



NOTICE OF PROPOSED AMENDMENT (NPA) 2012-11

DRAFT DECISION OF THE EXECUTIVE DIRECTOR OF THE EUROPEAN AVIATION SAFETY AGENCY

**amending Decision No. 2003/12/RM of the Executive Director of the European Aviation Safety Agency of 5 November 2003 on Acceptable Means of Compliance for airworthiness of Products, Parts and Appliances
(« AMC-20 »)**

***'Recognition of ED-12C/DO-178C in EASA AMC 20-115
(Software Considerations for Airborne Systems and Equipment Certification)'***

and

***'Certification of Aircraft Propulsion Systems Equipped with Electronic Controls'
(AMC 20-1)***

and

***'Certification of Essential APUs Equipped with Electronic Controls'
(AMC 20-2)***

and

***'Certification of Engines Equipped with Electronic Engine Control Systems'
(AMC 20-3)***

and

***'Airworthiness Approval and Operational Criteria For the Use of Navigation Systems
in European Airspace Designated For Basic RNAV Operations'
(AMC 20-4)***

and

***'Airworthiness Approval and Operational Criteria for RNP
APPROACH (RNP APCH) Operations Including APV BAROVNAV'
(AMC 20-27)***

EXECUTIVE SUMMARY

The scope of this rulemaking activity is to upgrade a number of AMCs following upgrade of EUROCAE document ED-12 from version 'B' to version 'C' and parallel upgrade of RTCA DO-178.

Although software matters, in the current mandate of the Agency, cover several subjects, much beyond the safety considerations for software hosted in airborne systems and equipment during related initial airworthiness processes, only the latter are in the scope of this NPA, which proposes amendments to the following Acceptable Means of Compliance (AMC) for airworthiness approval (i.e. series of AMC 20-XX):

- AMC 20-115 on software considerations for airborne systems and equipment;
- AMC 20-1 on certification of aircraft propulsion systems equipped with electronic controls;
- AMC 20-2 on certification of essential APU equipped with electronic controls;
- AMC 20-3 on certification of engines equipped with electronic engine control systems;
- AMC 20-4 on airworthiness approval and operational criteria for use of navigation systems in European airspace designated for basic RNAV operations; and
- AMC 20-27 on airworthiness approval and operational criteria for RNP APPROACH (RNP APCH) operations including APV BARO-VNAV operations.

References to ED-12B and RTCA DO-178B have already been removed from CS-25 through amendment 12 published on 6 July 2012.

CS-ETSO will be updated through RMT.0206 (ETSO.011) planned to be initiated in 2013.

ED-12C does not change the basic approach for software Development Assurance Level (DAL) in comparison to previous edition 'B' published in 1992. So the impact on software developers is minimal. But the new edition 'C' is aligned with the progress of the state of the art achieved during the last 20 years and, furthermore, it is supported by a number of associated guidance documents. ED-12C is also technically equivalent to RTCA DO-178C and related supporting documents, which is an excellent basis for world-wide harmonisation.

It is anticipated that the adoption of the proposed rules will lead to improved safety without creating undue burden or other adverse effects such as the discontinuation of established and well-proven software DAL processes for software hosted in aircraft, engine or APU systems and equipment.

The purpose of this Notice of Proposed Amendment is to collect the opinions of stakeholders on the proposed amendments to the mentioned six AMC 20-XX.

Based on the outcome of the consultation on this NPA, the Agency might decide to amend the mentioned AMC 20-XX.

TABLE OF CONTENTS

| | |
|--|-----------|
| A. EXPLANATORY NOTE | 4 |
| I. GENERAL | 4 |
| II. CONSULTATION | 5 |
| III. COMMENT RESPONSE DOCUMENT | 5 |
| IV. CONTENT OF THE DRAFT OPINION/DECISION | 5 |
| SOFTWARE AND SOFTWARE DEVELOPMENT PROCESSES..... | 5 |
| BACKGROUND OF DOCUMENT ED-12C | 7 |
| SUMMARY OF DIFFERENCES BETWEEN ED-12C AND ED-12B | 9 |
| SUPPLEMENTS TO ED-12C | 9 |
| AMENDMENT 12 TO CS-25 | 11 |
| ENVISAGED CHANGES TO CS-ETSO | 11 |
| DRAFT DECISION AMC 20-115 | 11 |
| DRAFT DECISION AMC 20-1 | 12 |
| DRAFT DECISION AMC 20-2 | 12 |
| DRAFT DECISION AMC 20-3 | 13 |
| DRAFT DECISION AMC 20-4 | 13 |
| DRAFT DECISION AMC 20-27 | 13 |
| V. REGULATORY IMPACT ASSESSMENT | 14 |
| B. DRAFT DECISION(S) | 23 |
| I. DRAFT DECISION AMC 20-115C - SOFTWARE CONSIDERATION FOR CERTIFICATION OF AIRBORNE SYSTEMS AND EQUIPMENT | 24 |
| II. DRAFT DECISION AMC 20-1 - CERTIFICATION OF AIRCRAFT PROPULSION SYSTEMS EQUIPPED WITH ELECTRONIC CONTROLS | 28 |
| III. DRAFT DECISION AMC 20-2 - CERTIFICATION OF ESSENTIAL APUS EQUIPPED WITH ELECTRONIC CONTROLS..... | 29 |
| IV. DRAFT DECISION AMC 20-3 - CERTIFICATION OF ENGINES EQUIPPED WITH ELECTRONIC ENGINE CONTROL SYSTEMS | 30 |
| V. DRAFT DECISION AMC 20-4 - AIRWORTHINESS APPROVAL AND OPERATIONAL CRITERIA FOR THE USE OF NAVIGATION SYSTEMS IN EUROPEAN AIRSPACE DESIGNATED FOR BASIC RNAV OPERATIONS . | 34 |
| VI. DRAFT DECISION AMC 20-27 - AIRWORTHINESS APPROVAL AND OPERATIONAL CRITERIA FOR RNP APPROACH (RNP APCH) OPERATIONS INCLUDING APV BAROVNAV OPERATIONS | 35 |

A. Explanatory Note

I. General

1. The purpose of this Notice of Proposed Amendment (NPA) is to envisage amending Decision 2003/12/RM of the Executive Director of 05 November 2003¹ to replace AMC 20-115B (recognition of EUROCAE ED-12B/RTCA-178B) by the new version AMC 20-115C. The revised AMC recognises edition 'C' of EUROCAE/RTCA documents ED-12/DO-178 concerning 'Software Considerations in Airborne Systems and Equipment Certification'. In addition also other Agency's AMCs are being aligned with the mentioned recent industry standards.
2. The scope of this rulemaking activity is outlined in the Terms of Reference (ToR) RMT.0462, Issue 1, of 6 July 2012 on software considerations for airborne systems and equipment and is described in more detail below.
3. The European Aviation Safety Agency (hereinafter referred to as the 'Agency') is directly involved in the rule-shaping process. It assists the European Commission in its executive tasks by preparing draft regulations, and amendments thereof, for the implementation of the Basic Regulation² which are adopted as 'Opinions' (Article 19(1)). It also adopts Certification Specifications, including Airworthiness Codes and Acceptable Means of Compliance and Guidance Material to be used in the certification process (Article 19(2)).
4. When developing rules, the Agency is bound to follow a structured process as required by Article 52(1) of the Basic Regulation. Such a process has been adopted by the Agency's Management Board and is referred to as 'The Rulemaking Procedure'³.
5. This rulemaking activity is included in the Agency's Rulemaking Programme for 2013-16 and it implements the rulemaking task RMT.0462 'software considerations for airborne systems and equipment'.
6. The text of this NPA has been developed by the Agency. It is submitted for consultation by all interested parties in accordance with Article 52 of the Basic Regulation and Articles 5(3) and 6 of the Rulemaking Procedure.
7. The proposed rule is not related to the development of European Union or international law (ICAO), but it is related to harmonisation with the rules of other authorities of the European Union main partners as set out in the objectives of article 2 of the Basic Regulation. In fact the proposed rule is harmonised with recent amendments to EUROCAE voluntary standards, paralleled by equivalent standards published by the American Radio Technical Commission for Aeronautics (RTCA). The latter are usually recognised by FAA and TCCA.

¹ Decision No. 2003/12/RM of the Executive Director of the European Aviation Safety Agency of 5 November 2003 on Acceptable Means of Compliance for airworthiness of Products, Parts and Appliances (« AMC-20 »). Decision as last amended by Decision 2011/001/R of the Executive Director of the Agency of 30 March 2011.

² 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, 19.03.2008, p. 1). Regulation as last amended by Regulation 1108/2009 of the European Parliament and of the Council of 21 October 2009 (OJ L 309, 24.11.2009, p. 51).

³ EASA MB Decision 01-2012 of 13 March 2012 amending and replacing MB Decision 08-2007 concerning the procedure to be applied by the Agency for the issuing of opinions, certification specifications and guidance material ('Rulemaking Procedure').

II. Consultation

8. To achieve optimal consultation, the Agency is publishing the draft decision of the Executive Director on its internet site. Comments should be provided within 3 months in accordance with Article 6(4) of the Rulemaking Procedure.
9. Please submit your comments using the **automated Comment-Response Tool (CRT)** available at <http://hub.easa.europa.eu/crt/>.⁴
10. The deadline for the submission of comments is **22 November 2012**.

III. Comment response document

11. All comments received in time will be responded to and incorporated in a Comment-Response Document (CRD). The CRD will be available on the Agency's website and in the Comment-Response Tool (CRT).

IV. Content of the draft Opinion/Decision**Software and software development processes**

12. Software (SW) is already widely used in civil aviation for innumerable applications, many of which can have safety implications. The number of SW applications constantly grew during the past decades and this trend is expected to continue, if not to accelerate. In order to maintain high and uniform safety for European civil aviation, all the SW related development processes need to be regulated and subject to proportionate oversight, either directly by the competent authorities or through the safety/software management implemented by certified organisations based on legally binding (implementing) rules.
13. However, due to the extreme variability and flexibility of SW, detailed SW development processes are better regulated through non-legally binding rules, such as Acceptable Means of Compliance (AMCs) or Certification Specifications (CSs). Any 'soft rule' adopted and published by the Agency must have a legal basis in the Basic Regulation and be in compliance with the provisions of related implementing rules or other EU legislation.
14. The current mandate of the Agency covers several subjects, much beyond the safety considerations for SW hosted in airborne systems and equipment during related initial airworthiness processes and before integration at product (or APU) level. In other words the scope of this NPA is much narrower than the scope of EASA for SW matters. In this Explanatory Note the proposed 'soft rules' are hence put into the context of the Agency's mandate for the 'total aviation system'.
15. The current Agency's mandate covers all aviation domains (i.e. initial airworthiness, continuous airworthiness, design and production of ATM/ANS systems and constituents, software considerations for services consisting in the origination and processing of data and formatting and delivering data to general air traffic for the purpose of safety-critical air navigation, as well as management of the SW throughout its life cycle, mainly by aircraft operators and Air Navigation Service Providers (ANSPs).
16. The processes involving SW development are several and all of them have a basis in applicable Regulations, as summarised in Table 1 below:

| SW life cycle | Segments | Sub-domain | Legal basis | Commission Regulations | Agency's 'soft rules' |
|----------------------|-----------------|-------------------|--------------------|-------------------------------|------------------------------|
| Airborne SW | Airborne | Initial | Art. 5 | Part 21 | CS-23, 25, 27 & |

⁴ In case the use of the Comment-Response Tool is prevented by technical problems please report them to the CRT webmaster (crt@easa.europa.eu).

| | | | | | |
|------------------------------|---|---|----------------------------------|--|--|
| | systems and equipment | airworthiness (IAW) of aircraft | B.R. | | 29 and several AMC 20-XX |
| | | IAW of engines | | | CS-E |
| | | IAW of APU | | | CS-APU |
| | | IAW of SW hosted by systems and equipment | | | CS-ETSO |
| | | Integrated Modular Avionics (IMA) | | | No published 'soft' rules |
| | Electronic Flight Bags (EFB) | Art. 5 and 8 B.R. | Proposed by NPA 2012-02 | Proposed by NPA 2012-02 | |
| Ground/space segments | ATM/ANS systems and constituents | | Regulation 482/2008 ⁵ | No published 'soft' rules | |
| Data bases | ATS routes including instrument procedures | | Art. 8b B.R. | Annex V to Regulation 73/2010 ⁶ | No published 'soft' rules |
| | Aeronautical Information Publications (AIP) or equivalent digital information | | | | No published 'soft' rules |
| | Data for navigation | | | | 'common requirements' for ANSPs ⁷ |
| | Other data for EFB | | Art. 5 and 8 B.R. | OPS rules proposed by NPA 2012-02 | Proposed by NPA 2012-02 |
| Management during operations | Design | Changes to SW | Art. 5, 8, 8b B.R. | Part 21 and Reg. 482/2008 | N.A. |
| | Continuous Airworth. (CAW) | | Art 5 B.R. | Part M | Not published |
| | Administr. EFB | | Art. 8 B.R. | OPS rules proposed by NPA 2012-02 | Proposed by NPA 2012-02 |
| | ATM/ANS SW management | | Art. 8b B.R. | Regulation 482/2008 | No published 'soft' rules |

Table 1: Regulated SW processes in aviation

17. Neither SW aspects nor ED-12/DO-178, are mentioned in detail in the following CSs, for which an update is hence not necessary in the context of this NPA:

- CS-22 (Sailplanes and Powered Sailplanes);
- CS-23 (Normal, Utility, Aerobatic and Commuter Aeroplanes);
- CS-27 (Small Rotorcraft);
- CS-29 (Large Rotorcraft);
- CS-31GB (Gas Balloons);
- CS-31HB (Hot Air Balloons);
- CS-34 (Aircraft Engine Emissions and Fuel Venting);
- CS-36 (Aircraft Noise);
- CS-AWO (All Weather Operations);
- CS-LSA (Light Sport Aeroplanes);

⁵ Commission Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005 (*OJ L 141, 31.5.2008, p. 5-10*).

⁶ Commission Regulation (EU) No 73/2010 of 26 January 2010 laying down requirements on the quality of aeronautical data and aeronautical information for the single European sky (*OJ L 23, 27.1.2010, p. 6-27*).

⁷ Commission implementing Regulation (EU) No 1035/2011 of 17/10/2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010 (*OJ L/271, 18/10/2011, p.23*).

- CS-P (Propellers);
 - CS-VLA (Very Light Aeroplanes); and
 - CS-VLR (Very Light Rotorcraft).
18. The management or maintenance of SW during operations (either by aircraft operators or by Air Navigation Service Providers (ANSPs) and the development and management of data bases are also out of scope of this NPA.
19. Equally out of scope are the processes for the development of SW used in ground and space constituents of operational ATM/ANS systems.
20. In the domain of initial airworthiness:
- CS-23, CS-27, CS-29, CS-E and CS-APU mention SW processes, but without specific reference to ED-12 or any other industry standards: therefore it is not necessary to amend such CSs;
 - references to ED-12B/DO-178B in CS-25 have already been replaced by reference to AMC 20-115 in amendment 12⁸ of CS-25; and
 - they will be amended in CS-ETSO through RMT.0206 (ETSO.011).
21. In conclusion, the scope of this NPA is only to propose amendments to the following AMC for airworthiness approval (i.e. series of AMC 20-XX):
- AMC 20-115 on airborne SW hosted in aircraft (or engine) systems and equipment;
 - AMC 20-1 on certification of aircraft propulsion systems equipped with electronic controls;
 - AMC 20-2 on certification of essential APU equipped with electronic controls;
 - AMC 20-3 on certification of engines equipped with electronic engine control systems;
 - AMC 20-4 on airworthiness approval and operational criteria for use of navigation systems in European airspace designated for basic RNAV operations; and
 - AMC 20-27 on airworthiness approval and operational criteria for RNP APPROACH (RNP APCH) operations including APV BAROVNAV operations.

Background of document ED-12C

22. In May 1980, the Radio Technical Commission for Aeronautics, now RTCA Inc., established Special Committee 145 (SC-145), "Digital Avionics Software", to develop and document software practices that would support the development of software based airborne systems and equipment. The European Organisation for Civil Aviation Electronics, now the European Organisation for Civil Aviation Equipment (EUROCAE), had previously established Working Group 12 (WG-12) to produce a similar document.
23. EUROCAE elected to work in concert with RTCA to develop a common set of guidelines. SC-145 produced RTCA Document DO-178, "Software Considerations in Airborne Systems and Equipment Certification", which was published in January 1982. EUROCAE published the first edition of ED-12 shortly thereafter.
24. Early in 1983 RTCA determined that DO-178 should be revised to reflect the experience gained in the certification of the aircraft and engines containing software-based systems and equipment. It established the new Special Committee 152 (SC-152) for this purpose.

⁸ Decision No. 2003/02/RM of the Executive Director of the European Aviation Safety Agency of 17 October 2003 on certification specifications, including airworthiness codes and acceptable means of compliance, for large aeroplanes (« CS-25 »). Decision as last amended by Decision 2012/008/R of the Executive Director of the Agency of 06 July 2012(CS-25 Amendment 12).

25. A revised RTCA document, DO-178A, "Software Considerations in Airborne Systems and Equipment Certification", was hence published in 1985. Shortly thereafter, EUROCAE published ED-12A, which was identical in technical content to DO-178A.
26. In early 1989, the FAA formally requested to RTCA to establish once more a Special Committee for the review and revision of DO-178A. In fact since 1985, aircraft manufacturers, avionics industry and competent airworthiness authorities world-wide had used DO-178A or the equivalent EUROCAE ED-12A as the primary source of the guidelines to determine the acceptability of airborne systems and equipment containing software. But rapid advances in software technology and differing interpretations in some crucial areas, indicated that the guidelines required revision.
27. An RTCA ad hoc group was consequently formed to review the issues and experience associated with the application of DO-178A. RTCA Special Committee 167 (SC-167) produced version 'B', published in 1992 and once more paralleled by ED-12B. ED-12B and DO-178B provided the aviation community with guidance for determining, in a consistent manner and with an acceptable level of confidence, that the software aspects of airborne systems and equipment comply with airworthiness requirements and has served its purpose for about 20 years, including after recognition by the Agency in 2003, through publication of AMC 20-115B.
28. Since 1992, aviation industry and certification authorities around the world have used the considerations in ED-12B/DO-178B as an acceptable means of compliance for software approval in the certification of airborne systems and equipment. As experience was gained in the use of ED-12B/DO-178B, questions arose regarding the document's content and application. Some of these questions were addressed through the work of SC-190/WG-52 which culminated in the development of ED-94B/DO-248B.
29. However, ED-94B/DO-248B did not contain additional guidance for use as compliance: only clarifications. Additionally, advances in hardware and software technology resulted in software development methodologies and issues that were not adequately addressed in either ED-12B/DO-178B or ED-94B/DO-248B.
30. Therefore in 2004, the FAA, the JAA and aviation industry representatives initiated a discussion with the RTCA and EUROCAE concerning the advances in software technology since 1992, when ED-12B/DO-178B had been published. In December 2004, the RTCA and EUROCAE approved the sponsorship of a joint special committee/working group, Special Committee 205/Working Group 71 (SC-205/WG-71) with the purpose of:
 - Evaluating the reported issues in SW development;
 - Modifying ED-12B/DO-178B to become ED-12C/DO-178C;
 - Modifying ED-94B/DO-248B to become ED-94C/DO-248C;
 - Consolidating Software Development Guidance and Guidelines;
 - Developing and documenting technology-specific or method-specific guidance and guidelines;
 - Modifying ED-109/DO-278 to become ED-109A/DO-278A;
 - Maintaining the objective-based approach for software assurance;
 - Maintaining the technology independent nature of the ED-12B/DO-178B and ED-109/DO-278 objectives.
31. The cooperative efforts of SC-205 and WG-71 culminated in the publication of RTCA document DO-178C and EUROCAE document ED-12C (January 2012).
32. The revised ED-12C guidance is intended to provide an acceptable means of compliance to achieve approval of software aspects of airborne systems. The primary purpose of the revision to ED-12B are:
 - to continue to promote safe implementation of aviation software;

- to provide clearer and more consistent relationships to the systems development processes and safety assessment processes;
- to address emerging trends and technologies in software development; and
- to provide an approach that is flexible and allows change in the technology.

Summary of differences between ED-12C and ED-12B

33. The ED-12C update covers:
- a. Errors and Inconsistencies: ED-12C introduced editorial changes to remove errors and inconsistencies which emerged during concrete application of ED-12B;
 - b. Consistent Terminology: specific terms such as "guidance", "guidelines", "purpose", "goal", "objective", and "activity" are now used consistently throughout the document;
 - c. Wording Improvements: ED-12C introduced wording improvements throughout the document to make it more precise and clear; these changes did not alter the original intent of ED-12B;
 - d. Objectives and Activities: ED-12C reinforced the point that, in order to fully understand the recommendations, the full body of this document should be considered;
 - e. Supplements: ED-12C recognized that new software development techniques may result in new issues. Rather than expanding the text to account for all the current software development techniques (and revising it yet again to account for future techniques), ED-12C acknowledged that one or more supplements may be used in conjunction with ED-12C to modify the guidance for specific techniques;
 - f. Tool Qualification: The terms "development tool" and "verification tool" are replaced by three tool qualification criteria that determine the applicable tool qualification level (TQL) in regard of the software level. The guidance to qualify a tool is removed in ED-12C, but provided in a domain independent, external document, referenced to in ED-12C;
 - g. Coordinated System/Software Aspects: ED-12C updated system aspects relating to software development to reflect current system practices. The updates were based upon coordination with the committees that were updating ED-79/ARP4754 (system-level guidance) at the same time SC-205/WG-71 was updating ED-12B (software-level guidance);
 - h. ED-12B "Hidden" Objectives: ED-12C added the so-called "hidden objectives" such as a means for detecting additional code that is not directly traceable to the Source Code and a means to ensure its verification coverage are defined, as well as assurance that software plans and standards are developed and reviewed for consistency.
 - i. General Topics: ED-12C addressed some general topics that resulted in changes to several sections of the document. The topics included a variety of subjects such as applicants' oversight of suppliers, parameter data items, and traceability. In addressing these topics, two additional objectives were added;
 - j. ED-12B Gaps and Clarifications: finally ED-12C addressed several specific issues that resulted in changes to only one or two paragraphs. Each such change may have an impact upon the applicant as these changes either addressed clear gaps in ED-12B or clarified guidance that was subject to differing interpretations.

Supplements to ED-12C

34. EUROCAE has also published supplements to ED-12C that extend the guidance to specific techniques. Supplements are to be used in conjunction with the ED-12C document and may be used in conjunction with one another.

35. These supplements are:

- ED-94C "Supporting Information for ED-12C and ED-109A";
- ED-215 "Software Tool Qualification Considerations";
- ED-218 "Model-based Development and Verification Supplement to ED-12C and ED-109A";
- ED-217 "Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A";
- ED-216 "Formal Methods Supplement to ED-12C and ED-109A".

Amendment 12 to CS-25

36. This NPA proposes no changes whatsoever to CS-25. However, only for information purposes, it is recalled that the already mentioned amendment 12 to CS-25 includes changes stemming from other rulemaking tasks, as well as editorial changes. The latter include removing references to ED-12/DO-178 and replacing them by references to AMC 20-115. This avoids in the future the need to amend CS-25 if new editions of SW related RTCA or EUROCAE documents are published.
37. The paragraphs of CS-25 affected by this change of reference were:
- a. AMC 25.703: Take-off Configuration Warning Systems;
 - b. AMC 25.729: Retracting Mechanism;
 - c. AMC 25.735: Brakes and Braking Systems Certification Tests and Analysis;
 - d. AMC 25.1309: System Design and Analysis;
 - e. AMC No. 1 to CS 25.1329: Flight Guidance System;
 - f. AMC 25.1581, Appendix 1: Computerized Aeroplane Flight Manual; and
 - g. General AMC 25.11: Electronic Flight Deck Displays.

Envisaged changes to CS-ETSO

38. ED-12B and DO-178B are mentioned in paragraph 2.2 in Subpart A (General) of CS-ETSO. This Subpart therefore also needs to be updated. The Agency intends to do this in the context of:
- The second NPA of RMT.0186 (ETSO.007), planned around the end of 2012, for subpart A (General) of CS-ETSO; and
 - RMT.0206 (ETSO.011), planned to be initiated in 2013, for the individual ETSOs (i.e. subpart C of CS-ETSO).
39. In preparation of RMT.0206, stakeholders' indications, in the form of comments on this NPA, for which ETSOs should be amended in relation to the new edition 'C' of ED-12 and associated guidance, are welcomed.

Draft Decision AMC 20-115

40. AMC 20-115B⁹ on recognition of EUROCAE ED-12B/RTCA DO-178B concerning SW considerations in airborne systems and equipment certification, was published through Decision No. 2003/12/RM of 05 November 2003.
41. It is obvious that this AMC needs to be updated from edition 'B' to 'C' in order to recognise the new editions 'C' of mentioned EUROCAE/RTCA documents. In doing so, the opportunity will be taken not only to also mention the additional guidance documents developed by EUROCAE and RTCA, but in general to improve the clarity of the AMC and to introduce as well some editorial changes.
42. AMC 20-115B (and the new proposed edition C) apply to the certification of any aircraft type, other product, APU, airborne system or equipment where SW is embedded, irrespective of the Certification Specification (CS-23, CS-25, CS-29 or other) used to build the certification basis for the product.

⁹ http://www.easa.europa.eu/agency-measures/docs/agency-decisions/2003/2003-012-RM/decision_ED_2003_12_RM.pdf

43. Hence, this NPA proposes to update AMC 20-115 from edition 'B' to 'C', but also, as explained below, to refer only to this AMC from any other Agency CSs or AMC 20-XX. This will avoid in the future the need to update multiple documents if new editions of ED-12 or DO-178 (or related documents and supplements) are published, as well as preventing possible discrepancies on SW provisions across various Agency regulatory documents.
44. The major envisaged changes are to:
- introduce a title (i.e. 'Software considerations ...') more related to the subject and possibly clearer for readers;
 - clarify and limit the purpose and scope of the AMC to airborne SW (i.e. excluding e.g. data bases and excluding SW used on the ground for ATM/ANS systems and constituents);
 - update the reference to ED-12 and DO-178 from edition 'B' to 'C', but also referring to the associated guidance documents and supplements;
 - provide more background and explanatory information; and
 - better specify the conditions under which previous editions of ED-12/DO-178 may be used.
45. The proposed text applies to newly developed SW modules, for which the airworthiness request is received after the entry into force of the new version C of the AMC. An earlier version of AMC 20-115, if requested by the applicant, may apply to changes to pre-existing software, on the basis of rule 21A.101(b)3, when the TC/STC basis for the product included such earlier version, under the conditions specified in par; 8 of the proposed AMC 20-115c.
46. Where necessary, in relation to the paragraph immediately above, the Agency may in any case issue special conditions in compliance with Part 21A.16B, in particular for reuse of equipment hosting already approved SW in new product designs.

Draft Decision AMC 20-1

47. AMC 20-1¹⁰ on certification of aircraft propulsion systems equipped with electronic controls was published through Decision No. 2003/12/RM of 05 November 2003. It gives guidance on the precautions to be taken for the use of electronic technology, including SW, for engine/propeller control, protection and monitoring and, where applicable, for integration of functions specific to the aircraft.
48. Par. 4.3 therein requires that the associated SW must have a quality level and architecture appropriate to its criticality. This general principle does not need to be amended.
49. However, par. 4.5.1 therein currently refers to ED-12A and DO-178A. These references need to be deleted and replaced by reference to AMC 20-115.

Draft Decision AMC 20-2

50. AMC 20-2¹¹ on certification of essential APU equipped with electronic controls was equally published through Decision No. 2003/12/RM of 05 November 2003. It provides guidance for electronic (analogue and digital) essential APU control systems, on the interpretation and means of compliance with the relevant APU and aircraft certification requirements.

¹⁰ http://www.easa.europa.eu/agency-measures/docs/agency-decisions/2003/2003-012-RM/decision_ED_2003_12_RM.pdf

¹¹ http://www.easa.europa.eu/agency-measures/docs/agency-decisions/2003/2003-012-RM/decision_ED_2003_12_RM.pdf

51. Par. 4.3 therein still refers to ED-12A and DO-178A. These references need to be deleted and replaced by reference to the latest edition of AMC 20-115.

Draft Decision AMC 20-3

52. AMC 20-3¹² on certification of engines equipped with electronic engine control systems was published in Annex III to ED Decision 2007/019/R of 19 December 2007. It gives guidance on the precautions to be taken for the use of electrical and electronic technology for engine control, protection, limiting and monitoring functions, and, where applicable, for integration of aircraft or propeller functions.
53. ED12A/DO-178A and ED-12B/DO-178B are mentioned in paragraphs (3) and (6)(e)(ii)(B) therein. This NPA proposes to replace such references by reference to the latest edition of AMC 20-115.
54. The entire paragraph (10) in AMC 20-3 is devoted to software design and implementation. Of course also this paragraph needs to be aligned with recent developments of related industry standards.

Draft Decision AMC 20-4

55. Also AMC 20-4¹³ on airworthiness approval and operational criteria for use of navigation systems in European airspace designated for Basic RNAV operations was published through Decision No. 2003/12/RM of 05 November 2003. It provides guidance related to navigation systems intended to be used for Basic RNAV operations and considers existing airworthiness approval standards as providing acceptable means of compliance.
56. In the list of related documents contained in paragraph 2 therein, neither ED12 nor DO-178 are mentioned. However, not even AMC 20-115 is listed. This needs to be corrected.
57. Furthermore, reference to ED-12B/DO-178B in Annex I in AMC 20-4 needs to be replaced by reference to AMC 20-115.

Draft Decision AMC 20-27

58. Finally, AMC 20-27¹⁴ on airworthiness approval and operational criteria for RNP APPROACH (RNP APCH) operations including APV BARO VNAV published through Decision No. 2009/019/R of 16 December 2009, needs to be aligned with the new editions of ED-12 and DO-178. AMC 20-27 includes airworthiness and operational criteria related to RNAV systems based on a GNSS standalone receiver, or multi-sensor systems including at least one GNSS sensor, intended to be used under Instrument Flight Rules, including in Instrument Meteorological Conditions, in designated European airspace. It contains also airworthiness and operational criteria related to systems based upon the use of barometric altitude and RNAV information in the definition of vertical paths and vertical tracking to a path to conduct APV BAROVNAV operations.
59. In the list of related documents contained in paragraph 4.2.2 therein AMC 20-115 is not listed, while ED12 and DO-178 are mentioned in 4.2.5. This NPA proposes to eliminate reference to ED-12 and DO-178, while introducing reference to AMC 20-115.

¹² [http://www.easa.europa.eu/agency-measures/docs/agency-decisions/2007/2007-019-R/Annex%20to%20Decision%202007-019-R%20-%20\(New%20AMC%2020-3\).pdf](http://www.easa.europa.eu/agency-measures/docs/agency-decisions/2007/2007-019-R/Annex%20to%20Decision%202007-019-R%20-%20(New%20AMC%2020-3).pdf)

¹³ http://www.easa.europa.eu/agency-measures/docs/agency-decisions/2003/2003-012-RM/decision_ED_2003_12_RM.pdf

¹⁴ <http://www.easa.europa.eu/agency-measures/docs/agency-decisions/2009/2009-019-R/Annex%20III%20-%20AMC%2020-27.pdf>

60. Furthermore, reference to ED-12B/DO-178B in Annex I in AMC 20-27 needs to be replaced by reference to AMC 20-115. The same for Note 4 in paragraph 6.4 therein.

V. Regulatory Impact Assessment

1. Issue analysis and risk assessment

1.1. What is the issue and the current regulatory framework?

General

a. Issue which the NPA is intended to address

For about 40 years, software (SW) has been more and more used in airborne systems, including for safety related applications. The traditional techniques (e.g. calculations, tests in laboratory or flight test) to demonstrate compliance of aircraft and related systems with safety rules are not suitable to assess the safety of SW.

Since 1980, the aviation industry has therefore developed guidance material. In particular RTCA and EUROCAE published in 1982 the first edition of respective documents DO-178 and ED-12. These documents have been widely recognised as one, albeit not the unique, Acceptable Means of Compliance (AMC) by several aviation authorities including the FAA and the Agency.

In the '80s the evolution of the state of the art on SW development quickly evolved, leading to subsequent editions A (1985) and B (1992) of said documents.

But of course, the evolution of the state of the art did not stop and now, after 20 years from editions B, both RTCA and EUROCAE have published new editions C accompanied by a set of additional guidance documents.

Currently a number of Agency's AMC make explicit reference to EUROCAE ED-12B and RTCA DO-178B. But these documents are now obsolete, due to the recent publication of edition C. It is true that applicants could always request to use as AMC a more recent document, but of course the optimum would be offering to industry updated guidance and so avoiding discussions on deviations with the Agency.

The issue discussed in this RIA is therefore the need and the best way to modernize the guidance offered by Agency to industry for development of airborne SW.

Scale of the issue

Currently there are 288 valid Design Organisation Approvals (DOA) issued by the Agency. It is estimated that at least 250 organisations deliver parts or products including digital computers and hence SW. Not all these companies develop SW by themselves, but they need to know which are the SW requirements, even if this SW is procured by other specialized companies.

Since its establishment in 2003, the Agency has issued (i.e. in 10 years), about 220 TCs to aeroplanes, 23 to rotorcraft and 91 to engines. Almost all aircraft in the Agency's competence today embed SW to execute functions relevant at aircraft level and also several engines.

Furthermore the Agency has issued, in about 10 years of his life, about 5000 Supplemental Type Certificates (STCs), i.e. about 500 per year. It is estimated that about 200 per year include also SW modules.

1.2 Who is affected?

All potential applicants for Agency airworthiness approvals of airborne SW (i.e. airborne parts, systems or products hosting SW).

1.3 What are the safety risks

Even without aligning its guidance to the state of the art, the Agency can check the safety of the SW following applications for airworthiness approvals. Although the absence of material aligned with the state of the art could require more effort for both the Agency and the applicant, nevertheless the probability of the materialization of hazards linked to improper SW processes is estimated as **extremely improbable**.

SW malfunctions are generally not deemed capable of causing catastrophic consequences. However, since SW applications are becoming more and more important for the functionality of essential airborne systems, the worst credible severity of the effects of a SW malfunction could be estimated as **hazardous**.

According to AMC 25.1309¹⁵ 'hazardous' refers to a failure condition (e.g. a mechanical or electrical failure, but also a SW malfunction while the HW remains serviceable), which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be:

- (i) A large reduction in safety margins or functional capabilities;
- (ii) Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or
- (iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew.

¹⁵ <http://www.easa.europa.eu/agency-measures/docs/certification-specifications/CS-25/CS-25%20Amdt%2012.pdf>.

The above considerations are summarised in the following risk matrix¹⁶:

Table 1: Safety risk matrix¹⁷

| Probability of occurrence | | Severity of occurrence | | | | |
|-----------------------------|---|------------------------|-------|-------|-----------|--------------|
| | | Negligible | Minor | Major | Hazardous | Catastrophic |
| | | 1 | 2 | 3 | 5 | 8 |
| Extremely improbable | 1 | | | | X | |
| Improbable | 2 | | | | | |
| Remote | 3 | | | | | |
| Occasional | 4 | | | | | |
| Frequent | 5 | | | | | |

From the above safety risk matrix one can observe that the risk index is 5, which means that there is no urgent need to do anything to solve a safety issue.

2. Objectives

The general objectives given by the EU legislator to the Agency are listed in Article 2 of the Basic Regulation, go however beyond safety. In fact they include the objectives to:

- establish and maintain a high uniform level of civil aviation safety in Europe; but also
- facilitate the free movement of goods, persons and services (e.g. by having rules aligned with the latest industry state of the art);
- promote cost-efficiency in the regulatory and certification processes (e.g. by avoiding discussions on possible 'obsolescence' of Agency's rules);

¹⁶ The matrix is based on the ICAO Safety Management Manual. [Doc 9859 Safety Management Manual – 2nd Edition - 2009](#). The green boxes correspond to low significance issues, the yellow to medium significance issues, and the red to high significance issues. See also the Annex for further details on the risk matrix.

¹⁷ Enter the risk index in the appropriate box. For example, an issue that has been identified as 'improbable' and 'catastrophic' would get a risk index of $2 \times 8 = 16$. Put the result in the appropriate box of the table.

- provide a level playing field for all actors in the internal aviation market (e.g. by publishing clear and updated rules, available to all from the web, instead of agreeing to apply the latest industry standards only with individual applicants).

The specific objectives of this NPA are hence to update a number of Agency's AMCs to:

- maintain high safety for the airworthiness approval of airborne SW;
- promote cost-efficiency during certification programmes, as well as a level playing field and the free movement of SW (or products or parts incorporating SW) based on the latest achievements of the state of the art.

3. Identification of options

The following five options have been identified:

| No. | Option |
|-----|---|
| 0 | 'Do nothing' in which case the Agency's rules would continue to refer to editions 'B' of ED-12 and DO-178 and the possibility of using more modern AMCs could be negotiated with applicants on a case-by-case basis. |
| 1 | Simple 'recognition' of edition 'C' of ED-12/DO-178, without mentioning additional guidance material and without providing even minimal explanations. |
| 2 | Publish a revised AMC 20-115C of no more than five pages, containing also some explanation and reference not only to ED-12C/DO-178C, but also to the associated documents; in parallel, introduce in other Agency's 'soft rules' only reference to AMC 20-115 (i.e. not directly to industry standards). |
| 3 | As 2 for AMC 20-115 but directly refer to ED-12C/DO-178C and associated industry documents in all other affected Agency 'soft rules'. |
| 4 | Reproduce the total content of ED-12C and its associated documents in AMC 20-115C, whose size would then become more than one hundred pages. |

4. Impacts

All identified impacts are qualitatively assessed (RIA light) and expressed in terms of a score = a numerical single digit from -3 (highly negative) to +3 (highly positive).

Safety scores — since safety is the primary objective of the Agency as per Article 2 of the Basic Regulation — are assigned a weight of 3. Environmental scores, based on the same article, have a weight of 2. Other scores have a weight of 1.

i. Safety

Although current safety index (5 as estimated above) does not require urgent action (= even the 'do nothing' option is sufficiently safe), some of the possible options may however be safer or less safe in comparison of each other. A safety assessment is hence appropriate.

The five options can be compared from the safety perspective in the table below:

| | 0 | 1 | 2 | 3 | 4 |
|----------------------------|--------------------------------------|-----------------------------|------------------------------|---|---|
| Options | Do nothing | AMC 20-115C = 1 page | AMC 20-115C = 5 pages | As 2, but ED-12C referred in other rules | AMC 20-115C = 100 pages (or more) |
| Assessment | No safety impact | No safety impact | No safety impact | Possible future mismatch between AMC 20-115 and other rules | As 2, but also possible mismatch with industry standards, even if only for edition errors |
| Score (un-weighted) | 0 | 0 | 0 | -1 | -2 |
| Weight | Multiply the un-weighted score by: 3 | | | | |
| Score (weighted) | 0 | 0 | 0 | -3 | -6 |

ii. Social

All identified options are neutral from the social point of view.

iii. Economic

The five options can be compared from the economic perspective in the table below:

| Options | 0 | 1 | 2 | 3 | 4 |
|----------------------------|--|---|---|--|--|
| | Do nothing | AMC 20-115C = 1 page | AMC 20-115C = 5 pages | As 2, but ED-12C referred in other rules | AMC 20-115C = 100 pages (or more) |
| Assessment | None of the identified options introduces new requirements for industry | | | | |
| | Possible lengthy discussions during certification projects due to Agency's rules not aligned with the state of the art | Discussions avoided = cost-efficient certification processes. No adverse economic impact identified | Clearer but still short guidance material for industry No adverse economic impact identified | Need to check and align several Agency's rules, should industry update its documents | Additional rulemaking work and additional time for stakeholders to read. Plus infringement of the EUROCAE copyright, with potential economic consequences for Agency. |
| Score (un-weighted) | -1 | 2 | 2 | -1 | -3 |
| Weight | Multiply the un-weighted score by: 1 | | | | |
| Score (weighted) | -1 | 2 | 2 | -1 | -3 |

iv. Environmental impact

All identified options are neutral from the environmental point of view.

v. *Proportionality issues*

The five options can be compared from the proportionality perspective in the table below:

| Options | 0 | 1 | 2 | 3 | 4 |
|---------------------|--|---|--|--|---|
| | Do nothing | AMC 20-115C = 1 page | AMC 20-115C = 5 pages | As 2, but ED-12C referred in other rules | AMC 20-115C = 100 pages (or more) |
| Assessment | Small and Medium Enterprises (SMEs) may have difficulties in understanding the misalignment of the Agency's rules with respect to industry documents | SMEs will lack even minimum clarification before purchasing EUROCAE or RTCA documents | Before purchasing EDs or DOs SMEs would have minimum information to orient their choice towards the documents really required for them | As 2 | Even more guidance to SMEs through documents available through the web free of charge |
| Score (un-weighted) | -1 | -1 | 2 | 2 | 3 |
| Weight | Multiply the un-weighted score by: 1 | | | | |
| Score (weighted) | -1 | -1 | 2 | 2 | 3 |

vi. *Regulatory coordination and harmonisation*

The five options can be compared from the harmonisation perspective in the table below:

| | 0 | 1 | 2 | 3 | 4 |
|----------------------------|---|-----------------------------|------------------------------|---|--|
| Options | Do nothing | AMC 20-115C = 1 page | AMC 20-115C = 5 pages | As 2, but ED-12C referred in other rules | AMC 20-115C = 100 pages (or more) |
| Assessment | Probably misaligned with FAA/TCCA rules, which may well recognise RTCA DO-178C and associated documents | Aligned with FAA/TCCA | Aligned with FAA/TCCA | Aligned with FAA/TCCA | Infringement of legal rules on the copyright |
| Score (un-weighted) | -2 | 2 | 2 | 2 | -3 |
| Weight | Multiply the un-weighted score by: 1 | | | | |
| Score (weighted) | -2 | 2 | 2 | 2 | -3 |

5. Conclusion and preferred option

a. *Comparison of the positive and negative impacts for each option evaluated*

Using the Multi-Criteria Analysis (MCA) methodology, the 'weighted' scores assigned above are algebraically summed:

| | 0 | 1 | 2 | 3 | 4 |
|----------------------|-----------------------|-----------------------------|------------------------------|---|--|
| Options | Do nothing | AMC 20-115C = 1 page | AMC 20-115C = 5 pages | As 2, but ED-12C referred in other rules | AMC 20-115C = 100 pages (or more) |
| | Weighted score | | | | |
| Safety | 0 | 0 | 0 | -3 | -6 |
| Social impact | 0 | 0 | 0 | 0 | 0 |
| Economic | -1 | 2 | 2 | -1 | -3 |

| | | | | | |
|---------------------------------|-----------|-----------|----------|----------|-----------|
| impact | | | | | |
| Environment | 0 | 0 | 0 | 0 | 0 |
| Proportionality | -1 | -1 | 2 | 2 | 3 |
| Regulatory harmonisation | -2 | 2 | 2 | 2 | -3 |
| TOTAL | -4 | 3 | 6 | 0 | -9 |

b. Final assessment and recommendation of a preferred option

Options 3 (ED-12C/DO-178C referred directly in multiple Agency's documents) and 4 ('copy and paste' of all EUROCAE material in AMC 20-115C) have a negative safety score (this means that they would make today's safe situation worse). But, even more important, Option 4 would potentially infringe the laws on copyright, while option 3 would be (as today) cumbersome for the Agency to maintain, having referred ED-12 in multiple regulatory documents. Neither option 3 nor 4 is therefore recommended.

Options 0, 1 and 2 are all neutral from the safety perspective (i.e. risk index remains at 'safe' level of 5 as today).

However option 0 ('do nothing') shows an overall negative score, since not aligned with current state of the art.

The remaining two options 1 and 2 exhibit a positive total (weighted) score and are equivalent and neutral in terms of safety. Among them, however, option 2 has the highest total score and, in particular, it is the best one in terms of proportionality, since, before purchasing ED or DO documents, small and medium-sized enterprises (SMEs) would have minimum information to orient their choice towards the documents really required for them.

Therefore, Option 2 (i.e. AMC 20-115C of no more than 5 pages and reference to it in other Agency 'soft rules') is the preferred one.

B. Draft Decision(s)

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

1. deleted text is shown with a strike through: ~~deleted~~
2. changed or new text is highlighted with grey shading: **new**
3. ... indicates that the remaining text is unchanged in front of or following the reflected amendment.

I. Draft Decision AMC 20-115C - Software consideration for certification of airborne systems and equipment

AMC 20-115C

~~Recognition of Eurocae ED-12B / RTCA DO-178B~~

Software considerations for certification of airborne systems and equipment

1 PURPOSE

This Acceptable Means of Compliance (AMC) provides a means that can be used to demonstrate that the safety aspects of software hosted on airborne systems and equipment comply with requirements for initial airworthiness in order to obtain an airworthiness approval.

In particular, the purpose of this document is to provide guidelines for the production of software for airborne systems and equipment that performs its intended function with a level of confidence in safety that complies with airworthiness requirements.

2 SCOPE

This AMC discusses those aspects of airworthiness certification that pertain to the production of software for airborne systems and equipment used on aircraft, engines, propellers, APU or others parts.

In discussing those aspects, the system life cycle and its relationship with the software life cycle are considered to aid in the understanding of the certification process.

Other system and software life cycle processes are out of scope of this AMC. For instance, out of scope are:

- system safety assessment and validation processes at product level, in the context of initial airworthiness certification of aircraft and engines;
- software considerations for the verification of ground and space systems and constituents of Air Traffic Management (ATM)/Air Navigation Services (ANS);
- software considerations for services consisting of the origination and processing of data and formatting and delivering data to general air traffic for the purpose of safety-critical air navigation;
- administration and management of software throughout its life cycle by aircraft operators, including for Electronic Flight Bags (EFB), and by Air Navigation Service Providers (ANSP).

Since certification issues for initial airworthiness are discussed only in relation to the software life cycle, the operational aspects of the resulting software are not discussed. For example, the certification, approval and management aspects of user-modifiable data are beyond the scope of this document.

This document does not provide guidelines concerning the structure of the applicant's organization, the relationships between the applicant and its suppliers, or how the responsibilities are divided.

Personnel qualification criteria are also beyond the scope of this document.

Compliance with this AMC is not mandatory and hence an applicant may elect to use an alternative means of compliance. However, those alternative means of compliance must meet

the relevant requirements, ensure an equivalent level of software safety and be approved by the European Aviation Safety Agency on a product basis.

3 PROCEDURES; METHODS AND TOOLS FOR SOFTWARE CONSIDERATION

This AMC ~~acceptable means of compliance calls attention to~~ recognises that the European Organisation for Civil Aviation Equipment (EUROCAE) document ED-12BC, "Software Considerations in Airborne Systems and Equipment Certification", issued in January ~~December~~ ~~1992~~ 2012, related guidance documents and supplements or equivalent RTCA Inc. documents, constitute an acceptable means of compliance for software (SW) aspects of certification that pertain to the production of software for airborne systems and equipment used on aircraft, engines, propellers and auxiliary power units. It discusses how the document may be applied to certification programmes administered by the European Aviation Safety Agency.

2 4 RELATED DOCUMENTS

4.1 EUROCAE document ED-12C, "Software Considerations in Airborne Systems and Equipment Certification", describes the acceptable processes to develop and verify SW for airborne systems and equipment.

4.2 ~~2.1~~ EUROCAE document ED-12BC is technically equivalent to RTCA Inc. document DO-178BC. A reference to one document, at the same revision level, may be interpreted to mean either document.

4.3 The application of ED-12C/DO-178C may be supported by the following related documents and supplements:

- ED-94C/DO-248C "Supporting Information for ED-12C and ED-109A" documents;
- ED-215/DO-330 "Software Tool Qualification Considerations" document;
- ED-216/DO-333 "Formal Methods - Supplement to ED-12C and ED-109A";
- ED-217/DO 332 "Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A"; and
- ED-218/DO-331 "Model-based Development and Verification - Supplement to ED-12C and ED-109A".

~~2.2~~ 4.4 The technical content of this AMC is ~~based on~~ harmonised with FAA AC 20-115-B, dated 11 January 1993 equally based on ED-12/DO-178.

3 5 RELATED CERTIFICATION SPECIFICATIONS (CSs)

Part 21, CS-22, CS-23, CS-25, CS-27, CS-29, CS-AWO, CS-E, CS-P, CS-APU, CS-ETSO and CS-VLA. Existing references to ED-12/DO-178, and ED-12A/DO-178A and ED-12B/DO-178B in the above CSs will be amended, at the next opportunity, to take into account the principles spelt out in paragraph 6. below replaced by reference to this AMC to provide a single source of regulatory material on airborne software, applicable to any aeronautical product, APU or equipment.

4.6 BACKGROUND

~~4.1~~ EUROCAE document ED-12BC was developed to establish software considerations for developers, installers and users when the aircraft system or equipment design is implemented developed using software based techniques. Current and future avionics designs will make extensive use of this technology. The EUROCAE document provides guidelines for establishing software levels, software life cycle planning, development, verification, configuration management, and quality assurance and certification liaison processes disciplines to be used in software-based systems.

The guidelines provided in ED-12C are in the form of:

- objectives for software life-cycle processes;
- descriptions of activities and design considerations for achieving those objectives; and
- descriptions of the evidence that indicates that the objectives have been satisfied.

Document ED-94C was developed to provide supporting information for ED-12C and the ED-215 document was developed to explain Software Tool Qualification Considerations. They should both be considered as supplemental documents to be used jointly with ED-12C.

ED-216 is a supplement to ED-12C that was developed to provide specific considerations regarding Formal Methods.

ED-217 is a supplement to ED-12C that was developed to provide specific considerations regarding Object-Oriented Technology and Related Techniques.

ED-218 is a supplement to ED-12C that was developed to provide specific considerations regarding the techniques of Model-based Development and Verification.

Whenever one or more of the techniques addressed by these last three supplements is used in software-based systems, the corresponding supplement or supplements to ED-12C / DO-178C should be applied in addition to ED-12C / DO-178C itself.

~~4.2~~ The document ED-12C and related supplements specifies specify the information to be made available and/or delivered to the Agency. Guidance is also provided also for dealing with software developed to earlier standards, tool qualification and alternative methods which may be used.

5.7 USE OF EUROCAE ED-12BC AND RELATED DOCUMENTS AND SUPPLEMENTS PROCEDURES

An applicant for EASA certification for any software-based equipment or system may use the considerations outlined in EUROCAE document ED-12BC and its related documents and applicable supplements, as a means, but not the only means, to secure approval. The Agency may publish acceptable means of compliance for specific CSs, stating the required relationship between the criticality of the software-based systems and the software levels as defined in EUROCAE document ED-12BC. Such acceptable means of compliance will take precedence over the application of EUROCAE document ED-12BC.

6.8 USE OF PREVIOUS VERSIONS

Previous ED-12/DO-178 and ~~ED-12A/DO-178A~~ versions may will continue to be accepted for modifications to the software of already certified systems and equipment where these have been accepted as the basis for approval or certification, provided that:

- the Software development assurance level of the software is not increased;

- the Software is installed in the same type of aircraft or engine as that in which the original software was installed;
- the techniques described in the ED-12C / DO-178C supplements (MBD, OOTRT, Formal Methods) are not introduced into the new project; otherwise, ED-216 and/or ED-217 and/or ED-218 should be applied;
- the software development and verification processes and environment are not significantly changed;
- the initial software development and verification processes and environment have been adequately maintained and can still be used;
- the Software change is not major (see the software criteria given within Appendix A to GM 21A.91) and the system change is not significant (see GM 21A.101);
- no new software development or verification tools are used;
- no new software tool qualification is needed; otherwise ED-215 should be applied;
- no new Parameter Data Item files are introduced;
- there are no changes in the operational use of the system.

Early coordination with EASA is strongly recommended to validate the above assumptions. Appropriate Certification Review Items might be raised if necessary.

7.9 AVAILABILITY OF EUROCAE DOCUMENTS ~~ED-12B~~

Copies may be purchased from EUROCAE, 17 rue Hamelin, 75783 PARIS Cedex 16, 102 rue Étienne Dolet, 92240 Malakoff, France, (Fax : 33 1 46 55 62 65 4505 7230).

II. Draft Decision AMC 20-1 - Certification of Aircraft Propulsion Systems Equipped with Electronic Controls

.....

4.5 Precautions Relating to Failure Modes Common to More Than One Engine/Propeller

4.5.1 System design

For digital systems, any residual errors not activated during the software development and ~~certification~~ verification processes could cause a failure common to more than one Engine/Propeller. ~~RTCA DO178B (or the equivalent EUROCAE ED 12B)~~ The latest edition of AMC 20-115 constitutes an acceptable means of compliance for software development and ~~certification~~ verification.

It should be noted ~~however that the DO178A states in paragraph 3.3—~~
~~It is appreciated that, with the current state of knowledge,~~ the software disciplines described in ~~this document~~ AMC 20-115 may not, in themselves, be sufficient to ensure that the overall system safety and reliability targets have been achieved. This is particularly true for certain critical systems, such as full authority fly-by-wire digital engine control systems. In such cases, it is accepted that other measures, usually within the system, in addition to a high level of software discipline, may be necessary to achieve these safety objectives and demonstrate that they have been met.

It is outside the scope of ~~this document~~ AMC 20-115 to suggest or specify these measures, but in accepting that they may be necessary, it is also the intention to encourage the ~~development~~ use of software techniques which could support meeting the overall system safety objectives.¹

...

III. Draft Decision AMC 20-2 - Certification of Essential APUs Equipped with Electronic Controls

...

4.3 Precautions relating to APU control, protection and monitoring

The software associated with APU control, protection and monitoring functions must have a quality development assurance level (DAL) and architecture appropriate to their criticality of those functions (see paragraph 4.2).

For digital systems, any residual errors not activated detected during the software development and certification verification processes could cause an unacceptable failure. (RTCA DO178A (or the equivalent EUROCAE ED-12A) The latest edition of AMC 20-115 constitutes an acceptable means of compliance for software development, verification and software aspects of certification. The APU software should be at least level B2 according to this the industry documents referred in AMC 20-115. In some specific cases, level A1 may be more appropriate.

It should be noted however that the DO178A states in paragraph 3.3—
~~It is appreciated that, with the current state of knowledge,~~ the software disciplines described in this document AMC 20-115 may not, in themselves, be sufficient to ensure that the overall system safety and reliability targets have been achieved. This is particularly true for certain critical systems, such as full authority fly-by-wire digital control systems. In such cases it is accepted that other measures, usually within the system, in addition to a high level of software discipline, may be necessary to achieve these safety objectives and demonstrate that they have been met.

It is outside the scope of this document AMC 20-115 to suggest or specify these measures, but in accepting that they may be necessary, it is also the intention to encourage the development use of software techniques which could support meeting the overall system safety objectives.¹

...

IV. Draft Decision AMC 20-3 - Certification of Engines Equipped with Electronic Engine Control Systems

...

(3) RELEVANT SPECIFICATIONS AND REFERENCE DOCUMENTS

Although compliance...

...

The following documents are referenced in this AMC 20-3:

- International Electrotechnical Commission (IEC), Central Office, 3, rue de Varembé, P.O. Box 131, CH - 1211 GENEVA 20, Switzerland
 - IEC/PAS 62239, Electronic Component Management Plans, edition 1.0, dated April 2001.
 - IEC/PAS 62240, Use of Semiconductor Devices Outside Manufacturers' Specified Temperature Ranges, edition 1.0, dated April 2001.
- RTCA, Inc. 1828 L Street, NW, Suite 805, Washington, DC 20036 or EUROCAE, 17, rue Hamelin, 75116 Paris, France
 - ~~RTCA DO-178A/EUROCAE ED-12A, Software Considerations in Airborne Systems and Equipment Certification, dated March 1985~~
 - ~~RTCA DO-178B/EUROCAE ED-12B, Software Considerations in Airborne Systems and Equipment Certification, dated December 1, 1992~~
 - RTCA DO-254/ EUROCAE ED-80, Design Assurance Guidance for Airborne Electronic Hardware, dated April 19, 2000.
- AMC 20-115 on software considerations for certification of airborne systems and equipment.

...

(6) SYSTEM DESIGN AND VALIDATION

(a) Control Modes - General

...

(e) Environmental conditions

...

(i) Declared levels

...

(ii) Test procedures

(A) General

...

(B) Open loop and Closed loop Testing

HIRF and lightning tests should be conducted as system tests on closed loop or open loop laboratory set-ups.

The closed loop set-up is usually provided with hydraulic pressure to move actuators to close the inner actuating loops. A simplified Engine simulation may be used to close the outer Engine loop.

Testing should be conducted with the Engine Control System controlling at the most sensitive operating point as selected and detailed in the test plans by the applicant. The system should be exposed to the HIRF and lightning environmental threats while operating at the selected condition. There may be a different operating point for HIRF and lightning environmental threats.

For tests in open and closed loop set ups, the following factors should also be considered:

- If special EECs test software is used, that software should be developed and implemented by guidelines defined for software levels of at least ~~Level 2 in DO-178A, Level DAL C in DO-178B, or equivalent~~ as defined in the industry documents referred in the latest edition of AMC 20-115. In some cases, the application code is modified to include the required test code features.
- The system test set-up should be capable of monitoring both the output drive signals and the input signals.
- Anomalies observed during open loop testing on inputs or outputs should be duplicated on the Engine simulation to determine whether the resulting power or thrust perturbations comply with the pass/fail criteria.

...

(10) SOFTWARE DESIGN AND IMPLEMENTATION**(a) Objective**

For Engine Control Systems that use software, the objective of CS-E 50 (f) is to prevent as far as possible software errors that would result in an unacceptable effect on power or thrust, or any unsafe condition.

It is understood that it may be impossible to establish with certainty that the software has been designed without errors. However, if the applicant uses the software level appropriate for the criticality of the performed functions and uses an approved software development ~~and verification processes method~~, the Agency would consider the software to be compliant with the requirement to minimise errors. In multiple Engine installations, the possibility of software errors common to more than one Engine Control System may determine the criticality level of the software.

(b) Approved Methods

Methods for developing software, compliant with the guidelines ~~contained in the latest edition of AMC 20-115 documents RTCA DO-178A/EUROCAE ED-12A and RTCA DO-178B/EUROCAE ED-12B, hereafter referred to as DO-178A and DO-178B, respectively,~~ are acceptable methods. Alternative methods for developing ~~and verifying~~ software may be proposed by the applicant and are subject to approval by the Agency.

Software which is not developed using ~~DO-178B~~ AMC 20-115 is referred to as legacy software. In general, changes made to legacy software applicable to its original installation are assured in the same manner as ~~in~~ the original certification. When legacy software is used in a new aircraft installation that requires ~~DO-178B~~ AMC 20-115, the original approval of the legacy software is still valid, assuming equivalence to the required software level can be ascertained.

If the software equivalence is acceptable to the Agency, the legacy software can be used in the new installation that requires ~~DO-178B~~ AMC 20-115 software. If equivalence cannot be substantiated, all the software changes should be assured using ~~DO-178B~~ AMC 20-115.

(c) Level of software design assurance

In multiple Engine installations, the design, implementation and verification of the software in accordance with ~~Level 1 (DO-178A)~~ or Level A (~~DO-178B~~ AMC 20-115) is normally needed to achieve the certification objectives for aircraft to be type certificated under CS-25, CS-27-Category A and CS-29-Category A.

The criticality of functions on other aircraft may be different, and therefore, a different level of software ~~design~~ development assurance may be acceptable. For example, in the case of a piston engine in a single-engine aircraft, level C (~~DO-178B~~ AMC 20-115) software has been found to be acceptable.

Determination of the appropriate software level may depend on the Failure modes and consequences of those Failures. For example, it is possible that Failures resulting in significant thrust or power increases or oscillations may be more severe than an Engine shutdown, and therefore, the possibility of these types of Failures should be considered when selecting a given software level.

It may be possible to partition non-critical software from the critical software and design and implement the non-critical software to a lower level as defined by the RTCA industry documents referred in AMC 20-115. The adequacy of the partitioning method should be demonstrated. This demonstration should consider whether the partitioned lower software levels are appropriate for any anticipated installations. Should the criticality level be higher in subsequent installations, it would be difficult to raise the software level.

(d) On-Board or Field Software Loading and Part Number Marking

The following guidelines should be followed when on-board or field loading of Electronic Engine Control software and associated Electronic Part Marking (EPM) is implemented.

For software changes, the software to be loaded should have been documented by an approved design change and released with a service bulletin.

For an EECS unit having separate part numbers for hardware and software, the software part number(s) need not be displayed on the unit as long as the software part number(s) is(are) embedded in the loaded software and can be verified by electronic means. When new software is loaded into the unit, the same verification requirement applies and the proper software part number should be verified before the unit is returned to service.

For an EECS unit having only one part number, which represents a combination of a software and hardware build, the unit part number on the nameplate should be changed or updated when the new software is loaded. The software build or version number should be verified before the unit is returned to service.

The configuration control system for an EECS that will be on-board/field loaded and using electronic part marking should be approved. The drawing system should provide a compatibility table that tabulates the combinations of hardware part numbers and software versions that have been approved by the Agency. The top-level compatibility table should be under configuration control, and it should be updated for each change that affects hardware/software combinations. The applicable service bulletin should define the hardware configurations with which the new software version is compatible.

The loading system should be in compliance with the guidelines of ~~DO-178B~~ AMC 20-115.

If the applicant proposes more than one source for loading, (e.g., diskette, mass storage, etc.), all sources should comply with these guidelines.

The service bulletin should require verification that the correct software version has been loaded after installation on the aircraft.

(e) Software Change Category

The processes and methods used to change software should not affect the design assurance level of that software. For classification of software changes, refer to §4 in Appendix A of GM 21A.91.

(f) Software Changes by Others than the TC Holder

There are two types of potential software changes that could be implemented by someone other than the original TC holder:

- option-selectable software, or
- user-modifiable software (UMS).

Option-selectable changes would have to be pre-certified utilising a method of selection which has been shown not to be capable of causing a control malfunction.

UMS is software intended for modification by the aircraft operator without review by the certification authority, the aircraft applicant, or the equipment vendor. For Engine Control Systems, UMS has generally not been applicable. However, approval of UMS, if required, would be addressed on a case-by-case basis.

~~The necessary guidance for UMS is contained in DO-178B, paragraph 2.4. In essence, it conveys the position that~~ In principle, persons others than the TC holder may modify the software within the modification constraints defined by the TC holder, if the system has been certified with the provision for software user modifications. To certify an Electronic Engine Control System with the provision for software modification by persons others than the TC holder, the TC holder should (1) provide the necessary information for approval of the design and implementation of a software change, and (2) demonstrate that the necessary precautions have been taken to prevent the user modification from affecting Engine airworthiness, whether the user modification is correctly implemented or not.

In the case where the software is changed in a manner not pre-allowed by the TC holder as "user modifiable", the "non-TC holder" applicant will have to comply with the requirements given in Part 21, subpart E.

...

V. Draft Decision AMC 20-4 - Airworthiness Approval and Operational Criteria For the Use of Navigation Systems in European Airspace Designated For Basic RNAV Operations

...

2 SCOPE

...

Related navigation documents

EASA Acceptable means of Compliance

AMC 25-11 Electronic Display Systems

AMC 20-5 Acceptable Means of Compliance for Airworthiness Approval and Operational Criteria for the use of the NAVSTAR Global Positioning System (GPS)

AMC 20-115() Software considerations for certification of airborne systems and equipment

...

ANNEX 1

GPS Integrity Monitoring (RAIM) Prediction Program

Where a GPS Integrity Monitoring (RAIM) Prediction Program is used as a means of compliance with paragraph 5.2(a) of this document, it should meet the following criteria:

1. The program should provide prediction of availability of the integrity monitoring (RAIM) function of the GPS equipment, suitable for conducting Basic RNAV operations in designated European airspace.
2. The prediction program software should be developed in accordance with at least ~~RTCA DO-178B/EUROCAE-12B~~, level D guidelines as defined in the industry documents referred in the latest edition of AMC 20-115.
3. The program should use either a RAIM algorithm identical to that used in the airborne equipment, or an algorithm based on assumptions for RAIM prediction that give a more conservative result.
4. The program should ...

VI. Draft Decision AMC 20-27 - Airworthiness Approval and Operational Criteria for RNP APPROACH (RNP APCH) Operations Including APV BAROVNAV Operations

...

4.2.2 EASA

| | |
|--------------------------|---|
| AMC 25-11 | Electronic Flight Deck Display |
| AMC 20-5 | Airworthiness Approval and Operational Criteria for the use of the Navstar Global Positioning System (GPS) |
| AMC 20-115() | Software considerations for certification of airborne systems and equipment |
| ETSOC115() | Airborne Area Navigation Equipment using Multi-Sensor Inputs |
| ETSOC129() | Airborne Supplemental Navigation Equipment Using the Global Positioning System (GPS) |
| ETSOC145() | Airborne Navigation Sensors Using the Global Positioning System (GPS) Augmented by the Wide Area Augmentation System (WAAS) |
| ETSOC146() | Stand-Alone Airborne Navigation Equipment Using the Global Positioning System (GPS) Augmented by the Wide Area Augmentation System (WAAS) |
| ETSOC106() | Air Data Computer |
| EASA OPINION Nr. 01/2005 | Conditions for Issuance of Letters of Acceptance for Navigation Database Suppliers by the Agency (i.e. an EASA Type 2 LoA). EASA OPINION Nr. 01/2005 on "The Acceptance of Navigation Database Suppliers" dated 14 Jan 05 |

...

4.2.5 EUROCAE/RTCA, SAE and ARINC

| | |
|---------------------------|--|
| ED 26 | MPS for airborne Altitude measurements and coding systems |
| ED 72A | Minimum Operational Performance Specification for Airborne GPS Receiving Equipment |
| ED75()/DO236() | Minimum Aviation System Performance Standards: Required Navigation Performance for Area Navigation |
| ED76/DO200A | Standards for Processing Aeronautical Data |
| ED12()/DO178() | Software considerations in airborne systems and equipment certification |
| ED77/DO201A | Standards for Aeronautical Information |
| DO 88 | Altimetry |
| DO 187 | Minimum operational performances standards for airborne area navigation equipment using multi-sensor inputs |
| DO 208 | Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS) |
| DO229() | Minimum Operational Performance Standards for Global Positioning System/Wide Area Augmentation System Airborne equipment |
| ARINC 424 | Navigation System Data Base |
| ARINC 706 | Mark 5 Air Data System |

...

6.4 Integrity

...

Note 4: Traditionally, this requirement has not specifically addressed the airborne system operational software or airborne system databases (e.g. navigation database). However, it is expected that where the RNAV airborne software has been previously shown compliant with the criteria of ~~ED12B/DO178B~~, as a minimum Level C in the industry documents referred in the latest edition of AMC 20-115, as a minimum, it is acceptable for the operations associated with this AMC.

...