European Aviation Safety Agency

Comment-Response Document 2016-07

Appendix 2
to ED Decision 2017/015/R

Table of contents

1. Summary of the outcome of the consultation

58 comments were received from 16 stakeholders (Airbus, Bombardier, DGAC France, Embraer, Eurocontrol, FOCA Switzerland, Garmin International, GE Aviation, GAMA, LBA, Textron Aviation, Thalès Avionics, Boeing, CAA UK, and two individuals).

Some stakeholders consider that introducing the level of confidence of the development assurance processes as a ‘safety objective’ is controversial. Therefore, the proposed newt text under Chapter 8.a of AMC 25.1309 has been withdrawn.

Otherwise, the other changes proposed in the NPA are either unchanged or improved/clarified based on the comments received.

2. Individual comments and responses

In responding to comments, a standard terminology has been applied to attest EASA's position. This terminology is as follows:

(a) **Accepted** — EASA agrees with the comment and any proposed amendment is wholly transferred to the revised text.

(b) **Partially accepted** — EASA either agrees partially with the comment, or agrees with it but the proposed amendment is only partially transferred to the revised text.

(c) **Noted** — EASA acknowledges the comment but no change to the existing text is considered necessary.

(d) **Not accepted** — The comment or proposed amendment is not shared by EASA.

(General comments) -

comment *2* comment by: *EUROCONTROL*

The EUROCONTROL Agency does not have comments on NPA 2016-07.

response Noted.

comment *9* comment by: *UK CAA*

Thank you for the opportunity to comment on NPA 2016-07, Regular update of CS-25.
Please be advised there are no comments from the UK Civil Aviation Authority.

response Noted.

comment *15* comment by: *UoY*

I am in favour of these clarifications. I believe that they put safety requirements at the right level of decomposition of the document set. Random and systematic failure should be treated with different requirements at this level. There are a number of mistakes and omissions that are very widely made that are addressed in this NPA.

response Noted.

comment *16* comment by: *Thales Avionics- JD Chauvet*

Thales would like to thank EASA for consulting industry for this topic, and understand the EASA willing to clarify the Mean of Compliance of CS25.1309.
Nevertheless Thales consider that such amendment should be
- fully consistent and not overlaping with ED79A
- fully harmonized with FAA AC25.1309 in order to ensure industry level playing field

response Noted.

comment

17 comment by: *Airbus*

As far as FDAL/IDAL aspects are concerned, it is agreed that AMC 25.1309 might provide the following fundamental messages:
Development should be commensurate with the severity of the Failure Conditions it is contributing to.
Guidelines which may be used for FDAL/IDAL assignment are described in the document referenced in (3)(b)(2) – ARP4754A/ED79A.
The Agency recognises that credit can be taken from system architecture.
Assigning FDAL/IDAL is not a Safety Objective.
This NPA 2016-07 implicitly considers F/IDAL as a Safety Objective, which is brand new and not accepted by Airbus.
As a consequence, specific comments to the NPA core (paragraphs 8 & 9) are provided.

response

Partially accepted.

When supporting compliance with the safety objectives of CS 25.1309, the applicant needs to address random failures, as well as errors in development, manufacturing, installation, and maintenance.
As far as development errors are concerned, EASA considers that the safety objective, e.g. Extremely Improbable, is translated into a level of confidence in the development assurance process, e.g. Development Assurance Level A. This level of confidence is to be met. Thus, Section 8 of the AMC 25.1309 was selected to be amended.
In order to satisfy this level of confidence, EASA recognises the use by the applicant of the development assurance guidelines laid down in the ED79A/ARP4754A. Thus, Section 9 of the AMC 25.1309 was selected to be amended.
EASA acknowledges that introducing the level of confidence of the development assurance processes as a 'safety objective' is deemed controversial by several stakeholders. As a consequence, this does not fit in the scope of RMT.0673 and the proposal is withdrawn.

comment

43 comment by: *DGAC France*

Please note that DGAC France has no specific comments on this NPA.

response

Noted.

comment

44 comment by: *Federal Office of Civil Aviation (FOCA), Switzerland*

The Federal Office of Civil Aviation (FOCA) appreciates the opportunity to comment on this NPA.

response

Noted.

2. ExplanatoryNote -2.1. Overview of the issues to be addressed p. 4

comment

47 comment by: *Bombardier*

Interfaces between CS 25.1309 and CS 25.810/CS 25.812
The proposed amendments to CS 25.1309(b) will exclude functional failures related to function availability of cabin safety equipment. This essentially only addresses two systems:

escape slides and emergency lighting. Given the proliferation of electric / electronic equipment in the design of interior furnishings, we propose that functional failures of other systems that do not affect operation of the airplane, but for which there is safety effect in the event of a crash landing, should also be excluded from the requirement.

This is considered to be a separate issue from survivability of a system.

For example, is a CS 25.1309 analysis required for seating systems that have electronically controlled actuators to allow adjustment of the seat back, leg rest and other features, given that the seat must be properly configured for takeoff and landing to ensure that occupants are protected from injury in the event of a crash landing? Such a seat would be equipped with mechanical override features to allow the seat to be properly configured in the even there is a loss of power or malfunction.

Relationship between the severity of failure conditions and DALs (AMC 25.1309)

Likewise, application of DAL to those interior systems for which there is no safety impact for failure except in combination with a crash landing is inconsistent with the intent of the applicable standards (ie DO-178 and DO-254) in that these standards, as well as ARP 4765, were developed to address increasingly complex and highly integrated basic airplane systems associated with safe operation of the airplane. For that reason, these systems do not need to meet the requirements of CS 25.1309.

The concern is that relatively simple systems that incorporate electronic packages, such as microcontrollers or PLDs, for control or monitoring will be inappropriately subject to DAL requirements even though their functional failure has no direct effect on safe operation of the airplane.

Of particular interest would be the seat example discussed above – if the seat features software / complex hardware, it is clear that a functional failure does nothing to increase the probability of an accident (i.e. there is no safety impact). In theory however, the occupant could suffer serious injury if there is a crash landing in combination with a software / hardware error that results in the seat not being configured properly for landing.

response

Interfaces between CS 25.1309 and CS 25.810/CS 25.812

Not accepted. EASA acknowledges the request. However, extending the exclusion is not considered non-complex and non-controversial at this stage, and as such, would not fit in the scope of RMT.0673. The purpose of this NPA is limited to clarify the already existing interfaces between CS 25.1309 and CS 25.810/CS 25.812.

Relationship between the severity of failure conditions and DALs (AMC 25.1309)

Not accepted. Please refer to the response to comment 17 above.

comment

54 comment by: *Textron Aviation*

The second issue described in this NPA seeks to provide the description of a relationship "between the severity of a failure condition and DALs" which is absent in the current AMC 25.1309. However, this relationship is also absent from the regulation. Therefore, this issue must first be addressed by adding the relationship to the regulation.

Suggested Change

Amend the regulatory paragraphs of CS25.1309 to describe the relationship between severity of a failure condition and DALs similar to how it already describes the relationship between the severity of a failure condition and its allowable quantitative probability.

response

Not accepted.

Please refer to the response to comment 17 above.

2. Explanatory note - 2.2. Objectives p. 4

comment

3 comment by: *GE Aviation*

The proposed wording aligning Development Assurance Levels, where used, with the severity of function failure is in line with accepted practice and is not controversial. GE Aviation supports this clarifying and helpful change.

GE Aviation is concerned that attempts continue to apply the Development Assurance process to simple mechanical systems. Existing traditional methods of certifying simple mechanical systems have been highly successful and delivered a steadily improvement in safety and reliability over the years. Application of the DAL concept would not be likely to add value, and risks disrupting a process which works well.

The Explanatory Note to the NPA implies that the use of DALs is appropriate and necessary for all aircraft systems, even those where direct techniques are traditional and effective . Some of the proposed wording changes in the NPA text promote the use of DALs for mechanical systems; possibly unintentionally.

response

Noted.

In line with ED-79A/ARP4754A Sections 5.2.3.3 and 5.4, EASA agrees that components that can be fully assured by a combination of testing and analysis, relative to their requirements and identified failure conditions may be considered to provide a level of confidence equivalent to IDAL A, provided the design has been validated and verified. Examples include mechanical components, electro-mechanical devices, electro valves, or servo valves.

Nevertheless, the proposed changes of the wording in Section 8 of NPA 2016-07, which were considered potentially misleading in this respect, are not retained. Please refer to the response to comment 4.

2. Explanatory note - 2.4. Overview of the proposed amendments p. 4-5

comment

37 comment by: *The Boeing Company*

Proposed text states:

Figure 2 of current AMC 25.1309(8)(b) provides an inverse relationship between the severity of a failure condition and the allowable quantitative probability of such a condition. This kind of relationship between the severity of a failure condition and DALs is currently not provided.

Suggested change:

Figure 2 of current AMC 25.1309(8)(b) provides an inverse relationship between the severity of a failure condition and the allowable quantitative probability of such a condition. This kind of relationship between the severity of a failure condition and DALs is currently not provided. A similar relationship exists between severity of a failure condition and the level of rigor necessary to provide confidence in its development process.

Justification:

As noted in Paragraph #3 on page 5, the current industry practice is contained within Section 5.2 of EUROCAE ED-79A/SAE ARP4754A. Further, in Paragraph #3 on page 5, the following is included: “Therefore, it is proposed to amend AMC 25.1309 to reflect the current aircraft development practices that make use of the assignment of DALs.” Boeing is accustomed to current use of ARP for DAL guidance, for this reason the addition to the AMC is not necessary, however, if EASA feels it is needed in the AMC, we suggest the rewrite above.

By writing as currently proposed, it could be concluded that there is a relationship between the probability of a failure and the associated DAL (contrary to Table 2 Note 2).

response

Noted.
The comment is agreed, however, the explanatory note of the NPA will not be re-issued.

comment

55 comment by: *Textron Aviation*

The overview of the proposed amendment regarding DALs describes the application of a development assurance process based on failure condition severity which is used to "limit the likelihood of development errors." None of these concepts are described in the regulatory paragraphs and do not support a showing of compliance as written.
Suggested Change
Amend the regulatory paragraphs of CS25.1309 to describe the relationship between severity of a failure condition and DALs similar to how it already describes the relationship between the severity of a failure condition and its allowable quantitative probability.

response

Not accepted.
Please refer to the response to comment 17.

3. Proposed amendments - 3.1 Draft CS - CS 25.1309 p. 6

comment

20 comment by: *General Aviation Manufacturers Association*

3.1. 1. Fifth Sentence (Page 6) [Editorial]
Recommend changing "functional failures" to "failure conditions".
The expression "failure condition" is the preferred term to describe a condition where a function is not available or performed incorrectly, regardless of cause.
Currently SAE S-18 is replacing all instances of "functional failure", "functional failure condition", "functional hazard" and other expressions currently used with this meaning, using "failure condition" consistently in the upcoming revisions to ARP4754 and ARP4761.

response

Accepted.

comment

21 comment by: *General Aviation Manufacturers Association*

3.1. 1. Fifth Sentence (Page 6) [Editorial]
Recommend changing "function availability" to "loss of function".
While this use of the expression "function availability" is correct in the context of functional hazard assessment, the term "availability" is also used in the context of utilization (i.e., availability for dispatch). The current proposed text could be misinterpreted to mean that the availability of the cited items for dispatch does not need to be considered.
The alternate text suggested above has no ambiguity.
"The ~~functional failures~~ failure conditions related to ~~function availability~~ loss of function of cabin safety equipment…"

response

Partially accepted.
The use of the term 'failure conditions' is retained. The text related to 'function availability' is deleted from the CS but the proposed change, i.e. use of 'loss of function', is retained in the AMC.

comment

22 comment by: *General Aviation Manufacturers Association*

3.1. 1. Fifth Sentence (Page 6) [Editorial]
Recommend changing “cabin safety” to “the” and “covered by” to "required by".
The expression "covered by" could refer to "functional failures related to functional availability" (or "failure conditions related to loss of function" incorporating the previously suggested changes), or to "cabin safety equipment". The first interpretation is possible because CS 25.810 and CS 25.812 mention certain failure cases.
The current proposed text could, therefore, be interpreted to mean that only the specific failures mentioned in CS 25.810 and CS 25.812 are excepted.
The alternate text suggested above makes this misinterpretation less likely, making it clear that the loss of function failure conditions of all "equipment required by CS 25.810 and CS 25.812" is excepted.
“The ~~functional failures~~ failure conditions related to ~~function availability~~ loss of function of ~~cabin safety~~ the equipment ~~covered by~~ required by CS 25.810 and CS 25.812 are excepted from the requirements of CS 25.1309(b).”

response

Not accepted.
The first interpretation is actually correct. The expression ‘covered by’ refers to the failure conditions related to loss of function. Failure conditions related to malfunction, e.g. untimely activation of a function, are not excepted from CS 25.1309.
The final text of the AMC is clarified in order to reflect the above.

3. Proposed amendments - 3.2 Draft AMC - AMC 25.1309 p. 7-12

comment

1 comment by: *Syiad AL-DURI*

This is generally very desirable.
The AMC here uses the term *failure condition* in relation to the DALs. This is misleading, because the intent of assigning a DAL is not to prevent *failures* or reduce their probability. People not already familiar with the matter may be confused by this. They might misinterpret the intent of DAL application as to improve item integrity, i.e. reduce the failure occurrence rate, similar to the approach per CS-E 515. It would be better to only use the word *condition*, e.g. 'a Hazardous condition', in the context of development errors and DALs.
This distinction becomes even more important with common cause considerations. While a *failure* typically only affects one item at a time, a development error could negate redundancies. Therefore, a (e.g. Catastrophic) *condition* may arise from a development error affecting multiple, identical redundant systems, without any failure.
Where defined terms are used, like the severity and probability categories, they should be written beginning with capital letters, e.g. 'Remote' instead of 'remote'. This is to make it clear that the specific term is meant instead of the more casual use of the same word.
Furthermore, I would like to make two suggestions:

1. The development assurance levels are used here together with defined terms for the severity of a failure condition and its probability. The severity and probability categories are defined within the AMC. Similarly, a rough definition of the development assurance levels should be given. Alternatively, the Agency may prescribe requirements or objectives for the development assurance levels assigned to the different severity categories.

2. EUROCAE ED-79A / SAE ARP4754A offer options for the assignment of lower DALs for functional failure sets with multiple members. While it would be inappropriate to replicate this within the AMC, it would be useful to include a statement that such options are not precluded by the AMC.

response

There are four proposals in this comment:

a. Proposal to replace 'failure conditions' by 'condition':
Not accepted.
This terminology reflects current practices and recognised industry standards such as ED-79A/ARP4754A.

b. "Where defined terms are used, like the severity and probability categories, they should be written beginning with capital letters, e.g. 'Remote' instead of 'remote'."
Not accepted.
Although this point may be acceptable, this is beyond the scope of this NPA.

c. 'A rough definition of the development assurance levels should be given':
Not accepted.
Paragraph 9 is already stating: 'Guidelines, which may be used for providing development assurance, are described for aircraft and systems in the document referenced in paragraph 3b(2), and for software in the documents referenced in paragraph 3a(3).'

d. 'EUROCAE ED-79A/SAE ARP4754A offer options for the assignment of lower DALs for functional failure sets with multiple members. While it would be inappropriate to replicate this within the AMC, it would be useful to include a statement that such options are not precluded by the AMC.':
Noted.
The NPA already includes a proposal in Section 9.b.(4) that system architecture may be considered when assigning development assurance levels.

comment

4 comment by: *GE Aviation*

GE Aviation suggests that text advocating the use of DALs contain a qualifier on the systems for which the DAL approach is appropriate, such as:
8a……..
In addition, to minimise the risk of development errors for those systems where direct techniques showing compliance are not used, there is a need to establish development assurance activities at a level that provides an adequate level of confidence that the aeroplane/system functions and items satisfy the objectives of CS 25.1309.

response

Not accepted.
Paragraph 8 describes the safety objectives and paragraph 9 the acceptable means of compliance. The consideration of mechanical systems (not containing software/airborne electronic hardware) is considered to be a means of compliance discussion and is considered appropriately addressed in paragraph 9.b.(4): 'Errors made during the 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 which perform a limited number of

functions and which are not highly integrated with other aeroplane systems.’

comment

5 comment by: *GE Aviation*

GE Aviation also requests that the current wording of AMC 25.1309 9 b 4 stand;
“there is no agreed Development Assurance standard for ~~airborne electronic~~ hardware.” This wording makes it clearer that neither airborne electronic hardware, nor simple mechanical hardware, has agreed Development Assurance Standards.

response

Not accepted.
In the approach of development assurance, EASA only focuses on airborne electronic hardware, software, and systems. Mechanical hardware is not intended to be covered in the commented AMC statement.

comment

6 comment by: *Thales Avionics- JD Chauvet*

"In addition, to minimise the risk of development errors, there is a need to establish ....function or item, the associated Development Assurance process is assigned Level E."
As this text is a partial copy of ED-79A §5.2.1 "General Principle", there is a STRONG risk of miss-interpretation leading to non-recognition of the ALL other DAL combinations accepted today by ED-79A (e.g. A,C,C or B,B,C,C for catastrophic)
Furthermore, there is no added value of copying such information
In conclusion, Thales consider the ED79A being sufficient and covering the topic and therefore propose to remove the text proposed by this NPA.

response

Partially accepted.
Please refer to the response to comment 17.

comment

7 comment by: *Thales Avionics- JD Chauvet*

Concern applies on amendments of Figure 2:
- modification of the Figure 2 title
- adding of the row"Allowable Development Assurance Level (FDAL/IDAL) (See Note 2)"
- Note 2
1) Adding DAL in the Figure 2 :
- induces confusion that DAL is associated to a failure condition, whereas a DAL can be associated only to a function/item, and final DAL assignment of an item or a function is the consequence of the analyses of all contributing Failure Conditions
- implies that all DAL combinations authorized by ED79A from system architecture could no more be authorized by miss-intrepretation (see previous comment)
2) Concerning Note2: Thales recognizes that miss-understanding of certain readers pointed out in Note2 may exist today. Nevertheless, this is manageable by industry through the several internal company courses performed within each company. Thales does not see any significant benefit of adding this Note2 in AMC25.1309
Thales strongly request the removal of all modifications proposed in Figure 2 as being inconsistent with ED79A approach

response

Partially accepted.
Please refer to the response to comment 17.

comment

8 comment by: *Thales Avionics- JD Chauvet*

"(function development assurance level ... may be considered for the assignment process."
Again, the Figure 2 and in general §8 should not be amended and a reference to ED79A is sufficient for §9
Consequently Thales propose to amend the NPA proposal by the following text:
"*The level of Development Assurance (function development assurance level (FDAL)/item development assurance level (IDAL)) should be commensurate with the severity of the Failure Conditions it is contributing to. Guidelines, which may be used for the assignment of development assurance levels to aeroplanes and system functions (FDAL) up to items (IDAL), are described in the document referenced in (3)(b)(2) above. Through this document, the Agency recognises that credit can be taken from system architecture (e.g. functional or item development independence) for the assignment of FDAL/IDAL.*"

response

Accepted.

comment

10 comment by: *Luftfahrt-Bundesamt*

LBA comment:
AMC 25.1309, chapter 9b.(4)
2nd sentence: " Errors made during the design and development..."
comment: delete the words "design and"
justification: in line with the definition in chapter 5j, a mistake in design is a development error

response

Accepted.

comment

11 comment by: *UoY*

1. **Definitions**
a. Development error. This is in-line with current understanding and is the basis of the ED-79a acceptable means of compliance. It indicates the scope of the activities covered by cs-25.1309 clearly
b. Item. This is also in-line with current understanding. It is required to clearly understand the distinction between elements of a design covered by functional guidance (ed-79a) and element level guidance (covered by DO-178c, etc). Both of these levels must be addressed to meet the requirements of cs-25.1309 and having the distinction enshrined at all levels is important for efficient certification activities. This distinction aids both the applicant and the regulator in their discussions.

response

Noted.

comment

12 comment by: *UoY*

1.Explicit definition of the link between failure condition classification and top level DAL.

- a. The wording is strictly correct. Using the phrase level instead of DAL is good as it avoids confusion with early versions of ED-79.
- b. Architectural means may be employed to allow the FDAL / IDAL of lower level functions and items to be allocated different levels to the overall level, as per ED-79a. This could be attached as a note.

- c. Overall, I agree that the discussion is at the right level for cs-25.1309. It should be here to avoid confusion… see point 3. Explanation of the link of "level X" to FDAL / IDAL and architectural decomposition is the remit of ed-79a.

response

a. Noted
b. Noted.
The NPA already includes in Section 9.b.(4) that system architecture may be considered when assigning development assurance levels.
c. Noted.

comment

13 comment by: *UoY*

1. Figure 2: Relationship between severity of failure condition, probability and development assurance levels (DALs)

- a. Clarifying the link between effect and the safety requirements placed on organisations is vital.
- b. Many organisations read the existing cs-25 as giving a numerical probability target based on the severity classification
- c. They are not aware that in fact there are two safety requirements being placed on them

i. Development assurance targets (FDAL / IDAL) to address the impact of systematic errors

ii. Probability targets to address the impact of random failures
Once they look at the acceptable means of ED-79a they see that they have to undertake FDAL / IDAL work. The immediate and obvious response is having done this activity what can I claim for this against my overall target (which they think is a probability target). They therefore try to equate FDAL / IDAL processes to a probability. This is theoretically and practically incorrect! I could point you to several occurrences of this in the real world and many more discussions that I have had to stop people going down this line.
I therefore fully endorse the aim to have both probability and development assurance requirements in cs25.1309. I even more emphatically endorse the explicit statement (Note 2) about the lack of correlation between DALs and Probability.

response

Noted.

comment

14 comment by: *UoY*

1. I think the situation could be made even clearer by giving a three table decomposition, instead of figure 2

- a. Table showing the correspondence between effects on aircraft, crew and occupants (rows 1 to 3) and the classification of a failure condition (row 7)
- b. Table showing the correspondence between the assigned classification of a failure condition (row 7) and the allowable probability (rows 4 and 5). Note 1 would apply here.
- c. Table showing the correspondence between the assigned classification of a failure condition (row 7) and the allowable probability (row 6)

The text can then make it clear that table c does not imply the development of a probability.

Nor should a probability be produced that tries to combine the results from work relating to table b and c.

This is not contentious. It is stated in the ED-79a clearly and agreed by industry. However, the way that it is presented in the current version allows for erroneous interpretation. This erroneous interpretation is commonly made.

response

Partially accepted.

Proposals a. and b. will be introduced in the amended table.

Proposal c. is not accepted. Please refer to the response to comment 17.

comment

17 ❖ comment by: *Airbus*

As far as FDAL/IDAL aspects are concerned, it is agreed that AMC 25.1309 might provide the following fundamental messages:
Development should be commensurate with the severity of the Failure Conditions it is contributing to.
Guidelines which may be used for FDAL/IDAL assignment are described in the document referenced in (3)(b)(2) – ARP4754A/ED79A.
The Agency recognises that credit can be taken from system architecture.
Assigning FDAL/IDAL is not a Safety Objective.
This NPA 2016-07 implicitly considers F/IDAL as a Safety Objective, which is brand new and not accepted by Airbus.
As a consequence, specific comments to the NPA core (paragraphs 8 & 9) are provided.

response

Partially accepted.
Please refer to the response to comment 17.

comment

18 comment by: *Airbus*

Current AMC 25.1309 paragraph 8 should remain unchanged. Changes introduced through this NPA are not acceptable, for the reasons explained in our general comment # 17.

response

Partially accepted.
Please refer to the response to comment 17.

comment

19 comment by: *Airbus*

Attachment #1

Within paragraph 9, subparagraph b(4), we request the following change:
~~The level of Development Assurance (function development assurance level (FDAL)/item development assurance level (IDAL)) should be determined bycommensurate with the severity of the Failure Conditions as per Figure 2 of (8)(b) abovepotential effects on the aeroplane in case of system malfunctions or loss of functions.~~
~~Guidelines, which may be used for the assignment of development assurance levels to aeroplanes and system functions (FDAL) up to items (IDAL), are described in the document referenced in (3)(b)(2) above. Through this document, the Agency recognises that system architecture (e.g. functional or item development independence) may be considered for the assignment process.~~

The level of Development Assurance (function development assurance level (FDAL)/item development assurance level (IDAL)) should be ~~determined~~ commensurate with the severity of the Failure Conditions it is contributing to. ~~Failure Conditions' classes of severity are driving inputs to FDAL/IDAL assignment process.~~ Guidelines, which may be used for the assignment of development assurance levels to aeroplanes and system functions (FDAL) up to items (IDAL), are described in the document referenced in (3)(b)(2) above. Through this document, the Agency recognises that credit can be taken from system architecture (e.g. functional or item development independence) for the assignment of FDAL/IDAL.

The reasons for this proposed change are explained in our comment # 17.

Taking into account this comment should result in paragraph 9.b(4) as proposed in the attached file.

response

Accepted.

comment

23 comment by: *General Aviation Manufacturers Association*

3.2. 8. a. (5) (Page 9) [Conceptual]

The current proposed text implies that development assurance activities are additional and separate activities performed to gain confidence in the development.

While there are additional activities that contribute to achieving a development assurance level, the principal benefit comes from performing the core development activities themselves as a structured and disciplined process.

The alternative text suggested above makes it clear that the entire development effort is raised to a level of assurance that provides confidence.

"In addition, to minimise the risk of development errors, ~~there is a need to establish development assurance activities at a level that provides an adequate level of confidence~~ there is a need to perform development activities at a level of assurance that provides adequate confidence that the aeroplane/system functions…"

response

Not accepted.

The proposed use of the term 'development activities' in lieu of 'development assurance activities' is not consistent with ED-79A/ARP4754A terminology. Development assurance activities include validating requirements, and verifying that requirements are met, together with the necessary configuration management and process assurance activities. These activities are necessary to establish confidence in the development process.

In any case, the proposed changes of the wording in Section 8 of NPA 2016-07 are withdrawn (please refer to response to comment 4).

comment

24 comment by: *General Aviation Manufacturers Association*

3.2. 8. a. (5) (1) (Page 9) [Conceptual]

Comment (conceptual):

Recommend replacing "Development Assurance processes" with "development processes".

As previously noted, the function or item development assurance level applies to the development activities as a whole, not only to processes or activities that exist specifically for development assurance.

"if a catastrophic failure condition that could result from a possible development error in an aeroplane/ system function or item, the associated ~~Development Assurance processes~~ development processes are assigned Level A…"

response

Not accepted.

	Please refer to response to comment 23.
comment	*25* comment by: *General Aviation Manufacturers Association* 3.2. 8. a. (5) (1) (Page 9) [Conceptual] Comment (conceptual): Recommend replacing “Development Assurance processes” with "development processes". As previously noted, the function or item development assurance level applies to the development activities as a whole, not only to processes or activities that exist specifically for development assurance. “if a catastrophic failure condition that could result from a possible development error in an aeroplane/ system function or item, the associated ~~Development Assurance processes~~ development processes are assigned Level A…”
response	Not accepted. Pleas refer to the response to comment 23.
comment	*26* comment by: *General Aviation Manufacturers Association* 3.2. 8. a. (5) (2) (Page 9) [Conceptual] Recommend replacing “Development Assurance processes” with "development processes". See previous rationale. “if a hazardous failure condition that could result from a possible development error in an aeroplane/ system function or item, the associated ~~Development Assurance processes~~ development processes are assigned Level B…”
response	Not accepted. Please refer to the response to comment 23.
comment	*27* comment by: *General Aviation Manufacturers Association* 3.2. 8. a. (5) (2) (Page 9) [Editorial] Recommend replacing “assigned Level B” with "assigned Level B or higher". Each development process may be related to multiple failure conditions, and will be assigned the assurance level associated to the most severe failure condition. The current proposed text may be interpreted to mean that the specific level mentioned must be assigned, however the level is a minimum acceptable level. The alternate proposed text clarifies that higher levels are also acceptable. “if a hazardous failure condition that could result from a possible development error in an aeroplane/ system function or item, the associated ~~Development Assurance processes~~ development processes are assigned Level B or higher; Please note that “Development Assurance processes” was changed as part of comment 7 in this comment response document.
response	Not accepted. Although it is correct that higher DAL can be assigned, many other comments received from other industry stakeholders (in particular CS-25 aircraft manufacturers and their suppliers) show that the main concern is that DAL combinations authorised by ED79A based on system architecture considerations could be miss-intrepretated as non-authorised. Regarding the proposal to replace ‘Development assurance processes’ by ‘development

processes', please refer to the response to comment 23.

comment

28 comment by: *General Aviation Manufacturers Association*

3.2. 8. a. (5) (3) (Page 9) [Conceptual]
Recommend replacing "Development Assurance processes" with "development processes".
See previous rationale.
"if a major failure condition that could result from a possible development error in an aeroplane/ system function or item, the associated ~~Development Assurance processes~~ development processes are assigned Level C…"

response

Not accepted.
Please refer to the response to comment 23.

comment

29 comment by: *General Aviation Manufacturers Association*

3.2. 8. a. (5) (3) (Page 9) [Editorial]
Recommend replacing "assigned Level C" with "assigned Level C or higher".
See previous rationale.
"if a major failure condition that could result from a possible development error in an aeroplane/ system function or item, the associated ~~Development Assurance processes~~ development processes are assigned Level C or higher;

response

Not accepted.
Please refer to the response to comment 27.

comment

30 comment by: *General Aviation Manufacturers Association*

3.2. 8. a. (5) (4) (Page 9) [Conceptual]
Recommend replacing "Development Assurance processes" with "development processes".
See previous rationale.
"if a minor failure condition that could result from a possible development error in an aeroplane/ system function or item, the associated ~~Development Assurance processes~~ development processes are assigned Level D…"

response

Not accepted.
Please refer to the response to comment 23.

comment

31 comment by: *General Aviation Manufacturers Association*

3.2. 8. a. (5) (5) (Page 9) [Conceptual]
Recommend replacing "Development Assurance processes" with "development processes".
See previous rationale. Note that in this case a "development assurance process" may not even be required.
"if a no safety effect failure condition that could result from a possible development error in an aeroplane/ system function or item, the associated ~~Development Assurance processes~~ development processes are assigned Level E…"

response

Not accepted.
Please refer to the response to comment 23.

comment

32 comment by: *General Aviation Manufacturers Association*

3.2. 8. a. (5) (5) (Page 9) [Editorial]
Recommend replacing “assigned Level E” with "assigned Level E or higher".
See previous rationale.
“if a no safety effect failure condition that could result from a possible development error in an aeroplane/ system function or item, the associated ~~Development Assurance processes~~ development processes are assigned Level E or higher;

response

Not accepted.
Please refer to the response to comment 27.

comment

33 comment by: *General Aviation Manufacturers Association*

3.2. 8. b. (Page 10) Figure 2 [Editorial]
Recommend replacing the word “Allowable” in row 6 of Figure 2 with "Minimum".
As previously noted, the FDAL/IDAL associated to each failure severity is the minimum for the associated development processes.
Alternatively, the term "Allowable" could be retained here, and the content of the table modified to "Level E or higher", "Level D or higher", etc.
“Allowable Minimum Development Assurance Level (FDAL/IDAL) (See Note 2)”

response

Not accepted.
Please refer to the response to comment 23. In addition, please note that EASA’s initial proposed wording was consistent with FAA AC 23.1309-1E Figure 2 and ASTM F3061/F3061M Table 4.

comment

34 comment by: *General Aviation Manufacturers Association*

3.2. 8. b. (Page 10) Figure 2 [Editorial]
Recommend moving the last row in Figure 2 up three positions, such that it appears above the "Allowable Quantitative Probability".
The proposed addition of the FDAL/IDAL row has further separated the classifications from the effects that define them.
This change would make the table closer reflect the Safety Process, which identifies effects, then classifies, then establishes safety objectives (i.e., the classification precedes the quantitative and qualitative objectives).
Move the last row of Figure 2 “Classification of Failure Conditions” up three positions in the table to be located above the row title “Allowable Quantitative Probability”.

response

Accepted.

comment

35 comment by: *General Aviation Manufacturers Association*

3.2. 9. b. (4) (Page 11) [Editorial]
Recommend replacing “up” with "and" in the first sentence of Paragraph 2 in this section.
The relationship between aircraft, systems and items is generally referred to in the "down" direction in that order (i.e., item level is considered "lower" than system level).
In this case, however, simply using "and" is effective.
“Guidelines, which may be used for the assignment of development assurance levels to

aeroplanes and system functions (FDAL) ~~up~~ and to item (IDAL), are described…”

response Accepted.

comment *36* comment by: *Embraer S.A.*

Embraer understands that the statement *"There is currently no agreed Development Assurance standard for airborne electronic hardware"* should be clarified in section 9.b.(4). The DO-254 is recognized by AC 20.152 as an acceptable means of compliance for Airborne Electronic Hardware (AEH) and this standard defines the different development assurance activities required for different AEH DALs in a similar matter as described for embedded software in DO-178B/C. The DO-254 has been used by Embraer suppliers in all programs for compliance with EASA Certification Memo for AEH.

response Partially accepted.
EASA agrees that DO-254 provides some guidance for development of custom AEH, but it is also recognised that the document might be insufficient for some other AEH. An AMC 20-152 is under development, it is intended to update AMC 25.1309 when AMC 20-152 will be published.

comment *38* comment by: *The Boeing Company*

THE PROPOSED TEXT STATES:“In addition, to minimise the risk of development errors, there is a need to establish development assurance activities at a level that provides an adequate level of confidence that the aeroplane/system functions and items satisfy the objectives of CS 25.1309. A logical and acceptable inverse relationship must exist between the development assurance levels (DALs) and the severity of failure conditions, such that:
(1) if a catastrophic failure condition could result from a possible development error in an aeroplane/system function or item, the associated Development Assurance processes are assigned Level A;
(2) if a hazardous failure condition could result from a possible development error in an aeroplane/system function or item, the associated Development Assurance processes are assigned Level B;
(3) if a major failure condition could result from a possible development error in an aeroplane/system function or item, the associated Development Assurance processes are assigned Level C;
(4) if a minor failure condition could result from a possible development error in an aeroplane/system function or item, the associated Development Assurance processes are assigned Level D; and
(5) if a no safety effect failure condition could result from a possible development error in an aeroplane/system function or item, the associated Development Assurance process is assigned Level E.”
REQUESTED CHANGE:
“In addition, to minimise the risk of development errors, there is a need to establish development assurance activities at a level ~~that provides an adequate level of confidence that the aeroplane/system functions~~ commensurate with the failure condition classification severity ~~and items satisfy the objectives of CS 25.1309~~. A logical and acceptable inverse relationship must exist between the development assurance levels (DALs) and the severity of failure conditions, such that: …”
ADD at the End: “Note that these initial DAL assignments are made from the severity

classification of the failure conditions prior to consideration of system architecture that may be introduced by following the guidance of reference 3(b)(2).”
Justification:
Current industry practice includes requirements to assign DAL levels commensurate with the severity of the failure condition. Industry practices contained in EUROCAE ED-79A/SAE ARP4754A (reference 3(b)(2), includes DAL assignment guidance with consideration for system architecture. Current AMC 25.1309 section 9.b.(4) already contains guidance for Development Assurance, and is the more appropriate section for this. Also see comment #3.

response

Noted.
The concern is accepted but the proposed text, which is referred to in the comment, has been withdrawn (please refer to the response to comment 4).

comment

39 comment by: *The Boeing Company*

THE PROPOSED TEXT STATES: Figure 2
REQUESTED CHANGE: We suggest to reorder table rows to put Classification of Failure Conditions directly below Effect on Flight Crew and above Allowable Quantitative Probability.
JUSTIFICATION:
The table would be easier to follow if it made the distinction that the top three rows (Effect on Aeroplane, Occupants excluding Flight Crew, and Flight Crew) are used to develop the failure condition classification (which should be the next row), then the remaining rows (for qualitative and quantitative probability and DAL) are based on the determination of the failure condition classification.

response

Partially accepted.
The Figure 2 is reorganised to have a direct link between the severity of the effects and the classification of a failure condition.

comment

40 comment by: *The Boeing Company*

THE PROPOSED TEXT STATES: “Note 2: There is no direct correlation between the function development assurance level (FDAL)/item development assurance level (IDAL) and the quantitative probabilities of a failure condition.”
REQUESTED CHANGE: “Note 2: The FDAL/IDAL assignment is based on the classification of the failure conditions and can consider system architecture (per Section 5.2 of ARP 4754A), as such, while both FDAL/IDAL and probability requirements are related to severity, there is no direct correlation between the FDAL/IDAL function development assurance level (FDAL)/item development assurance level (IDAL) and the quantitative probabilities of a failure condition.”
JUSTIFICATION:
As written, this note seems contradictory, since both DAL and Probability are shown as directly correlated to the hazard classification of the failure condition in the table. While the note is true, it is not effective in communicating why this is true, we suggest the rewrite above.

response

Noted.
The concern is accepted but the proposed text, which is referred to in the comment, has been withdrawn (please refer to the response to comment 4).

comment 41 comment by: *The Boeing Company*

THE PROPOSED TEXT STATES: "…The level of Development Assurance (function development assurance level (FDAL)/item development assurance level (IDAL)) should be determined by commensurate with the severity of the Failure Conditions as per Figure 2 of (8)(b) above. Guidelines, which may be used for the assignment of development assurance levels to aeroplanes and system functions (FDAL) up to items (IDAL), are described in the document referenced in (3)(b)(2) above. Through this document, the Agency recognises that system architecture (e.g. functional or item development independence) may be considered for the assignment process."
REQUESTED CHANGE: "…The level of Development Assurance (function development assurance level (FDAL)/item development assurance level (IDAL)) should be determined by commensurate with the severity of the Failure Conditions as per Figure 2 of (8)(b) above following the general principles for DAL assignment taking into account failure conditions and severity classifications (as described in the document referenced in (3)(b)(2)). Guidelines, which may be used for the assignment of development assurance levels to aeroplanes and system functions (known as function development assurance level or FDAL) and to items (known as item development assurance level or IDAL), are further described in the document referenced in (3)(b)(2). Through this document, the Agency recognises that system architecture (e.g. functional or item development independence) may be considered in for the assignment process.
JUSTIFICATION:
Ultimately, FDAL/IDAL may be assigned levels based on architecture, not just the failure condition as per Figure 2 of 8(b). Thus, we recommend referencing the guidance already established in the applicable industry document. The statement regarding aeroplane and systems development is redundant to the previous paragraph.

response Partially accepted.
The concern is accepted, but the suggested change is not retained. Instead, paragraph 9 is updated based on Airbus and Thales' common suggestion. Please refer to the responses to comments 8 and 19.

comment 42 comment by: *The Boeing Company*

THE PROPOSED TEXT STATES: "There is currently no agreed Development Assurance standard for airborne electronic hardware."
REQUESTED CHANGE: "There is currently no agreed Development Assurance standard for EUROCAE ED-80/DO-254, Design Assurance Guidance for Airborne Electronic Hardware provides standard for airborne electronic hardware."
JUSTIFICATION:
EUROCAE ED-80/DO-254 has been used and accepted as a standard for AEH development for several years, and is now recognized in AMC20-152.

response Partially accepted.
Please refer to the response to comment 36.

comment 45 comment by: *Federal Office of Civil Aviation (FOCA), Switzerland*

Comment FOCA: it is unclear what happened to 8c. and 8 d. as there is no "(...)" after 8b.

response Accepted.

The NPA text should have contained "(...)" after 8b in order not to give the impression that 8c. and 8 d. paragraphs are proposed to be deleted.

comment

46 comment by: *Federal Office of Civil Aviation (FOCA), Switzerland*

Comment FOCA: the Development Assurance Level (DAL) definition is not in line with ED 12C. From SW design perspective, this DAL does not include the verification of SW.

response

Not Accepted.
The terminology ‘development assurance level (DAL)’ or ‘item development assurance level (IDAL)’ is indeed not used in ED-12C/DO-178C which relies on the generic term ‘software level’. However the definition of ‘Software level’ refers back to the system safety assessment process and introduces a note mentioning the terminology ‘IDAL’. Moreover, the link is made in ED-79A/ARP4754A which states that ‘IDAL is the appropriate Software level in ED-12B / DO-178B’ (which was the applicable standard at the time of publication of ED79A and is equivalent to ED-12C/DO-178C for this matter).

comment

48 comment by: *Garmin International*

See page 10, Section (8.)(a.), after Figure 1.
ARP 4754A allows architectural mitigations to assign lower Design Assurance Levels (DALs) to items as long as the functional development is commensurate to the Failure Condition.
NPA 2016-07 Paragraph 2.4, under the Relationship between the severity of failure conditions and DALs (AMC 25.1309) heading, states:
“… the current practices used for the development of aircraft systems are based on the assignment of DALs to aircraft/system functions and items (FDAL/IDAL) as laid down in Section 5.2 of EUROCAE ED-79A/SAE ARP4754A.
Therefore, it is proposed to amend AMC 25.1309 to reflect the current aircraft development practices that make use of the assignment of DALs.”
The text in proposed AMC 25.1309 section 8.a., after Figure 1 includes:
“… A logical and acceptable inverse relationship must exist between the development assurance levels (DALs) and the severity of failure conditions, such that:
(1) if a *catastrophic failure condition* could result from a possible development error in an aeroplane/system function or item, the associated Development Assurance processes are assigned Level A;
(2) …”
This does not fully reflect SAE 4754A, paragraph 5.2.1, which also has the Development Assurance Process assignment principle based on two or more independently developed aircraft/system functions or items.
Using only the Catastrophic Failure condition example. 4754A, paragraph 5.2.1 states:
“When a Catastrophic FC is involved, the assignment principles are:
• If a Catastrophic Failure Condition (FC) could result from a possible development error in an aircraft/system function or item, then the associated Development Assurance process is assigned level A.
• If a Catastrophic Failure Condition could result from a combination of possible development errors between two or more independently developed aircraft/system functions or items then, either one Development Assurance process is assigned level A, or two Development Assurance processes are assigned at least level B. The other independently developed aircraft/system functions or items are assigned no lower than Development Assurance Level C. The Development Assurance process establishing that the

two more independently developed aircraft/system functions or items are in fact independent should remain level A."
As shown above, the proposed AMC 25.1309 text in section 8.a. after Figure 1 only reflects half of the catastrophic DAL assignment principles.
The proposed AMC 25.1309 text should be updated to be consistent with the practices defined in 4754A, section 5.2.
Garmin suggests either the text needs to add the additional DAL assignment principles for failure conditions as defined in 4754A
or
the text needs to be deleted so one can reference Section 5.2 of ARP4754A for the definition of assignments of DALs to aircraft/system functions and items (FDAL/IDAL).

response

Noted.
The concern is accepted but the proposed text, which is referred to in the comment, has been withdrawn (please refer to the response to comment 4).

comment *49* comment by: *Textron Aviation*

The addition of the DAL (Allowable Development Assurance Level) as related to the Severity of Failure Condition to Figure 2 of section 8.b. implies that these DALs are absolute with no possibility of allocation. ARP4754A, Table 3, outlines minimum level of DAL at each functional level (i.e. DAL lower than C is not permitted for Catastrophic failure conditions). ARP4754A, Table 3, also allows for allocation to lower level DALs as depicted by Option 1 and Option 2 of ARP4754A, Table 3.
By changing the header for this row to "TOP-LEVEL FUNCTION FDAL ASSIGNMENT", this will direct linkage to ARP4754A, Table 2.
Suggested Change
Section 8.b. Figure 2: change the header for the NPA proposed row "Allowable Development Assurance Level (FDAL/IDAL)" (first column, 6th row) to read "TOP-LEVEL FUNCTION FDAL ASSIGNMENT".

response

Noted.
The concern is accepted but the proposed text, which is referred to in the comment, has been withdrawn (please refer to the response to comment 4).

comment *50* comment by: *Textron Aviation*

The paragraph “(1) if a *catastrophic failure condition* could result from a possible development error in an aeroplane/system function or item, the associated Development Assurance processes are assigned Level A;” conflicts with paragraph 5.2.1 in SAE ARP 4754A. The implication is that two DAL B paths would not compliant as described in the second bullet of 5.2.1 in SAE ARP 4754A.

Suggested Change

Either modify the text on page 9 to point to paragraph 5.2.1 or add text to say that while the top level is assigned A, this does not supersede the general principles found in paragraph 5.2.1 of SAE ARP 4754A

response

Noted.

The concern is accepted but the proposed text, which is referred to in the comment, has been withdrawn (please refer to the response to comment 4).

comment

51 comment by: *Textron Aviation*

The paragraph “(2) if a *hazardous failure condition* could result from a possible development error in an aeroplane/system function or item, the associated Development Assurance processes are assigned Level B;” conflicts with paragraph 5.2.1 in SAE ARP 4754A. The implication is that two DAL C paths would not compliant as described in the fourth bullet of 5.2.1 in SAE ARP 4754A.

Suggested Change

Either modify the text on page 9 to point to paragraph 5.2.1 or add text to say that while the top level is assigned B, this does not supersede the general principles found in paragraph 5.2.1 of SAE ARP 4754A.

response

Noted.

The concern is accepted but the proposed text, which is referred to in the comment, has been withdrawn (please refer to the response to comment 4).

comment

52 comment by: *Textron Aviation*

The paragraph ” (3) if a *major failure condition* could result from a possible development error in an aeroplane/system function or item, the associated Development Assurance processes are assigned Level C;” conflicts with paragraph 5.2.1 in SAE ARP 4754A. The implication is that two DAL D paths would not compliant as described in the sixth bullet of 5.2.1 in SAE ARP 4754A.

Suggested Change

Either modify the text on page 9 to point to paragraph 5.2.1 or add text to say that while the top level is assigned C, this does not supersede the general principles found in paragraph 5.2.1 of SAE ARP 4754A

response

Noted.

The concern is accepted but the proposed text, which is referred to in the comment, has been withdrawn (please refer to the response to comment 4).

comment

53 comment by: *Textron Aviation*

The row titled “Allowable Development Assurance Level (FDAL/IDAL)” implies that only these levels are acceptable for each of the hazard classifications. This conflicts with paragraph 5.2.1 and table 3 in SAE ARP 4754A.

Suggested Change
Either modify the table on page 10/Figure 2 to point to paragraph 5.2.1 and Table 3 in SAE ARP 4754A or explain further the intent of the text “Allowable”.
Another option would be to use the approach the FAA use in Figure 2 of AC 23.1309-C/D/E when describing Development Assurance Levels, and modify it for 4754A. Catastrophic, Top Level is DAL A, Two independent DAL B IDALs may be used to support the DAL A, with the remaining IDALs of C or B. Hazardous, Top Level is DAL B, Two independent DAL C IDALs may be used to support the DAL B, with the remaining IDALs of D or C. Major, Top Level is DAL C, Two independent DAL D IDALs may be used to support the DAL C, with the remaining IDALs of E or D.

response

Noted.
The concern is accepted but the proposed text, which is referred to in the comment, has been withdrawn (please refer to the response to comment 4).

comment

56 comment by: *Textron Aviation*

The definition of “development error” clarifies that this concept does not directly relate to failures or CS25.1309.
Suggested Change
Amend the regulatory paragraphs of CS25.1309 to describe the relationship between failure conditions and development errors.

response

Not accepted.
Please refer to the response to comment 17.

comment

57 comment by: *Textron Aviation*

Revisions to section 8, Safety Objective, seeks to add concepts which “minimise the risk of development errors” and “establish development assurance activities at a level that provides an adequate level of confidence that the aeroplane/system functions and items satisfy the objectives of CS 25.1309.” However, minimizing “the risk of development errors” and “development assurance activities” are not concepts found in regulatory paragraph CS25.1309. Therefore, this NPA is introducing new concepts that are not aligned with the current regulatory paragraph. The addition of Note 2 in Figure 2 further clarifies that the Development Assurance Levels cannot be used to quantify the probability of failure occurrence. Therefore, the update to regulatory guidance does not support the regulation to which it references.
Suggested Change
Amend the regulatory paragraphs of CS25.1309 to describe the relationship between severity of a failure condition and DALs similar to how it already describes the relationship between the severity of a failure condition and its allowable quantitative probability.

response

Not accepted.
Please refer to the response to comment 17.

comment

58 comment by: *Textron Aviation*

As noted in paragraph 9b(4), paragraph 9b(1)(iii) should not require that any analysis necessary to show compliance with CS 25.1309(b) must consider the possibility of development errors since these concepts to not appear in CS 25.1309(b). As clarified by the

	definition of “development error,” no such concepts exist in the regulation, therefore, cannot be necessary to show compliance. **Suggested Change** Amend the regulatory paragraphs of CS25.1309 to describe the relationship between severity of a failure condition and development error.
response	Not accepted. Please refer to the response to comment 17.

2.1. Attachments

NPA prposed paragraph 9 .pdf

Attachment #1 to comment #19