European Aviation Safety Agency

Notice of Proposed Amendment 2018-09

Regular update of AMC-20: AMC 20-152 on Airborne Electronic Hardware and AMC 20-189 on Management of Open Problem Reports

RMT.0643

EXECUTIVE SUMMARY

This Notice of Proposed Amendment (NPA) is a joint proposal by the European Aviation Safety Agency (EASA) and the Federal Aviation Adminstration (FAA) to amend in harmonisation both the EASA AMC-20 and FAA AC-20 documents, as follows:

— create a new EASA AMC 20-152A, amend the FAA AC 20-152, and create a new FAA AC 00-72, on the development of airborne electronic hardware (AEH);
— create a new EASA AMC 20-189, new FAA AC-20-189 and AC 00-71, on the management of open problem reports (OPRs).

The objective of the proposal is to update AMC-20 and AC-20 in order to reflect the current state of the art.

Overall, the proposed documents would significantly increase the harmonisation between EASA and the FAA, have no safety, social or environmental impacts, and provide economic benefits by streamlining the certification process.

Action area:	Regular updates/review of rules		
Affected rules:	EASA AMC-20: General acceptable means of compliance for airworthiness of products, parts and appliances; FAA AC 20-152: RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware		
Affected stakeholders:	Aircraft and equipment designers and manufacturers		
Driver:	Efficiency/proportionality	**Rulemaking group:**	No
Impact assessment:	None	**Rulemaking Procedure:**	Standard

20.7.2015	**24.8.2018**	**2019/Q1**

An agency of the European Union

Table of contents

1. About this NPA 3
1.1. How this NPA was developed 3
1.2. How to comment on this NPA 3
1.3. The next steps 3
2. In summary — why and what 4
2.1. Airborne electronic hardware 4
2.1.1. Why we need to change the rules — issue/rationale 4
2.1.2. What we want to achieve — objectives 4
2.1.3. How we want to achieve it — overview of the proposals 4
2.1.4. What are the expected benefits and drawbacks of the proposals 5
2.2. Open problem reports 5
2.2.1. Why we need to change the rules — issue/rationale 5
2.2.2. What we want to achieve – objectives 5
2.2.3. How we want to achieve it – overview of the proposals 6
2.2.4. What are the expected benefits and drawbacks of the proposals 6
3. Proposed amendments and rationale in detail 7
3.1. Draft acceptable means of compliance and guidance material (EASA AMC/FAA AC) on AEH 7
3.1.1. Draft acceptable means of compliance (EASA AMC/FAA AC) 7
3.1.2. Draft EASA guidance material (GM) / FAA AC 00-72 34
3.2. Draft Acceptable Means of Compliance and Guidance Material (EASA AMC/FAA AC) on OPRs 49
3.2.1. Draft acceptable means of compliance (EASA AMC/FAA AC) 49
3.2.2. Draft EASA guidance material (GM) / FAA AC 00-71 60
4. Impact assessment (IA) 67
5. Proposed actions to support implementation 68
6. References 69
6.1.1. Related regulations 69
6.1.2. Affected EASA decisions and FAA AC material 69
6.1.3. Other reference documents 69

1. About this NPA

1.1. How this NPA was developed

EASA jointly developed this NPA with the FAA. The NPA is 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 European Plan for Aviation Safety (EPAS) 2018-2022[3] under rulemaking task RMT.0643.

The text of this NPA is hereby submitted to all interested parties[4] for consultation.

1.2. 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/**[5].

The deadline for submission of comments is **5 October 2018 (CET)**.

1.3. The next steps

Following the closing of the public commenting period, EASA and the FAA will jointly review all the comments received.

Based on the comments received, EASA will develop a decision amending AMC-20 (introducing a new AMC 20-152A on the development of airborne electronic hardware (AEH) and a new AMC 20-189 on the management of open problem reports (OPRs)) and the FAA will publish a revision of its Advisory Circular (AC) 20-152,a new AC 00-72 on AEH, as well as a new AC 20-189 and AC 00-71 on OPRs.

The comments received and the EASA/FAA responses thereto, will be reflected in a comment-response document (CRD). The CRD will be annexed to the EASA decision. The FAA will publish the same responses to the comments along with the revised AC material on the FAA website.

---

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) (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1467719701894&uri=CELEX:32008R0216).

2 EASA is bound to follow a structured rulemaking process as required by Article 52(1) of Regulation (EC) No 216/2008. Such a process has been adopted by the EASA Management Board (MB) and is referred to as the 'Rulemaking Procedure'. See MB Decision No 18-2015 of 15 December 2015 replacing Decision 01/2012 concerning the procedure to be applied by EASA for the issuing of opinions, certification specifications and guidance material (http://www.easa.europa.eu/the-agency/management-board/decisions/easa-mb-decision-18-2015-rulemaking-procedure).

3 https://www.easa.europa.eu/document-library/general-publications/european-plan-aviation-safety-2018-2022

4 In accordance with Article 52 of Regulation (EC) No 216/2008 and Articles 6(3) and 7) of the Rulemaking Procedure. The FAA will publish a notice at https://www.faa.gov/aircraft/draft_docs/ac/

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

2. In summary — why and what

2.1. Airborne electronic hardware

2.1.1. Why we need to change the rules — issue/rationale

The current EASA guidance on airborne electronic hardware is not available in the form of an AMC, and its topics were subject to certification review items (CRIs) raised project by project and available in the form of an EASA certification memorandum. Producing an AMC 20 document would avoid the need for issuing CRIs and would provide common guidance material and acceptable means of compliance that are usable across all certification domains (large aeroplanes, rotorcraft, general aviation, engines, propellers, and European technical standards order (ETSO) articles). The proposed AMC 20-152A would supersede the above mentioned EASA CM-SWCEH-001.

Additionally, some elements of the EASA guidance in the above mentioned CRIs and CM on the development of airborne electronic hardware need to be consolidated for certain areas such as the use of commercial-off-the-shelf (COTS) devices, the development of custom devices and the use of COTS intellectual property (a design function/module/functional block, used to design and implement a part of a custom device).

The current guidance on airborne electronic hardware (AEH) is not harmonised between EASA and the FAA, and this lack of harmonisation has created misalignment and necessitated additional activities in validation projects. EASA and the FAA decided to join their efforts to harmonise their views, by developing common EASA AMC and FAA AC material. For that reason, the proposed EASA AMC 20-152A starts from revision A, in order to facilitate the linkwith its equivalent FAA Advisory Circular (AC) 20-152A.

2.1.2. What we want to achieve — 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 2.1.

The aim of RMT.0643 is to improve the cost-efficiency of the AEH certification process for industry on one side, and for both EASA and the FAA on the other side.

The specific objectives of this proposal are to:

— develop guidance dealing with the development of AEH that is fully harmonised between EASA and the FAA;

— establish a stand-alone document, supplementing the EUROCAE ED-80/RTCA DO-254 industry standard and covering novel technologies in the domain; and

— define objectives for the AEH domain that are generic for all projects so that AEH guidance is no longer defined project by project.

2.1.3. How we want to achieve it — overview of the proposals

The main steps in the development of the new guidance material for AEH development assurance are:

— analysis of experience from past projects that used ED-80/DO-254, and of existing guidance from EASA and the FAA;

— analysis of the topics that are not addressed or not sufficiently addressed in order to avoid elements of the compliance demonstration being missed;

— definition of guidance using objective oriented wording in order to allow applicants some flexibility to propose their own means to satisfy the objectives;

— inclusion of guidance for the development of custom devices;

— inclusion of guidance for the use of COTS intellectual property;

— inclusion of guidance for the use of COTS devices;

— identification of best practices to be located in the EASA guidance material (GM) and FAA AC 00-72.

2.1.4. What are the expected benefits and drawbacks of the proposals

Overall, the proposed amendments would significantly increase the harmonisation between the EASA and FAA AEH guidance, would have no safety, social or environmental impacts, and would provide for economic benefits by streamlining the certification process.

The proposed amendments would significantly reduce or eliminate the number of CRIs or issue papers in the AEH domain.

No drawbacks are expected.

2.2. Open problem reports

2.2.1. Why we need to change the rules — issue/rationale

The current guidance on the management of open problem report (OPR) is not harmonised between EASA and the FAA. It has been decided to include this topic in the software and AEH guidance harmonisation effort that is ongoing, by creating joint EASA AMC and FAA AC material for OPR management, replacing the material currently available through Certification Memoranda EASA CM-SWCEH-001,EASA CM-SWCEH-002, and FAA Order 8110.49.

In addition, OPR management is an overarching issue that encompasses not only the software and AEH domains but also the systems/equipment domains. The available guidance for these domains is not consistent and the new OPR management guidance is an opportunity to align practices across these domains.

Moreover, years of use of the current EASA guidance on OPR management have unveiled several issues and the potential for misinterpretation..

2.2.2. What we want to achieve – 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 section 2.1.

The aim of RMT.0643 is to improve the cost-efficiency of the certification process for industry on one side, and for both EASA and the FAA on the other side.

The specific objectives of this proposal are to:

— develop guidance for OPR management that is harmonised between EASA and the FAA,

— create a stand-alone document for the three domains (Systems, Software and AEH);

— establish a common approach applicable across all certification domains for large aeroplanes, rotorcraft, general aviation, engines and propellers, and ETSO/TSO articles; and

— eliminate the need to issue project specific guidance through EASA means of compliance CRI or FAA issue paper.

2.2.3. How we want to achieve it – overview of the proposals

The main steps in the development of the new OPR management guidance material are:

— analysis of the existing OPR guidance and of experience from past projects (based on authority experience and feedback from industry);

— inclusion of guidance for problem report (PR) management to avoid EASA and the FAA having to discuss problem report reduction plans or acceptable quantitative objectives with applicants;

— inclusion of guidance for OPR classification and assessment;

— inclusion of guidance for OPR reporting;

— clarification of the responsibilities for the different levels of stakeholders;

— identification of best practices to be located in the EASA GM and FAA AC 00-71.

2.2.4. What are the expected benefits and drawbacks of the proposals

Overall, the proposed amendments would significantly increase the harmonisation of the EASA and FAA OPR guidance, would have no safety, social or environmental impacts, and would provide for economic benefits by streamlining the certification process.

No drawbacks are expected.

3. Proposed amendments and rationale in detail

The draft EASA decision consists of:

— a draft acceptable means of compliance (AMC 20-152A): see Section 3.1.1; and

— a draft guidance material document (GM to AMC 20-152A): see Section 3.1.2;

— a draft acceptable means of compliance (AMC 20-189): see Section 3.2.1; and

— a draft guidance material document (GM to AMC 20-189): see Section 3.2.2.

The draft FAA guidance consists of:

— a draft acceptable means of compliance (AC 20-152A): see Section 3.1.1; and

— a draft best practices document (AC 00-72): see Section 3.1.2;

— a draft acceptable means of compliance (AC 20-189): see Section 3.2.1; and

— a draft best practices document (AC 00-71): see Section 3.2.2.

Note: to facilitate the identification of the differences between the EASA and the FAA text proposals, both the AMC and AC material have been presented in Sections 3.1.1 and 3.2.1 of this NPA for AEH and OPR, respectively. Similarly, the GM and AC 00-72 have been compiled into one single Section numbered 3.1.2 of this NPA for AEH, and the GM and AC 00-71 have been compiled into one single Section numbered 3.2.2 of this NPA for OPR. Markings using square brackets '**[**…**]**' and '**<AMC>**'/'**<AC>**' markers have been introduced to facilitate the identification of those differences.

3.1. Draft acceptable means of compliance and guidance material (EASA AMC/FAA AC) on AEH

3.1.1. Draft acceptable means of compliance (EASA AMC/FAA AC)

[**<AMC>** AMC 20-152A: **Development Assurance for Airborne Electronic Hardware**]

[**<AC>** AC 20-152A: **Development Assurance for Airborne Electronic Hardware**]

1. Purpose [of this Advisory Circular (AC)]

1.1 This **[**AMC**]/[**AC**]** describes an acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations for the electronic hardware aspects of airborne systems and equipment in **[**Product**]/[**Type**]** Certification or **[**ETSO Authorisation**]/[**TSO Authorization**]**. **[<AMC>** Compliance with this AMC is not mandatory and an applicant may elect to use an alternative means of compliance. However, the alternative means of compliance must meet the relevant requirements, ensure an equivalent level of safety, and be approved by EASA on a product or ETSO article basis**.] [<AC>** This AC is not mandatory and does not constitute a regulation. However, if you use the means described in the AC, you must follow it in all applicable respects**.]**

1.2 This **[**recognises**]/[**recognizes**]** EUROCAE ED-80, Design Assurance Guidance for Airborne Electronic Hardware, dated April 2000, and RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware, dated April 19, 2000.

1.3 This **[**AMC**]/[**AC**]** describes when to apply EUROCAE ED-80/ RTCA DO-254 and supplements EUROCAE ED-80/ RTCA DO-254 with additional guidance and clarification for the development of custom devices, including the use of commercial off the shelf (COTS) intellectual property (IP), and for the use of complex COTS devices.

Note: EUROCAE ED is hereafter referred to as ED; RTCA DO is hereafter referred to as DO. Where the notation 'ED-80/DO-254' appears in this document, the referenced documents are **[**recognised**]/[**recognized**]** as being equivalent.

2. Applicability

This **[**AMC**]/[**AC**]** may be used by applicants, design approval holders, and developers of airborne systems and equipment containing airborne electronic hardware (AEH) to be installed on **[**type-certified**]/[**type certificated**]** aircraft, engines, and propellers. This applicability includes developers of **[**ETSO**]/[**TSO**]** articles.

This **[**AMC**]/[**AC**]** is applicable to airborne electronic hardware that contributes to functions with a hardware development assurance level (DAL) A, DAL B, or DAL C. For airborne electronic hardware contributing to functions with a hardware DAL C, a limited set of objectives may be applied. When an objective is not applicable to a specific hardware DAL, the applicability restriction is directly indicated within the objective text.

Even though there is a benefit in having a structured development process that ensures a proper flow down of requirements to the hardware and the fulfilment by the hardware of the intended function, demonstration of compliance with the objectives described in this **[**AMC**]/[**AC**]** is not required for circuit board assemblies or for airborne electronic hardware contributing to functions with a hardware DAL D. **[**Appendix**]/[**AC 00-72, Best Practices for Airborne Electronic Hardware Design Assurance Using EUROCAE ED-80( ) and RTCA DO-254( )**]** provides some clarifications that may be used to ensure that the DAL D hardware performs its intended function.

3. <AMC> Document History/<AC> Cancellation

[<AMC>This document is the initial issue of AMC 20-152. This initial issue, harmonised with FAA AC 20-152A, is intentionally set at revision A.**]**

[<AC> This AC cancels AC 20-152, *RTCA, INC., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware*, dated June 30, 2005.**]**

4. Background

This **[**AMC**]/[**AC**]** is related to the development of custom devices in AEH, including the use of commercial-off-the-shelf intellectual property (COTS IP) within custom devices and the use of Complex COTS devices. Each of these three topics is **[**organised**]/[**organized**]** with:

— Background information dedicated to each major topic,

— Applicability, and

— Sections where objectives are described and uniquely identified.

A unique identifier for each objective is defined with a prefix and an index number (i) as follows:

— For the development of custom devices, the identifier is CD-i;

— For the use of COTS IP in custom devices, the identifier is IP-i;

— For the use of COTS devices, the identifier is COTS-i.

The applicant should document in the Plan for Hardware Aspects of Certification (PHAC), or any other related document, the process and activities that the applicant intends to perform to satisfy the objectives of this **[**AMC**]/[**AC**]**.

5. Custom Device Development

This section provides guidance for the development assurance for programmable logic devices (PLDs), field programmable gate arrays (FPGAs), or application specific integrated circuits (ASICs), referred to as custom devices. These custom devices are addressed in ED-80/DO-254, section 1.2, Item 3 as 'custom micro-coded components'.

Developing a custom device demands a well-defined development process. However, it is understood that the process to develop complex custom devices requires more comprehensive activities and **[**artefacts**]/[**artifacts**]** than for a simple device.

Section 5.1 identifies custom devices that are within the scope of this **[**AMC**]/[**AC**]**.

Section 5.2 provides guidance on simple/complex classification for custom devices.

Sections 5.3 and 5.4 respectively, provide guidance on development assurance for complex custom devices and simple custom devices.

Sections 5.5 through section 5.10 provide clarifications on ED-80/DO-254.

Section 5.11 provides background information and guidance specific to COTS IP used in custom devices, and identifies COTS IP that are within the scope of this **[**AMC**]/[**AC**]**.

5.1. Applicability

Section 5 is applicable to a digital or mixed signal custom device that contributes to functions with a hardware DAL A, DAL B, or DAL C.

Appendix A to ED-80/DO-254 modulates ED-80/DO-254 life cycle data based on the DAL allocated to the hardware function. This document **[**recognises**]/[**recognizes**]** Appendix A for the modulation of the life cycle data according to the hardware DAL for the development of custom devices.

5.2. Simple/Complex Classification

ED-80/DO-254 has two definitions of a simple hardware item. This section clarifies and provides criteria that could be used to classify a device as simple by considering the design content of the custom device and subsequently the ability to comprehensively verify the device.

A hardware custom device is classified as simple only if a technical assessment of the design content supports the ability of the device to be verified by a comprehensive combination of deterministic tests and analysis that ensures correct functional performance under all foreseeable operating conditions with no anomalous **[**behaviour**]/[**behavior**]**. The following criteria should be used for assessing whether a device should be classified as simple:

— Simplicity of the functions and their number,

— Number of interfaces,

— Simplicity of data/signal processing or transfer functions,

— Independence of functions/blocks/stages.

Additional criteria specific to digital designs include:

— Whether the design is synchronous or asynchronous,

— The number of independent clocks,

— The number of state machines, number of states, and state transitions per state machine,

— The independence between the state machines.

The applicant may propose other or additional criteria for the technical assessment of simplicity.

When an item cannot be classified as simple, it should be classified as complex. However, note that an item constructed entirely from simple items may itself be complex.

Objective CD-1

For each custom device, the applicant should document in the PHAC or any related document:

1. *The development assurance level,*
2. *The simple or complex classification, and*
3. *If a device is classified as simple, the justification based on the simple classification criteria.*

5.3. Development Assurance for Complex Custom Devices

ED-80/DO-254 is **[**recognised**]/[**recognized**]** as the industry standard for development assurance of the complex custom devices.

The applicant should comply with ED-80/DO-254 and the additional objectives or clarifications described in this **[**AMC**]/[**AC**]**.

5.4. Development Assurance for Simple Custom Devices

For the development of simple custom devices, it is understood that the life cycle data might be significantly reduced compared to the data required for a complex custom device.

ED-80/DO-254 states that 'For a simple hardware item, extensive documentation of the design process is unnecessary. The supporting processes of verification and configuration management need to be

performed and documented for a simple hardware item, but extensive documentation is not needed. Thus, there is reduced overhead in designing a simple hardware item to comply with this document.'

However, it is important that a simple custom device performs its intended function, and is under configuration management allowing the device to be reproduced, conformed, and **[**analysed**]/[**analyzed**]** to ensure continued operational safety.

Objective CD-2

The applicant should propose a process in the PHAC or any other appropriate hardware plan to develop simple custom devices that encompass:

1. *Definition of the device functions,*
2. *Complete verification of the device functions, through tests and analyses,*
3. *Configuration management of the device.*

Sections 5.5.2.3 and 5.5.2.4 of this document also apply to the verification process of simple custom devices.

The life cycle data for simple devices can be combined with other hardware data.

If tools are used for the simple custom device development process, the objectives or clarifications of those objectives described in section 5.8 of this document are also applicable.

When the applicant intends to reuse a previously developed simple device, ED-80/DO-254 section 11.1 and the clarifications provided in section 5.9 of this document should be used.

5.5. Clarifications to ED-80/DO-254 Validation and Verification Processes

5.5.1 Validation Process

Establishing a correct and complete set of requirements is the cornerstone of the development assurance process. ED-80/DO-254 section 6.1 addresses the validation process to ensure the completeness and correctness of derived requirements. The upper level requirements allocated to the custom device are often refined or restated at the custom device level and in terms that support the hardware design. These requirements should also be correct and complete.

Objective CD-3

The applicant should validate all the custom device requirements by following the ED-80/DO-254 validation process (ED-80/DO-254, sections 6 and 10). This validation activity covers the derived requirements and the requirements which are traceable to the upper-level requirements.

For DAL A and B development, validation activities should be performed with independence.

Note: ED-80/DO-254 Appendix A defines acceptable means for establishing independence.

5.5.2 Verification Process

ED-80/DO-254 describes the verification process but additional guidance is needed to ensure the verification of the custom device is complete.

5.5.2.1 Detailed Design Review

Detailed design is the process of generating, from conceptual design and requirements, a hardware description language (HDL) representation or analog schematic constraints (e.g. timing constraints, pinout, I/O characteristics) to implementation, and hardware-software interface description.

ED-80/DO-254 introduces design reviews in section 6.3.3.2. A design review is considered to be an essential step during the detailed design process (ED-80/DO-254, section 5.3), supporting the implementation process, and complementing requirements-based verification.

Objective CD-4

For hardware DAL A or DAL B, the applicant should review the detailed design in order to demonstrate that it satisfies the custom device requirements, the conceptual design, and the hardware design standards.

5.5.2.2. Implementation Review

Within a custom device development process, tools are used to convert the detailed design data into the physical implementation. While ED-80/DO-254 does not explicitly address it, a review of the design tool reports (e.g. synthesis and place and route reports) is necessary to ensure that the tool execution to generate its output was performed correctly. Since this step is considered part of the verification of the implementation, no separate objective exists.

5.5.2.3. Test Cases and Procedures

ED-80/DO-254 introduces verification coverage analysis in section 6.2.2 Item 4 to satisfy the ED-80/DO-254 verification process objectives and determine whether the verification process is correct and complete. A part of the coverage analysis is clarified by the following objective.

Objective CD-5

Each verification case and procedure should be reviewed to confirm that it is appropriate for the requirements to which it traces and that the requirements are correctly and completely covered by the verification case and procedure.

5.5.2.4. Verification of the Implementation

ED-80/DO-254, section 6.2 addresses the verification of the implementation. Implementation is the process to generate the physical custom device from the detailed design data. The post-layout netlist is the closest virtual representation of the physical custom device, resulting from synthesis (for digital) and place and route.

While it is recommended to test the implementation in its intended operational environment (physical test), verification using the post-layout netlist may be necessary to complement the verification of the implementation for certain requirements (e.g. features not accessible from the I/O pins of the device,

timings, abnormal conditions, or robustness cases). In such cases, the coverage of the requirements by means other than a physical test should be justified.

The requirement to capture activities in ED-80/DO-254, section 5.1.2 Item 4.g, introduces the need for requirements to address signal timing characteristics over normal and worst-case conditions. Nevertheless, ED-80/DO-254 does not explicitly address the necessity to verify the performance of the device under all possible (best-case and worst-case) timing conditions that could possibly occur during device operation.

The following objective clarifies the need to take into account the variation of the environmental conditions (temperature, voltage, etc.) during evaluation of the timing performance of the design.

Objective CD-6

*The applicant should verify the timing performance of the design accounting for the temperature and power supply variations applied to the device and the semiconductor device fabrication process variations as **[**characterised**]/[**characterized**]** by the semiconductor device manufacturer.*

Note: Static timing analysis (STA) with the necessary timing constraints and conditions is one of the possible means of compliance with this objective for digital part of custom devices.

5.6. Clarifications to ED-80/DO-254 robustness aspects

ED-80/DO-254 mentions robustness defects but does not explicitly address robustness. Robustness of the design is defined as the expected **[**behaviour**]/[**behavior**]** of the design under abnormal and boundary/worst-case operating conditions of the inputs and internal design states. These conditions are often captured as derived requirements when they are not allocated from the upper level process. When subjected to these conditions, it is understood that the design may not continue to perform as it would under normal conditions.

Objective CD-7

*For DAL A or DAL B hardware, the abnormal and boundary conditions and associated expected **[**behaviour**]/[**behavior**]** of the design should be defined as requirements.*

5.7. Recognition of HDL Code Coverage Method

HDL code coverage analysis is an assessment of whether the HDL code of the design has been exercised through HDL simulations.

The HDL code coverage method provides an assessment of the coverage of the design logic structure, giving an indication of what logic structure aspect is or is not exercised.

When performed during requirements-based verification (per ED-80/DO-254 section 6.1), HDL code coverage is [recognised]/[recognized] as a method to perform ED-80/DO-254 elemental analysis per Appendix B, section 3.3.1, for digital devices. HDL code coverage supports the assessment that the HDL code elements are fully covered by requirements-based simulations. As such, it does not represent an

assessment of the completeness of requirements-based testing activities or the effectiveness of requirement coverage.

Objective CD-8

*For hardware DAL A or DAL B, where HDL code coverage is used to perform elemental analysis (ED-80/DO-254, Appendix B, section 3.3.1), the applicant should define in the planning documents the detailed coverage criteria of the HDL code elements used in the design. The criteria should ensure coverage over the various cases of the HDL code elements used in the design (e.g. branches, conditions, etc.). Any non-covered case should be **[**analysed**]/[**analyzed**]** and justified.*

Note: Code coverage might need to be complemented by additional analysis for any hardware items that are identified as not covered by the code coverage analysis, in order to complete the elemental analysis of all elements. This situation may occur in the use of some COTS IP instantiations.

5.8. Clarifications to ED-80-DO-254 Tool Assessment and Qualification

ED-80/DO-254 introduces the notion of tool assessment and qualification. ED-80/DO-254, Figure 11-1 includes a flow chart indicating the tool assessment considerations and activities, and provides guidance for when tool qualification may be necessary. This **[**AMC**]/[**AC**]** uses the flowchart and its related text as a basis for providing further clarification, as follows:

Figure 11-1 Item 1. - Identify the Tool

Information capturing the environment required for tool operation and the tool revision should be included with the tool identification.

Figure 11-1 Item 2. - Identify the Process the Tool Supports

When identifying the design or verification process that the tool supports, it is important to also identify what objectives/activities the tool satisfies. While assessing the tool limitations, evidence of formal assessment of the tool problem reports is not required when the tool output has been completely and independently assessed.

Figure 11-1 Item 3. - Is the Tool Output Independently Assessed?

The purpose of tool output assessment is to completely cover the potential errors the tool can introduce into the design or fail to detect in verification with an independent means.

Objective CD-9:

When the applicant intends to independently assess a tool output, the applicant should propose an independent assessment that verifies the correctness of the tool output. The independent assessment

should justify sufficient coverage of the tool output. The completeness of the tool assessment should be based on the design/implementation and/or verification objectives that the tool is used to satisfy.

Figure 11-1 Item 5. - Does the Tool have Relevant History?

In ED-80/DO-254, the supporting text for Figure 11-1 Item 5 can be misinterpreted to suggest that when the tool has been previously used, no further tool assessment is necessary. Item 5 should be understood as the applicant will provide sufficient data and justification to substantiate the relevance and credibility of the tool history.

Objective CD-10:

When the applicant intends to claim credit for the relevant history of a tool, sufficient data should be provided to demonstrate that there is a relevant and credible tool history to justify that the tool will produce correct results for its proposed use.

Figure 11-1 Item 9. – Design Tool Qualification

For design tools, contrary to the note in the supporting text for Figure 11-1 Item 9, tool history should not be used as a stand-alone means of tool assessment and qualification. Relevant tool history may be used to compensate for some particular gaps in the tool assessment and qualification process, for example, to explain the method of independent assessment of the tool output. In this case, relevant tool history is considered as a complementary activity providing more assurance for a tool.

Coverage Tool

ED-80/DO-254, Figure 11-1 Item 4 of the tool assessment/qualification flow excludes the need for activities for tools 'used to assess the completion of verification testing, such as in an elemental analysis.' However, it is necessary to provide some further clarifications.

— This document **[**recognises**]/[**recognizes**]** the Figure 11-1 Item 4 exclusion of tool assessment/qualification activities for code coverage tools only when they are used to assess whether code has been exercised by requirements-based testing/simulations.
— If test cases or procedures are automatically generated by a tool and this tool uses coverage to determine the completion of requirements verification, then the coverage tool should be considered a verification tool and should be assessed as such.

5.9. Clarifications to ED-80/DO-254 Previously Developed Hardware

Previously developed hardware (PDH) is defined as a custom-developed hardware device that has been approved through a certification process (i.e. type certificate (TC)/supplemental type certificate (STC)/(E)TSO). The section providing clarification on the use of PDH also covers PDH that has been developed and approved prior to the use of ED-80/DO-254 in civil certification.

This section provides guidance on the use of ED-80/DO-254, section 11.1, for PDH.

Objective CD-11

When an applicant and/or hardware developer proposes to reuse PDH, the applicant should use ED-80/DO-254, section 11.1 and its subordinate paragraphs. The applicant should perform the assessments and analysis required in ED-80/DO-254, section 11.1, in order to ensure that using the PDH is valid and that the compliance shown during the previous approval was not compromised by any of the following:

1. *Modification of the PDH for the new application;*
2. *Change to the function, change to its use, or change to a higher failure condition classification of the PDH in the new application; or*
3. *Change to the design environment of the PDH.*

The results should be documented in the PHAC or any other appropriate planning document.
In the context of custom device development, any one of these three points potentially invalidates the original development assurance credit for the PDH. In case of change or modification, the applicant is required to assess these changes using ED-80/DO-254 section 11.1 and its subordinate paragraphs. When the original design assurance of the PDH is invalidated by one of the above points, the custom device should be upgraded based on the assessment per ED-80/DO-254, section 11.1. When upgrading the hardware, the applicant should consider the objectives of this document that are applicable per the assessment.

5.10. Clarifications to ED-80/DO-254 Appendix A

This section clarifies the life cycle data referenced in ED-80/DO-254 Appendix A as follows.

— The row corresponding to 10.2.2, 'Hardware Design Standard' in Table A-1 should also indicate HC2 for Level C.
— The top-level drawing, also called Hardware Configuration Index (HCI), completely identifies the hardware configuration, the embedded logic, and the development life cycle data. To support consistent and accurate replication of the custom device (ED-80/DO-254, section 7.1), the Top-Level Drawing includes hardware life cycle environment or refers to a Hardware Environment Configuration Index (HECI) document.

5.11. Use of COTS IP in Custom Design Development

This section addresses COTS IP that is instantiated within FPGAs/PLDs/ASICs during the development of the custom device.
Section 5.11 addresses COTS IP and its integration within custom devices, and describes objectives to support the demonstration of compliance with the applicable airworthiness regulations for hardware aspects of airborne systems and equipment certification.
Section 5.11.2, on 'Applicability', identifies COTS IP that are within the scope of section 5.11.

5.11.1 Background

IP refers to design functions (design modules or functional blocks – including IP libraries) used to design and implement a part of or a complete custom device such as a PLD, FPGA, or ASIC. IP is considered to be commercial-off-the-shelf intellectual property, i.e. 'COTS IP', when it is a commercially available function, used by a number of different users, in a variety of applications and

installations. Custom IP, developed for a few specific aircraft equipment, is not considered to be COTS IP.
COTS IP are available in various source formats. COTS IP are **[**categorised**]/[**categorized**]** as Soft IP, Firm IP, or Hard IP based on the stage in the custom device design flow where the IP is instantiated. A function can be a combination of source formats and each part needs to be addressed. Definitions for Soft IP, Firm IP, and Hard IP can be found in the Appendix A Glossary.

Figure 1 shows a 'simplified' design flow of a PLD, FPGA, or ASIC, and where Soft IP, Firm IP, and Hard IP are located in the design flow.

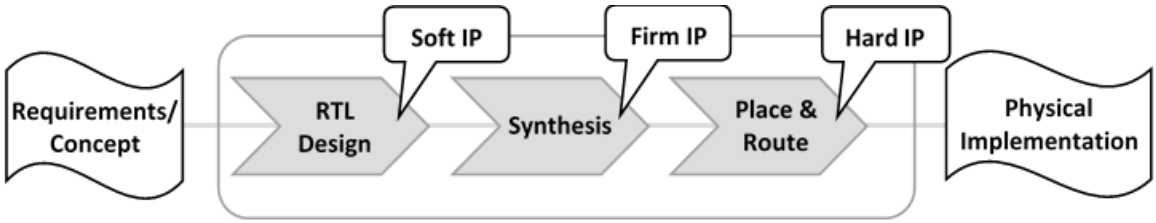

Figure 1 – Position of COTS IP within a 'simplified' design representation flow

The availability of a COTS IP does not guarantee that it is suitable to be used in a custom device for aircraft systems. Some COTS IP may have been developed using ED-80/DO-254 and will therefore have the necessary lifecycle data to demonstrate satisfaction of ED-80/DO-254. However, most COTS IP are not developed to meet aviation development assurance standards and, therefore, there are risks associated with their use in a custom device for aircraft systems or equipment.

The risks of using COTS IP may include:

— Incomplete or missing documentation/data regarding:
  - the **[**behavioural**]/[**behavioral**]** operation of the COTS IP,
  - how to integrate it into the design;
— Insufficient verification performed by the COTS IP provider;
— Deficient quality of the COTS IP.

The potential for design errors may be increased by the lack of development assurance, and/or by insufficient service experience.

Possible design errors within COTS IP or in the use of the COTS IP may lead to a failure mode. Risk factors for these types of errors include:

— Unknown level of **[**rigour**]/[**rigor**]** of the COTS IP design and verification process;
— Misalignment between the intended usage of the COTS IP by the IP provider and the usage in the custom device by the IP user;
— Incomplete or missing details regarding the detailed operation of the COTS IP;
— Incorrect integration of the COTS IP with the rest of the custom device design;
— integrator lacking expertise with the function of the IP.

Additionally, the COTS IP user completes the development of the integrated COTS IP up to the physical implementation of the device. The COTS IP user may introduce a design error while completing the

physical implementation of the COTS IP because of the user's incomplete knowledge of the internal design of the COTS IP.

5.11.2 Applicability

Section 5.11 is applicable to COTS IP used in a custom device that meets the definition of commercial-off-the-shelf intellectual property in the Appendix A Glossary. This scope encompasses digital, analog, and mixed-signal COTS IP.

Note: Analog COTS IP is within the above-mentioned scope, as it could be instantiated within a custom mixed-signal device.

Section 5.11 is applicable to COTS IP contributing to functions with a hardware DAL A, DAL B, or DAL C.

Section 5.11 is applicable to Soft IP, Firm IP, and Hard IP that are inserted within a custom device by the applicant. However, section 5.11 does not apply to Hard IP that is embedded in the silicon of an FPGA or a PLD by the FPGA/PLD device manufacturer. This type of IP is considered to be part of the COTS device and is covered in section 6, Use of Commercial Off-the-Shelf Devices.

5.11.3 Development Assurance for COTS IP

A COTS IP development assurance approach should be based on the category of the COTS IP (soft, firm, hard) and on the identified risks of failure due to a design error in the COTS IP itself or an error in the way it is used in the custom device.

This section provides objectives addressing development assurance when using COTS IP. These objectives are intended to cover the particular aspects of development when using COTS IP, and are expressed in connection with the custom device development process that follows ED-80/DO-254 and the custom device objectives of this document.

The development aspects related to COTS IP start from the custom device process that captures the allocated requirements for the function that will be performed by the COTS IP. From this entry point, the following steps are used as a basis to define development assurance objectives for COTS IP:

— Selection of the COTS IP,
— Assessment of the IP provider and the IP data,
— Planning activities, including the verification strategy,
— Definition of requirements/derived requirements,
— Design integration, implementation, and verification of the COTS IP in the custom device.

5.11.3.1 Selection of the COTS IP to Implement the Function

COTS IP can be available in different forms/source formats and various levels of quality. Some COTS IP may not be acceptable for use in airborne systems. Selection criteria are intended to address the essential characteristics that are considered a minimum for use in custom AEH devices.

Objective IP-1

The applicant should select a COTS IP that is considered to be an acceptable solution, based on at least the following criteria:

1. *The IP is technically suitable for implementing the intended function, commensurate with the DAL of the custom device;*
2. *The description of the COTS IP architecture or IP design concept provides an understanding of the functionality, modes, and configuration of the IP. The architecture should also include an understanding of the source format or combination of source formats of the COTS IP;*
3. *The availability and quality of data and documentation allow the understanding of all aspects of the COTS IP functions, modes, **[**behaviour**]/[**behavior**]**, and enable the integration and verification of the COTS IP (e.g. datasheets, application notes, user guide, knowledge of errata, etc.);*
4. *It is feasible, and information exists for the IP user to create the physical implementation of the COTS IP (e.g. synthesis constraints, usage and performance limits, physical implementation, and routing instructions);*
5. *It can be demonstrated that the COTS IP fulfils its intended function to commensurate with the hardware DAL of the custom device.*

5.11.3.2 Assessment of the COTS IP Provider & COTS IP Data

Objective IP-2

The applicant should assess the COTS IP provider and the associated data of the COTS IP based on at least the following criteria:

1. *The IP provider provides all the information necessary for the integration of the COTS IP within the custom device and to support further implementation of the COTS IP within the device (e.g. synthesis constraints, usage domain, performance limits, physical implementation, and routing instructions);*
2. *The configurations, selectable options, and scalable modules of the COTS IP design are documented so that the implementation of the COTS IP can be properly managed;*
3. *The COTS IP has been verified following a trustworthy and reliable process, and the verification covers the applicant's specific use case for the COTS IP (including the used scale for scalable IP and the IP function selected for selectable functions);*
4. *The known errors and limitations are available to the IP user;*
5. *The COTS IP has service experience data that shows reliable operation for the applicant's specific use case for the COTS IP.*

When these criteria cannot be completely met using the IP provider's data, the applicant should define an appropriate development assurance activity to address the associated risk of development error. The development assurance activity should be based on ED-80/DO-254 objectives.

5.11.3.3 Planning of the Hardware Development Assurance Approach Related to COTS IP

5.11.3.3.1 General Aspects

The applicant has to define the activities that are needed for the hardware development assurance approach related to COTS IP.

Objective IP-3

The applicant should describe in the PHAC, or any related planning document, a hardware development assurance approach for using the COTS IP that at least includes:

1. *Identification of the selected COTS IP (version) and its source format(s) associated with the point(s) in the design flow where the COTS IP is integrated into the custom device;*
2. *A summary of the COTS IP functions;*
3. *The development assurance process that the applicant defines to satisfy the objectives of section 5.11.3;*
4. *The process related to the design integration and to the usage of the COTS IP in the custom device development process;*
5. *Tool assessment and qualification aspects when the applicant uses a tool to perform design and/or verification steps for the COTS IP.*

5.11.3.3.2 Verification Strategy for the COTS IP Function

In addition to the verification of the custom device functions supported by the COTS IP, there is a need to ensure that aspects related to the COTS IP and its usage are addressed. This section focuses on defining a verification strategy to cover those aspects.

The verification performed by the COTS IP provider typically does not follow the ED-80/DO-254 verification process but may provide some credit to be used for the verification strategy. However, the verification process of COTS IP generally differs from one IP vendor to another, and the level of assurance varies depending on the IP provider's development practices.

The verification strategy may combine different means to complement the traditional requirements-based testing approach.

Based on the applicant's assessment of the IP provider and the IP data through objective IP-2, the applicant is expected to establish a verification strategy. The aim of this verification strategy is to cover all three of the following aspects:

— The COTS IP – the purpose is to ensure that the COTS IP is verified, addressing the risk identified from the IP-2 Item 3 objective;

— Its implementation – the purpose is to ensure that the COTS IP still performs its allocated function, and that no design errors have been introduced by the design steps performed by the applicant (e.g. synthesis/place and route);

— Its integration within the custom device – the purpose is to ensure that the COTS IP has been properly connected, configured, and constrained within the custom device.

The strategy may accomplish more than one aspect within a common verification step.

This section identifies a general objective for the verification of COTS IP used in a custom device, enabling various verification approaches.

Objective IP-4

The applicant should describe in the hardware verification plan, PHAC, or any related planning document, a verification strategy that should encompass all three of the following aspects:

1. *The verification of the COTS IP itself,*
2. *The verification of the COTS IP after the design steps performed by the applicant (e.g. synthesis/place and route),*
3. *The verification of the integrated COTS IP functions within the custom device.*

Note 1: Reliable and trustworthy test data, test cases or procedures from the COTS IP provider may be used as part of the verification strategy to satisfy this objective.
*Note 2: If the COTS IP implements functions based on an industry standard, proven **[**standardised**]/[**standardized] test vectors verifying compliance with the standard may be used in the verification strategy of the COTS IP.*
Note 3: the verification strategy covers at a minimum the used functions of the COTS IP and ensures that the unused functions are correctly disabled or deactivated and do not interfere with the used functions.

5.11.3.4 Requirements for the COTS IP Function and Validation

Custom device requirements would typically contain requirements that relate to the function supported by the COTS IP. The granularity of these requirements may be very different depending on the COTS IP function and the visibility of the function supported by the IP at the custom device level.

Depending on the extent of requirements-based testing as a part of the chosen verification strategy of the COTS IP, the level of detail, and granularity of the AEH custom device requirements may need to be refined to specifically address the COTS IP function and the implementation of the COTS IP.

In addition, requirements should be captured to encompass all necessary design detail used to connect, configure, and constrain the COTS IP and properly integrate it in the AEH custom device.

Objective IP-5

The requirements related to the allocated COTS IP functions should be captured to an extent commensurate with the verification strategy.

In addition, derived requirements should be captured to cover the following integration aspects of the COTS IP into the custom device design:

1. *COTS IP used functions (including parameters, configuration, selectable aspects),*
2. *Deactivation or disabling of unused functions,*
3. *Correct control and use of the COTS IP.*

When the applicant chooses a verification strategy (see section 5.11.3.3.2) that solely relies on requirements-based testing, a complete requirement capture of the COTS IP following ED-80/DO-254 is necessary.

Regarding validation aspects, the COTS IP requirements should be validated as a part of the validation process of the AEH custom device.

5.11.3.5 Verification

The applicant should ensure that the COTS IP is verified as a part of the overall custom device verification process per ED-80/DO-254 and based on the verification strategy for the COTS IP that has been described in the PHAC or related planning document.

For the requirements-based verification part, the applicant should satisfy ED-80/DO-254, section 6.2 for verification of requirements related to the COTS IP (see section 5.11.3.4 above). This can be performed as a part of the overall custom device process, therefore there is no separate objective.

5.11.3.6 DO-254 Appendix B Considerations

When developing a custom device with a hardware DAL A or DAL B , ED-80/DO-254, Appendix B is applicable.

Code coverage analysis that is **[**recognised**]/[**recognized**]** as part of elemental analysis (refer to section 5.7 of this document) might not be possible for the COTS IP part of the design. However, ED-80/DO-254 Appendix B offers other acceptable methods, including safety-specific analysis. The following objective further clarifies the expectations when using safety-specific analysis.

Objective IP-6

For COTS IP used in DAL A or DAL B hardware, the applicant should satisfy ED-80/DO-254, Appendix B.

The applicant may choose safety-specific analysis methods to satisfy Appendix B on the COTS IP functionality and its integration within the custom device functions. This safety-specific analysis should identify the safety-sensitive portions of the COTS IP and the potential for design errors in the COTS IP that could affect hardware DAL A and DAL B functions in the custom device or system. For unmitigated aspects of the safety-sensitive portions of the IP, the safety-specific analysis should determine what additional requirements, design features, and verification activities are required for the safe operation of the COTS IP in the custom device.

Any additional requirements, design features, and/or verification activities that result from the analysis should be fed back to the appropriate process.

6. Use of Commercial-Off-the-Shelf Devices

Applicants are increasingly using COTS electronic devices in aircraft/engines/propellers/airborne systems, which may have safety implications for the aircraft, engines/propellers, or systems.

Section 6 addresses the use of COTS devices through objectives that support the demonstration of compliance with the applicable airworthiness regulations for hardware aspects of airborne systems and equipment certification when using complex COTS devices. section 6.2, 'Applicability', enables applicants to identify the COTS devices that are within the scope of section 6.

Note: The term 'COTS device' used in this document applies to a semi-conductor product that is fully encapsulated in a package. This term does not apply to circuit card assemblies.

6.1 Background

COTS devices continue to increase in complexity and are highly configurable. COTS devices provide 'off the shelf' already developed functions, some of which are highly complex. Their development and production processes undergo a semi-conductor industry qualification based on the consumer market. Their usage by the aerospace industry provides additional integration and higher performance capabilities than were possible in the past.

The design data for these COTS devices are usually not available to the COTS user. Since these devices are generally not developed for airborne system purposes, assurance has not been demonstrated that the **[**rigour**]/[**rigor**]** of a COTS manufacturer's development process is commensurate with the safety risks.

ED-80/DO-254 introduces a basis for the development assurance for the use of COTS devices in section 11.2, 'COTS components usage.' This section states that 'the use of COTS components will be verified through the overall design process, including the supporting processes.'

Since ED-80/DO-254 was released in the year 2000, the number of functions embedded and integrated in a single COTS device has significantly increased. Functions which were previously split into various components, making the interface between those components accessible for verification, are now embedded within a single chip. While there are clearly some benefits of integrating more functions within a device, the increased level of integration makes it difficult to verify the different hardware functions in the device due to lack of access to the interfaces between functions. Since these devices are more complex and highly configurable than the older separate devices, the risk is greater that the COTS device will not achieve the intended function in particular use cases over the required operating conditions.

Furthermore, some additional assurance is needed because design errors may still be discovered after the COTS device is released to the market or when an applicant extends the use of the device beyond the manufacturer's specifications.

6.2 Applicability

Section 6 is applicable to digital, hybrid, and mixed signal COTS devices that contribute to functions with a hardware DAL A, DAL B, or DAL C. For COTS devices contributing to functions with a hardware DAL C, a limited set of objectives of this section will apply.

Section 6 is also applicable to FPGA and PLD devices that embed Hard IP (see definition) in their produced/manufactured silicon, but only for the COTS part of FPGAs/PLDs.

Section 6.4 only applies to COTS devices that are complex as determined by the following COTS complexity assessment.

6.3 COTS Complexity Assessment

In order to define which COTS devices are complex, the following high-level criteria should be used:

A COTS device is complex when the device:

1. Has multiple functional elements that can interact with each other;
2. Offers a significant number of functional modes; and
3. Offers configurability of the functions, allowing different data/signal flows and different resource sharing within the device.

Or when the device:

4. Contains advanced data processing, advanced switching, or multiple processing elements (e.g. multicore processors, graphics processing, networking, complex bus switching, interconnect fabric with multiple masters, etc.)

For complex COTS devices, it is impractical to completely verify all possible configurations of the device and it is difficult to assess or identify all the failure modes.

Objective COTS-1

The applicant should assess the complexity of the COTS devices used in the design according to the high-level criteria of section 6.3 and document the list of relevant devices, including the classification rationale.

Note 1: The applicant is not expected to assess the complete bill of material to meet the above objective, but only those devices that are relevant for the classification, including devices that are at the boundary between simple and complex. The resulting classification (simple or complex) for those devices that are at the boundary and those that are definitely complex should be documented.

Note 2: A classification rationale is required for those devices that are on at the boundary and are classified as simple.

6.4 Development Assurance for Use of Complex COTS

ED-80/DO-254, section 11.2.1 identifies electronic component management process items when using a COTS device. ED-80/DO-254, section 11.2.2 and section 6.1 of this document identify some concerns with using a COTS device. The following objectives acknowledge and supplement ED-80/DO-254, section 11.2 in clarifying how to gain certification credit when using complex COTS devices.

6.4.1 Electronic Component Management Process

As stated in ED-80/DO-254, section 11.2, 'the use of an electronic component management process, in conjunction with the design process, provides the basis for COTS components usage.'

Objective COTS-2

The applicant should ensure that an electronic component management process exists to address the selection, qualification, and configuration management of COTS devices. The electronic component management process should also address the access to component data such as the user manual, the datasheet, errata, installation manual, and access to information on changes made by the component manufacturer.

As part of the electronic component management process, for devices contributing to functions with a hardware DAL A or DAL B, the process for selecting a complex COTS device should consider the maturity of the COTS device and, where risks are identified, they should be appropriately mitigated.

Note: **[**Recognised**]/[**Recognized**]** industry standards describing the principles of electronic component management may be used to support the development of the electronic component management process.

6.4.1.1 Using a Device Outside the Ranges of Values Specified in its Datasheet

ED-80/DO-254, section 11.2.1 Item 4 mentions, 'The component has been qualified by the manufacturer… which establish the component reliability.' ED-80/DO-254, section 11.2.1 Item 6 mentions that the basis of the device selection is the technical suitability of the device for the intended application.

In some cases, the applicant may need to use the device outside the specified operating conditions guaranteed by the device manufacturer. ED-80/DO-254, section 11.2.1 Item 4 and Item 6 should be addressed when the device is used outside its guaranteed specification. The following objective describes what to achieve when using a device outside the ranges of values specified in its datasheet.

Objective COTS-3

When the complex COTS device is used outside the device manufacturer's specification (such as recommended operating limits), the applicant should establish the reliability and the technical suitability of the device in the intended application.

6.4.1.2 Considerations when the COTS Device has Embedded Microcode

COTS devices may need microcode to execute some hardware functions. When those functions are used by the applicant, there is a risk if the microcode has not been verified by the device manufacturer during the COTS device qualification, or if the microcode is proposed to be modified by the applicant.

When the microcode is delivered by the device manufacturer, is controlled by the device manufacturer's configuration management system, and is qualified together with the device by the device manufacturer, it is accepted that the microcode is part of the qualified COTS device. If the microcode is not qualified by the device manufacturer or if it is modified by the applicant, the microcode cannot be considered as part of the qualified COTS device.

Objective COTS-4

If the microcode is not qualified by the device manufacturer or if it is modified by the applicant, the applicant should ensure that a means of compliance for this microcode integrated within the COTS device is proposed by the appropriate process and commensurate with the usage of the COTS device.

6.4.2 COTS Device Malfunction

Some COTS devices may contain errors that may or may not have been detected by the device manufacturer.

Objective COTS-5

The applicant should assess the errata of the COTS device that are relevant to the use of the device in the intended application, and identify and verify the means of mitigation for those errata. If the mitigation means is not implemented in hardware, the mitigation means should be fed back to and verified by the appropriate process.

Note: The above objective refers to any mitigation means (such as hardware, software, system, or other means). Errata of the COTS device may be caused by a limitation, an incompatibility, or an error in the microcode.

Objective COTS-6

For the usage of COTS devices contributing to functions with a hardware DAL A or DAL B, the applicant should identify the failure modes of the used functions of the device and feed these back to the system safety assessment process.

For usage of COTS devices contributing to functions with a hardware DAL A, the possible associated common modes should be fed back to the system safety assessment process.

6.4.3 COTS Device Usage

Complex COTS devices can have multiple functions and many configurations of those functions. The configuration of a device should be managed in order to provide the ability to consistently apply the required configuration settings, to replicate the configuration on another item, and to modify the configuration in a controlled manner, when modification is necessary.

The configuration of the device addresses at least the following topics:

— The used functions (e.g. identification of each function, configuration characteristics, mode of operation),

— The unused functions and the means (internal/external) used to deactivate them,

— The means to control any inadvertent activation of unused functions, or inadvertent deactivation of used functions,

— The means to manage device resets,

— The power-on configuration,

— The clocking configuration (e.g. identification of the different clock domains),

— The operating conditions (e.g. clock frequency, power supply level, temperature, etc.).

Objective COTS-7

The applicant should ensure that the usage of the COTS device has been defined and verified according to the intended function of the hardware. This also includes the hardware-software interface and the hardware to (other) hardware interface.

When a COTS device is used in a function with a hardware DAL A or DAL B, the applicant should show that the COTS device unused functions do not compromise the integrity and availability of the COTS device used functions.

Note: For unused COTS device functions, it is recommended that an effective deactivation means is used and verified, when available.

Note 1: Verification should be performed at an appropriate level (hardware, software, equipment).

Note 2: ED-80/DO-254, section 10.3.2.2.4 introduces hardware/software (HW/SW) interface data that can be used as a reference to define the software interface data of the COTS device.

Some additional consideration should be given to the critical configuration settings. Those are defined as the settings that are deemed necessary by the applicant for the proper usage of the hardware, which, if inadvertently altered, could change the **[**behaviour**]/[**behavior**]** of the COTS device, causing it to no longer [fulfil]/[fulfill] its intended function.

Objective COTS-8

If the complex COTS device contributes to DAL A or B functions, the applicant should develop and verify a means that ensures an appropriate mitigation is specified in the event of any inadvertent alteration of the 'critical configuration settings' of the COTS device.

Note: The mitigation means might be defined at the hardware, software, or system level, or a combination of these. The mitigation means may also be defined by the safety assessment process.

7. [<AMC>] Related Regulatory, Advisory, and Industry Material

(a) Related EASA Certification Specifications (CSs)

(1) CS-23, *Certification Specifications and Acceptable Means of Compliance for Normal, Utility, Aerobatic, and Commuter Category Aeroplanes*;

(2) CS-25, *Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes*;

(3) CS-27, *Certification Specifications and Acceptable Means of Compliance for Small Rotorcraft*;

(4) CS-29, *Certification Specifications and Acceptable Means of Compliance for Large Rotorcraft*;

(5) CS-E, *Certification Specifications and Acceptable Means of Compliance for Engines, and AMC 20-3A, Certification of Engines Equipped with Electronic Engine Control Systems*;

(6) CS-P, *Certification Specifications for Propellers, and AMC 20-1, Certification of Aircraft Propulsion Systems Equipped with Electronic Control Systems*;

(7) CS-ETSO, *Certification Specifications for European Technical Standard Orders*;

(8) CS-APU, *Certification Specifications for Auxiliary Power Units*; and AMC 20-2A, *Certification of Essential APU Equipped with Electronic Controls*.

(b) FAA ACs

(1) AC 20-152*, Development Assurance for Airborne Electronic Hardware*

(2) *AC 00-72, Best Practices for Airborne Electronic Hardware Design Assurance Using EUROCAE ED-80( ) and RTCA DO-254()*;

(3) AC 27-1309, *Equipment, Systems, and Installations (included in AC 27-1, Certification of Normal Category Rotorcraft*);

(4) AC 29-1309, *Equipment, Systems, and Installations (included in AC 29-2, Certification of Transport Category Rotorcraft*).

(c) Industry Documents

(1) EUROCAE ED-79A, *Guidelines for Development of Civil Aircraft and Systems,* dated December 2010;

(2) EUROCAE ED-80, *Design Assurance Guidance for Airborne Electronic Hardware,* dated April 2000;

(3) RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware,* dated April 19, 2000;

(4) SAE International Aerospace Recommended Practice (ARP) 4754A, *Guidelines for Development of Civil Aircraft and Systems,* dated December 21, 2010.**]**

[<AC> Related Regulatory, Advisory, and Industry Material

(a) 14 CFR Applicable Sections. 14 CFR parts 21, 23, 25, 27, 29, 33 and 35.

(b) FAA ACs.

(1) AC 00-72, *Best Practices for Airborne Electronic Hardware Design Assurance Using EUROCAE ED-80( ) and RTCA DO-254()*;

(2) AC 20-174, Development of Civil Aircraft and Systems;

(3) AC 21-50, *Installation of TSOA Articles and LODA Appliances;*

(4) AC 23.1309-1, *System Safety Analysis and Assessment for Part 23 Airplanes;*

(5) AC 25.1309-1, System Design and Analysis;

(6) AC 27-1309*, Equipment, Systems, and Installations* (included in AC 27-1, *Certification of Normal Category Rotorcraft*)*;*

(7) AC 29-1309, *Equipment, Systems, and Installations* (included in AC 29-2, *Certification of Transport Category Rotorcraft*)*;*

(8) AC 33.28-1, *Compliance Criteria for 14 CFR § 33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems;*

(9) AC 33.28-2, *Guidance Material for 14 CFR 33.28, Reciprocating Engines, Electrical and Electronic Engine Control Systems;*

(10) AC 33.28-3, *Guidance Material for 14 CFR § 33.28, Engine Control Systems;*

(11) AC 35.23-1, *Guidance Material for 14 CFR 35.23, Propeller Control Systems*.

(c) EASA Acceptable Means of Compliance (AMC)

(1) AMC 20-152(), *Development Assurance for Airborne Electronic Hardware*.

(d) Industry Documents

(1) SAE International Aerospace Recommended Practice (ARP) 4754A, *Guidelines for Development of Civil Aircraft and Systems,* dated December 21, 2010;

(2) RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware,* dated April 19, 2000;

(3) EUROCAE ED-80, Design Assurance Guidance for Airborne Electronic Hardware, dated April 2000.**]**

8. [<AMC> Availability of Documents

(1) EASA Certification Specifications (CSs) and Acceptable Means of Compliance (AMC) may be downloaded from the EASA website: www.easa.europa.eu.

(2) FAA Advisory Circulars (ACs) may be downloaded from the FAA website: www.faa.gov.

(3) EUROCAE documents may be purchased from:

European Organisation for Civil Aviation Equipment
102 rue Etienne Dolet, 92240 Malakoff, France
Telephone: +33 1 40 92 79 30, Fax: +33 1 46 55 62 65
(E-mail: eurocae@eurocae.net, website: www.eurocae.net)

(4) RTCA documents may be purchased from:

RTCA, Inc.
1150 18th Street NW, Suite 910, Washington DC 20036, USA
(E-mail: info@rtca.org, website: www.rtca.org).**]**

[<AC> Where to Find this AC.

1. You may find this AC at http://www.faa.gov/regulations_policies/advisory_circulars/.
2. If you have suggestions for improvement or changes, you may use the template at the end of this AC.

Michael Romanowski

Director, Policy & Innovation Division

Aircraft Certification Service**]**

Appendix A. Glossary

Batch – A manufacturing lot of a semiconductor device that is reproduced using the same semiconductor fabrication process.

Commercial off-the-shelf (COTS) device – A device, integrated circuit or multi-chip module developed by a supplier for a wide range of customers (not only airborne systems), whose design and configuration is controlled by the supplier or an industry specification. A COTS device can encompass digital, analog, or mixed signal technology. COTS electronic components are developed by the semi-conductor industry for the commercial market, not particular to the airborne domain. These devices have widespread commercial use and are developed according to the semi-conductor manufacturer's proprietary development processes.

COTS device usage – This is defined as an exhaustive list of conditions/constraints (such as configuration settings, usage rules, protocol, timing constraints, input output (IO) interface, and addressing schemes) associated with performance characteristics of implemented COTS functions. Respecting the defined COTS usage will ensure the expected performance of the device for a given set of constraints.

Commercial-off-the-shelf intellectual property (COTS IP) – Intellectual Property (IP) refers to design functions (design modules or functional blocks – including IP libraries) used to design and implement a part of or a complete custom device such as a PLD, FPGA, or ASIC. Intellectual Property is considered to be 'COTS IP' when it is a commercially available function, used by a number of different users, in a variety of applications and installations. In this document, the terminology 'a/the COTS IP' refers to a piece of hardware that is COTS IP per this definition. COTS IP is available in various source formats:

a. Soft IP

Soft IP is COTS IP defined as register transfer level (RTL) code, captured in a HDL such as Verilog or VHDL, that may be readable or encrypted. It is instantiated by the IP user within the custom device HDL code or by selecting the COTS IP function in a library. Soft IP will be **[**synthesised**]/[**synthesized**]**, placed and routed in the AEH custom device.

In this document, the terminology 'a/the Soft IP' refers to a piece of hardware that is Soft IP per this definition.

b. Firm IP

Firm IP is COTS IP defined as a technology-dependent netlist. It is instantiated within the custom device netlist (inserted by the user, called from a library, or selected by the user as a library function). Firm IP will be placed and routed in the AEH custom device.

In this document, the terminology 'a/the firm IP' refers to a piece of hardware that is firm IP per this definition.

c. Hard IP

Hard IP is COTS IP defined as a physical layout (stream, polygon, GDSII format, etc.).

Hard IP is instantiated by the IP user during the physical design layout stage; alternatively, Hard IP is embedded into the silicon of the FPGA/PLD by the FPGA provider/device manufacturer.

In this document, the terminology 'a/the Hard IP' refers to a piece of hardware that is Hard IP per this definition.

Complex COTS device maturity – A complex device is mature when the risk of unintended function or **[**misbehaviour**]/[**misbehavior**]** is low. The risk of anomalous **[**behaviour**]/[**behavior**]** decreases as a device is widely used and device errata are documented and communicated to the user of the device.

Critical configuration settings – Those configuration settings that the applicant has determined to be necessary for the proper usage of the hardware, which, if inadvertently altered, could change the **[** behaviour**]/[**behavior**]** of the COTS device, causing it to no longer fulfil its intended critical function.

Development assurance for use of COTS device – All the planned and systematic activities conducted to provide adequate confidence and evidence that the complex COTS device safely performs its intended function under its operating conditions.

Hardware design assurance level of a function – Refer to ED-80/DO-254, table 2-1 for the definition of DAL A, B, C, and D functions.

Hybrid device – An integrated circuit combining different semiconductor die and passive components on a substrate.

IP libraries – 'IP libraries' used in the COTS IP definition refers to all sub-modules, sub-blocks, or other design sub-functions that are formally/commercially made available by a COTS IP provider and intended for integration within a COTS IP by the COTS IP user. However, Macro Cells for FPGAs or Standard Cells for ASICs are not considered to be IP libraries, hence they are not related to the COTS IP topic referred to in this document.

Microcode – This term often refers to a hardware-level set of instructions. It is typically stored in the COTS device's high speed memory and microcode instructions are generally translated into sequences of detailed circuit-level operations. Microcode may be used in general-purpose microprocessors, microcontrollers, digital signal processors, channel controllers, disk controllers, network interface controllers, network processors, graphics processing units, and other hardware. A Basic Input/Output System (BIOS) is an example of microcode, which is used to **[**initialise**]/[**initialize**]** microprocessor inputs and outputs process operations.

Mixed-signal device – A device that combines digital and analog technologies.

Note: A note in this document is supporting information used to provide explanatory material, **[**emphasise**]/[**emphasize**]** a point, or draw attention to related items which are not entirely within context.

Objective – An objective in this document is a requirement for development assurance that should be met to demonstrate compliance with the applicable airworthiness requirements.

Qualification of a device – SAE EIA-STD 4899 defines component qualification as 'The process used to demonstrate that the component is capable of meeting its application specification for all the required conditions and environments.' Component qualification results in a 'qualified device.' Note that the use of qualification is not intended to refer to ED-14/DO-160 environmental qualification testing.

[<AC> Appendix B. Advisory Circular Feedback Form

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to 9-AWA-AVS-AIR-DMO@faa.gov, or (2) faxing it to the attention of the AIR Directives Management Officer at (202)-267-3983.

Subject: _____ Date: _____

Please check all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph _____ on page _____.

☐ Recommend paragraph _____ on page _____ be changed as follows:

☐ In a future change to this AC, please cover the following subject: *(Briefly describe what you want added.)*

☐ Other comments:

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____]

3.1.2. Draft EASA guidance material (GM) / FAA AC 00-72

[<AC> AC 00-72: Best Practices for Airborne Electronic Hardware Design Assurance Using EUROCAE ED-80( ) and RTCA DO-254( )**]**

<AMC> Appendix - Guidance Material to AMC 20-152A]

[<AMC> A.1][<AC> 1.0] Purpose

[<AC> This advisory circular (AC) provides information in the form of 'best practices' and, as such, is not intended as guidance but rather as complementary information to ED-80/DO-254 and AC 20-152A.**]** This document provides additional clarifications, explanatory text, or illustrations that could be helpful when addressing objectives of **[**AMC 20-152A**]/[**AC 20-152A**]**. This document does not intend to cover each section of **[**AMC 20-152A**]/[**AC 20-152A**]**.

[<AC> 2.0 Audience
[<AMC>This AMC is**]/[<AC>**We wrote this AC as**]** a means of assisting applicants, design approval holders (DAH), and developers of airborne systems and equipment containing electronic hardware intended to be installed on type-certificated aircraft, engines, and propellers, or to be used in technical standard order (TSO) articles.]

3.0 Best practices][<AMC> A.2 Guidance Material]
[<AMC> A.2.1 - Custom Devices]/[<AC> 3.1 Custom Devices

[<AMC> This guidance material provides**]/[<AC>** These practices provide**]** complementary information to [AMC 20-152A]/[AC 20-152A], Custom Device Development, section 5. Applicants may **[<AMC>** use this guidance material**]/[<AC>** consider using these best practices**]** when developing custom devices.

[<AMC> A.2.1.1][<AC> 3.1.1] Clarifications to ED-80/DO-254 Appendix A for Top-level Drawing

[<AMC> A.2.1.1.1][<AC> 3.1.1.1] Hardware Environment Configuration Index (HECI)

The purpose of the HECI is to aid reproduction of the hardware life cycle environment for hardware regeneration, re-verification, or hardware modification. The HECI may be included or referenced in the Hardware Configuration Index (HCI). The HECI should identify:

1. The life cycle environment hardware (e.g. computer or workstation) and operating system (OS) when relevant,
2. Hardware development tools,
3. The test environment and validation/verification tools, and
4. Qualified tools and qualification data.

[<AMC> A.2.1.1.2][<AC> 3.1.1.2] Hardware Configuration Index (HCI)

The purpose of the HCI is to identify the configuration of the hardware product. The HCI should include:

1. The **[**ASIC/PLD**]/[**application specific integrated circuit (ASIC)**/**programmable logic device (PLD)**]** product - part number,
2. Media (e.g. PLD programming file or ASIC netlist),
3. Identification of each source code component, including constraints, scripts,
4. Identification of previously developed hardware (e.g. Intellectual Property, macrocells),
5. Hardware life cycle data and versions as defined in ED-80/DO-254 Table A1,
6. Archive and release media, including media for a PLD programming file or ASIC netlist,
7. Instructions for building a PLD programming file or ASIC netlist,
8. The reference to the HECI,
9. Data integrity checks for PLD programming file (N/A for ASICs).

[<AMC> A.2.1.2][<AC> 3.1.2] Additional Information for Objective CD-1 on Simple/Complex classification

Based on the definition of simple hardware in ED-80/DO-254, a custom device with complex functions that is exhaustively verified with the help of a formal analysis or a verification tool could be theoretically classified as simple. This **[**AMC 20-152A**]/[**AC 20-152A**]** clarifies that classification as simple or complex is based on the design content of the device regardless of the proposed verification method. Therefore, such a device would be classified as complex following the criteria of the **[**AMC 20-152A**]/[**AC 20-152A**]**.

[<AMC> A.2.1.3][<AC> 3.1.3] Additional Information for Objective CD-2 on the Development Assurance for Simple Custom Devices

A simple device is defined and designed to implement specific hardware functions. Due to its simplicity, the life cycle data is reduced.

The functional performance of the device has to be ensured by verification means in order to demonstrate that the simple device adequately and completely performs its expected functions within the operating conditions without anomaly.

The functions of a simple device may be defined through a requirement capture process or may be part of the definition of functions for the overall hardware.

Operating conditions, in addition to the environmental conditions, encompass all functional modes for the device configurations and all associated sets of inputs as determined to completely cover the functions of the device in its intended hardware implementation.

[<AMC> A.2.1.4][<AC> 3.1.4] Additional Information for Objective CD-6 on Verification of the Implementation

CD-6 specifies to verify the timing performance of the design accounting for the temperature and power supply variations applied to the device and the semiconductor device fabrication process variations.

There are certain variations in the conditions in which the device performs its function that may impact the timing behavior of the device. If not all cases are verified, the timing aspects might result in device malfunctions under certain conditions.

The following examples identify constraints that may impact the timing behavior of a device and information to help assess them:

— The temperature range is a design constraint input from the equipment environment or taken from the device limitation/[characterisation]/[characterization] limits. Two different temperatures need to be managed:

  - static timing analysis (STA) tools and technology limitations are based on junction temperatures;
  - application constraints are related to the external temperature.

  Conversion between these two constraints has to be carefully managed when analysis is performed.

— For voltage ranges, it is the same situation with two characteristics to take into account: Constraints from the environment (board, voltage generator accuracy) and constraints from the chosen device. Note that the voltage aspect is unambiguous.

— Device process variation is related to the chosen device, and the device manufacturer often [characterises]/[characterizes] the technology variations within the library.

To verify the timing performance of the design accounting for the temperature and power supply variations applied to the device and the semiconductor device fabrication process variations, , an analysis is expected to be performed on all corner cases to measure the impact of such constraints (temperature, voltage, and process) in terms of timing that could also affect the frequency at which the device can operate.

Static Timing Analysis can be used to conduct such an analysis. The source of each STA constraint (delay and frequency constraints) has to be identified. In addition, timing parameters to be considered for launching an STA include:

— Input frequency: an external constraint with different characteristics (e.g. accuracy, duty cycle),

— Input/output delays (e.g. setup, hold, skew).

STA provides timing results that highlight setup and hold violations, but doesn't **[**analyse**]/[**analyze**]** delays longer than a clock period (multi-cycle paths, pulse width generation, etc.).

[<AMC> A.2.1.5][<AC> 3.1.5] Additional Information for Objective CD-8 on HDL Code Coverage Analysis

For Objective CD-8, the applicant determines the code coverage criteria that support the code coverage method. The applicant should define criteria covering the hardware description language (HDL) code elements that are used in design and exercising the various cases of HDL code. The following items suggest the type of criteria that could be used to cover the HDL logic. These criteria are still to be translated into the specific metrics proposed by the chosen code coverage tools:

1. Every statement has been reached;
2. All possible branch directions were exercised;
3. All conditions expressed in a statement or for taking a branch were exercised;
4. Every state of a finite state machine (FSM) and every state transition has been exercised.

[<AMC> A.2.1.6][<AC> 3.1.6] Additional Information for Objective CD-9 on Tool Assessment and Qualification

As described in Objective CD-9, in a context where the applicant plans to use a verification tool for a DAL A or B custom device, or a design tool for a DAL A, B, or C custom device, the applicant can choose to provide confidence in the use of the tool through an independent assessment of the tool outputs.

Example:

Custom device development using the following tools:

— Design tools: synthesis tool, layout tool, programming file generation tool,

— Verification tools: simulation tool, STA tool.

Confidence in design tools can be gained through the fact that the outputs from the design tools are independently verified by simulation and physical tests during requirements-based testing. No further tool assessment is needed.

Confidence in verification tools can also be gained through independent assessment. In this case, physical tests re-run part of the simulation test sequences that allows confirmation of the results generated via the simulation test cases or procedures. The following criteria can be used to determine whether the tool can be independently assessed using this approach:

— a significant and representative set of custom device requirements is covered by both simulation and physical tests, and

— the resulting outputs are identical.

Generally, independent assessment of the tool outputs is the preferred method for tool assessment.

When the applicant largely covers custom device requirements through physical tests, it reinforces the confidence in the tools.

[<AMC> A.2.1.7][<AC> 3.1.7] Additional Information for Objective CD-10 on Tool Assessment and Qualification

When the applicant intends to present tool history to claim credit for tool assessment, Objective CD-10 expects the applicant to provide sufficient data and justification to substantiate the relevance and credibility of the tool's history.

If the tool hasn't been used by the applicant's company in the frame of another custom device development, it is preferable not to use the tool history for assessing the tool, and instead to conduct an independent assessment approach.

A list of characteristics/criteria that can be part of the service history data of the tool includes:

— The similarity of the tool operational environment in which the tool service history data was collected to the one used by the applicant;

— The stability/maturity of the tool linked to the change history of the tool;

— The service history of the custom device developed using the tool;

— The tool has a good reputation and is well supported/maintained by the tool supplier;.

— The number of tool users is significant;

— The tool has already been used in the applicant's company on certified developments without raising any major concern;

— The list of errata is available and shows that these errata do not impact the use of the tool in the development of the particular custom device.

[<AMC>A.2.1.8][<AC> 3.1.8] Use of COTS IP in Custom Device Development

[<AMC> This guidance material**]/[<AC>** These practices] provide complementary information to **[**AMC 20-152A**]/[**AC 20-152A**]**, Custom Device Development, section 5.11. Applicants may **[<AMC>** use this guidance material**]/[<AC>** consider using these best practices**]** when using commercial-off-the-shelf intellectual property (COTS IP) in a custom device.

[<AMC> A.2.1.8.1][<AC> 3.1.8.1] Clarification of Objective IP-2 on Assessment of the COTS IP Provider & COTS IP data

[<AMC> A.2.1.8.1.1][<AC> 3.1.8.1.1] Assessment of the Service Experience of COTS IP

The COTS IP should have been used in numerous application cases, and the IP errata should be available and stable. The applicant will assess and document the relevance of the service experience from data collected from previous or current usage of the component and consider the equivalence of the usage domain, to ensure a certain level of maturity of the IP for the user's application. This data might be obtained with the support of the COTS IP provider, but it might be difficult to demonstrate 'relevant' service experience especially for Soft and Firm IPs. Some additional development assurance needs to be defined to address the risk of insufficient or unrelated service experience.

[<AMC> A.2.1.8.1.2][<AC> 3.1.8.1.2] Assessment of the COTS IP Provider & COTS IP data

The following paragraph provides some high-level examples of assessment on different COTS-IP; they are included for illustration only.

Two typical cases of insufficient coverage when assessing COTS IP with the Objective IP-2 criteria:

— A Soft IP proposed by an experienced provider, but with unknown COTS IP service experience. The COTS IP provider offers limited support for COTS IP, which may be part of an FPGA provider's **[**catalogue**]/[**catalog**]**.

— A new Soft IP proposed by a new company with some documentation. The COTS IP provider does not offer support. There is insufficient evidence of complete verification to make it trustworthy. The applicant may be the first user.

An example of COTS IP assessment with the Objective IP-2 criteria that help define appropriate development assurance activity on the COTS IP:

— A communication Soft IP proposed by an experienced provider. The COTS IP has existed for more than two years and has been used in many applications by many customers. The IP version is stable, and errata are available. The COTS IP is also available as COTS hardware in an FPGA family. The Soft IP is distributed with a set of design constraints and associated implementation results are usable for various sets of technology targets (could be PLDs/FPGAs or ASICs). The test procedures used by the COTS IP provider are not available, but a report providing results of those tests is delivered. Moreover, compliance with the communication standard has been established by the COTS IP provider through an external set of procedures and reports that are also available. This assessment and availability of external sets of procedures support the applicant in defining an acceptable verification strategy.

[<AMC> A.2.1.8.2][<AC> 3.1.8.2] Clarification of Objective IP-4 on Verification Strategy for the COTS IP Function

The COTS IP assessment should determine the extent to which the COTS IP provider verified their IP. This verification could vary from IP with no/little verification performed to IP that is delivered with detailed lifecycle data. The amount of verification performed by the IP provider will drive the applicant's verification strategy.

Taken together, the verification performed by the COTS IP provider and the verification performed by the applicant in the integrated device, shows complete verification of all the used functions of the COTS IP. Thus, if there is little verification data from the COTS IP provider, the applicant will need to do more verification activities to verify the functionality of the IP. If extensive data is provided, then the applicant may only need to show the proper implementation and integration of the IP within the custom device. This activity may be supported by the use of COTS IP provider test cases or by proven test vectors for a COTS IP performing a for a **[**standardised**]/[**standardized**]** interface function.

The verification strategy describes the verification data delivered with the COTS IP, and the verification activities that the applicant proposes to address missing items in order to show the proper implementation and integration of the IP within the custom device.

[<AMC> A.2.1.8.3][<AC> 3.1.8.3] Clarification of Objective IP-5 on Requirements for the COTS IP Function and Validation

Depending on the need for requirements-based testing as a part of the chosen verification strategy for the COTS IP, the level of detail and granularity of the AEH custom device requirements may need to be extended to particularly address the COTS IP function and further design steps of the COTS IP.

When custom device requirements need to be refined to capture the COTS IP functions per the verification strategy, it will be done using all the documentation and design data available. The requirement capture process will encompass all the IP functions, including unused ones for deactivation.

The following aspects could be captured as derived requirements:

1. Error or failure mode detection and correction [AMC behaviour]/[AC behavior]performed by the IP;
2. Design constraints that control the interaction of the IP with the rest of the custom device design;
3. Configuration parameters or settings used to alter or limit the function provided by the IP;
4. Controlling or deactivating unused features or characteristics of the design;
5. Design constraints to properly perform implementation and mitigate the use of the IP features, modes, and design characteristics with known failures or limitations; for DAL A and DAL B, the **[**behaviour**]/[**behavior**]** of the IP during robustness conditions, boundary conditions, failure conditions, and abnormal inputs and conditions;
6. Mitigation of known errata that would adversely affect the correct operation of the function.

When the applicant chooses a verification strategy that solely relies on requirements-based testing, a complete requirement capture of the COTS IP following ED-80/DO-254 is necessary. It is recommended that this activity begins with a thorough understanding of the COTS IP architecture, and both its used and unused functions. The applicant could propose a method in the Plan for Hardware Aspects of Certification (PHAC) for determining and assessing the completeness of the requirements capture process, in order to guarantee that the requirements cover all the used functions and deactivation means for the unused ones (for non-interference with the used functions).

[<AMC>A.2.2]/[<AC> 3.2] COTS DEVICES

These practices provide complementary information to [AMC 20-152A]/[AC 20-152A], COTS Devices, section 6. Applicants may **[<AMC>** use this guidance material**]/[<AC>** consider using these best practices**]** when using COTS devices.

[<AMC>A.2.2.1][<AC>3.2.1] Additional information for COTS Section 6.3 and Objective COTS-1 on COTS complexity assessment

The applicant has to assess the complexity of the COTS devices used in the design and produce the list of all the complex COTS devices. This list of complex COTS is expected to be known at an early stage

and documented in the PHAC or delivered together with the PHAC. It is understood that the list may evolve during development. Ultimately, the Hardware Accomplishment Summary (HAS) captures the final list of complex COTS devices.

As stated in **[**AMC 20-152A**]/[**AC 20-152A**]**, the applicant is not expected to assess the complete bill of material to meet Objective COTS-1, but only those devices that are relevant for the classification, including devices that are on the boundary between simple and complex. The assessment and the resulting classification (simple or complex) for those devices that are on the boundary and classified as simple would be documented in a life cycle data item that is referred to in the PHAC and HAS.

The following examples provide some characteristics of complex and simple devices for illustration. These examples are provided for illustration only. Other combinations of characteristics will occur in actual projects.

EXAMPLES OF COTS DEVICES AND ASSOCIATED CHARACTERISTICS	COMPLEXITY
An example of a single-core processor/microcontroller with: — Multiple and complex functional elements that interact with each other - PCIe interface, Ethernet, Serial RapidIO, a single core processor; — Significant number of functional modes where each interface has several selectable channels/modes of operation; and — Configurable functions allowing different data/signal flows and different resource sharing within the device so the different data paths within the device are fully configurable in a dynamic manner.	Complex
An example of a single-core processor/microcontroller with: — Single advanced reduced instruction machine core processor; — Inter-processor communication uses simple mailbox protocol; — Programmable real-time unit (PRU) subsystem contains 2 RISC processors and complex access to many peripherals; — PRU is highly programmable with 200 registers, each of the peripherals is also configurable. The PRU is complex.	Complex
An example of a single-core processor/microcontroller with: — Several functional elements that interact with each other PCI interface, SPI, I2C, JTAG, 1 core processor — Significant number of functional modes where interface has few modes of operation; and — Limited configurable functions allowing one major data path using a limited number of discretes on SPI or I2C. There is no different resource sharing in the device.	Simple
An example of a 32 nit reduced instruction set computing (RISC) microcontroller with: — Internal buses are all simple master-slave protocol, — Processor has dedicated resources,	Simple

— No interconnect fabric, no multiple masters, — Single point of access to all peripherals, — independent time processor units (TPU) with microcode that are accessed through the slave peripheral control unit.	
An example of a stand-alone controlled area network (CAN) controller with a serial peripheral interface (SPI) with: — A single controller with one SPI bus.	Simple
An example of a communications infrastructure digital signal processor (DSP) with: — A single DSP, — Interconnect between DSP and peripherals is an interconnect switch with multiple masters, multiple slaves and is highly configurable, — Multiple internal bridges between the peripherals and the interconnect switch and programmable priorities.	Complex
An example of an analog to digital converter with: — 8-Channel/16-Channel, software selectable, 24-Bit ADC.	Simple
An example of a digital SPI temperature sensor with: — Analog temperature sensor, — Conversion to digital, — SPI output.	Simple
An example of a FPGA component with some Hard IP embedded in silicon with: — FPGA fabric (out of the COTS scope), — Embedded RAM/ROM memories, — Embedded FIFOS, — PCI port, — A/D and D/A converters, — 16x16 configurable multiplier blocks.	Simple
An example of an FPGA component with Hard IP embedded in silicon with: — FPGA fabric (out of the COTS scope), — Embedded RAM/ROM memories, — Embedded FIFOS, — PCIe port, — Processor Core, — Coherency fabric/interconnect, — A/D and D/A converters.	Complex

[<AMC> A.2.2.2][<AC>3.2.2] Additional Information for COTS Section 6.4.1 Electronic Component Management Process

[<AMC> A.2.2.2.1] [<AC>3.2.2.1] Clarification of Objective COTS-2 on Electronic Component Management Plan

IEC 62239 and SAE EIA-STD4899B define items and processes that support the establishment of industry electronic component management plans which would be considered as industry recommended standards to support the topics mentioned in Objective COTS-2.

Generally, the ECMP describes a standard process that is re-used and re-applied from certification project to certification project. This approach is understood to ease the certification process.

Regarding assessment of maturity:

When selecting a device, the applicant assesses the maturity of the device and **[**analyses**]/[**analyzes**]** whether its maturity is sufficient to ensure that the potential for design errors has been reduced. This assessment of maturity could encompass some of the following items:

— Time of the device in service,

— Widespread use in service: an indication of widespread use could be given (multiple applications, large minimum number of chips sold, etc.),

— Product service experience per DO-254/ED-80, section 11.3 from any previous or current usage of the device,

— Maturity of intellectual property embedded into the device,

— Decreasing rate of new errata.

There are no quantitative targets expressed but there is a necessity for an engineering assessment of the device maturity, starting with the selection process.

[<AMC> A.2.2.2.2] [<AC> 3.2.2.2] Clarification of Objective COTS-3 on Using a Device Outside the Ranges of Values Specified in its Datasheet

Establishing the reliability of a complex COTS device that is used outside its specification (recommended operating limits), determined by the device manufacturer, is considered to be difficult and might introduce risks that should be mitigated.

One process to qualify the device, called an 'uprating' process, could be applied to verify the appropriate operation of the device itself and to guarantee that performance is achieved in the target environment in all operating conditions over the lifetime of the equipment. This uprating process takes into account the different technology variations (variation of performance over different batches/over different dies).

Thermal uprating is addressed in IEC/TR 62240-1. It 'provides information to select semiconductor devices, to assess their capability to operate, and to assure their intended quality in the wider temperature range. It also reports the need for documentation of such usage.'

It is understood that each case of uprating might follow a different process depending on the 'uprated' characteristics (frequency, temperature, voltage, etc.) and the performance guaranteed by the device

manufacturer's datasheet. For that reason, Objective COTS-3 is separated from Objective COTS-2 and is only to be applied in cases of COTS device uprating.

IEC/TR 62240-1 states the following: 'For each instance of device usage outside the manufacturer's specified temperature range relevant data are documented and stored in a controlled, retrievable format.' This is considered to be a best practice for any uprating case as evidence satisfying Objective COTS-3.

Note: when a simple COTS device is used outside its datasheet, applying an uprating process would be considered to be a best practice to ensure that the device functions properly within the newly defined and intended environment/usage conditions.

[<AMC> A.2.2.3][<AC> 3.2.3] Additional information for COTS Section 6.4.2 COTS Device Malfunction

The applicant needs access to errata information on the device during the entire life cycle of the product (before and after certification).

In general, this assessment typically includes:

— Analysis of which errata are, or are not, applicable to the specific installation of the equipment, and for each of the applicable errata,

— The description of the mitigation implemented,

— The evidence that the implementations of errata mitigations are covered by relevant requirements, design data, and are verified.

Assessment of errata of simple COTS device is considered a best practice to remove the safety risks associated with device malfunctions.

While the applicant is expected to document the process applied for errata in the PHAC, the errata and evidence of assessment would typically be captured in other documents that can be referred to in the PHAC and HAS.

[<AMC> A.2.2.4][<AC>3.2.4] Additional information for Objective COTS-6 on COTS Device Malfunction

It is understood that the task linked with this objective is performed in close coordination with hardware, software, and system teams.

In order to support the safety analysis process, this objective focuses on the failure effects and not on their root causes. The hardware domain, knowing the detailed usage of the device, starts by identifying the effects of failures of the device on the intended functions. This information will be provided to the system safety process. When necessary, mitigation means will be defined and verified by the appropriate domain or across hardware, software, and system domains.

While the applicant is expected to document the process to satisfy Objective COTS-6 in the PHAC, the evidence would typically be captured in other documents that can be referred to in the PHAC and ultimately in the HAS.

When a simple COTS device interfaces with software, complying with Objective COTS-6 is considered best practice.

[<AMC>A.2.3][<AC> 3.3] Electronic Hardware Assembly Development

In the aviation domain, the applicant typically has internal procedures to develop the electronic hardware assembly. When the electronic hardware assembly contains complex devices, there is a clear benefit for the applicant (or developer of the airborne system and equipment) in having a structured process to address the development of electronic hardware assemblies (boards or a collection of boards) that encompasses requirements capture, validation, verification, and configuration management activities.

An applicant's (or developer's) internal structured process that encompasses these activities is an acceptable development assurance approach for their electronic hardware assembly.

Note 1: The applicant's internal procedures might be tailored according to the hardware complexity if necessary.

Note 2: The structure of the process life cycle data is at the discretion of the applicant's internal procedures.

Note 3: The electronic hardware assembly requirements may be verified at a higher level of integration.

[<AMC>A.2.4][<AC> 3.4] Development of airborne electronic hardware contributing to functions with a hardware DAL D

For airborne electronic hardware contributing to functions with a hardware DAL D, the acceptable means of compliance include ED-80/DO-254 or existing Level D hardware development assurance practices that demonstrate the requirements allocated to the DAL D airborne electronic hardware have been satisfied. Additionally, system level development assurance practices such as ED-79A/ARP 4754A or other means may be used if the applicant can demonstrate at the system level that the requirements allocated to the DAL D airborne electronic hardware have been satisfied.

[<AC> 4. Related Regulatory, Advisory, and Industry Material

(a) 14 CFR Applicable Sections. 14 CFR parts 21, 23, 25, 27, 29, 33 and 35.

(b) FAA ACs.

(1) AC 20-152A, *Development Assurance for Airborne Electronic Hardware*.

(2) AC 20-174, *Development of Civil Aircraft and Systems.*

(3) AC 21-50, *Installation of TSOA Articles and LODA Appliances.*

(4) AC 23.1309-1, *System Safety Analysis and Assessment for Part 23 Airplanes.*

(5) AC 25.1309-1, *System Design and Analysis.*

(6) AC 27-1309*, Equipment, Systems, and Installations* (included in AC 27-1, *Certification of Normal Category Rotorcraft*)*.*

(7) AC 29-1309, *Equipment, Systems, and Installations* (included in AC 29-2, *Certification of Transport Category Rotorcraft*)*.*

(8) AC 33.28-1, *Compliance Criteria for 14 CFR § 33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems.*

(9) AC 33.28-3, *Guidance Material for 14 CFR § 33.28, Engine Control Systems.*

(10) AC 33.28-3, *Guidance Material for 14 CFR § 33.28, Engine Control Systems.*

(11) AC 35.23-1, *Guidance Material for 14 CFR 35.23, Propeller Control Systems*.

(c) EASA Acceptable Means of Compliance (AMC)

(1) AMC 20-152(), *Development Assurance for Airborne Electronic Hardware*.

(d) Industry Documents

(1) SAE International Aerospace Recommended Practice (ARP) 4754A, *Guidelines for Development of Civil Aircraft and Systems,* dated December 21, 2010.

(2) RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware,* dated April 19, 2000.

(3) EUROCAE ED-80, *Design Assurance Guidance for Airborne Electronic Hardware,* dated April 2000.

5. Where to find this AC.

1. You may find this AC at http://www.faa.gov/regulations_policies/advisory_circulars/
2. If you have suggestions for improvement or changes, you may use the template at the end of this AC.

Michael Romanowski

Director, Policy & Innovation Division

Aircraft Certification Service]

Appendix A. GLOSSARY [<AMC> of GUIDANCE MATERIAL]

This glossary complements the terms defined in **[**AMC 20-152A**][**AC 20-152A**]** with terms used only in this **[**GM**]/[**AC 00-72**]**.

Uprating – adapted from the IEC/TR 62240-1 Thermal uprating definition – a process to assess the capability of a part to meet the performance requirements of the application in which the device is used outside the manufacturer's datasheet ranges.

[<AC> Appendix B. Advisory Circular Feedback Form

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to 9-AWA-AVS-AIR-DMO@faa.gov, or (2) faxing it to the attention of the AIR Directives Management Officer at (202)-267-3983.

Subject: _____ Date: _____

Please check all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph _____ on page _____.

☐ Recommend paragraph _____ on page _____ be changed as follows:

☐ In a future change to this AC, please cover the following subject: *(Briefly describe what you want added.)*

☐ Other comments:

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____]

3.2. Draft Acceptable Means of Compliance and Guidance Material (EASA AMC/FAA AC) on OPRs

3.2.1. Draft acceptable means of compliance (EASA AMC/FAA AC)

[**<AMC>** AMC 20-189: **Management of Open Problem Reports**]

[**<AC>** AC 20-189: **Management of Open Problem Reports**]

1. Purpose

The purpose of this **[**AMC**]/[**AC**]** is to describe an acceptable process for the management of open problem reports (OPRs) in [ETSO Authorisation]/[TSO Authorization]and type certification, for the System, Software and Airborne Electronic Hardware (AEH) domains.

2. Applicability This [AMC]/[AC] may be used by applicants, design approval holders, and developers of airborne systems and equipment to be installed on **[**type-certified**]/[**type certificated**]** aircraft, engines, and propellers. This **[**AMC**]/[**AC**]** applies to all airborne electronic systems and equipment, software and AEH embedded in those systems, which could cause or contribute to Catastrophic, Hazardous, or Major failure conditions. This **[**AMC**]/[**AC**]** is not applicable to electronic equipment embedded in airborne systems which could cause or contribute only to Minor failure conditions or to failure conditions having No Safety Effect. This **[**AMC**]/[**AC**]** is also not applicable to component partitions which could cause or contribute only to Minor failure conditions or to failure conditions having No Safety Effect.

3. Background3.1. Each of the System, Software and AEH domains relies on problem report (PR) management to ensure the proper management of open problem reports and to help ensure safe products at the time of approval (see definitions). However, existing guidance on PR and OPR management is inconsistent and incomplete across domains. Therefore, this **[**AMC**]/[**AC**]** provides consistent guidance across these domains for problem report management, OPR management, stakeholder responsibilities, reporting, and other aspects of OPR management. This **[**AMC**]/[**AC**]** complements but does not alleviate the project-applicable System, Software and AEH guidance.

3.2. The technical content of this **[**AMC**]/[**AC**]** is as far as practicable **[**harmonised**]/[** harmonized**]** with **[**Federal Aviation Administration (FAA) AC 20-189**]/[**European Aviation Safety Agency (EASA) AMC 20-189**]**.

3.3. [<AC> 3.3. **See AC 00-71, *Best practices for Management of Open Problem Reports*.]**

4. Definitions

4.1. Terms Used in this [AMC]/[AC]

Approval - The term 'Approval' in this document addresses approval by **[**EASA**]/[**the FAA**]** of the product or of changes to the product, or authorization of the **[**ETSO**]/[**TSO**]** article or of changes to the **[**ETSO**]/[**TSO**]** article.

Article - Refer to **[**EASA Part 21**]/[**14 CFR part 21**]**.

Development Assurance – All of those planned and systematic actions used to substantiate, with an adequate level of confidence, that errors in requirements, design, and implementation have been

identified and corrected such that the system satisfies the applicable certification basis (source: ARP4754A/ED-79A).

Equipment – An item or collection of items with a defined set of requirements.

Error – A mistake in requirements, design, or implementation with the potential of producing a failure.

Failure – The inability of a system or system component to perform a function within specified limits (source: DO-178C/ED-12C and DO-254/ED-80).

Item – A hardware or software element having bounded and well-defined interfaces (source: ARP4754A/ED-79A).

Open Problem Report (OPR) – A problem report that has not reached the state 'Closed'at the time of approval.

Problem Report (PR) – A means to identify and record the resolution of anomalous behavior, process non-compliance with development assurance plans and standards, and deficiencies in life cycle data (adapted from DO-178C/ED-12C).

Product – Refer to **[**EASA Part 21**]/[**14 CFR part 21**]**.

System – A combination of inter-related equipment, article(s), and/or items arranged to perform a specific function(s) within a product.

4.2. Possible States of PRs/OPRs.

Classified – A problem report is **[**categorised**]/[**categorized**]** in accordance with an established classification scheme.

Closed – A resolved problem report that underwent review and confirmation of effective resolution of the problem.

Recorded – A problem that has been documented using the problem reporting process.

Resolved – A problem report that has been corrected or fully mitigated, but which closure has not been reviewed and confirmed.

4.3. Classification of PRs/OPRs.

'Potential Safety': assessed at the product, system, or equipment level, a PR having an actual or potential Catastrophic, Hazardous or Major safety effect on the aircraft, or affecting compliance with operating rules.

Note: The 'potential safety effect' in this definition is based on Initial Airworthiness considerations (e.g. AMC/AC 25.1309), therefore PRs classified as 'Potential Safety' do not automatically relate to an unsafe condition per EASA part 21.A.3B(b) or FAA part 39.5.

'Functional': a PR having an actual or a potential impact on a function at the product, system, or equipment level.

'Process': a PR recording a process non-compliance, deficiency or deviation that cannot result in a potential safety, nor potential functional, impact.

'Documentary': a PR linked to a deficiency in a life cycle data item but not linked to a process deficiency or deviation. This includes typographical or editorial defects in life cycle documents.

'Other': a PR having no potential safety impact, no potential functional impact, and not linked to a process deficiency or a deviation or to a documentary deficiency.

5. Problem Report Management.

5.1 A PR management process across System, Software and AEH domains should be established and used during the development (both for initial certification and subsequent changes) of a product or **[**ETSO**]/[**TSO**]** article. The PR management process should address the review and resolution of PRs that impact the transition to other development assurance processes.

5.2 A problem recorded after approval should also be managed through the PR management process. Additionally, an applicant should identify and correct any related systemic process issues.

5.3 For PRs that cannot be resolved at the current stakeholder level and that have an impact on the next level stakeholder, the current stakeholder should report the PR in a manner that is understandable to the next level stakeholder.

6. OPR Management

An OPR management process should be established across System, Software and AEH domains, including the following process steps:

6.1 **Classification of OPRs.** The applicant should establish an OPR classification scheme including at a minimum, the following classifications: 'Potential Safety', 'Functional', 'Process', 'Documentary' and 'Other'. The classification scheme should be described in the appropriate planning document(s).

6.1.1 Each OPR should be assigned a single classification per the classification scheme. When multiple classifications apply, the OPR should be assigned the classification with the highest priority. The priority from highest to lowest is:

1. 'Potential Safety';
2. 'Functional';
3. 'Process';
4. 'Documentary';
5. 'Other' Impact.

6.1.2 The classification of an OPR should account for and document all mitigations known at the time of classification that are under the control of the classifying stakeholder. Mitigations that are controlled by a higher-level stakeholder, including any operational mitigation, should not be considered in the current level stakeholder's classification.

6.1.3 Stakeholders other than the type certificate (TC)/supplemental type certicate (STC) level applicant should consider the potential worst-case effect (as anticipated by the stakeholder) of the OPR in the classification.

6.1.4 The classification of an individual OPR may differ from one stakeholder level to another, depending on the known mitigations at the time of classification.

6.2 Assessment of OPRs. Each OPR should be assessed to determine:

1. Any resulting functional limitations and operational restrictions at equipment level (for **[**ETSO**]/[**TSO**]**) or at product level (for other types of approvals);
2. Relationships that may exist with other OPRs;
3. For 'Potential Safety' and 'Functional' OPRs, the applicant should determine the underlying technical cause of the problem.

6.3 Disposition: OPRs classified as 'Potential Safety' per the classification in paragraph 6.1.1, for which no sufficient mitigation or justification exists to substantiate the acceptability of the safety impact should be resolved prior to approval. OPR disposition may involve coordination with the certification authority.

6.4 Reporting: an OPR summary report (e.g. as contained in Software/Hardware Accomplishment Summaries or system-level OPR reports) should be prepared and provided to the affected stakeholder(s), and to the certification authority upon request. The summary report should contain the following information for each OPR:

6.4.1 Identification of the OPR (for example, OPR ID);

6.4.2 Identification of the affected configuration item(s) (for example, the item part number) or of the affected process(es);

6.4.3 The title or a summary of the problem, formulated in a manner understandable by the next level stakeholder(s);

6.4.4 A description of the problem, formulated in a manner understandable by the next level stakeholder(s);

6.4.5 Conditions under which the problem occurs;

6.4.6 OPR assessment results (per paragraph 6.2), including:

1. The classification of each OPR;
2. The functional limitations and operational restrictions, if any;
3. Relationships that are known to exist with other OPRs;
4. For OPRs classified as 'Functional' , any mitigations implemented to reduce the safety impact to minor or No Safety Effect;

5. The justification for allowing the OPR to remain open:

   — For OPRs classified as 'potential safety', any mitigations or justifications used to substantiate the acceptability of the safety impact (per paragraph 6.3);

   — For OPRs classified as 'functional', the assessment of no safety effect or, at most, a Minor safety effect, should be justified;

   — OPRs determined to be associated with a 'process' deficiency or deviation should be assessed for the extent or nature of deviations from the plans that may contribute to not satisfying the applicable development assurance objectives;

   — For 'other' OPRs, it should be justified that the error cannot cause a functional failure.

6.5 [ETSO]/[TSO] Specifics: The **[ETSO Authorisation]/[TSO Authorization]**holder should provide an OPR summary report to the affected stakeholder(s) (per paragraph 6.4) for all OPRs, except those classified as 'Process', 'Documentary' and 'Other' unless necessary for the installation approval. However, all OPRs should be available upon request by the certification authority for assessment in the frame of the **[**ETSO**]/[**TSO**]** approval. In addition, the **[ETSO Authorisation]/[TSO Authorization]**holder should provide:

6.5.1 A means to record and confirm the problems reported from outside the **[**organisation**]/[**organization**]** into a problem reporting system for tracking and disposition. This includes problems reported by the installation approval holders and operators.

6.5.2 A means to transmit new PRs relevant for airworthiness to installers and the certification authority.

7. Stakeholder Responsibilities.

Levels of stakeholders include: item, equipment or **[**ETSO**]/[**TSO**]** article, system, product, and certification authority. The actual levels for a specific project depend on the project **[**organisation**]/[**organization**]** and on the certification authority involvement.

7.1 PR management (per paragraph 5) should be performed by the stakeholder at each level. The applicant has responsibility for the overall PR process for all involved stakeholders.

7.2 OPR management (per paragraph 6) should be performed, at a minimum, at the **[**ETSO**]/[**TSO**]** article level, at the level of each individual system within a product and at the product level.

[<AMC> 8. RELATED REGULATORY, ADVISORY, AND INDUSTRY MATERIAL.

(a) Related EASA Certification Specifications (CSs)

(1) CS-23, *Certification Specifications and Acceptable Means of Compliance for Normal, Utility, Aerobatic, and Commuter Category Aeroplanes*.

(2) CS-25, *Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes*.

(3) CS-27, *Certification Specifications and Acceptable Means of Compliance for Small Rotorcraft*.

(4) CS-29, *Certification Specifications and Acceptable Means of Compliance for Large Rotorcraft.*

(5) CS-E, *Certification Specifications and Acceptable Means of Compliance for Engines, and AMC 20-3A, Certification of Engines Equipped with Electronic Engine Control Systems*.

(6) CS-P, *Certification Specifications for Propellers, and AMC 20-1, Certification of Aircraft Propulsion Systems Equipped with Electronic Control Systems.*

(7) CS-ETSO, *Certification Specifications for European Technical Standard Orders*.

(8) CS-APU, *Certification Specifications for Auxiliary Power Units*, and AMC 20-2A, *Certification of Essential APU Equipped with Electronic Controls.*

(b) EASA Acceptable Means of Compliance (AMC)

(1) AMC 20-115( ), *Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178*.

(2) AMC 20-152( ), Development Assurance for Airborne Electronic Hardware.

(c) FAA ACs

(1) AC 20-115, *Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( ).*

(2) AC 20-152, *Development Assurance for Airborne Electronic Hardware.*

(3) AC 27-1309, *Equipment, Systems, and Installations (included in AC 27-1, Certification of Normal Category Rotorcraft).*

(4) AC 29-1309, *Equipment, Systems, and Installations (included in AC 29-2, Certification of Transport Category Rotorcraft)*.

(d) Industry Documents

(1) EUROCAE ED-12, *Software Considerations in Airborne Systems and Equipment Certification*, dated May 1982 (no longer in print).

(2) EUROCAE ED-12A, *Software Considerations in Airborne Systems and Equipment Certification*, dated October 1985 (no longer in print).

(3) EUROCAE ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1992.

(4) EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification,* dated January 2012.

(5) EUROCAE ED-79A, *Guidelines for Development of Civil Aircraft and Systems*, dated December 2010.

(6) EUROCAE ED-80, *Design Assurance Guidance for Airborne Electronic Hardware*, dated April 2000.

(7) EUROCAE ED-94C, *Supporting Information for ED-12C and ED-109A*, dated January 2012.

(8) EUROCAE ED-215, *Software Tool Qualification Considerations,* dated January 2012.

(9) EUROCAE ED-216, *Formal Methods Supplement to ED-12C and ED-109A*, dated January 2012.

(10) EUROCAE ED-217, Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A, dated January 2012.

(11) EUROCAE ED-218, Model-Based Development and Verification Supplement to ED-12C and ED-109A, dated January 2012.

(12) RTCA DO-178, Software Considerations in Airborne Systems and Equipment Certification, dated January 1982 (no longer in print).

(13) RTCA DO-178A, Software Considerations in Airborne Systems and Equipment Certification, dated March 1985 (no longer in print).

(14) RTCA DO-178B, Software Considerations in Airborne Systems and Equipment Certification, dated 1 December 1992.

(15) RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification, dated 13 December 2011.

(16) RTCA DO-248C, Supporting Information for DO-178C and DO-278A, dated 13 December 2011.

(17) RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware, dated April 19, 2000.

(18) RTCA DO-297, Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations, dated 8 November 2005.

(19) RTCA DO-330, Software Tool Qualification Considerations, dated 13 December 2011.

(20) RTCA DO-331, Model-Based Development and Verification Supplement to DO-178C and DO-278A, dated 13 December 2011.

(21) RTCA DO-332, Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A, dated 13 December 2011.

(22)RTCA DO-333, Formal Methods Supplement to DO-178C and DO-278A, dated 13 December 2011.

(23)SAE International Aerospace Recommended Practice (ARP) 4754A, Guidelines for Development of Civil Aircraft and Systems, dated December 21, 2010.]

[<AC>8. RELATED REGULATORY, ADVISORY, AND INDUSTRY MATERIAL.

(a) 14 CFR Applicable Sections. 14 CFR parts 21, 23, 25, 27, 29, 33 and 35.

(b) FAA Advisory Circulars (ACs).

(1) AC 20-115, *Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )*.

(2) AC 20-152, *Development Assurance for Airborne Electronic Hardware (AEH)*.

(3) AC 20-170, *Integrated Modular Avionics Development, Verification, Integration and Approval using RTCA DO-297 and Technical Standard Order C-153*.

(4) AC 20-171, *Alternatives to RTCA/DO-178B for Software in Airborne Systems and Equipment*.

(5) AC 20-174, *Development of Civil Aircraft and Systems.*

(6) AC 21-46, *Technical Standard Order Program.*

(7) AC 21-50, *Installation of TSOA Articles and LODA Appliances.*

(8) AC 23.1309-1, *System Safety Analysis and Assessment for Part 23 Airplanes.*

(9) AC 25.1309-1, *System Design and Analysis.*

*(10)*AC 27-1309*, Equipment, Systems, and Installations* (included in AC 27-1, *Certification of Normal Category Rotorcraft*).

(11)AC 29-1309, Equipment, Systems, and Installations (included in AC 29-2, Certification of Transport Category Rotorcraft).

(12)AC 33.28-1, *Compliance Criteria for 14 CFR § 33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems.*

(13)AC 33.28-2, *Guidance Material for 14 CFR 33.28, Reciprocating Engines, Electrical and Electronic Engine Control Systems*.

(14)AC 33.28-3, *Guidance Material for 14 CFR § 33.28, Engine Control Systems.*

(15)AC 35.23-1, *Guidance Material for 14 CFR 35.23, Propeller Control Systems*.

(c) EASA Acceptable Means of Compliance (AMC).

(1) AMC 20-115( ), *Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178*.

(2) AMC 20-152( ), *Development Assurance for Airborne Electronic Hardware (AEH)*.

(d) Industry Documents.

(1) SAE International Aerospace Recommended Practice (ARP) 4754A, *Guidelines for Development of Civil Aircraft and Systems,* dated December 21, 2010.

(2) RTCA DO-178, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 1982 (no longer in print).

(3) RTCA DO-178A, *Software Considerations in Airborne Systems and Equipment Certification*, dated March 1985 (no longer in print).

(4) RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1, 1992

(5) RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 13, 2011.

(6) RTCA DO-248C, *Supporting Information for DO-178C and DO-278A*, dated December 13, 2011.

(7) RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware,* dated April 19, 2000.

(8) RTCA DO-297, *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations*, dated November 8, 2005.

(9) RTCA DO-330, *Software Tool Qualification Considerations*, dated 13 December 2011.

(10) RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A,* dated December 13, 2011.

(11) RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(12) RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(13) EUROCAE ED-12, *Software Considerations in Airborne Systems and Equipment Certification*, dated May 1982 (no longer in print).

(14) EUROCAE ED-12A, *Software Considerations in Airborne Systems and Equipment Certification*, dated October 1985 (no longer in print).

(15) EUROCAE ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1992.

(16) EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 2012.

(17) EUROCAE ED-79A, *Guidelines for Development of Civil Aircraft and Systems,* dated December 2010.

(18) EUROCAE ED-80, *Design Assurance Guidance for Airborne Electronic Hardware,* dated April 2000.

(19) EUROCAE ED-94C, *Supporting Information for ED-12C and ED-109A*, dated January 2012.

(20)EUROCAE ED-215, *Software Tool Qualification Considerations*, dated January 2012.

(21)EUROCAE ED-216, *Formal Methods Supplement to ED-12C and ED-109A*, dated January 2012.

(22)EUROCAE ED-217, *Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A*, dated January 2012.

(23)EUROCAE ED-218, *Model-Based Development and Verification Supplement to ED-12C and ED-109A*, dated January 2012.**]**

[<AMC>9. Availability of Documents

(1) EASA Certification Specifications (CSs) and Acceptable Means of Compliance (AMC) may be downloaded from the EASA website: www.easa.europa.eu.

(2) FAA Advisory Circulars (ACs) may be downloaded from the FAA website: www.faa.gov.

(3) EUROCAE documents may be purchased from:

European Organisation for Civil Aviation Equipment9-23 rue Paul Lafargue, "Le Triangle" 93200 Saint-Denis, FranceTelephone: +33 1 49 46 19 65(E-mail: eurocae@eurocae.net, website: www.eurocae.net)

(4) RTCA documents may be purchased from:

RTCA, Inc.1150 18th Street NW, Suite 910, Washington DC 20036, USA

(Email: info@rtca.org, website: www.rtca.org).**]**

[<AC>9. Where to find this AC

1. You may find this AC at http://www.faa.gov/regulations_policies/advisory_circulars/.
2. If you have suggestions for improvement or changes, you may use the template at the end of this AC.

Michael Romanowski
Director, Policy & Innovation Division
Aircraft Certification Service

Advisory Circular Feedback Form

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to 9-AWA-AVS-AIR-DMO@faa.gov, or (2) faxing it to the attention of the AIR Directives Management Officer at (202)-267-3983.

Subject: _____ Date: _____

Please check all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph _____ on page _____.

☐ Recommend paragraph _____ on page _____ be changed as follows:

☐ In a future change to this AC, please cover the following subject: *(Briefly describe what you want added.)*

☐ Other comments:

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____

3.2.2. Draft EASA guidance material (GM) / FAA AC 00-71

[<AC> AC 00-71: Best Practices for Management of Open Problem Reports

1. Purpose.

This advisory circular (AC) provides information in the form of 'best practices' and, as such, is not intended as guidance but rather as complementary information to AC 20-189.

2. Audience.

We wrote this AC as a means of assisting applicants, design approval holders and developers of airborne systems and equipment containing software or Airborne Electronic Hardware (AEH) intended to be installed on type certificated aircraft, engines, and propellers. This AC applies to all airborne electronic systems and equipment, software, and AEH embedded in those systems which could cause or contribute to Catastrophic, Hazardous or Major failure conditions. This AC is not applicable to electronic equipment embedded in airborne systems which could cause or contribute only to Minor failure conditions or to failure conditions having No Safety Effect. This AC is also not applicable to component partitions which could cause or contribute only to Minor failure conditions or to failure conditions having No Safety Effect.

3. Definitions.

3.1 Terms Used in this AC.

Approval – The term 'Approval' in this document addresses approval by the FAA of the product or of changes to the product, or authorization of the TSO article or of changes to the TSO article.

Article – Refer to 14 CFR part 21.

Development Assurance – All of those planned and systematic actions used to substantiate, with an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis (source: ARP4754A/ED-79A).

Equipment – An item or collection of items with a defined set of requirements.

Item – A hardware or software element having bounded and well-defined interfaces (source: ARP4754A/ED-79A).

Open problem report (OPR) – A problem report that has not reached the state 'Closed' at the time of approval.

Problem report (PR) – A means to identify and record the resolution of anomalous behavior, process non-compliance with development assurance plans and standards, and deficiencies in life cycle data (adapted from DO-178C/ED-12C).

Product – Refer to 14 CFR part 21.

System – A combination of inter-related equipment, article(s), and/ or item(s) arranged to perform a specific function(s) within a product.

3.2 Possible States of PRs/OPRs.

Classified – a problem report is **[**categorised**]/[**categorized] in accordance with an established classification scheme.

Closed – a resolved problem report that underwent review and confirmation of effective resolution of the problem.

Recorded – a problem that has been documented using the problem reporting process.

Resolved – a problem report that has been corrected or fully mitigated, but which closure has not been reviewed and confirmed.

3.3 Classification of PRs/OPRs.

'Potential Safety': assessed at the product, system, or equipment level, a PR having an actual or potential Catastrophic, Hazardous or Major safety effect on the aircraft, or affecting compliance with operating rules. Note: The "potential safety effect" in this definition is based on Initial Airworthiness considerations (e.g. AMC/AC 25.1309), therefore PRs classified as 'Potential Safety' do not automatically relate to an unsafe condition (based on EASA part 21.A.3B(b) or FAA part 39.5).

'Functional': a PR having an actual or a potential impact on a function at the product, system, or equipment level.

'Process': a PR recording a process non-compliance, deficiency, or deviation that cannot result in a potential safety, nor potential functional, impact.

'Documentary': a PR linked to a deficiency in a life cycle data item not linked to a process deficiency or deviation. This includes typographical or editorial defects in life cycle documents.

'Other': a PR having no potential safety impact, no potential functional impact, and not linked to a process deficiency or deviation or to a documentary deficiency.

4. BEST PRACTICES.]

[<AMC> GM 20-189 Open Problem Report Management

GM1 to AMC 20-189 :]/[<AC> 4.1] PR management. Typically, PR processes include the following aspects:

[<AC>4.1.]1. PR Recording: a means to document problems resulting from development activities.

[<AC>4.1.]2. PR Classification: a means to classify PRs prior to the time of approval of the product or of the [ETSO]/[TSO] article, as early in the life cycle as practical. While early classification may be preliminary, it will help to focus attention on PRs with potential safety or functional impacts, as well as process PRs that may impact the development or development assurance processes.

[<AC>4.1.]3. PR Assessment: a means to assess the effect of having a PR remain open at the time of approval. Typical review boards used for PRs classified as 'Potential Safety', 'Functional' or 'Process'

PRs may not be needed for PRs that are classified as 'Documentary' or 'Other', where peer reviews may be sufficient.

[<AC>4.1.]4. PR Resolution: a means to correct or mitigate PRs prior to the time of approval, as early in the life cycle as practical. The PR resolution process may depend on the classification of the PR; for example, shorter closure loops could be set for PRs with only 'Documentary' impact.

[<AC>4.1.]5. PR Closure: a means to close PRs, which includes the review and confirmation of resolution of the problem, and indicated through a documented authorization process (e.g., Change Control Board signoff). A PR can be closed only when the problem has been effectively resolved.

[<AMC> GM2 to AMC 20-189:]/[<AC> 4.2] OPR classification. The following classification scheme correlates the example classifications presented in DO-248C/ED-94C, DP #9, as a means of satisfying the guidance in **[**AMC**]/[**AC**]** 20-189 subparagraph 6.1.

[<AC>4.2.]1. Type 'Potential Safety': this typically maps to 'type 0'. However, some applicants may have used the 'type 1A' to **[**characterise**]/[**characterize**]** some PRs, for instance, those linked to Major failure conditions. The **[**AMC**]/[**AC**]** 20-189 scheme clarifies that those PRs potentially causing or contributing to Catastrophic, Hazardous or Major failure conditions, belong to the class 'Potential Safety'.

[<AC>4.2.]2. Type 'Functional': this typically maps to 'type 1A' or 'type 1B'. One way of creating the link between these two types and the [AMC]/[AC] 20-189 classification scheme is to consider 'type 1A' for PRs whose consequences can potentially lead to a Minor failure and 'type 1B' for PRs having No Safety Effect. Two separate classes could therefore be created in the applicant's classification scheme to ease the mapping: problems having an operational impact leading to a Minor failure condition could be classified separately (e.g. 'Functional 1') from the ones having No Safety Effect (e.g. 'Functional 2').

[<AC>4.2.]3. Type 'Process': this may map to type 3A, however, not in cases where the process deficiency or deviation could result in either not detecting a failure or creating a failure. An important clarification in **[**AMC**]/[**AC**]** 20-189 is the removal of the ambiguous notion of 'significant deviation from the plans or standards' used in the definition of 'type 3A'. The 'Process' classification in **[**AMC**]/[**AC**]** 20-189 should be used for PRs that record a process non-compliance or deviation, provided they cannot result in a potential safety or potential functional impact. An example of an OPR that should not be classified as a 'Process' PR is one related to a requirement that was not completely verified because of a process deficiency.

[<AC>4.2.]4. Type 'Documentary': this typically maps to 'type 3B'. The removal of the notion of 'non-significant deviation from the plans or standards' from the definition of 'type 3B' also helps to focus 'Documentary' PRs on pure documentary issues.

[<AC>4.2.]5. Type 'Other': this typically maps to 'type 2' and 'type 4' PRs, but may not be limited to those types. It serves as a default class to cover any remaining PRs that do not relate to any potential safety, potential functional, process or documentary impact.

[<AMC> GM3 to AMC 20-189:]/[<AC> 4.3] OPR reporting. Regarding **[**AMC**]/[**AC**]** 20-189 subparagraph 6.4.6. Item 5, when providing a justification for an OPR of classification 'Other':

[<AC>4.3.]1. For simple cases, this justification may be a statement based on engineering judgment;

[<AC>4.3.]2. In more complex cases, this justification may imply specific additional validation and/or verification activities.

[<AC>

5. Related Publications.

(a) 14 CFR Applicable Sections. 14 CFR parts 21, 23, 25, 27, 29, 33 and 35.

(b) FAA ACs.

(1) AC 20-115, *Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )*.

(2) AC 20-152, *Development Assurance for Airborne Electronic Hardware (AEH)*.

(3) AC 20-170, *Integrated Modular Avionics Development, Verification, Integration and Approval using RTCA DO-297 and Technical Standard Order C-153*.

(4) AC 20-171, *Alternatives to RTCA/DO-178B for Software in Airborne Systems and Equipment*.

(5) AC 20-174, *Development of Civil Aircraft and Systems.*

(6) AC 21-46, *Technical Standard Order Program.*

(7) AC 21-50, *Installation of TSOA Articles and LODA Appliances.*

(8) AC 23.1309-1, *System Safety Analysis and Assessment for Part 23 Airplanes.*

(9) AC 25.1309-1, *System Design and Analysis.*

(10) AC 27-1309*, Equipment, Systems, and Installations* (included in AC 27-1, *Certification of Normal Category Rotorcraft*).

(11) AC 29-1309, *Equipment, Systems, and Installations* (included in AC 29-2, *Certification of Transport Category Rotorcraft*).

(12) AC 33.28-1, *Compliance Criteria for 14 CFR 33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems.*

(13) AC 33.28-2, *Guidance Material for 14 CFR 33.28, Reciprocating Engines, Electrical and Electronic Engine Control Systems*.

(14) AC 33.28-3, *Guidance Material for 14 CFR 33.28, Engine Control Systems.*

(15) AC 35.23-1, *Guidance Material for 14 CFR 35.23, Propeller Control Systems*.

(c) EASA Acceptable Means of Compliance (AMC)

(1) AMC 20-115( ), *Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178*.

(2) AMC 20-152( ), *Development Assurance for Airborne Electronic Hardware (AEH)*.

(d) Industry Documents

(1) SAE International Aerospace Recommended Practice (ARP) 4754A, *Guidelines for Development of Civil Aircraft and Systems,* dated December 21, 2010.

(2) RTCA DO-178, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 1982 (no longer in print).

(3) RTCA DO-178A, *Software Considerations in Airborne Systems and Equipment Certification*, dated March 1985 (no longer in print).

(4) RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1, 1992

(5) RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 13, 2011.

(6) RTCA DO-248C, *Supporting Information for DO-178C and DO-278A*, dated December 13, 2011.

(7) RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware,* dated April 19, 2000.

(8) RTCA DO-297, *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations*, dated November 8, 2005.

(9) RTCA DO-330, *Software Tool Qualification Considerations*, dated 13 December 2011.

(10) RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A,* dated December 13, 2011.

(11) RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(12) RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(13) EUROCAE ED-12, *Software Considerations in Airborne Systems and Equipment Certification*, dated May 1982 (no longer in print).

(14) EUROCAE ED-12A, *Software Considerations in Airborne Systems and Equipment Certification*, dated October 1985 (no longer in print).

(15) EUROCAE ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1992.

(16) EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 2012.

(17) EUROCAE ED-79A, *Guidelines for Development of Civil Aircraft and Systems,* dated December 2010.

(18) EUROCAE ED-80, *Design Assurance Guidance for Airborne Electronic Hardware,* dated April 2000.

(19)EUROCAE ED-94C, *Supporting Information for ED-12C and ED-109A*, dated January 2012.

(20)EUROCAE ED-215, *Software Tool Qualification Considerations*, dated January 2012.

(21)EUROCAE ED-216, *Formal Methods Supplement to ED-12C and ED-109A*, dated January 2012.

(22)EUROCAE ED-217, *Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A*, dated January 2012.

(23)EUROCAE ED-218, *Model-Based Development and Verification Supplement to ED-12C and ED-109A*, dated January 2012.

6. Where to find this AC.

1. You may find this AC at http://www.faa.gov/regulations_policies/advisory_circulars/.
2. If you have suggestions for improvement or changes, you may use the template in appendix A at the end of this AC.

Michael Romanowski
Director, Policy & Innovation Division
Aircraft Certification Service

Advisory Circular Feedback Form

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to 9-AWA-AVS-AIR-DMO@faa.gov, or (2) faxing it to the attention of the AIR Directives Management Officer at 202-267-3983.

Subject: _____ Date: _____

Please check all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph _____ on page _____.

☐ Recommend paragraph _____ on page _____ be changed as follows:

☐ In a future change to this AC, please cover the following subject: *(Briefly describe what you want added.)*

☐ Other comments:

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____]

4. Impact assessment (IA)

The proposed amendments are expected to contribute to updating AMC-20, to reflect the current state of the art of aircraft certification and to improve harmonisation with the equivalent FAA regulations. Overall, the amendments would provide a moderate safety benefit, would have no social or environmental impact, and would provide economic benefits by streamlining the certification process. Therefore, there is no need to develop a regulatory impact assessment (RIA).

5. Proposed actions to support implementation

N/A

6. References

6.1.1. Related regulations

N/A

6.1.2. Affected EASA decisions and FAA AC material

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

— FAA AC 20-152, RTCA, INC., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware, dated 30 June 2005

6.1.3. Other reference documents

— EASA CM No.: EASA CM-SWCEH-001 'Development Assurance of Airborne Electronic Hardware', Issue 01, Revision 01

— EASA CM No.: EASA CM-SWCEH - 002 'Software Aspects of Certification', Issue 01, Revision 01

— FAA Order 8110.49 'Software Approval Guidelines'

— FAA Order 8110.105 'Simple and Complex Electronic Hardware Approval Guidance'