DOCUMENT COMMENT LOG

Document Title: EASA NPA- 2014-02: 'Specific risk and standardised criteria for conducting aeroplane-level safety assessments of critical systems'

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**§3.1 C25.671(d) §3.2 AMC25.671 section 5**	The definition of a "suitable runway" should be established in AMC25.671. It should be noted that with loss of all engines, and thus thrust reversers, the landing distance can be expected to be increased.	**Add a definition to AMC25.671: Suitable runway - a runway with the lateral dimensions, length and load bearing capability which meets the requirements defined in the Emergency procedures of the Airplane Flight Manual.**
Textron Aviation	**§3.1 CS25.671(e)**	The added requirement that "The flight control system must be designed to ensure that the flight crew is aware whenever the primary control means is approaching the limit of control authority." is overly restrictive for a purely mechanical system where the limit of control authority is defined by 25.143	**change 25.671(e) to "A powered flight control system must be designed to ensure that the flight crew is aware whenever the primary control means is approaching the limit of control authority."**
Textron Aviation	**AMC 25.1309 6.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 wording of this sentence seems awkward as indicated by the mark-up. It could be read to imply that all subsequent failures, regardless of probability, must be assumed to happen on the same flight. This would be an unbounded requirement with no real value to the safety process so we assume this is a wrong reading of it and request that it be clarified.	**Correct and/or clarify requirement.**
Textron Aviation	**AMC 25.1309 9.c Compliance with 25.1309(c)**	"The required information may be provided by dedicated indication and/or annunciation or made apparent by the inherent airplane responses." This is a reasonable statement but it directly conflicts the proposed language of the rule which does not allow for "inherent airplane responses". We would suggest changing the rule to recognize additional methods of providing information to the flight crew.	**Modify 25.1309(c) to allow credit for crew information from sources other than "alerting systems" per 25.1322.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**AMC 25.1309 9.c Compliance with 25.1309(c)**	"Any system operating condition which, if not detected and properly accommodated by crew action, would contribute to or cause one or more serious injuries should be considered as an 'unsafe system operating condition'." This would seem to require yet another system of classification for the hazards to the aircraft. Is there a compelling safety case for not aligning this requirement with established hazard classifications under 25.1309?	**Align unsafe system operation condition effects with other 25.1309 criteria.**
Textron Aviation	**AMC 25.1309 9.c.(2) Compliance with 25.1309(c)**	"but the loss of annunciation should be considered a major failure condition" The NPA provides no real justification for this requirement. There are many cases where the best design solution is a robust means of providing a function (like 10E-7) and then a single path warning system (10E-4) for the rare3 time that robust solution fails. How is this less safe (note that the example actually meets 10E-11 if adequately independent) than a 10E-5 solution with a 10E-5 annunciation?	**Remove added requirement of annunciation being "major".**
Textron Aviation	**AMC 25.1309 11e.(1)(v)**	Note that the title of 11.e is "Calculation of **average** [emphasis added] Probability per Flight Hour": what is the justification for using "maximum" exposure time for latent failures?	**Remove change to "maximum" exposure time for latent failures; return it to "average".**
Textron Aviation	**CS 25.933**	This NPA seems to be codifying into the EASA CS 25.933 regulation the same requirements that the FAA has been enforcing through issue papers and that EASA was providing guidance through the AMC for thrust reversers certified by reliability. As the regulation still allows for compliance by controllability as an alternate means, those aspects do not seem to be affected by this NPA.	**None**
Textron Aviation	**CS 25.629**	The proposed amendment is adding a new requirement, "and for the load factors specified in CS 25.333". The rationale for this additional requirement is not addressed in section 2.4, "Overview of the proposed amendments"	**Propose deletion of , "and for the load factors specified in CS 25.333":**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**CS 25.1309 Additional requirement (b) (4).**	Difficult to show compliance to "minimized to the extent practical". Even the AMC wording is vague with references to past experience and sound engineering judgment etc. The AMC states "There can be situations where it is not practical to meet the 1/1000 criterion. For example, if meeting this criterion would result in performing complex or invasive maintenance tasks on the flight line, thereby increasing the risk of incorrect maintenance." The AMC states that it is not expected to see a demonstration of compliance but that the minimization of significant latent failures is rather expected to be an integral part of each applicant's normal design practices. It is not clear how compliance can be shown with regards to "minimization" and "sound engineering judgment".	**Propose deleting this requirement because it would put an extra burden on the applicant when it only amounts to being a verification of the applicants normal design practices.**
Textron Aviation	**CS 25.1309 Additional requirement (b)(5**	Difficult to see how it can be shown that additional fault tolerance is impractical. Given that other proposed changes to CS 25.1309 are attempting to remove ambiguity, this change seems to be adding ambiguity.	**Propose that this section be re-written to remove the ambiguity.**
Textron Aviation	**CS 25.1309(c) Reworded requirement**	Deletion of "warning indication" and replacing with the crew alerting specific with CS 25.1322 deprives the analysis the ability to take credit for other means of indicating problems to the flight crew. It is possible some unsafe system operating conditions may result in, for instance, severe vibration. Or another example would be an abrupt departure from flight attitude (sudden roll or pitch). By requiring a specific crew alerting means (visual and/or aural) for each unsafe system operating condition, additional sensors and CAS (crew alerting) messages within the avionics system are required. These additional CAS messages for failure events that are obvious to the flight crew by tactile or other means would result in issues such as • More CAS messages to clutter the display • Increase weight to accommodate sensors • Increase complexity to accommodate sensors • Additional testing to show the CAS message works as intended, and is set at a point to allow flight crew response before the failure condition severity would increase. • Additional analysis to support the CAS message. • Additional analysis to ensure the new sensors does not have adverse effects on the airplane.	**Propose that the phrase "warning indication" be retained.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**CS 25.671(c)**	Change removes the language about "exceptional piloting skill and strength," however that phrase appears in other regulations. "Exceptional piloting skill and strength" is also struck from NPA AMC 25.671 Section 9 2nd paragraphs. However, NPA AMC 25.671 Section 9e1i 1st paragraph does state that CSFL procedures should not require exceptional piloting skill or strength.	**Propose that the words "exceptional piloting skill and strength" should be retained.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**CS25.671(c)(3) AMC 25.671 Section 9b 2nd paragraph AMC 25.671 Section 9c**	With regard to a single mechanical disconnect failures or jam, it should be acknowledged that there is some point in the approach, past which if the failure were introduced with the other criteria established in the AMC, recovery may not be able to be demonstrated within the time delays stated. Currently CS25.671(c) (3) allows an applicant to consider a jam is Extremely Improbable during any flight phase. The proposed CS25.671 (c) (3) removes this allowance, but specifically includes it in the jam evaluation for just before landing. However, it states that the use of a risk time in determining Extremely Improbable is not acceptable. "NPA AMC 25.671 Section 9c's opening paragraph attempts to describe the difficulty in dealing with jams in the landing phase without giving much additional information on what makes jams in the landing phase problematic from a compliance standpoint (namely, the time delays imposed by the AMC). Given a finite time (hence altitude) to recover from a jam (esp. given the delay times stated in the AMC), there is no practical means by which recovery could be demonstrated for compliance all the way to touchdown, for a jam occurring just prior to touchdown. There is some point in the approach past which a compliance demonstration of recovery could not be assured when delays are considered. AMC 25.671 Section 9c does state two conditions where jams in the landing phase may be shown to be Extremely Improbable, however one will be impossible to comply with, and the other will become a source of inconsistency between certification agencies and ACO's. In the first condition in AMC 25.671 Section 9c, states jams in the landing phase should be shown to be extremely improbably using relevant reliability data from in-service experience, without considering "risk time" in this determination; the jam itself must be 10e-9, without considering "risk time". Such a standard will be impossible to comply with. Even during the FCHWG deliberation, in-service data showed a jam probability of approximately 10e-7 (FCHWG Section 9 paragraph 6). Furthermore, no OEM has sufficient service history to justify a 10e-9 jam probability. In the second condition in AMC 25.671 Section 9c2, jams in the landing phase should be shown to be extremely improbably by a qualitative assessment covering the design features intended to prevent jams, and a description of the means by which a jam could be alleviated. Unfortunately, the AMC provides no guidance on what types of design features would be considered adequate. Further, how does this qualitative assessment and description differ from that already required for compliance with the "prevention of jams" language of CS 25.685(a)? Lacking objective guidance this will become a source of inconsistency between certification agencies and ACOs. It is believed that the failure rate of a single mechanical disconnect in a primary flight control system is similar to that of a flight control jam. Consistency would require that both be excluded from showing CSFL in this small exposure time. Yet, the proposed AMC25.671(c) (I) does not allow a probability assessment to exclude this disconnect condition or a specific exclusion as in proposed FAR 25.671 (c) (3) (ii) for jams. Applicants have historically not been required to evaluate this type of disconnect failure just before touchdown for FAA certification. Current JAA 25.671(c)(I) would allow an applicant to consider a mechanical disconnect in this small time exposure Extremely Improbable	**Propose that the single mechanical disconnects and jams should be re-evaluated and allowance given for the small time exposure immediately before landing. There is sufficient experience to allow single mechanical disconnects and jams occurring immediately before landing to be allowed to be considered extremely Improbable based on the small exposure time immediately before landing.** **Adopt the FCHWG 25.671(c) (ii) language which excluded jams "during the time immediately before landing where recovery may not be achievable when considering time delays in initiating recovery. In addition, adopt the language of FCHWG AC 25.671 Section 9b 2nd paragraph, which provides the rationale for the exclusion in the regulation.** **Remove the language of AMC 25.671 Section 9c which excludes consideration for a jam on landing only if it can be shown to be extremely improbable without considering the limited risk time of the landing phase. Alternately, any such extremely improbable determination should inherently include the limited risk time of the landing phase.** **Remove the language of AMC 25.671 Section 9c2 which excludes consideration for a jam on landing following a qualitative assessment of the design features intended to prevent jams as it is redundant with CS 25.685(a). Alternately, provide objective guidance on what types of features are considered adequate to exercise this exclusion.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**AMC 25.671**	While part of the NPA state that the 1/1000 combined with "remote" (10e-5) failure rates only need to be for two failures leading to HAZ/CAT, the example presented in the NPA has numerous failures in the fault tree, not just two.	**Please clarify.**
Textron Aviation	**AMC 25.671**	Since the "1 in 1000" criteria is new, it could potentially be miss-understood, therefore it would be useful to provided examples on how the new "1 in 1000" criteria should be interpreted and applied. This could prevent unintended interpretations/applications of "1 in 1000."	**Propose examples be provided on how the new "1 in 1000" criteria should be interpreted and applied.**
Textron Aviation	**AMC 25.671 Section 5k5**	NPA AMC 25.671 Section 5k5 breaks runaways and handovers into two different types. The 1st paragraph talks about failures internal to the airplane, and states that they are handled addressed under CS 25.671(c) (1) and (c) (2). The 2nd paragraph talks about external events which may cause a runway and that they are dealt with under CS 25.671(c) (4). How a runaway/hardcover happens should not be cause to treat them under different paragraphs. Whether caused internally or externally, the end effect on the airplane is the same. Hence they should be handled under the same regulation. Splitting runaways/handovers into two different classes adds unnecessarily complications and adds needless work to the OEM and certification authorities. FCHWG's proposed FAR 25.671(c)(4), proposed AC 25.671 Section 5k5, and proposed AC 25.671 Section 9d treated all runaways/handovers, whether internal or external, the same.	**Propose eliminating the two classes (internal/external) of runaways from the NPA and treat all runaways/handovers the same.** **Propose deleting "…that is caused by an external source" from CS 25.671(c) (4).** **Propose changing "…under CS 25.671(c) (1) and (c) (2)" in AMC 25.671 Section 5k5's 1st paragraph to "under CS 25.671(c) (4)."** **Propose deleting the 2nd paragraph of AMC 25.671 Section 5k5.** **Propose adding FCHWG's AC 25.671 Section 9d titled "Runaway to an Adverse Position – FAR/JAR 25.671(c) (4)."**
Textron Aviation	**AMC 25.671 Section 9a**	NPA AMC 25.671 Section 9a 3rd paragraph indicates that "single probable" remains, as it states "…following should be assumed to occur and be addressed within the scope of CS 25.629: any dual power system failure, any single failure in combination with any probable failure, any single failure in combination with any power system failure." However, with the words "within the scope of CS 25.629.", does this mean that those "single probable" combinations only need to be shown flutter-free under 25.629, but need not be held to the CSFL standard of 25.671?	**Propose clarification be provided that those "single probable" combinations only need to be shown flutter-free under 25.629, but need not be held to the CSFL standard of 25.671?**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**AMC 25.671 Section 9b 6th paragraph AMC 25.671 Section 9b1iii**	NPA AMC 25.671 Section 9b1iii (and the 6th paragraph of Section 9b) adds consideration for jammed lateral control during the landing flare during a 15knot crosswind, but states that it's to maintain wings level. Pilot's using a "kick out" crosswind landing technique may not even input much, if any, of a lateral control input as the wings are generally level in the crabbed approach anyway. A pilot using the "wing-low" crosswind technique would not be maintaining wings-level as that would cause the airplane to drift across the runway. Hence, the proposed criteria is pilot-technique dependent (at best). Furthermore, the deflection will be based on the airspeed (i.e., as airspeed decreases, deflection would need to increase). Compared with the other, objective/performance-based criteria of the AMC, this particular criterion is open-ended, vague, and subject to pilot technique, which will lead to differing interpretations by OEMs and certification authorities. (Compare the proposed criteria to Section 9b1i, which also is the deflection for wings-level in a cross-wind, but specifies a speed of V1. In that case, the stated airspeed eliminates the variation of deflection with different airspeeds. Furthermore, at V1 the aircraft is still on the ground, hence pilot technique is not as relevant as the landing flare.)	**Propose removing AMC 25.671 Section 9b1iii.**
Textron Aviation	**AMC 25.671 Section 9b2iii**	NPA AMC 25.671 Section 9b2iii adds consideration for jammed longitudinal control during the landing flare, without providing guidance for pilot technique. (Compare this to Section 9b2i, where an objective pitch rate is provided, these minimizing differences due to pilot technique.) Pilot's using an aggressive flare for minimal sink rate will have a significantly different longitudinal control position than one performing a minimal flare with subsequent firmer touchdown. Compared with the other, objective/performance-based criteria of the AMC, this particular criteria is open-ended, vague, and subject to pilot technique, which will lead to differing interpretations by OEMs and certification authorities	**Propose removing AMC 25.671 Section 9b2iii.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**AMC 25.671 Section 9b3iii**	NPA AMC 25.671 Section 9b3iii adds consideration for jammed directional control during the landing flare during a 15knot crosswind, yet does not give allowance nor guidance on how the landing is to be conducted, which will result in the surface deflection being highly pilot-technique dependent. Pilot's using the "wing-low" crosswind technique may have a significantly different directional control position than a pilot using a "kick out" crosswind landing technique. (Furthermore, the deflection will be dependent on airspeed: slower airspeed, until NWS becomes effective, would result in larger deflections once on the ground.) Compared with the other, objective/performance-based criteria of the AMC, this particular criterion is open-ended, vague, and subject to pilot technique, which will lead to differing interpretations by OEMs and certification authorities.	**Propose removing AMC 25.671 Section 9b3iii.**
Textron Aviation	**AMC 25.671 Section 9e2ii 4th paragraph**	NPA AMC 25.671 Section 9e2ii 4th paragraph states "Local structural failure (e.g., via mechanical fuse or shear out) that could lead to a surface departure from the aircraft should not be used as a means of jam alleviation." While in principle this seams a reasonable addition, it seems buried in the text as it is under a section covering "structural strength for flight control system failures." A better place for such language would be where the jams, procedures following a jam, and controllability following a jam is discussed (earlier in Section 9).	**Propose moving to earlier in Section 9 where jams, procedures following a jam, and controllability following a jam is discussed (i.e., not buried in a section dealing with structural strength).**
Textron Aviation	**AMC 25.671 Section 9e2iii**	NPA AMC 25.671 Section 9e2iii adds "a flexible aircraft model should be used for loads calculations." Depending on the aircraft, fully-flexible loads models may not always be used, on all axes. Some OEMs may use a flexible model on some axes (pitch and roll) where aeroelastic effects may be more pronounced, but rigid models on other axes (yaw) where aeroelastics are not significant. Requiring a flexible loads model on all axes would increase the analysis burden on the OEM, likely with no increase in loads fidelity or safety.	**Propose removing the sentence "A flexible aircraft model should be used for loads calculations."**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**CS 25.671(d)(4)-(5) AMC 25.671 Section 10b5**	NPA AMC 25.671 Section 10b5 adds the ground controllability and deceleration capability. However, the NPA is vague in its acceptance criteria for ground control and deceleration: How much lateral deviation is allowed for ground control and still be acceptable? How much deceleration is needed to be acceptable? NPA AMC 25.671 Section 10b5 states "positive deceleration" must be provided, but if that deceleration was only 5% of normal braking deceleration, would that be acceptable?	**Propose removal of ground controllability and deceleration capability from the effect of all-engines out on the flight control systems and leave "aircraft controllability up to the point of touchdown in a landing flare". Reinstate the "to the point of touchdown" language from FCHWG FAR 25.671(d) and FCHWG AC 25.671 Section 10a and Section 10b1-4**
Textron Aviation	**AMC 25.671 Section 11a**	NPA AMC 25.671 Section 11a adds "whether or not it is pilot-commanded." FCHWG was "not pilot-commanded." NPA language would require near-full-authority annunciation even in cases when it was pilot-commanded. Wouldn't an annunciation of near-full-authority, while the pilot is commanding that authority, be distracting?	**Propose replacing "whether or not it is pilot-commanded" with "not pilot-commanded" per the FCHWG draft AC.**
Textron Aviation	**AMC 25.1309 Section 4h**	Does the addition of NPA AMC 25.1309 Section 4h mean that the airplane OEM now has to consider means within the airplane/systems to prevent such external hazards? If so, does that mean some sort of sensor forward of the nacelle which would be tied into an engine's run/stop logic? While this may potentially address the risk to ground crew, it may increase the risks to the airplane/occupants by yielding additional failure modes which could shutdown an engine in-flight. This seems to overreach the control that an OEM would have on such ground operations.	**Propose removing external ground operations hazards to persons other than the occupants/crew. Ground operational procedures (i.e., beacons on when engines running, ground crews clearing the area around the nacelle prior to engine start, ramp markings for engine ingestion zones) are better suited to such hazards than additional airplane systems.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**AMC 25.1309 Section 5v**	NPA AMC 25.1309 Section 5v (and NPA CS 25.1309(b) (4)) introduces the concept of a "Significant Latent Failure" as a latent failure which would, in combination with one or more specific failures or events result in a Hazardous or Catastrophic Failure Condition. While the concept of a "Significant Latent Failure" may be understood to mean a latent failure which carries more importance because it may be the last remaining part of a fault tree guarding against HAZ or CAT failures, as worded this is unclear. Many HAZ/CAT fault trees contain latent failures requiring inspection intervals. As defined in NPA AMC 25.1309 Section 5v, ALL of the latent failures in ANY fault tree leading to HAZ/CAT top event are "Significant Latent Failures" because they, in combination with one or more failures or events, results in HAZ/CAT. If "or more failures" were struck from the definition, the increased importance of the Significant Latent Failure would be justified as that latency, coupled with one other failure, could result in HAZ/CAT, and hence deserves potential additional scrutiny. Is the intent to have ALL latent failures in ANY fault tree leading to HAZ/CAT being considered "Significant,"?	**Propose striking "or more failures".**
Textron Aviation	**AMC 25.1309 Section 6bii**	NPA AMC 25.1309 Section 6bii adds "effect of combinations of failures that are not extremely improbable should not be catastrophic" is redundant as that concept is already covered in the concept of severity vs. frequency of occurrence in the broader existing CS 25.1309 and guidance material	**Propose deleting the last sentence of AMC 25.1309 Section 6bii "The effect of combinations of failures…not extremely improbable…not be catastrophic." as it is redundant with the concept of severity vs. frequency of occurrence already part of CS 25.1309 and related guidance.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**CS 25.1309(b)(5) AMC 25.1309 Section 8c3**	NPA AMC 25.1309 Section 8c3 (and NPA CS 25.1309(b) (5)) adds that for catastrophic failure conditions, resulting from two failures, either of which is latent for more than one flight, "is remote when either one is pre-existing." Since the existing AMC 25.1309 Section 7c1ii defines "remote" as a failure rate less than 10e-5 but greater than 10e-7, the addition is more severe than the former "single + probable" interpretation, which only required failure rates less than 10e-5. The FCHWG sought to remove "per flight hour" and "failure rate" terms and rather focus on probabilities (which include inspection intervals, failure rates, and flight durations) by introducing the concept of "1 in 1000" – which the proposed NPA language seeks to undo. While the initial impetus for "1 in 1000" was for just such conditions where two failures (either of which could be latent) could lead to a CAT event, the "1 in 1000" concept was broad enough that it would and did apply to any combination of failures. Furthermore, NPA CS 25.1309(b) (5) (iii) states that in addition to the "remote" criteria, the probability should be less than 1/1000 for the latent's only. The FCHWG's 1/1000 applied to all additional failures, latent or active.	**Propose striking the NPA language in favor of a broad "1 in 1000" criteria, (per the FCHWG) which would cover the underlying reason for the NPA addition, in a more straightforward manner. There appears to be nothing gained by a "remote" as well as a "1/1000" criteria.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**AMC 25.1309 Section 9b6i**	NPA AMC 25.1309 Section 9b6i seems needlessly circular and vague, with opportunities for inconsistent application among OEMs. First, "A" says significant latents should be eliminated to the extent practical. "B" says if it cannot be practically eliminated, the latency should be <1/1000 (i.e., failure rate * inspection interval). "C" says that if "1/1000" cannot be practically met, it should be minimized. This seems like a circular argument: minimize to be less than 1/1000 unless it can't be less than 1/1000, in which case minimize. Second, if the "Significant Latent Failure" definition of NPA AMC 25.1309 5v really is intended to capture ALL latent failures in ANY fault tree leading to HAZ/CAT are considered Significant, imposing the 1/1000 criteria on EACH of those Significant latent failures in the fault tree will likely force shorter inspection intervals (which may increase chances to introduce failures as part of the inspection). Furthermore, the resulting top event probability is likely to be *significantly* less than 10e-9; and what is gained by making an extremely improbable event even more extremely improbable? Third, the last paragraph of NPA AMC 25.1309 Section 9b6i says that dedicated compliance with the "significant latent failures" provisions above is not expected to be a dedicated demonstration of compliance, but rather only "where the Agency identifies a…failure of concern and deems it practical to eliminate or further reduce the exposure…" This seems to mean that compliance is "not required, until it is required by the agency" with the onus on the applicant to justify impracticality of meeting 1/1000. If minimization criteria are to be the standard, then it should state such. If a 1/1000 criteria is to be the standard, then it should state such.	**Propose the 1/1000 standard be applied (per the FCHWG) at the top-event level, not at the component failure level of the latent failure. As worded, it is neither. Furthermore, if it is to be a standard, then it should be applied rather than to state a "standard" which later is described as "not expect a demonstration of compliance" which seems to not be a standard.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**AMC 25.1309 Section 9b6ii**	NPA AMC 25.1309 Section 9b6ii also applies a dual standard of 1/1000 on the latency itself (as does Section 9b6i), as well as "remote" on the other failure of the dual failure combination leading to HAZ/CAT. Assuming Section 9b6i stands and the circular argument with it resolved the 1/1000 on the latency in Section 9b6ii is redundant as it is already covered under Section 9b6i. Furthermore, imposing an additional "remote" criteria is more severe than the former "single + probable" interpretation, which only required failure rates less than 10e-5, since existing AMC 25.1309 Section 7c1ii defines "remote" as a failure rate less than 10e-5 but greater than 10e-7. However, the last paragraph of NPA AMC 25.1309 Section 9b6ii seems to redefine "remote" as being 10e-6, not 10e-5. The language of NPA AMC 25.1309 Section 9b6ii is confusing as it speaks to "the *sum of all subsequent* single active failures" and yet the opening sentence of Section 9b6ii says it's for "CAT…involving *two* failures…" If it were conditions of *two* failures, one of which could be remote, then there would be no "*sum* of subsequent failures"…there would be merely "the remaining active failure." Either this applies to specific cases of *two* failures leading to a CAT, in which case the remaining failure would have to pass the "remote" criteria (i.e.,. there would be no "summing" of one failure rate), or if the "sum of subsequent failures" must pass "remote" criteria, then is this really limited to special cases where only two failures could lead to CAT? The math at the end of NPA AMC 25.1309 Section 9b6ii 4th paragraph mixes probability and failure rate, which neglect the flight duration. The original intent of FCHWG's "1/1000" was to also capture the remaining flight time in the calculation. Meaning that the top event probability be 1/1000, which for a long duration flight would drive the need for lower failure rates depending on the flight duration. In other words, flight duration is taken into account in the 1/1000 probability. The NPA places a "probability of 1/1000" on the latent failure, claiming that it would drive the active failure's failure rate…as well as stating that the "remote" criteria on the active failure could drive the failure rate of latency in order to meet its 1/1000…but neither description considers the flight duration.	**Propose striking the NPA language in favor of a broad "1 in 1000" criteria, as proposed by FCHWG, which inherently includes the flight duration, and would cover the underlying reason for the NPA addition, in a more straightforward manner. There appears to be nothing gained by a "remote" as well as a "1/1000" criteria.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**25.671d**	The aircraft brake and nose wheel steering systems are designed to meet the specific certification requirements under CS25.735 and CS25.745, respectively. CS25.671 is a control system specific paragraph and should not be expanded to include aircraft level safety requirements. The aircraft level safety requirements are already adequately defined under CS25.1309.	
Textron Aviation	**25.671d**	Items d (1) thru d (5) do not include use of the word "landing" in reference to ground operations. As such it is understood that the specific definition of "landing" in section 5d is not invoked to add requirements above the system specific requirements of CS25.735 and CS25.745 and aircraft level safety requirements of CS25.1309.	**Confirmation in discussion published with this rule that it is not the intent to levy additional requirements in place of system specific rules, but to require that dual engine failure does not disable both primary and emergency means of aircraft directional control.**
Textron Aviation	**CS 25.1309**	Object to "(4) Any significant latent failure is minimized to the extent practical; and" because the requirement for meeting the rule is not clear and unambiguous. As a result, it is to open for interpretation by the authorities and will create an unlevel level of safety across different aircraft OEMs.	**Recommends that this be struck or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**
Textron Aviation	**For CS 25.1309**	Object to (5)(iii) because it violates one of the constraints imposed by TAEIG on the ASAWG tasking, that average risk would not be changed as a result of this tasking(!). This is a re-occurring theme in this proposal, and Cessna finds this an over reach by EASA and very troubling. The proposed (5) (iii) changes the use of average risk in the calculations to the risk on the last flight before the inspection to check against the latent failure. This approach is not supported by SAE ARP 4761, the Arsenal Draft of AC 25.1309-1B or by AC 23.1309-1E.	**Recommends that this be struck or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**AMC Subpart E Powerplant**	, "RELIABILITY OPTION": PROVIDE CONTINUED SAFE FLIGHT AND LANDING BY PREVENTING ANY IN FLIGHT THRUST REVERSAL, It should be pointed out that no credit is given for the consideration of fuselage mounted engines and the moments that they can produce compared to wing mounted engines. In our recent certification activity dealing with thrust reversers, the reliability option was not allowed, and Cessna had to demonstrate an in flight deployment. The effect on the aircraft and crew was not worse than minor for some flight phases, but we were not allowed to change the functional failure condition to agree with the results from flight test (!). This is not a consistent application of the requirements, and Cessna's position that the following change "Latent failures involved in unwanted in-flight thrust reversal should be avoided whenever practical. The design configurations in paragraphs 8.b. (2) and 8.b. (3) have traditionally been considered practical and deemed acceptable to the Agency." Cessna's position is that this statement is not clear and unambiguous. As a result this will introduce more inconsistency from aircraft OEM to OEM and not increase the overall level of safety.	**Recommends that this be struck or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**
Textron Aviation	**AMC Subpart F – Equipment, AMC 25.1309**	, "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." Cessna objects because the problem is not bounded by probability or cutsets. So any latent, even one in a 4th order cutest with a probability of 1e-13 when all the other failures are active becomes a significant latent failure. Cessna is not convinced that the modern tools can generate an exhaustive cutest listing, and, therefore, is not clear how to show compliance to this requirement.	**Recommends that this be struck or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**
Textron Aviation	**AMC Subpart F – Equipment, AMC 25.1309,**	"8. SAFETY OBJECTIVE (c) (3) Each Catastrophic Failure Condition, resulting from two failures, either of which is latent for more than one flight, is remote when either one is pre –existing". Cessna objects to the change based on the industry position voiced by ASAWG that this could lead to a "balanced fault tree" requirement where, for small part 25 business jets, the business model (i.e. warranty costs) drive us to design systems in that manner. Other, larger, OEMs don't have the same business model (scheduled airlines) and the "balanced trees" concept was not identified by ASAWG as a problem that ASAWG needed to address. This appears to be an attempt by EASA to "back door" a requirement to address a perceived problem. Again, where is the problem statement?	**Recommends that this be struck or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**AMC Subpart F – Equipment, AMC 25.1309 (b) (6)(i)**	Last paragraph. "The Agency does not expect a dedicated demonstration of compliance with CS 25.1309(b) (4). The minimization of significant latent failures is rather expected to be an integral part of each applicant's normal design practices. During review of the system safety analyses that demonstrate compliance with the other provisions of CS 25.1309(b), if the Agency identifies a significant latent failure of concern and deems it may be practical to eliminate or further reduce the exposure to that latent failure, then the applicant will be required to provide justification of impracticality. Justifications should be based on past experience, sound engineering judgment, or other reasonable arguments". Cessna does not support this position for several reasons; first, it is subject to interpretation by the regulatory agency. So it will not be uniformly applied, what may be OK for one applicant based on subjective criteria, may not be acceptable for another. This does not support the goal of a harmonized approach for safety and could drive changes to type design after a product has entered into service on one design, adding costly design changes without a commiserate benefit to safety, while not requiring any design changes to the other. Second, EASA seems to blurring the lines between the finding of compliance and the showing of compliance. This will likely lead to a discussion with the authorities on when an applicant is done. Again, both of these requirements for showing compliance to the rule are not clear and unambiguous	**Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**
Textron Aviation	**AMC Subpart F – Equipment, AMC 25.1309 (b) (6)(ii)**	Do not support the following statement, "In numerical terms, compliance with CS 25.1309(b)(1) and CS 5.1309(b)(5) together means the residual risk, i.e. the sum of all subsequent single active failures, must be on the order of 1x10-6 per flight hour when the latency is limited to 1/1000 to satisfy the Extremely Improbable safety objective. Conversely, if the reliability of the only residual component is 1x10-5 per flight hour, then latency is limited to a maximum probability of 1x10-4". During the ASAWG tasking, no consensus could be reached on what was meant by "on the order of". Industry had one perspective that worked for their sized product and the regulators had a different perspective that "would be acceptable" but there was no overlap between the two groups. Since there was no consensus, an industry member that signs up for this does not have a clear set of requirements to design to. So again, harmonization does not apply; the pass fail criteria are not clear and unambiguous.	**Recommend that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**AMC Subpart F – Equipment, AMC 25.1309 (c)**	Do not support the proposal that loss of annunciation is no worse than Major, and proposes that the crew action based on the annunciation be dealt with by showing compliance to 25.1302 (Human Factors). Cessna does not support the use of the term "unsafe operating condition" and in the interest of increasing safety or at least keeping the approach uniform across applicants, proposes that EASA and FAA coordinate on a term and definition that is usable and consistent. Such as "conditions requiring warning", and limit those to functional failure conditions that are Hazardous, since Catastrophic failure conditions are not required to be annunciated, and for our class business jets, the death of a single individual has been defined as Catastrophic by the FAA.	**Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**
Textron Aviation	**AMC Subpart F – Equipment, AMC 25.1309 (e)**	Do not support the proposal in (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", this should be based on the published methods in SAE ARP 4761, and not changed at the whim of the regulators without explanation or rationale. At the very least, they should define what the intent of the phrase "very short exposure window" means. When we compare our part 25 non ETOPs aircraft that have average flight duration of 1.5 hours, and carry 10 people, is that a "very short exposure window" compared to a 12 hour mission on an ETOPS that carries several hundred people? Cessna believes that it is. .	**Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11**
Textron Aviation	**For AMC Subpart F – Equipment, AMC 25.1309 (d)**	Do not support the proposal "When more than one flight is made with equipment known to be inoperative and that equipment affects the probabilities associated with hazardous and/or catastrophic failure conditions, time limits may be needed for the number of flights or allowed operation time in that aircraft configuration. These time limits should be established in accordance with the recommendations contained in CS-MMEL". Again, the pass fail criteria are not clear and unambiguous.	**Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**
Textron Aviation	**Appendix 1. Assessment Methods,**	Do not agree with the statement that "These analyses may also identify a combination of failures and effects that would otherwise not have been foreseen by FMEA or FTA." If the analysis is properly done top down and developed from a functional perspective, these common mode items will be identified by the FMEA, FTA or by both. If problems are showing up in the field because the analysis that the regulators are requiring are not identifying these issues, then maybe the regulators should step back, form a problem statement, and address this issue through the S-18 group and change the emphasis described in SAE ARP 4761.	**Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**Appendix 5,**	Cessna objects to the simplistic example that requests that EASA use a representative example from a recent part 25 certification effort. For our small part 25 business jet, these examples involve functionally constructed fault trees that span hundreds of pages and involve thousands of gates and basic events. One can only assume that the size and complexity of the tree would scale with the aircraft, and that an example from the Airbus 380 or Boeing 787 would be, say, 10 times as large. How this concept can be explained using a one page fault tree is not clear, but it is clear that the example presented in this appendix is made up of a reduced tree based on the members of the cutsets and not the logical flow of design details as the tree is constructed. This approach re-enforces the notion presented in the paragraph above that "These analyses may also identify a combination of failures and effects that would otherwise not have been foreseen by FMEA or FTA." So EASA has stated that there is a problem with the analysis, and then presented a simplified example to make their case. Again, Cessna cannot support a methodology along the lines of "An alternative but more conservative method would be to rerun the fault tree probability calculation assuming for each model rerun that a different latent primary event had failed." As described in the ASAWG minority position presented to TAEIG on this subject, the estimated cost for a new program to do this exercise is someplace between 3 and 4 million dollars without any safety benefit.	**Recommends that this change not be made or recommends that if this proposal goes forward, it be applied to aircraft that fall under the umbrella of 14 CFR 26.11.**

Commenter	Page/Paragraph	Comment	Suggested Change
Textron Aviation	**CS 25.671(c)(2)(ii) CS 25.671(c)(3)(iii) CS 25.1309(b)(5) AMC 25.671 Section 9a, 3rd paragraph AMC 25.671 Section 9d, 1st paragraph AMC 25.1309 Section 9b6i AMC 25.1309 Section 9b6ii AMC 25.1309 Appendix 5**	NPA's implementation of "1/1000" would place a significant and disproportionate burden/cost on small transport category aircraft manufacturers, without a commensurate safety/benefit, in order to show compliance. Cessna/Beech's dissenting opinion to ASAWG provided those details, which could be a significant percentage of the overall development costs for small transport category aircraft.	**In lieu of the "1/1000 specific risk" of the NPA being applicable to all aircraft, recommend that aircraft which do not meet the criteria of 14 CFR 26.11 (i.e., passenger capacity of 30 or more, or maximum payload capacity of 7500 lb or more) would be exempted from the "1/1000 specific-risk" aspects of NPA 2014-02. For aircraft which do not meet the criteria of 14 CFR 26.11, the average-risk methods of present 14 CFR 25.1309 (which would also apply to CS 25.671(c) (2) "combinations of failures not shown to be extremely improbable") would be sufficient for compliance.**
Textron Aviation	**CS 25.629 (d)(10)(iii)**	This NPA makes changes to replace "single + probable" in CS 25.671 & 25.1309, so why does it add "single+probable" into CS 25.629? This amounts to introducing a methodology to replace "single + probable" that would impose a significant burden on the small transport aircraft manufacturer without a commensurate safety/benefit while retaining "single + probable" in related regulations.	**Propose deleting CS 25.629 (d) (10) (iii). The average risk implementation of 25.1309 should be sufficient, unless the aircraft falls under the umbrella of 14 CFR 26.11.**