Proposed Equivalent Safety Finding to CS 25.671(c)(2) : Control System – Applicable to Large Aeroplanes

Issue 1

Introductory note:

The hereby presented Equivalent Safety Finding to the EASA Certification Basis shall be subject to public consultation, in accordance with EASA Management Board decision 12/2007 dated 11 September 2007, Article 3 (2.) of which states:

"2. Deviations from the applicable airworthiness codes, environmental protection certification specifications and/or acceptable means of compliance with Part 21, as well as important special conditions and equivalent safety findings, shall be submitted to the panel of experts and be subject to a public consultation of at least 3 weeks, except if they have been previously agreed and published in the Official Publication of the Agency. The final decision shall be published in the Official Publication of the Agency."

Statement of issue

Any large aeroplane must be shown capable of Continued Safe Flight and Landing (CSFL), without requiring exceptional piloting skill or strength, for single failures and certain combinations of failures not shown to be extremely improbable.

Part 21A.21(c)(2) states that a type certificate may be issued it if found that the applicable regulations are met or "that any airworthiness provisions not complied with are compensated for by factors that provide an equivalent level of safety".

The requirements for the consideration of failure conditions in the flight control systems are covered specifically by CS25.671 and in general by CS25.1309.

CS 25.671(c)(2) requires that the aeroplane is shown to be capable of Continued Safe Flight and Landing (CSFL) within the normal flight envelope, and without requiring exceptional piloting skill or strength, after "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)".
The "single plus probable" criterion stipulated in subparagraph (c)(2) has generated a fair amount of confusion in terms of the expected means of compliance. The strictest interpretation of the rule is not easily met, and it has not been uniformly applied. An ARAC group was established to address this and other elements of §25.671. The ARAC recommendation proposes to replace the current "single plus probable" criterion with a clearer standard.

An harmonized set of Failure Condition criteria for the flight control system, is recommended by the Aviation Rulemaking Advisory Committee (ARAC), for coverage of combinations of failures which are not shown to be Extremely Improbable, addressed by 25.671(c)(2).

Equivalent Safety Finding CS 25.671(c)(2) : Control System Large Aeroplane category

EASA Proposal:

In lieu of paragraph 25.671(c)(2), the following, as proposed in the ARAC recommendation, would apply:

"(c) The airplane must be shown by analysis, test, or both, to be capable of continued safe flight and landing after any of the following failures, including jamming, in the flight control system and surfaces (including trim, lift, drag, and feel systems) within the normal flight envelope, without requiring exceptional piloting skill or strength. Probable failures must have only minor effects and must be capable of being readily counteracted by the pilot.

…

(2) Any combination of failures not shown to be extremely improbable. Furthermore, in the presence of any single failure in the flight control system, any additional failure states that could prevent continued safe flight and landing shall have a combined probability of less than 1 in 1000. This paragraph excludes failures of the type defined in (c)(3)."

EASA Safety Equivalency Demonstration proposal

Definitions

- 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 (AMC 25.1309 5.o).
- Latent = dormant = hidden

In adopting a clear definition of acceptable risk level for subsequent failures, the approach recommended by ARAC has the advantage of

(1) addressing latency, and
(2) eliminating possible dubious judgments in the determination of probable failures.

However, it is not evident that this is sufficient to provide an ESF to the existing CS25.671(c)(2). Therefore, EASA proposes the following approach:

1) Double failures, with either one latent, that can lead to a Catastrophic Failure Condition shall be avoided in system design.

2) Latent failures contributing to Hazardous or Catastrophic repercussions should be avoided in system design.

3) 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", as per AMC 25.1309 9.c.6.

4) It is recognised that, on occasion, there may be no possibility to meet 1) and 2). In such cases:

   a) The remaining latent failures shall be recorded and justified in the PSSA/SSA and reviewed during the design review process for acceptance,

   b) Acceptance should be based on both previous experience and sound engineering judgement and shall assess:

i) the failure rates and service history of each component,

ii) the inspection type and interval for any component whose failure would be latent, and

iii) any possible common cause of cascading failure modes.

c) The integrity of the evident part of the significant failure condition shall meet a minimum standard:

i) For Catastrophic failure combinations comprising only one evident failure, the probability per flight hour of the evident part should be <= 10^{-5}/Fh, and

ii) For Hazardous failure combinations comprising only one evident failure, the probability per flight hour of the evident part should be <= 10^{-4}/Fh.

d) In addition, a Specific Risk calculation should be considered in accepting the presence of a latent failure. For each combination composed of one evident failure and latent failures and leading to a Catastrophic Failure Condition:

i) The probability of the latent part of the combination (e.g. “Sum of the products of the failure rates multiplied by the exposure time” of any latent failure) must be equal or less than $1x10^{-3}$ (=1/1000) on average.

e) The periodic maintenance checks, which may result from the compliance to this Specific Risk criterion (d), will be considered as CMR candidates, in addition to the CMR Candidates already selected for compliance to CS 25.1309.

The objective is to obtain a design with a minimum number of significant latent failures. Each significant latent failure will be highlighted in the system safety assessment, subject to review by the Authorities.