AMC 20-152A

AMC 20-152A Development Assurance for Airborne Electronic Hardware (AEH)

1 PURPOSE

1.1 This AMC 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 certification or ETSO authorisation. 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.

1.2 This AMC recognises 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 19 April 2000.

1.3 This AMC describes when to apply EUROCAE ED-80/RTCA DO-254, and it 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), for the use of COTS devices and for the development of circuit board assemblies (CBAs).

The additional guidance and clarifications are provided in the form of objectives. The applicant is expected to describe the process and activities to satisfy the objectives of this AMC.

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 as being equivalent.

1.4 This AMC does not address the Single Event Effects (SEE) aspects or the assessment of the hardware susceptibility to SEE. AMC SEE aspects are usually addressed through a certification review item (CRI), and further guidance may be found in EASA CM-AS-004 Issue 01, issued 8 January 2018.

However, the Plan for Hardware Aspects of Certification may still be used to document the certification considerations for SEE.

2 APPLICABILITY

This AMC 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 aircraft, engines, and propellers. This applicability includes the developers of ETSO articles.

This AMC is applicable to AEH that contributes to hardware development assurance level (DAL) A,
DAL B, or DAL C functions.

When an objective is not applicable to a specific hardware DAL, the applicability restriction is directly indicated within the objective text with the following convention, for instance 'For DAL A hardware, …' For AEH contributing to hardware DAL C functions, only a limited set of objectives applies.

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, the use of this AMC is not required for AEH contributing to hardware DAL D functions. Appendix B provides some clarifications that may be used to ensure that the DAL D hardware performs its intended function.

3 DOCUMENT HISTORY

This document is the initial issue of AMC 20-152. This initial issue, jointly developed with FAA, is intentionally set at Revision A.

4 BACKGROUND

This AMC 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, the use of COTS devices, and the development of circuit board assemblies (CBAs). Each of these topics is organised 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';

— for the development of CBAs, the identifier is 'CBA-i'.

Objectives are also differentiated from the rest of the text by formatting in italics.

The applicant should document in the Plan for Hardware Aspects of Certification (PHAC), or any other related planning document, the process and activities that the applicant intends to perform to satisfy the objectives of this AMC. The PHAC, as well as those related planning documents, should be submitted for certification.

5 CUSTOM DEVICE DEVELOPMENT

This section provides guidance for the development assurance of programmable logic devices (PLDs), field-programmable gate arrays (FPGAs), or application-specific integrated circuits (ASICs), which are collectively 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 than for a simple device.

Section 5.1 identifies custom devices that are within the scope of this AMC.

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

Section 5.3 provides guidance on development assurance for complex custom devices.

Section 5.4 provides guidance on development assurance for simple custom devices. In particular, Section 5.4 defines which sections from 5.5 to 5.11 are applicable to the development assurance of simple electronic devices.

Sections 5.5 to 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.

5.1 Applicability to Custom Devices

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

Appendix A to ED-80/DO-254 modulates the ED-80/DO-254 life-cycle data based on the DAL allocated to the hardware function. This document recognises 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 introduces the notion of simple and complex hardware items. 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 analyses that ensure correct functional performance under all foreseeable operating conditions with no anomalous behaviour. The following criteria should be used for assessing whether a device should be classified as simple:

— simplicity of the functions and their number,

— number and the simplicity of the interfaces,

— simplicity of the data/signal processing or transfer functions, and

— independence of functions/blocks/stages.

Additional criteria specific to the digital part of the design include:

— whether the design is synchronous or asynchronous,

— number of independent clocks,

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

— 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 planning 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 as the industry standard for the development assurance of complex custom devices.

The applicant should satisfy ED-80/DO-254 and the additional objectives or clarifications described in this AMC from Sections 5.5 to 5.11.

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 with the data required for a complex custom device.

ED-80/DO-254 acknowledges that the documentation for the design process of a simple hardware device is less extensive than the one needed for a complex device. In addition, while verification and configuration management are also needed, these supporting processes also require less documentation for a simple device.

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

Objective CD-2

The applicant should propose a process in the PHAC, or any other appropriate planning document, to develop simple custom devices which encompasses the following:

1. *definition of the device functions,*
2. *complete verification of the device functions through tests and analyses,*
3. *configuration management of the device, including problem reporting and the instructions to reproduce the device,*
4. *assessment of the build conformance of the device.*

Sections 5.5.2.4 and 5.5.2.5 of this document also apply to the verification process for 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.

If the applicant intends to use COTS IP, the objectives or clarifications of those objectives described in Section 5.11 of this document are also applicable.

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. Nevertheless, the validation process is essential for all the requirements. Indeed, the upper-level requirements allocated to the custom device are often refined, decomposed or restated at the custom device level, and in terms that support the hardware design. These custom device requirements, which are traceable from/to the upper-level requirements and, therefore, not considered to be 'derived', 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 Section 6). This validation activity covers both derived and non-derived 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 broadly describes the verification process, but additional guidance is needed to ensure the verification of the custom device is complete, particularly in the area of:

— design reviews,

— reviews of test cases and procedures, and

— verification of the implementation.

5.5.2.1 Conceptual Design Review

Conceptual design is the process of generating a high-level design description from the hardware requirements (see ED-80/DO-254 Section 5.2). The conceptual design review is typically used to ensure that the outcome of the conceptual design activities (see ED-80/DO-254 Section 5.2.2) is consistent with the requirements, and identifies constraints for the interfacing components (hardware or software) and architectural constraints for the detailed design activities of the custom device.

Since this conceptual design review is already addressed in ED-80/DO-254 Section 5.2.2 through the note, no separate objective is needed.

5.5.2.2 Detailed Design Review

Detailed design is the process of generating, from the conceptual design and the requirements, a hardware description language (HDL) or analogue representation of the design, constraints for the implementation (e.g. timing constraints, pinout, I/O characteristics), and the 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 with respect to the design standards, and review the traceability between the detailed design and the custom device requirements, in order to demonstrate that the detailed design covers the custom device requirements, is consistent with the conceptual design, and is compliant with the hardware design standards.

For hardware DAL C, the applicant should demonstrate that the detailed design satisfies the hardware design standards.

5.5.2.3 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 execution of the tool to generate its output was performed correctly.

Objective CD-5

When tools are used to convert the detailed design data into the physical implementation, the applicant should review the design tool reports (e.g. synthesis and place and route reports) to ensure that the tool executed properly when generating the output.

5.5.2.4 Review of Verification 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-6

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 cases and procedures.

5.5.2.5 Verification of the Timing Performance of the Implementation

ED-80/DO-254 Section 6.2 addresses the verification of the implementation. The implementation results from 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 the digital part of the device) and place and route.

While it is recommended to test the implementation in its intended operational environment (i.e. by a 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, timing, 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 the activities in ED-80/DO-254 Section 5.1.2 Item 4.g introduces the need for the requirements to address signal timing characteristics under 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 the operation of the device.

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

Objective CD-7

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 by the manufacturer of the semiconductor device.

Note: Static timing analysis (STA) with the necessary timing constraints and conditions is one of the possible means of compliance with this objective for the digital parts 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. The robustness of the design is defined as the expected behaviour 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-8

For DAL A or DAL B hardware, the abnormal and boundary conditions and the associated expected behaviour 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 which aspects of the logic structure are exercised and which are not.

When performed during requirements-based verification (per ED-80/DO-254 Section 6.2), HDL code coverage is recognised 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 of whether the HDL code elements are fully covered by requirements-based simulations. As such, it does not represent an

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

Objective CD-9

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 or element should be analysed 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 uses the flow chart and its related text as a basis for providing further clarification, as follows:

ED-80/DO-254 — 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.

ED-80/DO-254 — 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 purpose or activity within the hardware development process the tool satisfies. While assessing the tool limitations, evidence of formal assessment of the tool problem reports is not required if the tool output has been completely and independently assessed.

ED-80/DO-254 — Figure 11-1 Item 3 — Is the Tool Output Independently Assessed?

The purpose of assessing the tool output is to completely cover, with an independent means, the potential errors that the tool could introduce into the design or fail to detect during verification.

Objective CD-10

When the applicant intends to independently assess a tool output, the applicant should propose an independent assessment that verifies the tool output is correct. The independent assessment should justify that there is 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.

ED-80/DO-254 — Figure 11-1 Item 4 — Is the Tool a Level A, B or C Design Tool or a Level A or B Verification 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'.

The last statement is misleading regarding the intent of code coverage tools used for elemental analysis. As stated in Section 5.7 of this document, 'when a code coverage tool is used for elemental analysis, it does not represent an assessment of the completeness of the requirements-based testing activities or the effectiveness of the requirement coverage'.

It is therefore necessary to provide some further clarifications.

— This document recognises the Figure 11-1 Item 4 exclusion of tool assessment/qualification activities for code coverage tools only when they are used to assess whether the code has been exercised by requirements-based testing/simulations (elemental analysis).

— If test cases or procedures are automatically generated by a tool and this tool uses coverage to determine the completion of the requirements verification, then the tool should be considered to be a verification tool to answer the question raised in Figure 11-1 Item 4.

ED-80/DO-254 — 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 to mean that the applicant will provide sufficient data and justification to substantiate the relevance and credibility of the tool history.

Objective CD-11

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

ED-80/DO-254 — 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, the tool history should not be used as a stand-alone means of tool assessment and qualification. A 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, a relevant tool history is considered to be complementary data, providing more assurance for a tool.

In addition to what is already referenced in ED-80/DO-254 Figure 11-1 Item 9 for tool qualification guidance, ED-12C/DO-178C and ED-215/DO-330 may also be used.

5.9 Clarifications to ED-80/DO-254 regarding Previously Developed Hardware (PDH)

Previously developed hardware (PDH) is defined as custom-developed hardware that has been installed in an airborne system or equipment either approved through EASA type certification (TC/STC) or authorized through ETSOA. The section providing clarification on the use of PDH also covers PDH that was 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-12

When an applicant 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 analyses 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 or for obsolescence management;*
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 should 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 10.1.6 ‘Hardware Process Assurance Plan’ in Table A-1 should also indicate HC2 for Level C to be consistent with row 10.8.

— The row corresponding to 10.2.2 ‘Hardware Design Standard’ in Table A-1 should also indicate HC2 for Level C. HDL Coding Standards are part of the Hardware Design Standards.

— The row corresponding to 10.3.2.2 ‘Detailed Design Data’ in Table A-1 should indicate HC1 for Levels A, B and C.

— The row corresponding to 10.4.2 ‘Hardware Review and Analysis Procedures’ in Table A-1 should also indicate HC2 for Level C to be consistent with row 10.4.3.

— The Top-Level Drawing referenced in ED-80/DO-254 Appendix A corresponds to a Hardware Configuration Index (HCI) document. The HCI document 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 the hardware life cycle environment or refers to a Hardware Environment Configuration Index (HECI) document.

5.11 Use of COTS IP in Custom Device Development

This section addresses COTS IP that is instantiated within FPGAs/PLDs/ASICs during the development of the custom device.

This section addresses COTS IP and its integration within custom devices and describes objectives to support the demonstration of compliance with the applicable airworthiness regulations for the hardware aspects of airborne systems and equipment certification.

Section 5.11.2, on 'Applicability to COTS IP', 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 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 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.

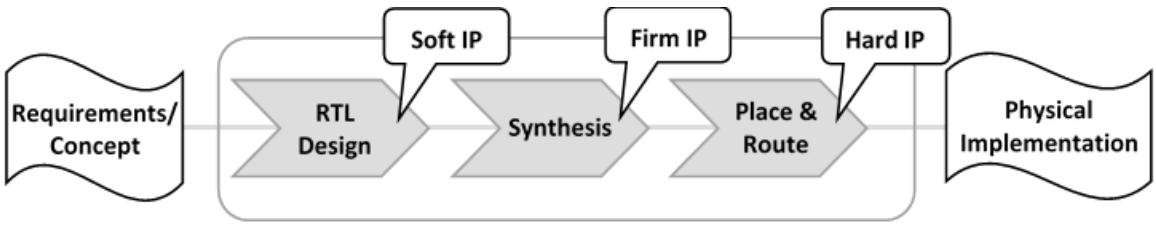

Figure 1 — Position of COTS IP within a 'simplified' design representation flow

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 life-cycle 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 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 COTS IP may lead to a failure mode. Risk factors for these types of errors include:

— Unknown level of rigour 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 to COTS IP

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 Glossary of Appendix A. This scope encompasses digital, analogue, and mixed-signal COTS IP.

Note: Analogue 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 hardware DAL A, B or C functions.

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 aspects provide a basis to define the development assurance objectives for the use of COTS IP:

— Selection of the COTS IP,

— Assessment of the IP provider and the IP data,

— Planning activities, including the verification strategy,

— Definition of the 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. The selection criteria below are intended to address the essential characteristics that are considered a minimum for the use of IP 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;*
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 description 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, and behaviour, and enable the integration and verification of the COTS IP (e.g. datasheets, application notes, user guide, knowledge of errata, etc.);*

4. *Information exists for the IP user to be able 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.*

5.11.3.2 Assessment of the COTS IP Provider and 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 the 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 by 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 functions selected for selectable functions);*

4. *The known errors and limitations are available to the IP user, and there is a process to provide updated information 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.*

The assessment should be documented. The results of the assessment should be submitted together with the planning documents.

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

5.11.3.3.1 Complementary Development Assurance

Objective IP-3

When the IP-2 Objective criteria items 1, 2, 4 or 5 cannot be completely met using the IP provider's data, the applicant should define an appropriate development assurance activity to mitigate the criteria that were not met and address the associated risk of development errors. The development assurance activity should be based on the ED-80/DO-254 objectives.

Note: The results of the assessment of Objective IP-2 Item 3 are considered in Section 5.11.3.3.2.

5.11.3.3.2 The Verification Strategy for COTS IP Functions

In addition to the verification of the custom device functions supported by the COTS IP, there is a need to ensure that the 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 for 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, addressing the risk identified from the IP-2 Item 3 objective;*
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 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.

5.11.3.3.3 COTS IP and Planning Aspects

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

Objective IP-5

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 development process of the custom device;*
5. *tool assessment and qualification aspects when the applicant uses a tool to perform design and/or verification steps for the COTS IP.*

5.11.3.4 Requirements for COTS IP Function and Validation

Custom device requirements 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 functions 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 the granularity of the AEH custom device requirements may need to be refined to specifically address the COTS IP functions and the implementation of the COTS IP.

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

Objective IP-6

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 aspects associated with the integration 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, in accordance with the data from the COTS IP provider.*

When the applicant chooses a verification strategy (see Section 5.11.3.3.2) that solely relies on requirements-based testing, the 'extent commensurate with the verification strategy' corresponds to a complete requirement capture of the COTS IP following ED-80/DO-254.

Regarding the 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 a related planning document.

For the requirements-based verification part, the applicant should satisfy ED-80/DO-254 Section 6.2 for the verification of the 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 hardware DAL A or B custom device, ED-80/DO-254 Appendix B is applicable.

Code coverage analysis that is recognised 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-7

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 function 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 the 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 which 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 to COTS devices' 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 semiconductor product that is fully encapsulated in a package. This term does not apply to circuit board assemblies (CBAs).

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 semiconductor industry qualification based on their intended market (consumer, automotive, telecom, etc.). 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 is 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 of a COTS manufacturer's development process is commensurate with the aviation 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 for the user 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 to COTS Devices

Section 6 is applicable to digital, hybrid, and mixed-signal COTS devices that contribute to hardware DAL A, B or C functions. For COTS devices contributing to hardware DAL C functions, a limited set of the 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 the 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, considering all functions of the device, including any functions intended to be unused:

A COTS device is complex when the device:

1. has multiple functional elements that can interact with each other; and
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 fabrics 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 identify all potential failures.

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 (see Note 1), including the classification rationale, in the PHAC or any related hardware planning document.

Note 1: The applicant is not expected to assess the complete bill of material to satisfy 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 at the boundary (meeting a part of the high-level criteria) and are classified as simple.

Some examples of classification are provided in the GM Appendix for illustration.

6.4 Development Assurance for Use of Complex COTS

ED-80/DO-254 Section 11.2.1 identifies some electronic component management process (ECMP) 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 (ECMP)

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 (ECMP) exists to address the selection, qualification, and configuration management of COTS devices. The ECMP 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 ECMP, for devices contributing to hardware DAL A or B functions, 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 industry standards describing the principles of electronic component management may be used to support the development of the ECMP. See Appendix B.

6.4.1.1 Using a Device outside Ranges of Values Specified in its Datasheet

The device reliability is established by the device manufacturer through the device qualification process (see definition of 'qualification of a device' in the glossary). ED-80/DO-254 Section 11.2.1 Item 6 mentions that a device is selected based on 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 limits of the device manufacturer's specification (such as the 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.

If 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 to be 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 is commensurate with the usage of the COTS device.

Note: The PHAC (or any other related planning document) should document the existence of the microcode and refer to the process (hardware, software, system) where it is addressed.

6.4.2 COTS Device Malfunctions

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).

Objective COTS-6

The applicant should identify the failure modes of the used functions of the device and the possible associated common modes, and feed both of these back to the system safety assessment process.

6.4.3 Usage of COTS Devices

This section focuses on the usage of complex COTS devices, while Section 7 covers the overall circuit board assembly development process. This Section 6.4.3 refers to the term 'intended function of the hardware', which is considered to be defined through the CBA development process.

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:

— Used functions (e.g. identification of each function, configuration characteristics, modes of operation),

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

— Means to control any inadvertent activation of the unused functions, or inadvertent deactivation of the used functions,

— Means to manage device resets,

— Power-on configuration,

— Clocking configuration (e.g. identification of the different clock domains), and

— 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 hardware DAL A or B function, the applicant should show that unused functions of the COTS device do not compromise the integrity and availability of the COTS device's used functions.

Note 1: For unused functions of the COTS device, it is recommended that an effective deactivation means is used and verified, when available.

Note 2: Verification should be performed at an appropriate level (hardware, software, equipment).

ED-80/DO-254 Section 10.3.2.2.4 introduces hardware/software (HW/SW) interface data, which 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 of the COTS device, causing it to no longer fulfil the hardware 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 Development Assurance of Circuit Board Assemblies (CBAs)

This section provides guidance for the development assurance of CBAs (a board or a collection of boards).

7.1 Applicability

Section 7 is applicable to CBAs that contribute to hardware DAL A, B or C functions.

7.2 Development Assurance of Circuit Board Assemblies (CBAs)

While it is already a common practice for applicants to have an internal process to address the development of CBAs, it is necessary to clarify the expectations for development assurance, including the flow-down of the equipment/system requirements to the hardware. For consolidation of the development and/or the use of complex devices, it is essential to ensure consistency in the overall development assurance approach for the hardware domain. Moreover, definition of the CBA function is also necessary to enable the allocation of requirements and their flow-down to the complex devices.

Objective CBA-1

The applicant should have a process to address the development of CBAs that contain complex custom devices or complex COTS devices, in order to ensure that the CBA performs its intended function. The process should include requirements capture, validation, verification, and configuration management activities, and ensure an appropriate flow-down of requirements. See Appendix B for additional information.

Note: The applicant's process to address the development of the CBA may be defined together with the equipment process, when relevant.

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 20-3B, Certification of Engines Equipped with Electronic Engine Control Systems*

(6) CS-P, *Certification Specifications for Propellers, and AMC 20-1A, 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 20-2B, *Certification of Essential APU Equipped with Electronic Controls*

(b) FAA Advisory Circulars (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 23.1309-1, *System Safety Analysis and Assessment for Part 23 Airplanes*

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

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

(6) 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
19 April 2000

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

(5) SAE International Aerospace Recommended Practice (ARP) 4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,* dated December 1996

9 AVAILABILITY OF DOCUMENTS

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

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

(c) 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

(Email: eurocae@eurocae.net, website: www.eurocae.net)

(d) 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)

Appendix A — Glossary

Abnormal conditions: conditions that are inconsistent with specified normal operating conditions.

Airborne electronic hardware: an electronic 'hardware item' (see ED-80/DO-254 for definition of 'hardware Item'), intended to be installed in airborne equipment/systems.

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 restricted to airborne systems), whose design and configuration is controlled by the supplier or an industry specification. A COTS device can encompass digital, analogue, or mixed-signal technology. COTS electronic components are generally developed by the semiconductor industry for the commercial market, not particular to the airborne domain. These devices have widespread commercial use and are developed according to the semiconductor manufacturer's proprietary development processes.

COTS device usage: definition of the used and unused functions that are implemented in the device. This is further defined as an exhaustive list of conditions/constraints (such as configuration settings, usage rules, protocol, timing constraints, input–output (I–O) interface, and addressing schemes) associated with the performance characteristics of the used COTS functions. Respecting the defined usage of the COTS 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 an 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 an 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, 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 an unintended function or misbehaviour is low. The risk of anomalous behaviour decreases as a device is widely used and device errata are documented and communicated to the users 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 of the COTS device, causing it to no longer fulfil its intended 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 dies and passive components on a substrate.

IP libraries: 'IP libraries' used in the COTS IP definition refers to all submodules, sub-blocks, or other design subfunctions 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 microprocessor input and output process operations.

Mixed-signal device: a device that combines digital and analogue technologies.

Note: a note in this document is supporting information used to provide explanatory material, emphasise 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.

Previously developed hardware (PDH): a custom-developed hardware device that has been installed in an airborne system or equipment either approved through EASA type certification (TC/STC) or authorised through ETSOA.

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.

Appendix B — Guidance Material to AMC 20-152A

B.1 Purpose

This document provides additional clarifications, explanatory text, or illustrations that could be helpful when addressing some of the objectives of AMC 20-152A. This document is not intended to cover each section of AMC 20-152A.

This AMC is 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-certified aircraft, engines, and propellers, or to be used in European technical standard order (ETSO) articles.

B.2 Guidance Material

B.2.1 Custom Devices

This guidance material provides complementary information to AMC 20-152A, Custom Device Development, Section 5. Applicants may use this guidance material when developing custom devices.

B.2.1.1 Clarifications to ED-80/DO-254 Appendix A for the Top-Level Drawing

B.2.1.1.1 Hardware Environment Configuration Index (HECI)

The purpose of the HECI is to aid the reproduction of the hardware life cycle environment for hardware regeneration, reverification, 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 design tools;
3. the test environment and validation/verification tools; and
4. qualified tools and qualification data.

B.2.1.1.2 Hardware Configuration Index (HCI)

The purpose of the HCI is to identify the configuration of the hardware item(s). The HCI should include:

1. ASIC/PLD part number;
2. Media used to produce the physical component (e.g. the PLD/FPGA programming file or ASIC netlist/GDSII);
3. Identification of each source code component, including individual source files, constraints, scripts and versions;
4. Identification of any previously developed hardware;
5. Identification of any COTS Intellectual Property;

6. Identification of the test bench source code and scripts, including the versions;
7. Hardware life-cycle data items and their versions as defined in ED-80/DO-254 Table A-1;
8. Archive and release media (e.g. for the source data);
9. Instructions for building a PLD programming file or ASIC netlist;
10. Instructions for loading the bitstream file into the target PLD or FPGA hardware;
11. Reference to the HECI; and
12. Data integrity checks for the PLD programming file (n/a for ASICs).

B.2.1.2 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. AMC 20-152A clarifies that the 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 AMC 20-152A.

Here below is an illustration of the types of criteria commonly used by industry, and it is not an exhaustive list. The applicant is responsible for determining the criteria that are applicable to its own development process:

— Simplicity of the functions, simplicity of data/signal processing or transfer functions;

— Number of functions, number of interfaces;

— Independence of functions/blocks/stages.

Specific to digital designs:

— Synchronous or asynchronous design;

— Number of independent clocks, number of state machines and their independence, number of states, and state transitions per state machine.

B.2.1.3 Additional Information for Objective CD-2 on Development Assurance of Simple Custom Devices

A simple device is defined and designed to implement specific hardware functions. Due to the simplicity of the device, 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 intended functions within the operating conditions without any anomalies.

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

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

B.2.1.4 Additional Information for Objective CD-7 on Verification of Implementation Timing Performance

Objective CD-7 specifies that applicants 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.

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

The following examples identify constraints that may impact the timing behaviour 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 limits. Two different temperatures need to be managed:

  — junction temperatures: the static timing analysis (STA) tools and technology limitations are based on the junction temperatures; and

  — external temperature: application constraints are related to the external temperature of the device.

  Conversions between these two constraints have to be carefully managed when analysis is performed.

— For voltage ranges, there are also two characteristics to take into account: constraints from the environment (the 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 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 the 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 (STA) can be used to conduct such an analysis. The source of each STA constraint (delays and frequency constraints) has to be identified. In addition, the timing parameters to be considered for launching an STA include:

— the input frequency: an external constraint with different characteristics (e.g. accuracy, duty cycle); and

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

STA provides timing results that highlight setup and hold violations, but does not analyse delays longer than a clock period (multi-cycle paths, pulse width generation, etc.). Additional verification may be needed to address those timing aspects not covered by STA.

B.2.1.5 Additional Information for Objective CD-9 on Recognition of HDL Code Coverage Method

For Objective CD-9, 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 the 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 the possible branch directions have been exercised;
3. All the conditions expressed in a statement or for taking a branch have been exercised;
4. Every state of a finite state machine (FSM) and every state transition has been exercised.

B.2.1.6 Additional Information for Objective CD-10 on Tool Assessment and Qualification

As described in Objective CD-10, 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 tools, layout tools, programming file generation tools;

— Verification tools: simulation tools, STA tools.

Confidence in design tools can be gained through the fact that the outputs from the design tools are independently verified by post-layout 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. For instance, physical tests, either by rerunning part of the simulation test sequences or retesting the requirements, allow 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 results for the simulation and the physical test of the same requirement are equivalent.

Another example of independent assessment can be to rerun simulation tests on a dissimilar simulation tool and compare the results obtained from each simulation tool to ensure their equivalence.

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.

B.2.1.7 Additional Information for Objective CD-11 on Tool Assessment and Qualification

When the applicant intends to present tool history to claim credit for tool assessment, Objective CD-11 expects the applicant to provide sufficient data and justification to substantiate the relevance and credibility of the tool history.

In general, the tool history is applicable to a specific version of the tool, because it is difficult to determine whether different versions or releases of the same tool constitute the same tool.

If using a different version of the tool compared with the one that has a relevant tool history, the applicant would then be expected to analyse the differences between the tool versions to ensure that the tool history is relevant to the version of the tool used.

A list of characteristics/criteria that can be part of the relevant 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 experience of the custom devices 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 concerns;

— 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.

If the tool has not 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.

B.2.1.8 Use of COTS IP in Custom Device Development

This guidance material provides complementary information to AMC 20-152A, Custom Device Development, Section 5.11. Applicants may use this guidance material when using commercial off-the-shelf intellectual property (COTS IP) in a custom device.

B.2.1.8.1 Clarification of Objective IP-2 on Assessment of the COTS IP Provider and COTS IP Data

B.2.1.8.1.1 Assessment of 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 IP. Some additional development assurance needs to be defined to address the risk of insufficient or unrelated service experience.

B.2.1.8.1.2 Assessment of the COTS IP Provider and COTS IP data

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

The following are two typical cases of insufficient coverage when assessing COTS IP with the Objective IP-2 criteria:

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

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

An example of a COTS IP assessment with the Objective IP-2 criteria that helps to define the appropriate development assurance activity on the COTS IP is as follows:

— A communication Soft IP is proposed by an experienced provider. The COTS IP has existed for more than 2 years and has been used in many applications by many customers. The version of the IP 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 the associated implementation results are usable for various sets of technology targets (which 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.

B.2.1.8.2 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 life-cycle 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 the COTS IP provider's test cases, or by proven test vectors for a COTS IP performing a standardised interface function.

The verification strategy describes the verification data delivered with the COTS IP, as well as the verification data to be developed by the applicant. The verification activities proposed by the applicant should address any missing items from the data delivered with the COTS IP and ensure the proper implementation and integration of the IP within the custom device.

B.2.1.8.3 Clarification of Objective IP-6 on the 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 the 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 performed using all the documentation and design data available. The requirement capture process will encompass all the IP functions, including the means to deactivate any unused functions.

The following aspects could be captured as derived requirements:

1. Error or failure mode detection and correction behaviour performed by the IP;
2. Design constraints that control the interaction of the IP with the rest of the design of the custom device;
3. Configuration parameters or settings used to alter or limit the functions provided by the IP;
4. Controlling or deactivating unused features or characteristics of the design;
5. Design constraints to properly perform the 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 of the IP during robustness conditions, boundary conditions, failure conditions, and abnormal inputs and conditions;

6. The 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 should begin 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 the deactivation means for the unused ones (for non-interference with the used functions).

B.2.2 COTS DEVICES

These practices provide complementary information to AMC 20-152A, COTS Devices, Section 6. Applicants may use this guidance material when using COTS devices.

B.2.2.1 Additional Information for COTS Section 6.3 and Objective COTS-1 on COTS Complexity Assessment

The applicant should 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 devices 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, and the list should be made available to the regulatory authority once the parts selection process is completed.

As stated in AMC 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, and on which the complexity assessment is performed by applying the generic criteria identified in Section 6.3. These examples are provided for illustration only. Other combinations of characteristics will occur in actual projects.

EXAMPLES OF COTS DEVICES AND THEIR ASSOCIATED CHARACTERISTICS	COMPLEXITY ASSESSMENT
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; — A significant number of functional modes where each interface has several selectable channels/modes of operation; — 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: — A single advanced, reduced instruction machine core processor; — Inter-processor communication that uses a simple mailbox protocol; — A programmable real-time unit (PRU) subsystem that contains 2 RISC processors and complex access to many peripherals; — A PRU that is highly programmable with 200 registers, and 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 the single core processor but not with each other: PCI interface, SPI, I2C, JTAG, 1 core processor; — A significant number of functional modes where the interface has few modes of operation; — Limited configurable functions allowing one major data path using a limited number of discrete signals on SPI or I2C. There is limited and fixed resource sharing in the device.	Simple
An example of a 32-bit reduced instruction set computing (RISC) microcontroller with: — Internal buses that are all simple master–slave protocol,	Simple

— A processor that has dedicated resources, — No interconnect fabric, no multiple masters, — A single point of access to all the peripherals, — Independent time processor units (TPUs) 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, — An interconnect between DSP and peripherals that 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 analogue-to-digital converter with: — An 8-channel/16-channel, software selectable, 24-bit ADC.	Simple
An example of a digital SPI temperature sensor with: — An analogue temperature sensor, — Conversion to digital, — An SPI output.	Simple
An example of an FPGA component with some Hard IP embedded in silicon with: — An FPGA fabric (outside the COTS scope), — Embedded RAM/ROM memories, — Embedded FIFOS, — A PCI port, — A/D and D/A converters, — 16×16 configurable multiplier blocks.	Simple
An example of an FPGA component with Hard IP embedded in silicon with: — An FPGA fabric (outside the COTS scope),	Complex

— Embedded RAM/ROM memories, — Embedded FIFOS, — A PCIe port, — A Processor Core, — A coherency fabric/interconnect, — A/D and D/A converters.	

B.2.2.2 Additional Information for COTS Section 6.4.1 on the Electronic Component Management Process (ECMP)

B.2.2.2.1 Clarification of Objective COTS-2 on the Electronic Component Management Process (ECMP)

IEC 62239 and SAE EIA-STD-4899 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 electronic component management process (ECMP) describes a standard process that is reused and reapplied from certification project to certification project. This approach is understood to ease the certification process.

Regarding the assessment of maturity:

When selecting a device, the applicant assesses the maturity of the device and analyses 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:

— The time of the device in service,

— Widespread use in service: an indication of widespread use could be given (multiple applications, a 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,

— The maturity of the intellectual property embedded into the device,

— A decreasing rate of new errata being raised.

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

B.2.2.2.2 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 (its recommended operating limits), as 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 focuses on the device itself and takes into account the different variations in technology (variation in performance over different batches/over different dies). This uprating process evaluates the performance of the device itself, so it is different from ED-14/DO-160 environmental qualification of equipment.

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 (the 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 values, 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.

B.2.2.3 Additional Information for Section 6.4.2 'COTS Device Malfunctions'

The applicant needs access to errata information on the device during the entire life cycle of the product (before and after certification). Refer to AMC, Section 6.4.1.

In general, this assessment typically includes the 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, and

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

The assessment of the errata of a 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.

B.2.2.4 Additional Information for Objective COTS-6 on COTS Device Malfunctions

It is understood that the task linked with this objective is performed in close coordination with the 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 the 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 to be a best practice.

B.2.3 Clarification of Objective CBA-1 on Circuit Board Assembly Development

In the aviation domain, the applicant typically has internal processes to develop circuit board assemblies. There is a clear benefit for the applicant (or developer of the airborne system and equipment) in having a process to address the development of a circuit board assembly (a board or a collection of boards) that encompasses the requirements capture, validation, verification, and configuration management activities, and ensures an appropriate requirements flow-down.

It is a common practice for the applicant's internal process to already encompass the above-mentioned activities that satisfy Objective CBA-1. Industry standards ED-80/DO-254 or ED-79A/ARP4754A provide guidance that may be used by applicants seeking further information.

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

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

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

B.2.4 Development of Airborne Electronic Hardware Contributing to Hardware DAL D Functions

For airborne electronic hardware contributing to hardware DAL D functions, the acceptable means of compliance include ED-80/DO-254 or existing Level D hardware development assurance practices that demonstrate that the requirements allocated to the DAL D airborne electronic hardware have been satisfied. Additionally, system-level development assurance practices such as ED-79A/ARP4754A 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.

Appendix C — Glossary of Guidance Material

This glossary complements the terms defined in AMC 20-152A with terms used only in this GM.

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

[Amdt 20/19]