EASA	COMMENT RESPONSE DOCUMENT
	Proposed Equivalent Safety Finding to CS 25.671(c)(2) : Control System (Applicable to Large Aeroplane category)

Commenter 1 : Airbus

Comment #[1] – EASA Safety Equivalency Demonstration proposal

On sub-part 4.c), related to evident failure / evident part, Airbus consider that the criteria expressed needs to be develop to avoid any misunderstanding:
- It is Airbus understanding that the term of “evident” means “evident for the flight crew”.

[*It*] is to say that the effect of the failure is not hidden. In such a case, the failure is considered as an active one (by opposition to an hidden / latent failure unknown by the flight crew). Based on this definition:

- Assuming a combination of two failures with one evident/active and one hidden/latent, by application of criteria i) or ii) of sub-part 4.c), the probability per flight hour of the evident part is the probability per flight hour of the evident/active failure.

- Assuming a combination of three failures with one evident/active and two hidden/latent, by application of criteria i) or ii) of sub-part 4.c), does the probability per flight hour of the evident part still remain the probability per flight hour of evident/active failure?

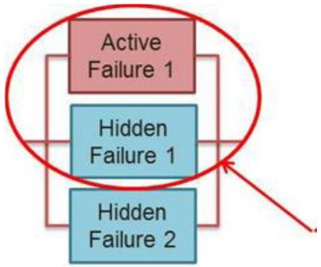
Comment :

Instead of current wording of sub-part 4.c), the following text is proposed :
In the event that there remain latent failures following application of the recommendations set out in paragraphs 1) and 2), the Specific Risk they represent to individual aircraft should be taken into consideration before acceptance.

The methodology for assessing the Specific Risk induced by latent failures consists of demonstrating that the system design is acceptably safe with the latent failures present.

One method of demonstrating that the design is acceptably safe is to assume that any individual failure which is not Extremely Remote (≤ 10^{-7}/fh) and is known to be latent and not detected at each flight or during daily check, has occurred prior to a given flight. During that flight, each Failure Condition which is Catastrophic and which involves that individual failure should be shown to occur at a rate less than or equal to 10^{-6} /Fh.
In addition, when one active failure is combined with two hidden ones, if advantage is taken from one latent failure to show compliance with this 10^{-6} objective, the cases for which the failure rate of the active part is higher than 10^{-4} per flight hour will be identified to the Authorities.
Similarly, each Failure Condition which is Hazardous and which involves that individual failure should be shown to occur at a rate less than or equal to 10^{-4} /fh.

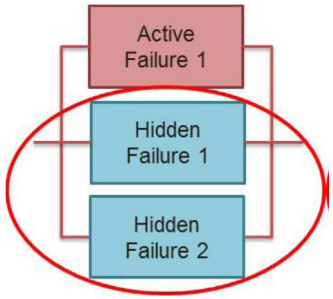
See example :



Assessment of any individual failure not Extremely Remote (≤ 10^{-7}/fh) and known to be hidden and not detected at each flight or during daily check, has occurred prior to a given flight.
Hidden Failure 2 is the individual failure :

- **(A1, H1) ≤ 10^{-6} /fh (CAT) / 10^{-4} /fh (HAZ)**

In the same way, sub-paragraph 4.d) could be illustrated as followed:



To be considered if A1 is the active failure:

- **P(H1, H2) ≤ 10^{-3}**

EASA response:
Noted - request for definition of "Evident". "Latent" is defined in AMC 25.1309 and in the ESF itself. Evident is the opposite.

In the sentence "Double failures, with either one or both latent, that can lead to a Catastrophic Failure Condition shall be avoided in system design.", propose to remove the words "or both", as this is confusing.

Proposal is PARTIALLY ACCEPTED - We believe that the proposed wording from Airbus has the same result as the existing Generic ESF, but EASA prefer to keep the existing wording. Airbus could propose to use the above wording for such an ESF on a specific project in the future.
The exception to this is that the exception for Latent failures <1E-07 is not acceptable. The criteria is also to be applied to combinations involving an Extremely Remote individual Latent Failure.

Comment #[2] – EASA Safety Equivalency Demonstration proposal

The term of "*active*" failure is used in the sub-part 4.d).

Comment
Should "*active*" and "*evident*" have the same meaning, Airbus recommend to use uniform term.

EASA response: Agreed
Need to be consistent. Evident is the same as Active, in the context of this ESF. Term "Evident" to be applied consistently.

Commenter 2 : Boeing Commercial Airplanes

Comment #[1} – Statement of issue

Part of the justification for ASAWG ARAC was to harmonize the specific risk related requirements in a way to make them consistent and to reduce the proliferation of inconsistent criteria. This ESF contradicts the criteria developed by the ASAWG ARAC (proposed in NPA 2014-02) and the spirit with which it was developed.

Comment :
The proposed generic ESF to CS 25.671(c)(2) includes additional, new specific quantitative and qualitative 25.671(c)(2) compliance criteria that go significantly beyond the current and draft harmonized 25.671 and 25.1309 rules and advisory material.
These additional criteria have been developed by EASA outside of the Aviation Rulemaking Advisory Committee covering flight control systems and other established rulemaking processes. Therefore, EASA is requested to submit any proposed generic ESF to CS 25.671(c)(2) to the ARAC covering flight control systems for review and development in accordance with established rulemaking processes.

EASA response: Disagreed

The term "Significantly" in the Boeing position is subjective.
Besides, the proposals are consistent with NPA 2014-02 and are to be replaced by the NPA when it is in place.
This Generic ESF comes from applicants' request to use 1/1000 criteria for 25.671c2, which alone is not considered sufficient.
The Generic ESF has been applied to a number of recent CS25 programmes, without difficulty in showing compliance. Thus we do not consider it to be onerous.

Comment #[2] – Statement of Issue (paragraph 4)

"…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.."

This is not criteria in the regulation, but an example of a "combination of failures not shown to be extremely improbable".

Comment :
Rather than provide an interpretation that expands an example statement so broadly as to incorporate a new compliance standard, specific risk, suggest that the parenthetical example just be removed. The Statement of Issue should reflect this.

EASA response: Disagreed
This is a direct quote from the CS, merely an example, and to remove these words would require future rulemaking. Thus, it remains. Note that the same wording exists in 14 CFR 25.

Comment #[3] – EASA Proposal (25.671(c)(2)

This criterion was proposed by the ARAC FCHWG. However, this criterion was not proposed by the ARAC ASAWG committee and would be in conflict with the NPA 2014-02 criteria that EASA proposed from the results of the ASAWG committee.

Comment :

The current wording :
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 and additional criteria:
1) Double failures, with either one or both 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.

is proposed to be amended as followed :

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 and ***basic objectives*** *:*

1) *Double failures, with either one or both 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.*

EASA response: Partially Agreed
There is no conflict with the ARAC FCHWG report. EASA is simply asking for slightly more, as has been applied successfully on a number of recent programmes.
The wording will be amended so it is neither "additional criteria" nor " basic objectives" : i.e. a full-stop after "…following approach".

Comment #[5] – EASA Safety Equivalency Demonstration proposal (Item 4a,b,c,d, and e)

"Shall be avoided" and "should be avoided" are subjective and not verifiable criteria, hence are not appropriate criteria to be perpetuated in an ESF. Treat them as objectives similar to Fail-safe design concepts described in AMC 25.1309.

4a) "Deviation" has specific regulatory meaning to EASA, and is used incorrectly here.

4c) to 4e): Boeing position is that specific risk criterion should not be perpetuated in specific regulations, but be applied equally across systems and therefore belong in 25.1309. This is consistent with findings of the ARAC ASAWG.

Comment :

The current wording :

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 and additional criteria:

1) *Double failures, with either one or both 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 comply with the above criteria 1) and 2). In such cases:*

   a) *The deviation 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 active 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.

is proposed to be amended as followed :

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 and ***basic objectives*** ~~*additional criteria*~~*: 4) It is recognised that, on occasion, there may be no possibility to* ***avoid the conditions described in*** ~~*comply with the above criteria*~~ *1) and 2). In such cases:*

a) The deviation 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 judgment 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 evidentpart 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 active 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 CS 25.671(c)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.

EASA response: ***(1) Partially Agree, as per previous comment: neither "basic objectives" nor "additional criteria" will be used.*** ***(2) Partially Agree – "avoid the conditions described in ~~comply with the above criteria"~~ will be amended to "Meet 1) and 2)".*** ***(3) Agree "deviation" is wrong word. "Remaining latent failures" is proposed instead.*** ***(4) Disagree for 4c to 4e. At this stage the approach is applied only to the Flight Control Systems (FCS), this being the subject of 25.671 and the ESF. EASA position is that a specific approach is needed for the FCS, given the exceptional criticality of this system. Again, it is to be noted that this approach has already been successfully applied to a number of programmes.***