed on landing. Flight safety regulation applied within this scope.

This scope has been significantly expanded by interpretation (not rulemaking). The proposed guidance here expands the definition of flight even further beyond what has recently been practiced.

Gulfstream proposes that the ICAO definition of an accident should be a widely acceptable basis for defining what a "flight" is.

"Accident. An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which (...)" - ICAO Annex 13.

CS 25.1309 would, therefore, be applicable between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked.

4. APPLICABILITY OF CS 25.1309. (h)

"Risks to persons other than airplane occupants should be taken into account when assessing failure conditions in compliance with CS 25.1309. Such risks include threats to people on the ground or adjacent to the airplane during ground operations, electric shock threats to mechanics, and other similar situations. Because such risks are usually less significant in comparison with the risk to the airplane and its occupants, applicants have not typically addressed these risks in demonstrating compliance with CS 25.1309. However, designs may be considered non-compliant due to an unacceptable potential threat to persons outside the airplane or to line mechanics."

- GAC Response:

"…shock threats to mechanics, "

Gulfstream disagrees that these issues are subject to CS 25.1309. Specific regulation exists for workplace safety, which applies when the aircraft is static, on the ground, and not in use with the intent of flight.

The proposed definition of flight operation based on the ICAO annex would not include maintenance operations conducted when the aircraft is not actively in a flight operation.

5. DEFINITION. (o)

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

"(2) Separation of responsibilities that assures the accomplishment of objective evaluation, e.g. validation activities not performed solely by the developer of the requirement of a system or item."

- GAC Response:

The following definition is proposed:

Independence. The absence of common sources of error or failure between systems, functions, or items.

5. DEFINITION. (v)

"Significant Latent Failure. A latent failure that would, in combination with one or more specific failures or events, results in a Hazardous or Catastrophic Failure Condition."

- GAC Response:

By this definition, a latent failure which combined with three remote non-latent failures results in a Hazardous or Catastrophic condition would be considered significant, even though the active failures alone render the scenario extremely improbable (and the specific risk when the latent failure is present remains <<1E-9).

The following definition is proposed:

Significant Latent Failure. A latent failure that would:

(1) In combination with a single non-latent failure or event, and any number of additional latent events, result in a Hazardous or Catastrophic failure condition; or

(2) When present, cause the average probability per flight hour of a Hazardous or Catastrophic failure condition to exceed its quantitative requirement by one or more orders of magnitude.

6. BACKGROUND. (b)(1)(ii)

"Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, ~~unless~~ and their joint probability with the first failure is shown to be extremely improbable. The effect of combinations of failures that are not extremely improbable should not be catastrophic."

- GAC Response:

"…also be assumed…"

As worded, the text seems to imply that subsequent failures should be assumed to occur (which contradicts the determination of probability).

Recommended:

Considered

6. BACKGROUND. (b)(1)(ii)

"Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, ~~unless~~ and their joint probability with the first failure is shown to be extremely improbable. The effect of combinations of failures that are not extremely improbable should not be catastrophic."

- GAC Response:

"…failure is shown…"

Delete.

9. COMPLIANCE WITH CS 25.1309. (b)(5)(i)(1)

"…system. This includes verification that the sensor coverage and logic that detects the situations and triggers the indicator is sufficient to always detect the situations considering various causes, flight phases, operating conditions, operational sequences, and environments."

- GAC Response:

All items are subject to failure, therefore this standard ("always") cannot be met.

It is sufficient that the indication function correctly in all foreseeable operating conditions (per CS 25.1301).

Recommended:

"This includes verification that the method of detection and indication is capable of detecting the condition in all environmental and operational conditions per CS 25.1309(a)(1)."

10. IDENTIFICATION OF FAILURE CONDITIONS AND CONSIDERATIONS WHEN ASSESSING THEIR EFFECTS. (b, 4)

"…and conducting Functional Hazard Assessments. With the increasing integrated system architectures, this traditional top down approach should also be complemented with a bottom up approach in order to properly address where one system contributes to several aeroplane level functions."

- GAC Response:

The need for performing these bottom-up activities is indeed (as noted) due to the limitations of the FHA methodology, however these methods cannot produce the same type of output as the FHA.

All bottom-up analysis methods are design dependent verification methods (FMEA, cascading failure analysis, etc.). These are fundamentally different from the FHA, which is a design independent assessment which generates requirements.

Adding this text at this location will generate confusion, as it seems to imply that bottom-up methods should be used to identify functional failure conditions (in addition to the FHA). No such bottom-up methods exist, or can exist.

This content is best added where discussing verification activities (system safety assessment, aircraft safety assessment).

Recommended:

Delete from this section. This content may be added to a section discussing system or aircraft level safety assessment.

11. ASSESSMENT OF FAILURE CONDITION PROBABILITIES AND ANALYSIS CONSIDERATIONS. (e, 1, iv)

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

- GAC Response:

Disagree with this stipulation. When a condition is limited to a short exposure on each flight, the exposure will occur much less frequently on aircraft that have long average flights than on aircraft with short average flights - over the same amount of flight hours.

This stipulation unnecessarily increases the strictness of quantitative requirements for long range aircraft, by preventing the limited exposure from being computed against the total flight time. There is no regulatory basis for this. Quantitative safety requirements are "per flight hour" average probability requirements.

When considering a hazard that only occurs on takeoff, an aircraft that performs one takeoff every 10 flight hours is objectively safer than an aircraft that performs 10 takeoffs every 10 flight hours.

The existing "no single failure" and the added specific risk requirements are sufficient to ensure that conditions caused by high failure rate failures would not be found compliant on the basis of limited exposure alone.

If there are any questions, or if I can be of further assistance, please do not hesitate to contact Steve Cottrell at (912) 965-6469 or GAC.Cert@Gulfstream.com.

Sincerely,

For
Kimberly Lascell, Director, Airworthiness & Certification