European Aviation Safety Agency

Notice of Proposed Amendment 2016-07

Regular update of CS-25

RMT.0673 — 26.7.2016

EXECUTIVE SUMMARY

This Notice of Proposed Amendment (NPA) is based on the 'systematic rulemaking projects' concept introduced into the European Aviation Safety Agency's Management Board Decision replacing Decision 01/2012 on the 'Rulemaking Procedure' (EASA MB Decision 18-2015 of 15 December 2015). This concept aims at improving the efficiency of the EASA rulemaking process.

The specific objective of this NPA is to propose an amendment to CS-25 following the selection of non-complex, non-controversial and mature subjects. The ultimate goal is to increase safety.

This NPA proposes to:

— amend CS 25.1309 and AMC 25.1309 in order to clarify the provisions related to the exception of cabin safety equipment from CS 25.1309(b); and

— amend AMC 25.1309 in order to reflect the current aircraft and systems development practices that make use of development assurance levels (DALs) assignments; the proposal introduces the relationship between the severity of a failure condition and the DAL.

The proposed changes are expected to contribute to updating CS-25 (Book 1 and Book 2) to reflect the available state of the art and facilitate the certification process. Overall, this would bring a moderate safety benefit, would have no social or environmental impacts, and may provide some minor economic benefits by streamlining the certification process.

Applicability		Process map	
Affected regulations and decisions:	ED Decision 2003/2/RM (CS-25)	Terms of reference (ToR), Issue 1:	27.4.2015
Affected stakeholders:	Large aeroplane manufacturers and other design organisations involved in safety assessments for large aeroplanes	Concept paper (CP):	No
		Rulemaking group (RMG):	No
		Regulatory impact assessment (RIA) type:	None
		Technical consultation during NPA drafting:	No
		NPA consultation duration:	2 months
Driver/origin:	Efficiency/proportionality	Review group (RG):	No
Reference:	N/a	Focused consultation:	No
		Opinion expected publication date in:	N/a
		Decision expected publication date in:	2016/Q4

Table of contents

1. Procedural information

1.1. The rule development procedure

The European Aviation Safety Agency (hereinafter referred to as the 'Agency') developed this Notice of Proposed Amendment (NPA) in line with Regulation (EC) No 216/2008[1] (hereinafter referred to as the 'Basic Regulation') and the Rulemaking Procedure[2].

This rulemaking activity is included in the Agency's 5-year Rulemaking Programme under RMT.0673.

The text of this NPA has been developed by the Agency. It is hereby submitted for consultation of all interested parties[3].

The process map on the title page contains the major milestones of this rulemaking activity to date and provides an outlook of the timescales of the next steps.

1.2. The structure of this NPA and related documents

Chapter 1 of this NPA contains the procedural information related to this task. Chapter 2 (Explanatory Note) explains the core technical content. Chapter 3 contains the proposed text for the amendment of CS-25. This NPA does not require a RIA (please refer to Chapter 4).

1.3. How to comment on this NPA

Please submit your comments using the automated **Comment-Response Tool (CRT)** available at **http://hub.easa.europa.eu/crt/**[4].

The deadline for submission of comments is **27 September 2016**.

1.4. The next steps in the procedure

Following the closing of the NPA public consultation period, the Agency will review all comments. The outcome of this consultation will be reflected in a comment-response document (CRD) which the Agency will publish concurrently with the decision. Based on the outcome of the NPA public consultation, the decision will contain the amendments to CS-25.

---

1 Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC (OJ L 79, 19.3.2008, p. 1).

2 The Agency is bound to follow a structured rulemaking process as required by Article 52(1) of the Basic Regulation. Such a process has been adopted by the Agency's Management Board (MB) and is referred to as the 'Rulemaking Procedure'. See MB Decision N° 18-2015 of 15 December 2015 replacing Decision 01/2012 concerning the procedure to be applied by the Agency for the issuing of opinions, certification specifications, acceptable means of compliance and guidance material.

3 In accordance with Article 52 of the Basic Regulation and Articles 6(3) and 7 of the Rulemaking Procedure.

4 In case of technical problems, please contact the CRT webmaster (crt@easa.europa.eu).

2. Explanatory Note

2.1. Overview of the issues to be addressed

This NPA addresses the following topics:

— Interfaces between CS 25.1309 and CS 25.810/CS 25.812

The introductory text of CS 25.1309 excepts the functional failures related to function availability from the CS 25.1309(b) provisions. These functional failures were considered adequately covered by CS 25.810 and CS 25.812. However, the current wording used does not clearly reflect the initial intent of this exception. The same applies to the corresponding material of AMC 25.1309.

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

Current AMC 25.1309 provides a relationship between the severity of a failure condition and the allowable quantitative probability of such a condition. However, no such relationship is provided between the severity of a failure condition and DALs.

2.2. Objectives

The overall objectives of the EASA system are defined in Article 2 of the Basic Regulation. This proposal will contribute to the achievement of the overall objectives by addressing the issues outlined in Chapter 2 of this NPA.

The specific objective of this NPA is to propose an amendment of CS-25 based on the selection of non-complex, non-controversial and mature subjects, with the ultimate goal being to increase safety.

2.3. Summary of the RIA

N/a (please refer to Chapter 4).

2.4. Overview of the proposed amendments

— Interfaces between CS 25.1309 and CS 25.810/CS 25.812

Through this NPA, the Agency proposes to clarify the interfaces between CS 25.1309 and CS 25.810/CS 25.812.

The purpose of the current CS 25.1309 introductory text is to except the functional failures related with function availability (e.g. loss of the function) from the CS 25.1309(b) provisions. These functional failures were considered adequately covered by CS 25.810 Emergency egress assisting means and escape routes, and CS 25.812 Emergency lighting. The current CS 25.1309(b) provisions remain applicable to functional failures related with function integrity (e.g. untimely activation of the function).

The current wording used in CS 25.1309, as well as in the corresponding AMC 25.1309, is deemed unclear, therefore an amendment of CS 25.1309 and AMC 25.1309 is proposed to better reflect the initial intent described above.

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

Errors in the requirements, design or implementation are mitigated by development assurance processes. These processes establish confidence that the development process of aircraft/system functions and items has been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety. The DAL is the measure of the rigour applied to the development process to limit, at an acceptable level of safety, the likelihood of errors occurring during the development process of aircraft/system functions and items that may have an adverse safety effect if they are exposed in service.

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.

However, 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.

3. Proposed amendments

The text of the amendment is arranged to show deleted text, new or amended text as shown below:

(a) deleted text is marked with ~~strike through~~;

(b) new or amended text is highlighted in grey;

(c) an ellipsis (…) indicates that the remaining text is unchanged in front of or following the reflected amendment.

3.1. Draft certification specifications (CSs) (Draft EASA Decision)

CS-25 — BOOK 1

SUBPART F — EQUIPMENT

1. CS 25.1309 is amended as follows:

CS 25.1309 Equipment, systems and installations

(See AMC 25.1309)

The requirements of this paragraph, except as identified below, are applicable, in addition to specific design requirements of CS-25, to any equipment or system as installed in the aeroplane. Although this paragraph does not apply to the performance and flight characteristic requirements of Subpart B and the structural requirements of Subparts C and D, it does apply to any system on which compliance with any of those requirements is dependent. Certain single failures or jams covered by CS 25.671(c)(1) and CS 25.671(c)(3) are excepted from the requirements of CS 25.1309(b)(1)(ii). Certain single failures covered by CS 25.735(b) are excepted from the requirements of CS 25.1309(b). The functional failures ~~effects~~related to function availability of cabin safety equipment covered by CS 25.810~~(a)(1)(v)~~ and CS 25.812 are excepted from the requirements of CS 25.1309(b). The requirements of CS 25.1309(b) apply to powerplant installations as specified in CS 25.901(c).

(…)

3.2. Draft acceptable means of compliance (AMC)/guidance material (GM) (draft EASA Decision)

CS-25 — BOOK 2

AMC — SUBPART F

1. AMC 25.1309 is amended as follows:

AMC 25.1309

System Design and Analysis

(…)

4. *APPLICABILITY OF CS 25.1309*.

Paragraph 25.1309 is intended as a general requirement that should be applied to any equipment or system as installed, in addition to specific systems requirements, except as indicated below.

(…)

d. The functional failures ~~effects~~related to function availability of cabin safety equipment covered by CS 25.810~~(a)(1)(v)~~ and CS 25.812 are excepted from the requirements of CS 25.1309(b). These functional ~~Failure Conditions associated with these cabin safety equipment installations~~failures are indeed associated with varied evacuation scenarios for which the probability cannot be determined. It has not been proven possible to define appropriate scenarios under which compliance with CS 25.1309(b) can be demonstrated. It is therefore considered more practical to require particular design features or specific reliability demonstrations, as described in CS 25.810 and CS 25.812 ~~and except these items of equipment from the requirements of CS 25.1309(b)~~. Traditionally, this approach has been found to be acceptable.

(…)

5. *DEFINITIONS.*

The following definitions apply to the system design and analysis requirements of CS 25.1309 and the guidance material provided in this AMC. They should not be assumed to apply to the same or similar terms used in other regulations or AMCs. Terms for which standard dictionary definitions apply are not defined herein.

(…)

j. *Development Error*. A mistake in requirements, design or implementation.

~~j~~k. *Error.* An omission or incorrect action by a crewmember or maintenance personnel, or a mistake in requirements, design, or implementation.

~~k~~l. *Event.* An occurrence which has its origin distinct from the aeroplane, such as atmospheric conditions (e.g. gusts, temperature variations, icing and lightning strikes), runway conditions, conditions of communication, navigation, and surveillance

services, bird-strike, cabin and baggage fires. The term is not intended to cover sabotage.

~~l~~m. *Failure.* An occurrence, which affects the operation of a component, part, or element such that it can no longer function as intended, (this includes both loss of function and malfunction). Note: Errors may cause Failures, but are not considered to be Failures.

~~m~~n. *Failure Condition.* A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.

~~n~~o. *Installation Appraisal.* This is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry-accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service.

p. *Item*. A hardware or software element having bounded and well-defined interfaces.

~~o~~q. *Latent Failure.* A failure is latent until it is made known to the flight crew or maintenance personnel. A significant latent failure is one, which would in combination with one or more specific failures, or events result in a Hazardous or Catastrophic Failure Condition.

~~p~~r. *Qualitative.* Those analytical processes that assess system and aeroplane safety in an objective, non-numerical manner.

~~q~~s. *Quantitative.* Those analytical processes that apply mathematical methods to assess system and aeroplane safety.

~~r~~t. *Redundancy.* The presence of more than one independent means for accomplishing a given function or flight operation.

~~s~~u. *System*. A combination of components, parts, and elements, which are inter-connected to perform one or more functions.

(…)

8. *SAFETY OBJECTIVE.*

a. The objective of CS 25.1309 is to ensure an acceptable safety level for equipment and systems as installed on the aeroplane. A logical and acceptable inverse relationship must exist between the Average Probability per Flight Hour and the severity of *failure condition* effects, as shown in Figure 1, such that:

(1) Failure Conditions with No Safety Effect have no probability requirement.

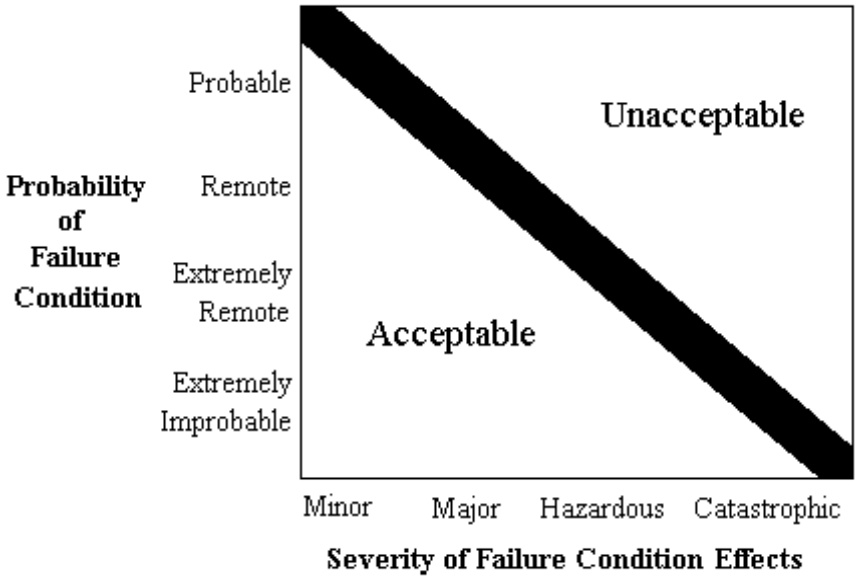
(2) Minor Failure Conditions may be Probable.

(3) Major Failure Conditions must be no more frequent than Remote.

(4) Hazardous Failure Conditions must be no more frequent than Extremely Remote.

(5) Catastrophic Failure Conditions must be Extremely Improbable.

Figure 1: Relationship between Probability and Severity of Failure Condition Effects



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.

b. The safety objectives associated with Failure Conditions are described in Figure 2.

Figure 2: Relationship Between ~~Probability and Severity of Failure Condition~~Severity of Failure Condition, Probability, and Development Assurance Level (DAL)

Effect on Aeroplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Allowable Qualitative Probability	No Probability Requirement	<-Probable->	<--Remote-->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative Probability: Average Probability per Flight Hour on the Order of:	No Probability Requirement	<----------> $<10^{-3}$ Note 1	<----------> $<10^{-5}$	<----------> $<10^{-7}$	$<10^{-9}$
Allowable Development Assurance Level (FDAL/IDAL) (See Note 2)	Level E	Level D	Level C	Level B	Level A
Classification of Failure Conditions	No Safety Effect	<---Minor--->	<---Major--->	<Hazardous>	Catastrophic

Note 1: A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category aeroplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.

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.

9. *COMPLIANCE WITH CS 25.1309.*

This paragraph describes specific means of compliance for CS 25.1309. The applicant should obtain early concurrence of the certification authority on the choice of an acceptable means of compliance.

(…)

b. *Compliance with CS 25.1309(b).*

(…)

(4) *Acceptable Application of Development Assurance Methods.* Paragraph 9b(1)(iii) above requires that any analysis necessary to show compliance with CS 25.1309(b) must consider the possibility of ~~requirement, design, and implementation~~development errors. Errors made during the design and 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. For more complex or integrated systems, exhaustive testing may either be impossible because all of the system states cannot be determined or impractical because of the number of tests which must be accomplished. For these types of systems, compliance may be shown by the use of Development Assurance. 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~~potential 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.

Guidelines, which may be used for providing Development Assurance, are described for ~~aircraft~~aeroplane and systems development in the ~~D~~document referenced in ~~paragraph~~ (3)(b)(2) above, and for software in Documents referenced in paragraph 3a(3). ~~(~~There is currently no agreed Development Assurance standard for airborne electronic hardware.~~) Because these documents were not developed simultaneously, there are differences in the guidelines and terminology that they contain. A significant difference is the guidance provided on the use of system architecture for determination of the appropriate development assurance level for hardware and software. EASA recognises that consideration of system architecture for this purpose is~~

~~appropriate. If the criteria of Document referenced in paragraph 3b(2) are not satisfied by a particular development assurance process the development assurance levels may have to be increased using the guidance of Document referenced in paragraph 3a(3).~~

(…)

4. RIA

This NPA does not introduce new provisions for applicants. Some clarifications of existing CSs (CS-25 Book 1 and Book 2) are proposed, based on common certification practices and recognised international standards. There is no need to develop a RIA.

5. References

5.1. Affected regulations

N/a

5.2. Affected decisions

Decision No. 2003/2/RM of the Executive Director of the Agency of 17 October 2003 on certification specifications, including airworthiness codes and acceptable means of compliance, for large aeroplanes ('CS-25')

5.3. Reference documents

— European Organisation for Civil Aviation Equipment (EUROCAE) ED-79A — Guidelines for Development of Civil Aircraft and Systems, November 2011

— Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A, Guidelines for Development of Civil Aircraft and Systems, 21 December 2010