Certification Memorandum

Development Assurance of Airborne Electronic Hardware

EASA CM No.: CM–SWCEH-001 Issue 01 Revision 02 issued 08 January 2018

Regulatory requirement(s): **CS 25.1301 and 1309 for Large Aeroplanes, CS 23.1301 and 23.1309 for Small Aeroplanes, CS27.1301 and 27.1309 for Small Rotorcraft, CS29.1301 and 29.1309 for Large Rotorcraft, CS E-50 (d, f) for engines, CS-P, CS-APU and CS-ETSO**

EASA Certification Memoranda clarify the European Aviation Safety Agency's general course of action on specific certification items. They are intended to provide guidance on a particular subject and, as non-binding material, may provide complementary information and guidance for compliance demonstration with current standards. Certification Memoranda are provided for information purposes only and must not be misconstrued as formally adopted Acceptable Means of Compliance (AMC) or as Guidance Material (GM). Certification Memoranda are not intended to introduce new certification requirements or to modify existing certification requirements and do not constitute any legal obligation.

EASA Certification Memoranda are living documents into which either additional criteria or additional issues can be incorporated as soon as a need is identified by EASA.

An agency of the European Union

Log of issues

Issue/Revision	Issue date	Change description
Issue 01 Revision 00	11.08.2011	First issue.
Issue 01 Revision 01	09.03.2012	First issue, first revision. Editorial corrections in sections 1, 2, 3, 4, 7, 8, 9, 12, 13.
Issue 01 Revision 02	08.01.2018	First issue, second revision. Editorial change in section 6 to reflect that the guidance material provided in section 6 is repealed and superseded by EASA CM-AS-004 Issue 01 Revision 00 on Single Event Effects (SEE) Caused by Atmospheric Radiation, dated 08.01.2018 To allow readers to see the detailed changes, the following format has been used: 1. text not affected by the revision remains the same: unchanged 2. deleted text is shown with a strike through: ~~deleted~~ 3. new text is highlighted with grey shading: new.

Table of Contents

An agency of the European Union

1. Introduction

1.1. Purpose and scope

The purpose of this Certification Memorandum is to provide specific guidance material on certification aspects associated with the use of electronic hardware in airborne systems (referred to as airborne electronic hardware). Airborne electronic hardware includes line replaceable units, circuit board assemblies, application specific integrated circuits, programmable logic devices, microprocessors, microcontrollers, integrated circuits, etc.

1.2. References

It is intended that the following reference materials be used in conjunction with this Certification Memorandum:

Reference	Title	Code	Issue	Date
ED-80 / DO-254	Design Assurance Guidance for Airborne Electronic Hardware. Note: Where, throughout this Certification Memorandum, reference is made to document ED-80, this may be interpreted as a reference to either EUROCAE document ED-80 or RTCA Inc. document DO-254 at the same revision level, the two documents being technically equivalent.	EUROCAE ED-80 RTCA DO-254	-	April 2000
ED-12B / DO-178B	Software Considerations in Airborne Systems and Equipment Certification.	EUROCAE ED-12 RTCA DO-178	B	December 1992
ED-94B / DO-248B	Final report for clarification of ED-12B / DO-178B "Software Considerations in Airborne Systems and Equipment Certification".	EUROCAE ED-94 RTCA DO-248	B	October 2001
ED-79 / ARP4754	Certification Considerations for Highly Integrated or Complex Systems.	EUROCAE ED-79 SAE ARP4754	-	November 1996
ED-79A / ARP4754A	Guidelines for Development of Civil Aircraft and Systems.	EUROCAE ED-79A SAE ARP4754A	A	December 2010
ED-135 / ARP4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.	EUROCAE ED-135 SAE ARP4761	-	1996-12

Wherever this Certification Memorandum refers to a section of ED-79 / ARP4754 or ED-79A / ARP4754A, EASA requests any applicants that have neither ED-79 / ARP4754 nor ED-79A / ARP4754A as part of their certification basis to describe and provide evidence for the parts of their processes that are equivalent to the ED-79 / ARP4754 or ED-79A / ARP4754A processes to which this document refers.

1.3. Abbreviations

AEH	Airborne Electronic Hardware
A/D	Analog/Digital
ASIC	Application Specific Integrated Circuit
CAST	Certification Authorities Software Team
CBA	Circuit Board Assembly
CEH	Complex Electronic Hardware
CGP	COTS Graphical Processor
CM	Certification Memorandum
COTS	Commercial Off-The-Shelf
CRI	Certification Review Item
CS	Certification Specification
D/A	Digital/Analog
DAL	Development Assurance Level Note: ED-80/DO-254 defines DAL as Design Assurance Level.
DOA	Design Organisation Approval
EMI	Electro Magnetic Interference
ETSO	European Technical Standard Order
FAA	Federal Aviation Administration
FDAL	Functional Development Assurance Level
FHA	Functional Hazard Analysis
FPGA	Field Programmable Gate Array
GAL	General Array Logic
GM	Guidance Material
HAS	Hardware Accomplishment Summary
HCI	Hardware Configuration Index

HCMP	Hardware Configuration Management Plan
HDL	Hardware Description Language
HDP	Hardware Development Plan
HECI	Hardware Life-cycle Environment Configuration Index
HMI	Hazardously Misleading Information
HPA(P)	Hardware Process Assurance (Plan)
HVaP	Hardware Validation Plan
HVeP	Hardware Verification Plan
IC	Integrated Circuit
IDAL	Item Development Assurance Level
IP	Intellectual Property
LOI	Level Of Involvement
LRU	Line Replaceable Unit
OpenGL	Open Graphics Library
OPR	Open Problem Report
P/N	Part Number
PA	Process Assurance
PAL	Programmable Array Logic
PCM	Project Certification Manager
PHAC	Plan for Hardware Aspects Of Certification
PLD	Programmable Logic Device
PSE	Product Service Experience
RTC	Restricted Type Certificate
SEE	Single Event Effect
SEH	Simple Electronic Hardware
SEU	Single Event Upset
SoC	System on Chip

STC   Supplemental Type Certificate

SW   Software

TAS   Tool Accomplishment Summary

TC   Type Certificate

TQP   Tool Qualification Plan

TSO   Technical Standard Order

UART   Universal Asynchronous Receiver Transmitter

WCET   Worst Case Execution Time

1.4. Definitions

Some terms of this CM are defined below; however, in order to improve the readability of this CM, some sections contain specific definitions (e.g. Section 4). In addition, the reader may need the definitions contained in Eurocae standards (e.g. ED-80/DO-254) as they are not repeated below.

Application Specific Integrated Circuit (ASIC)	Integrated Circuits which are developed to implement a function, including, but not limited to: gate arrays, standard cells, and full custom devices encompassing linear, digital, and mixed mode technologies. ASICs are mask-programmable components.
Complex Electronic Hardware (CEH)	All devices that are not simple are considered to be complex. See the definition of Simple Hardware.
COTS IC	Any COTS digital or hybrid electronic device which does not execute software in a specific core. COTS ICs may be bus controllers, flip-flops, multiplexers, converters, memories… The hardware functions implemented within these components may be simple or complex. (See also the definition of SEH below).
COTS IP (Commercial Off-The-Self Intellectual Property)	Any commercially available electronic function designed to be reused as a portion of a device which may be classified in the following three categories Soft IP, Firm IP or Hard IP.

See also:

- FAA, February 2009, Microprocessor evaluations for safety-critical, real-time applications: Authority for expenditure No. 43 Phase 3 Report, DOT/FAA/AR-08/55, U.S. Department of Transportation, Federal Aviation Administration:

  o *Soft IP cores contain the maximum data of detail and are generally specified in register transfer level description in languages such as Verilog or VHDL. Thus, soft IP cores allow detailed analysis and optimization of the system being integrated.*

  o *Firm IP cores are next in the decreasing level of detail and specified in technology-independent netlist level format (*). This allows the IP provider to hide the critical IP details and yet allow the system integrator to perform some limited amount of analysis and*

optimization during placement, routing, and technology-dependent mapping of the IP block.

Hard IP cores are the lowest in level of detail and specified in technology-dependent physical layout format using industry standard languages such as stream, polygon, or GDSII format. The hard IP cores are like black boxes and cannot be properly analysed and/or co-optimized. Hard IP cores come with a detailed specification of integration requirement in terms of clock, testing, power consumption, and host of other parameters.

COTS Graphical Processor	Any COTS microcontroller specifically designed for graphical applications.
COTS Microcontroller	Any IC which executes software in a specific core area (Central Processing Unit) <u>and</u> implements peripheral hardware elements such as, for example, input/output (I/O), bus controllers… Such a peripheral element may be considered simple (e.g. a UART, A/D, D/A) or complex (e.g. a bus controller). (See also definition of SEH below).
Integrated Circuit	A circuit (also IC, microcircuit, microchip, silicon chip, or chip) consisting of elements inseparably associated and formed in-situ on or within a single substrate to perform an electronic circuit function. Among the most advanced integrated circuits are the microprocessors or "processing cores", digital memory chips, ASICs and bus controllers. Integrated circuits can be classified into analog, digital and hybrid signal:

- Digital integrated circuits may be AND-Gates, microprocessors, or microcontrollers and work using binary mathematics to process "one" and "zero" signals.

- Analog ICs, such as sensors, power management circuits, and operational amplifiers, work by processing continuous signals. They perform functions like amplification, active filtering, demodulation, mixing, etc.

- Hybrid ICs can combine analog and digital circuits on a single chip to create functions such as A/D converters and D/A converters.

Digital and Hybrid ICs include ASICs, COTS ICs, highly complex COTS Microcontrollers, Microprocessors, COTS Microcontrollers, COTS Graphical Processors, PLDs, CEH, SEH.

Programmable Logic Device (PLD)	A component that is purchased as an electronic component and altered to perform an application specific function. PLDs include, but are not limited to: Programmable Array Logic components (PAL), General Array Logic components, Field Programmable Gate Array components (FPGA), and Erasable Programmable Logic Devices (EPLD).
Microprocessor	A single Central Processing Unit which executes software and does not contain any additional integrated peripheral hardware element such as a UART, A/D, D/A, bus controller, Time Processing Unit, Memory Management Unit, watchdog, etc.
Simple Electronic Hardware (SEH)	A hardware device is considered simple only if a comprehensive combination of deterministic tests and analyses appropriate to the DAL/IDAL can ensure correct functional performance under all foreseeable operating conditions with no anomalous behaviour.

- *Comment 1: For the purposes of this Guideline, this definition can be applied to airborne electronic hardware devices whose simplicity has been confirmed by a documented engineering analysis of the logic and the design. This analysis should be based on criteria denoting a measure of simplicity such as, for*

example, the number of states in the state machine, and hysteresis characteristics. Comment 2: For the purposes of this Guideline, this definition can be applied to airborne electronic hardware devices whose logic is simple enough to comprehend without the aid of analytical tools.

Some examples of Simple COTS could be: UARTs, A/D converters, D/A converters, PWMs

Panel 10 — The EASA panel in charge of software and AEH aspects of certification. This panel includes at least one software and AEH expert (the coordinator) and, depending on the size of the project, may include additional software and AEH experts.

2. Background

In the Certification Specifications (CS), there are no specific requirements for the certification aspects of airborne electronic hardware. In order to address CS 25.1301 and 1309[1] , the purpose of this Certification Memorandum is to define specific guidance for certification aspects associated with the use of electronic hardware in airborne systems.

This Certification Memorandum calls attention to the European Organisation for Civil Aviation Equipment (EUROCAE) document ED-80: "Design Assurance Guidance For Airborne Electronic Hardware", April 2000. It discusses how the document may be applied to the design of electronic hardware so as to provide the end user with the necessary confidence that the delivered hardware conforms to a standard commensurate with its intended use.

There are a number of specific issues that are either not addressed by ED-80/DO-254 or are in need of some additional discussion and explanation.

This Certification Memorandum:

- Provides specific guidance on the review process and organisation of EASA.

- Gives some information on the EASA Level Of Involvement.

- Provides guidelines for Single Event Effects.

- Defines the applicability of ED-80/DO-254 in relation to Line Replaceable Units (LRUs) and Circuit Board Assemblies that may be used in airborne systems.

- Complements the applicability of ED-80/DO-254 in relation to Complex Electronic Hardware devices which may be used in airborne systems. These devices are often as complex as software controlled microprocessor-based systems, hence they need a rigorous and structured development approach.

- Provides specific guidance applicable for Simple Electronic Hardware (SEH) devices.

- Complements the applicability of ED-80/DO-254 in relation to Commercial-Off-The-Shelf (COTS) components.

- Complements the applicability of ED-80/DO-254 in relation to the use of Commercial-Off-The-Shelf (COTS) Graphical Processors (CGP) in airborne display systems.

- Provides specific guidance for the management of Open Problem reports.

- Provides guidelines to properly oversee suppliers.

---

[1] This applies for Large Aeroplanes. For other products, please refer to CS23.1301 and 23.1309 for Small Aeroplanes, CS27.1301 and 27.1309 for Small Rotorcraft, CS29.1301 and 29.1309 for Large Rotorcraft, CS E-50 (d,f) for engines, CS-P, CS-APU and CS-ETSO.

- Provides guidelines to oversee AEH change impact analyses used to classify Major or Minor changes.

- Does not apply to singly packaged components (i.e. resistors, capacitors, transistors, diodes etc.) nor to Analog ICs nor Hybrid ICs.

2.1. Comparison between the contents of this document and the content of existing FAA Orders or CAST Papers

The format of this Certification Memorandum in terms of the order of the sections is intended to harmonise this EASA guidance material with the existing FAA guidance material. Sections 3 – 4 of this Certification Memorandum correspond to chapters 2 – 3 of FAA Order 8110.105. Sections 8 of this Certification Memorandum correspond to chapters 4 – 6 of FAA Order 8110.105.

Moreover Section 10 of this Certification Memorandum corresponds to CAST Paper 29.

Applicants should note, however, that apart from some minor differences in wording and paragraph numbering, in some cases, the content of the guidance contained in this Certification Memorandum is different from the guidance contained in FAA Order 8110.105 or CAST Papers. The major differences are described below.

a) The following section of this Certification Memorandum contain some significant differences from the guidance provided by the equivalent chapters of the FAA Orders that exist at the time of publication of this document –

- Section 8.5, Simple ASICs/PLDs.

b) The sections of this Certification Memorandum whose contents neither directly correspond to the contents of the existing FAA Orders nor CAST Papers are as follows –

- Section 6, Guidelines for Single Event Effects.

- Section 7, Guidelines for Electronic Hardware Development Assurance of Equipment and Circuit Board Assemblies.

- Section 9, Guidelines for Commercial Off-The-Shelf digital Airborne Electronic Hardware components

- Section 11, Properly Overseeing Suppliers.

- Section 12, Oversight of AEH Change Impact Analysis used to classify AEH changes as major or minor.

- Section 13, Guidelines on Management of Problem Reports.

3. EASA Certification Policy

3.1. EASA Policy

The EASA policy on electronic hardware aspects of certification is to permit applicants to use ED-80/DO-254 as an acceptable means of compliance with the EASA Certification Specifications, and to provide additional guidance to applicants who use ED-80/DO-254.

3.2. Whom this Certification Memorandum affects

The guidance contained in this Certification Memorandum applies to any applicants seeking approval from EASA for electronic hardware embedded in aircraft systems or engines that is intended to comply with ED-80/DO-254. It also applies to any personnel involved in the ED-80/DO-254 activities related to the airborne electronic hardware of those applicants.

For TCs and STCs, applicants should ensure they use the appropriate version of the Certification Memorandum called up in the applicable CRI.

For an ETSO, the applicant may decide to take into account all or part of this guidance contained herein, and may substantiate the details of their compliance in specific documentation (i.e. Declaration of Design and Performance, Software Accomplishment Summary, Hardware Accomplishment Summary or equivalent). Caution should be taken as the content of Certification Memoranda may have changed by the time the equipment is installed in the Aircraft/Engine. In any case, the installed equipment should finally comply with the Aircraft/Engine Certification Basis (including certain Certification Review Items).

When this Certification Memorandum is used outside of the scope of a TC, STC or ETSO (e.g. for pre-consultancy, pre-application , etc.), this guidance is provided for information only and caution should be taken as the content of the Certification Memorandum may have changed by the time of the application.

3.3. Background

This Certification Memorandum has been prepared to take EASA requirements and procedures into account in the scope of airborne electronic hardware development. It incorporates some material that was formerly provided in separate Certification Memoranda and Certification Authority Software Team (CAST) papers.

It should be noted that the term 'Type Certificate' (TC) in this Certification Memorandum refers both to Type Certificates (TCs) and to Restricted Type Certificates (RTCs).

4. Guidelines for the hardware review process

4.1. Purpose

This Section provides guidelines for conducting hardware reviews during the hardware development life-cycle of airborne systems and equipment that are developed to meet the objectives of ED-80/DO-254 and applicable CRIs. The guidelines below are used by EASA Panel 10 experts and may be used by the applicant as indicated in section 4.3.

4.2. Definitions

For the purpose of this section, the following definitions apply:

Review is the act of inspecting or examining hardware life cycle data, hardware project progress and records, and other evidence produced with the intent of finding compliance with ED-80/DO-254 objectives. Review is an encompassing term and may consist of a combination of reading, interviewing project personnel, witnessing activities, sampling data, and participating in presentations. A review may be conducted at one's own desk (desktop review), at an applicant's facility, or at an applicant's supplier's facility (on-site review).

Sampling is selecting a representative set of hardware life cycle data for inspection or analysis to attempt to determine the compliance of all the hardware life cycle data developed up to that point in time in the project. Sampling is the primary means of assessing the compliance of the hardware processes and data. Examples of sampling may include any or all of the following:

- Inspecting the traceability from system requirements to hardware requirements to hardware design to HDL code and from hardware requirements and design to test cases and procedures to test results.

- Reviewing any analyses used to determine the system safety classification and the hardware level or any reviews or analyses used to meet any ED-80/DO-254 objective (e.g., timing analysis or code review).

- Examining the code coverage of HDL code modules.

- Examining hardware process assurance records and configuration management records.

Finding is the identification of a failure to show compliance with one or more of the objectives of ED-80/DO-254 or with applicable Certification Review Items (CRIs).

Action is the description of the activity to be performed by the applicant/supplier in order to resolve a finding or any other deficiency detected by the auditor. Actions should be closed before a mutually agreed closure date. By default, all actions should be completed and closed before approval.

Observation is the identification of a potential hardware life cycle process improvement. An observation is not an ED-80/DO-254 compliance issue and does not need to be addressed before hardware approval.

Recommendation is the description of the activity to be performed by the applicant/supplier in order to resolve an observation identified by the auditor. Implementation of recommendations is not mandatory prior to approval.

4.3. Scope

a. ED-80/DO-254 Section 9 describes the certification liaison process. This process sets up communication and understanding between the certification authority and an applicant. Section 9.2 says that the authority may review the hardware design life cycle processes and data to assess compliance with ED-80/DO-254. This section does not change the intent of ED-80/DO-254 with regard to the hardware review process but clarifies the application of ED-80/DO-254.

b. The applicant should plan and perform his/her own hardware review process (independently from the EASA LOI defined in the CM section 5); this hardware review process may be tailored taking into account similar criteria to those defined in the CM section 5.

Indeed, per Commission Regulation (EC) No 1702/2003 and its annex (Part 21), a design assurance system should be maintained for the control and supervision of the design [paragraph 21A.239(a)], and should include an independent checking function [paragraph 21A.239(b)]. Per GM No. 1 to 21A.239(a), 'design assurance' means all those planned and systematic actions necessary to provide adequate confidence that the organisation has the capability to design products or parts.

As part of its investigations (per 21A.257), EASA may request the reports of the reviews performed by the applicant.

In case of a validation project, where the applicant is not a DOA holder (or AP to DOA holder), it is expected that the applicant also performs an equivalent set of reviews per the requirements of his/her national equivalent to Part 21.

Note: the reviews described in this section are basically separate from the hardware process assurance (as described in ED-80/DO-254 section 8). Nevertheless the hardware process assurance team may be involved or take an active part to the establishment of the hardware review reports.

c. Although desktop reviews may be used to successfully accomplish the hardware review process, this section primarily focuses on on-site reviews. Nevertheless, the preparation, performance, and reporting of desktop reviews will be similar to on-site reviews. The desktop review uses similar techniques to those of the on-site review but does not have the advantages of being on-site (e.g., access to hardware personnel, access to all automation, access to test set-up). Both on-site and desktop reviews may be delegated to properly authorised staff responsible for certification. Practical arrangements with the hardware developer for on-site reviews by certification authorities should include:

    (1) Agreement on the type of review(s) that will be conducted (i.e. planning, development, verification or final certification).

    (2) Agreement on the date(s) and location(s) of the review(s).

    (3) Identification of the certification authority personnel involved.

    (4) Identification of any staff responsible for certification who are involved.

    (5) Development of the agenda(s) and expectations.

(6)   Listing of the hardware data to be made available (both prior to the review(s) and at the review(s)).

(7)   Clarification of the procedures intended to be used.

(8)   Identification of any required resources.

(9)   Specification of date(s) and means for communicating review results (which may include corrective actions and other required post-review activities).

d.   The objectives of the hardware review process are found in paragraph 4.4 of this section. Paragraph 4.5 of this section primarily addresses the integration of the hardware review process with the hardware development life cycle. Paragraph 4.5 also identifies the four types of reviews and the hardware life cycle data and data assessment criteria for each type. Paragraph 4.6 of this section addresses additional considerations for the hardware review process. Paragraph 4.7 of this section provides guidelines for preparing, conducting, and documenting a hardware review.

e.   At board/LRU level, the hardware review process should follow the considerations introduced in section 7.

f.   For COTS, the hardware review process should be adapted with respect to the specific available life-cycle data as described in section 9.

4.4.   Objectives of the Hardware Review Process

a.   The certification authorities may review the hardware life cycle processes and associated data at their discretion to obtain assurance that the SEH and CEH product submitted as part of a certification application comply with the certification basis and the objectives of ED-80/DO-254. The hardware review process assists both the certification authorities and the applicant in determining whether a particular project will meet the certification basis and ED-80/DO-254 objectives by providing:

(1)   Timely technical interpretation of the certification basis, ED-80/DO-254 objectives and CRIs.

(2)   Visibility into the compliance of the implementation and the applicable data.

(3)   Objective evidence that the SEH and CEH of the project adhere to the approved hardware plans and procedures.

(4)   The opportunity for the certification authorities to monitor the activities of staff responsible for conducting certification-related activities under a DOA.

b.   The amount of certification authority involvement in a hardware project should be determined and documented as early as possible in the project life cycle. The type and number of hardware reviews will depend on the hardware levels of the project, the level of complexity (complex or simple), the amount and quality of support from staff responsible for certification activities, the experience and history of the applicant and/or hardware developer, any history of service difficulties, and several other factors. Section 5 of this CM provides specific guidelines for determining the EASA level of involvement.

4.5.   Interaction between the Hardware Review Process and Hardware Life Cycle

a.   The review should begin early in the hardware life cycle. Early certification authority involvement reduces the risk that the system, hardware, and planning decisions will not satisfy ED-80/DO-254 objectives. Early involvement requires timely communication between the certification authority and the applicant about planning decisions that may affect the hardware product and processes. Typically, developing hardware for an aircraft or engine product, or an ETSO appliance, takes several months or years.   Since the guidance of ED-80/DO-254 is process-oriented, reviews should be integrated throughout the hardware life cycle. This means that regular contact between the applicant and certification authorities should be established. This contact should provide gradually increasing confidence in the hardware life cycle processes and in the resultant product to both the applicant and

the certification authorities. The four types of reviews are described as follows:

(1) A hardware planning review should be conducted when the initial hardware planning process is complete (i.e. when the most of the plans and standards are completed and reviewed).

(2) A hardware development review should be conducted when all actions from the hardware planning review have been proposed for closure and at least 75% of the hardware development data (i.e. requirements, design and code) are complete and reviewed.

(3) A hardware verification review should be conducted when at least 75% of the hardware verification and testing data are complete and reviewed.

(4) A final certification hardware review should be conducted after the final hardware build is completed, the hardware verification is completed, a hardware conformity review has been conducted (see §8.4.6), and the hardware is ready for formal system approval.

b. The availability of hardware life cycle data does not imply that the data are always complete. However, the data should be mature enough so the certification authorities can conduct a reasonable review. Similarly, not all transition criteria may necessarily be complete at that time in the project, but there should be enough to ensure they are being applied to the project.

c. Discussions between the applicant and the certification authorities should occur early in the project life cycle and should determine the types, need, number, depth, and format of the hardware reviews. For the purpose of this section, four reviews are identified to assess compliance with ED-80/DO-254 objectives.

d. The following paragraphs define the goals of each of the four types of hardware reviews, criteria for each type of review (e.g. type and availability of data, and type of transition criteria) and the appropriate evaluation criteria to be used. Paragraph 4.6 of this section identifies additional considerations that may impact the type and timing of reviews.

e. Per ED-80/DO-254, Appendix A, Table A-1, some hardware life cycle data listed in the following tables may not apply to certain hardware DALs/IDALs.

4.5.1. Hardware Planning Review

a. **Identification of the Hardware Planning Review**. Hardware planning is the first process in the hardware life cycle for any hardware project. The planning process establishes the various plans, standards, procedures, activities, methods, and tools to develop, verify, control, assure, and produce the hardware life cycle data. The goal of the hardware planning review is to determine whether the applicant's plans and standards satisfy the objectives of ED-80/DO-254. This review can also reduce the risk of an applicant producing a hardware product that does not meet ED-80/DO-254 objectives or other certification criteria.

The hardware planning review should take place after the initial completion of the hardware planning process. Although the hardware planning process may continue throughout the hardware life cycle, and plans and standards may change as the project progresses, it is generally considered complete when the associated initial transition criteria are satisfied. The following transition criteria are indicative of typical hardware planning process completion criteria:

(1) Hardware plans and standards were internally reviewed based on company specified criteria and deficiencies resolved.

(2) Hardware plans and standards were evaluated by the hardware process assurance organization or other organization that oversees the process assurance and deficiencies were resolved.

(3) Hardware plans and standards were approved and placed under configuration control.

(4) The objectives of hardware life cycle data applicable to a hardware planning review in ED-

80/DO-254, Appendix A, Table A-1 were satisfied.

b. **Data required for the Hardware Planning Review.** The applicant should make available to the certification authority the hardware plans and standards shown in the table below. Supporting hardware data should be under configuration control as appropriate for the hardware level prior to the hardware planning review.

Hardware Data	ED-80/DO-254 Section
Plan for hardware aspects of certification [1]	10.1.1
Hardware design plan[1]	10.1.2
Hardware validation plan[1]	10.1.3
Hardware verification plan[1]	10.1.4
Hardware configuration management plan[1]	10.1.5
Hardware process assurance plan[1]	10.1.6
Hardware process assurance records (as applied to the planning activities)	10.8
Hardware requirements, design, HDL code, validation & verification, and archive standards	10.2.1, 10.2.2, 10.2.3, 10.2.4
Tool qualification plans[1], if applicable	11.4
Supplier Management Plan (may be merged with other planning documents)	See section 11.2.2 of this CM

(1) To be submitted to the authorities at least 15 working days before the review

c. **Evaluation Criteria for the Hardware Planning Review.** The objectives which apply to planning in ED-80/DO-254 should be used as the evaluation criteria for the hardware planning review. Additionally, the proposed hardware level(s) and the justification provided by the Safety Assessment Process, including potential hardware contributions to failure conditions, should be assessed. The relevance of the hardware plans and standards to the hardware level should also be evaluated.

4.5.2. Hardware Development Review

a. **Identification of the Hardware Development Review.** The hardware development includes processes for hardware requirements, hardware design, hardware design language (HDL), and integration. These are supported by hardware validation, configuration management, process assurance, and certification liaison processes. The goal of the Hardware Development Review is to assess the effective implementation of the applicant's plans and standards by examining the hardware life cycle data, particularly the hardware development data and integral data associated with it. During this review, the applicant and the certification authority may come to agreement on changes or deviations from plans and standards that were discovered, and document them. Before conducting a hardware development review, the hardware development data should be sufficiently complete and mature to ensure that enough evidence exists that the developer is complying with their approved plans, standards and transition criteria. The following are typical transition criteria for a sufficiently mature hardware development process:

(1) Hardware component requirements are documented, reviewed, and traceable to system requirements.

(2) Conceptual hardware design data are documented, reviewed, and traceable to hardware requirements. The hardware architecture is defined, and reviews and analyses are completed.

(3) Detailed design data are documented, reviewed, and traceable to conceptual hardware design data and to the hardware requirements.

(4) The hardware component is produced and the implementation and production data were reviewed.

b. **Data required for the Hardware Development Review.** For a hardware development review, the hardware data shown in the table below should be made available to the certification authorities. The supporting hardware data should be under configuration control, as appropriate for the hardware level, prior to the review. The data listed in section 4.5.1.b should also be available during the development review.

Hardware Data	ED-80/ DO-254 Section
Hardware Requirements, Design and HDL Code standards	10.2
Hardware Requirements	10.3.1
Hardware Design Data	10.3.2
HDL or Hardware Design Schematics	10.3.2
Hardware Traceability Data	10.4.1
Hardware Review and Analysis Procedures	10.4.2
Hardware Review and Analysis Results	10.4.3
Hardware Life Cycle Environment Configuration Index (development environment aspects)	See Section 8.4.5 of this CM
Problem Reports	10.6
Hardware Configuration Management Records	10.7
Hardware Process Assurance Records	10.8
Hardware Tool Qualification Data (if applicable)	11.4.2

c. **Evaluation Criteria for the Hardware Development Review.** The objectives which apply to development in ED-80/DO-254 should be used as evaluation criteria for this review. Additionally, the hardware life cycle data should be evaluated to determine how effectively the applicant's plans and standards have been implemented in the development process.

4.5.3. Hardware Verification Review

a. **Identification of the Hardware Verification Review.** The hardware verification process is typically a combination of inspections, demonstrations, reviews, analyses, tests, and verification coverage analysis. As with the other reviews, the hardware configuration management and process assurance processes are also active during these verification activities. The verification activities provide assurance that the hardware component implementation meets the requirements. The hardware verification review should, therefore, ensure that the hardware verification processes will provide this confirmation and will result in objective evidence that the hardware component has been sufficiently verified and that the hardware component meets its requirements.

The purpose of the hardware verification review is to: assess the effectiveness and implementation of the applicant's verification plans and procedures; ensure the completion of all associated hardware configuration management and process assurance tasks; and ensure that the hardware requirements, conceptual and detailed design have been verified and that the implementation meets the requirements.

Before conducting a hardware verification review, the hardware verification process should be sufficiently complete and mature to ensure that representative verification data exists to assess that the applicant's approved plans and standards are being complied with and evidence exists that transition criteria have been met. The following criteria are indicative of a mature verification process:

(1) Development data (requirements, design, HDL) are complete, reviewed, and under configuration control.

(2) Test cases and procedures are documented, reviewed, traceable to requirements data and placed under configuration control.

(3) Test cases and procedures have been executed.

(4) Completed test results are documented, as agreed to in the planning documents.

(5)   The hardware testing environment is documented and controlled.

b.   **Data required for the Hardware Verification Review**. For the purpose of compliance findings for the hardware verification review, the hardware data shown in the table below should be made available to the certification authorities. The supporting hardware data should be under configuration control, as appropriate for the hardware level, prior to the review. The data listed in section 4.5.1.b and 4.5.2.b should also be available during the verification review.

Hardware Data	ED-80/ DO-254 Section
Hardware Requirements Data	10.3.1
Hardware Design Representation Data	10.3.2 and subordinate sections
HDL or Hardware Design Schematics	10.3.2
Hardware Verification Procedures	10.4.1, 10.4.2, 10.4.3, 10.4.4
Hardware Verification Results	10.4.5
Hardware Life Cycle Environment Configuration Index (including the test environment)	See Section 8.4.5 of this CM
Problem Reports	10.6
Hardware Configuration Management Records	10.7, See Section 8.4.5 of this CM
Hardware Process Assurance Records	10.8
Hardware Tool Qualification Data (if applicable)	11.4.2

c.   **Evaluation Criteria for the Hardware Verification Review.** The objectives included in Section 6.2 (and subordinate sections) of ED-80/DO-254 should be used as the evaluation criteria for the Hardware Verification Review.

4.5.4.   Final Certification Hardware Review

a.   **Identification of the Final Certification Hardware Review.** The final hardware build establishes the hardware product's configuration considered by the applicant to comply with all objectives of ED-80/DO-254. This is the version of the hardware they intend to use in the certified system or equipment. The goal of this review is to:

(1)   Determine compliance of the final hardware product with ED-80/DO-254, as defined by the hardware level and other hardware policy and guidance;

(2)   Ensure that all hardware development, verification, process assurance, configuration management, and certification liaison activities are complete;

(3)   Ensure a Hardware Conformity Review was performed; and

(4)   Review the final Hardware Configuration Index (HCI), Hardware Lifecycle Environment Configuration Index (HECI, see Section 8.4.5 of this CM) or other appropriate hardware documentation that establishes the final hardware configuration, and the Hardware Accomplishment Summary (HAS).

The final certification hardware review should take place when the hardware project is completed and includes the following criteria:

(1)   The Hardware Planning, Hardware Development and Hardware Verification reviews (as described in the previous subsections of this CM) have been performed and any deficiencies resolved.

(2)   The Hardware Conformity Review has been performed and any deficiencies have been resolved.

(3)   The Hardware Accomplishment Summary and Configuration Indexes have been completed and reviewed.

(4) All hardware life cycle data has been completed, approved, and placed under configuration control.

b. **Data required for the Final Certification Hardware Review.** For the purpose of this review, all the hardware life cycle data of ED-80/DO-254 should be available to the certification authorities. However, only the data shown in the table below is of special interest for this review. The supporting hardware data should be under configuration control, appropriate for the hardware level, prior to the review.

Hardware Data	ED-80/DO-254 Section
Hardware Verification Results	10.4.5
Hardware Life Cycle Environment Configuration Index	See Section 8.4.5 of this CM
Hardware Configuration Index[1]	See Section 8.4.5 of this CM
Problem Reports	10.6
Hardware Configuration Management Records	10.7, See Section 8.4.5 of this CM
Hardware Process Assurance Records (including Hardware Conformity Review Report)	10.8
Hardware Accomplishment Summary[1]	10.9

(1) To be submitted to the authorities at least 15 working days before the review.

c. **Evaluation criteria for Final Certification Hardware Review.** Evaluation criteria for this review include all the objectives of ED-80/DO-254. All hardware-related problem reports, actions, certification issues, etc. should be addressed prior to certification or authorisation. Additionally, applicants have to demonstrate that the end hardware device is properly configured and identified per the appropriate hardware drawings/documents, including correctly programming a device such as an FPGA.

4.5.5. Summary

The following table provides a summary of the information presented in the preceding sub-sections in relation with the scope of the different hardware reviews.

Review objective N°	Objectives	Items to be reviewed	Documentation available during the review	Entry Criteria
1	Planning The objective is to obtain agreement on the plans.	HW/SW partitioning. Safety objectives. Hardware plans. Hardware tools policy. QA policy.	PHAC[1], HDP[1], HVaP[1], HVeP[1], HPAP[1,2], HCMP[1] requirement standards[2] design standards[2] HDL code standards[2] Tool Qualification Plan Supplier Management Plan (may be merged with other planning documents)	As soon as possible

Review objective N°	Objectives	Items to be reviewed	Documentation available during the review	Entry Criteria
2	Development The objective is to verify that the development and the validation activities have been performed according to the agreed plans.	Hardware Requirements vs. System requirements (traceability). Hardware design vs. Hardware Requirements (traceability). HVP vs. requirements and design. HDL code vs. standards. Follow-up of the previously open items.	System requirements data (if available) Hardware requirements data Hardware Design data[2] HDL All data previously mentioned All life cycle data down to HDL code. [2] Hardware Reviews and Analyses Procedures. Hardware Reviews and Analyses Results Life cycle data of qualified design tools.	When at least 75% of the development data is available and maintained in configuration.
3	Verification The objective is to assess that verification activities have been performed according to the agreed plans.	Design verification activity. Implementation verification activity. Follow-up of the previously open items. Coverage of tests (integration / validation).	Hardware Reviews and Analyses Procedures. Hardware Test Procedures. Hardware Reviews and Analyses Results. Hardware Test Results. HDL code. All data previously mentioned. Life cycle data of qualified verification tools.	When at least 75% of the verification data is available and maintained in configuration.
4	Final The objective is to verify that the Hardware Development complied with all objectives of RTCA/DO-254 for the HW version intended to be used in the certified system/equipment.	Traceability of the final documentation package. Traceability of change request / Problem Reports. Status of open items. Supplier quality actions. Configuration management.	Problem reports. Hardware Configuration Management Records. Process Assurance Records[2]. HAS[1]. HCI (top level drawing)[1]. HECI[2].	Once the AEH is ready for formal certification approval.

(1) To be submitted to the authorities at least 15 working days before the review – Some documents might be grouped (i.e. the PHAC may contain the HDP and/or HVaP, HVeP).

(2) Not required for SEH.

NOTE: for SEH, documentation can be merged and/or combined with other documents. For example, the SEH PHAC may contain other plans and may also be combined with the CEH PHAC.

4.6.   Additional Considerations for the Hardware Review

a.   Although this section proposes four types of on-site reviews, the type, number, and extent of those reviews may not be suitable for every certification project and applicant. Additional considerations and alternative approaches may be appropriate. The following list of considerations may influence the level of the certification authority involvement in the hardware review process:

   (1)   The hardware level(s), as determined by a Safety Assessment Process.

   (2)   The product attributes such as size, complexity, system function or novelty, and hardware design.

   (3)   The use of new technologies or unusual design features.

   (4)   Proposals for novel hardware methods or life cycle model(s).

   (5)   The knowledge and previous success of the applicant in hardware development compliant with the objectives of ED-80/DO-254.

   (6)   The availability, experience, and authorisation of staff responsible for hardware approval.

   (7)   The existence of issues associated with ED-80/DO-254, Section 11. These include (but are not limited to) reusing previously developed hardware, the presence of COTS IP cores used to program hardware components, and using reverse engineering as a primary development model.

   (8)   The issuance of CRIs for hardware-specific aspects of the certification project.

   Section 5 of this CM provides specific guidelines for determining the EASA level of involvement.

b.   On-site hardware reviews may be increased or decreased in number. Four reviews is a typical number for a Level A or Level B project. Fewer or no reviews may be appropriate for some equipment manufacturers. Furthermore, reviews may be merged into a combined review. It is the responsibility of the certification authority representative to determine the desired level of investigation, to plan the reviews, and to co-ordinate with the applicant.

4.7.   Preparing, Conducting and Documenting the Hardware Review

This paragraph of this Section provides guidelines for preparing for the on-site review, conducting the on-site review, and recording and communicating the review results:

a.   **Prepare for the On-Site Review.** The EASA review team includes at least the EASA Panel 10 expert who may be supported by the corresponding system panel expert (see CM section 5.2).The applicant should co-ordinate with the EASA review team regarding the upcoming hardware review at least four weeks in advance and should propose an agenda. To optimise the efficiency of the review team while on-site, the applicant should send each EASA review team member the hardware plans identified in ED-80/DO-254, Section 10.1, 15 working days prior to the review (if not agreed differently between EASA and the applicant). Each EASA review team member should review the plans prior to arriving at the applicant's facility. After the purpose of the review and the agenda have been restated, the applicant should provide a short briefing to facilitate an understanding of the system under review, the hardware life-cycle model, processes, tools used, and any additional considerations.

b.   **Notification.** The applicant should notify the EASA review team in writing regarding the details of the hardware review. The following information should be included in the notification letter:

   (1)   The purpose of the review and the type of review (i.e. planning, development, verification or final).

   (2)   The date and duration of the review.

   (3)   A list of review participants.

An agency of the European Union

(4) A confirmation that the hardware plans identified in ED-80/DO-254, Section 10.1, have been sent to each review participant.

(5) A confirmation that all pertinent life cycle data should be made available at time of review.

(6) An indication of which ED-80/DO-254 objectives will be assessed.

(7) An indication of the applicant's own self-assessment conducted prior to the review.

(8) A confirmation that the responsible managers, developers, verification, configuration management, and process assurance personnel be available for questions.

c. **Conduct the On-site Review.** A typical on-site review includes the following elements:

(1) Certification Authority Entry Briefing to Include: introduction of review team members; restatement of purpose of the review; and overview of the review agenda.

(2) Hardware Developer's Briefing to Include: availability of facilities; availability of life cycle data; personnel schedule constraints; overview of the system; interaction of the system with other systems; system architecture; hardware architecture; hardware life cycle model (including tools and methods); progress against previous actions or CRIs (if appropriate); current status of the development; and any additional considerations (per ED-80/DO-254 or applicable Certification Review Items (CRIs)).

(3) Certification authorities' review of the applicant/developer's processes.

(4) Certification authorities' review of the product.

(5) Certification authorities' review of the oversight of suppliers.

d. **Record the Review Results.** The review results should be recorded; the records should include the following, as a minimum:

(1) A list of each life cycle data item reviewed to include: document name; control identity; version and date; requirement identification (where applicable); HDL or hardware design schematic (where applicable); paragraph number (where applicable); and review results.

(2) The approach taken to establish the finding or observation.

(3) An explanation of the findings or observations as related to the objectives of ED-80/DO-254 (documented with detailed notes). Each unsatisfied objective requires a summary of what was done and a discussion as to why the objective was not satisfied. Examples should be included, when necessary. This will ensure that the approach and findings can be understood and reconstructed at some future date.

(4) Any necessary actions for either the applicant or the certification authorities.

(5) Listing of all current or potential CRIs.

e. **Deliver an Exit Briefing.** The final briefing to the equipment manufacturer under review should be factual and positive and should summarise the findings. Findings should be presented with specific reference to ED-80/DO-254, the certification basis, policy, guidance, or other certification documentation. The equipment manufacturer should be given the opportunity to respond to the findings.

f. **Prepare a Review Report.** During the review, the applicant should produce a review report to summarize all the review findings, observations, and required actions. The report should be reviewed and agreed with the certification authority representative and the developer before the end of the review.

g. **Identify and Prepare CRIs (as needed).** CRIs are a means of documenting technical and certification issues that should be resolved prior to system approval. They provide the necessary communication between applicant and certification engineer and management. CRIs should be identified, prepared, and

resolved as soon as possible after the issue is discovered. Co-ordination with the EASA PCM should be established, as dictated by the applicable project procedures.

5. Organisation, role and level of involvement of EASA and applicants in hardware projects

5.1. Purpose

The main purposes of this section are to present the role of EASA Panel 10 and of the applicant in the determination of the EASA Panel 10 level of involvement (LOI) in a certification project and to describe the relations between Panel 10 and the other EASA system panels.

In addition, the applicant's involvement may be tailored by considering criteria similar to those described in this section, however taking into account the procedures already defined at company level (e.g. DOA procedures).

NOTE: In addition to this section, the description of the organisation of EASA Panel 10, its role and its level of involvement in each specific hardware projects may be extended in the Project Information Document (PID) where it is applicable.

5.2. Background

a. Modern aircraft and engine designs include many items of integrated digital equipment, some of which perform critical functions. The activities of Panel 10 need to be well organised and closely coordinated with the activities of each system panel. The EASA system panels involved include:

Panel 1: Flight

Panel 2: Performance

Panel 3: Structures

Panel 4: Hydro Mechanical systems

Panel 5: Electrical systems

Panel 6: Avionics systems

Panel 7: Powerplant and fuel systems

Panel 8.1: Cabin Safety

Panel 8.2: Environmental Control systems

Panel 12: Safety

The system/hardware integration of many types of equipment brings the need for close coordination between system and Panel 10 experts. Each panel in charge of a system expected to use digital equipment shall be the primary panel for the certification requirements relevant to that system. Panel 10 stands as the secondary panel for some of those requirements (mainly chapters 1301 and 1309 from the Certification Specifications or CS-E 50 (d,f)). Panel 10 experts will perform the verification activities for the hardware documents under their responsibility and will issue recommendations for compliance statements to the Panel 10 coordinator (refer to section 5.3.1) as well as to the relevant system panels.

b. EASA relies on the applicant's DOA system (or equivalent) so they can be confident that compliance with certification requirements applicable to the airborne electronic hardware device has been achieved.

Within the scope described in Subpart J of Part 21 (particularly cf. § 21A.239, 21A.257 and 21A.263), the applicant shall be entitled to perform design activities and to propose documents for acceptance without EASA further verification.

The level of involvement of EASA Panel 10 for each item of equipment in a given project can vary between the levels of NONE, LOW, MEDIUM or HIGH involvement in the certification activities (refer to section 5.3.2b). Additionally, depending on the stage of advancement and the quality of the certification activities already performed, the level of involvement initially agreed by EASA for a given item of equipment may evolve during the project.

5.3. Discussion on EASA Panel 10 Level of Involvement

5.3.1. Organisation and role of Panel 10

a. Coordination within Panel 10

(1) The coordinator

The coordinator is in charge of coordination of the hardware aspects of certification for the program on behalf of EASA Panel 10. He/she is a member of Panel 10.

NOTE: the size of EASA Panel 10 can vary, depending on the size of the certification project and the number of pieces of digital equipment to be assessed. For small projects, Panel 10 may be limited to one person taking charge of the complete spectrum of tasks and responsibilities described in this section (including coordination).

    i. Within Panel 10, the coordinator

- is the focal point in the case where no member has been designated for the hardware aspects of certification for some on-board equipment and in this case, he/she may propose another Panel 10 member to be designated

- is the focal point in the event of the relevant Panel 10 expert being unavailable due to conflicting priorities and in this case, he/she may propose an alternate Panel 10 member to be designated

- is the focal point within the EASA team for resolving generic issues linked to hardware development/approval policy.

    ii. In addition, the coordinator should be informed:

- by the applicant and/or by the relevant EASA systems expert or other Panel 10 members of new developments affecting the approval of the hardware installed on the aircraft (except for minor changes).

- periodically (at least twice a year) by the applicant of the overall hardware approval activities scheduled and the coordinator should ensure that all Panel 10 members are adequately allocated in order to carry out the associated hardware approval activities in due time. Such information is typically exchanged during Type Board Meetings (TBMs).

    iii. Finally, the coordinator should report to the EASA PCM :

- periodically (at least twice a year) the results of the overall hardware approval activities carried out and attend relevant status meetings (e.g. Type Board Meetings)

- on PCM request, any relevant hardware approval activity findings made by Panel 10.

(2) Work distribution within EASA Panel 10

The **Panel 10 coordinator** is responsible for the definition and acceptance of the hardware certification basis and the acceptable means of compliance.

The **Panel 10 expert(s)** is responsible for the acceptance that the hardware development process is in line with the certification basis (including methodologies for hardware development) and consistent with the DAL/IDAL allocated by the relevant system panel.

b. Coordination with system panels

(1) Determination of the Certification basis and the Acceptable Means of Compliance

The relevant Panel 10 member should be invited to the familiarisation meetings for systems that include airborne electronic hardware devices for which Panel 10 will have to assess compliance. This Panel 10 expert should assist the applicant and the relevant system panel expert in the determination of the certification basis. This task includes the definition of the applicable requirements and interpretative material as well as the identification of the hardware related CRIs that are applicable to the system.

In addition, the relevant Panel 10 expert may recommend the system panel expert and the Panel 10 coordinator to open a new CRI and may submit proposals. The draft CRI will then be further developed by the Panel 10 coordinator with support from the relevant Panel 10 expert and relevant system panel expert if needed. The endorsement of the Panel 10 coordinator is necessary to issue the EASA position on this issued CRI.

(2) Development Assurance Level (DAL) allocation

Acceptance of the DAL (or FDAL and IDAL) allocation at system level is the responsibility of the system panel expert, with the support of Panel 10, based on the Functional Hazard Analysis (FHA) and the Preliminary System Safety Analysis (PSSA).

For this purpose, the applicant should provide the system panel and Panel 10 with any document justifying the DAL/IDAL allocation, including a DAL/IDAL reduction justification (when applicable).

(3) Compliance statement

The Panel 10 expert is responsible for the compliance verification activities that he/she performs: at the end of the compliance verification, he/she shall issue a compliance statement to the EASA PCM and send a copy of it to the relevant system panel expert and to the Panel 10 coordinator.

The Panel 10 coordinator is responsible for issuing the final Panel 10 compliance statement. As the primary panel, the system panel is responsible for the final compliance statement. If there is any inconsistency between the system panel compliance statement and the Panel 10 compliance statement (for example, where a system panel issues a compliance statement even though some of the corresponding hardware documents have not received a compliance statement recommendation from Panel 10), the issue shall be brought up and solved at PCM level.

5.3.2. Determination of EASA Panel 10 Level of Involvement

a. General

The AEH certification process involves both the EASA Panel 10 experts and the applicant's DOA system (or equivalent).

Early coordination should take place between Panel 10 and the applicant during an initial certification meeting in order to specifically address their involvement in the hardware certification activities.

The agenda and objectives of the initial certification meeting should cover the following topics:

(1) The applicant should produce a document (at aircraft level or alternatively at ATA chapter or system level) for EASA concurrence that lists the hardware (LRU, boards, devices) in all systems on the aircraft and shows the DAL (or FDAL and IDAL), the applicant's planned level of involvement and the suppliers involved for each hardware component.

(2) The applicant should present to EASA the activities they plan to monitor (a list of reviews and a schedule) and state the rationale for the activities they plan to conduct under their DOA system or equivalent.

(3) EASA Panel 10 should present to the applicant their intended overall level of involvement.

(4) EASA Panel 10 should present to the applicant their review planning and define the documentation

to be delivered before each review.

b.   Determination of the LOI

The outcome of the assessment performed during initial certification meetings will result in a level of involvement of NONE, LOW, MEDIUM or HIGH for Panel 10 in the certification activities. There are five major criteria that can influence the outcome of this assessment (see additional aspects on Section 4.6):

(1)   The hardware DAL/IDAL

(2)   The complexity of the hardware development

(3)   The hardware approval experience of the development team and/or applicant

(4)   The product service history

(5)   The need for a new EASA policy due to any novelties (such as new technology, new design methods, unusual tools, etc.)

5.3.3.   Influence of the LOI on the certification activities

a.   EASA Hardware reviews

Section 4 of this Certification Memorandum provides information regarding the hardware review process. Depending on the EASA level of involvement agreed, the number of hardware reviews can be adapted as described in table below:

LOI	Hardware reviews
HIGH	At least 2 on-site reviews (e.g. Design Review, Verification review) + desktop reviews (e.g. Planning Review, Final Certification Review) + additional technical meetings (e.g. novelty) + Review of applicant Review Reports (cf. b.)
MEDIUM	At least 1 on-site review (e.g. combined Design and Verification Reviews) + desktop reviews (e.g. Planning Review and Final Certification Review) + additional technical meetings + Review of applicant Review Reports (cf. b.)
LOW	Desktop reviews + Review of applicant Review Reports (cf. b.)
NONE	*Eventual review of applicant Review Reports* (cf. NOTE)

NOTE: In particular cases, EASA can increase their involvement.

b.   Applicant hardware reviews

The applicant should report to EASA about their own review process as follows:

(1)   Applicant Hardware Review Reports should be sent for information to EASA Panel 10.

(2)   The status of the applicant's hardware reviews should be presented to Panel 10 before starting an EASA hardware review.

c.   Documentation to be submitted to EASA

The Panel 10 experts and the system experts should agree with the applicant early in the project on the categories of documents they wish to review or receive for information.

The applicant should send hardware certification documents to Panel 10 and system certification documents to the relevant system panels. In addition, some system documents may be sent to Panel 10 for information

only (e.g. the FHA), and some hardware documents may be sent to system panels (e.g. HAS) for information only.

The table below gives an example of the documents that fall under the responsibility of Panel 10, depending on the LOI:

LOI	Documents to be delivered				
	PHAC	**HAS**	**HCI**	**Other HW plans**	**Applicant Hardware Review Reports**
HIGH	For agreement	For agreement	For information	For information	For information
MEDIUM	For agreement	For agreement	For information	For information	For information
LOW	For information	On request	On request	On request	For information
NONE	Not sent	Not sent	Not sent	Not sent	Not sent

NOTE: "on request" means "on request for information"

5.3.4. Revision of LOI

At any time, the level of involvement initially agreed between EASA and the applicant for given equipment may be revised by EASA. It may evolve either towards more involvement or towards less involvement, depending on the stage of advancement and the quality of the certification activities already performed.

5.4. Discussion on Applicant LOI

In a similar manner to the one described in this section, the applicant should define their hardware review process (described above in section 4) which may be tailored with respect to similar criteria to those defined in Section 5.3.2 (hardware DAL/IDAL, complexity, supplier experience, the presence of novelties etc.). This tailoring performed at the product level should take into account the company's organisation (e.g. DOA procedures). This tailoring should be presented to EASA (see section 5.3.2.a).

6. Guidelines for Single Event Effects

For Guidance on Single Event Effects see EASA CM-AS-004 on Single Event Effects (SEE) Caused by Atmospheric Radiation.

7. Guidelines for Electronic Hardware Development Assurance of Equipment and Circuit Board Assemblies

7.1. Purpose

ED-80/DO-254 was issued in the year 2000 to cover Development Assurance for Airborne Electronic Hardware and consistent with that, this Section clarifies the use of that standard at equipment level (e.g. LRU, IMA modules, etc.) and Circuit Board Assembly (CBA) level.

7.2. Applicability

For equipment and CBAs of DALs/IDALs A, B, C or D, the ED-80/DO-254 objectives of Appendix A that are defined for level D should be applied.

However for DAL/IDAL D equipment and CBAs, the applicant may choose to follow existing development assurance practices provided it can be justified that they meet objectives similar to those of ED-80/DO-254 for DAL/IDAL D.

7.3. Documentation

The following documentation should be submitted to the certification authority for DALs/IDALs A, B, C and D:

1. Plan for Hardware Aspects of Certification (PHAC) [ED-80/DO-254, Section 10.1.1].

2. Hardware Verification Plan [ED-80/DO-254, Section 10.1.4].

3. Hardware Configuration Index [ED-80/DO-254, Section 10b].

4. Hardware Accomplishment Summary [ED-80/DO-254, Section 10.9]

The above documentation can be combined with the other submitted documentation for other CBAs.

7.4. Activities

As stated in ED-80/DO-254 section 1.6 for simple hardware item, extensive documentation is not needed and the supporting process of verification (including validation) and configuration management should be performed. This should be performed according to the ED-80/DO-254 Appendix A objectives (for DAL/IDAL D).

Activities defined in ED-80/DO-254 should be conducted appropriately to finally ensure the validation of equipment/CBA requirements (correctness and completeness) and the verification of the associated design implementation.

Note: For equipment, an acceptable level of development assurance (regarding requirement validation and verification) may alternatively be provided from the validation and verification activities performed by compliance with ED-79/ARP-4754 or ED-79A/ARP-4754A objectives.

8. Guidelines for Development of ASIC/PLD Electronic Hardware

8.1. Purpose

Applicants are proposing to use Digital Airborne Electronic Hardware components such as ASICs and PLDs in aircraft/engine airborne systems that have safety implications for their aircraft.

NOTE: The word 'device' within this section means 'ASIC/PLD'.

In the Certification Specifications (CS), there are no specific requirements for the certification aspects of airborne electronic hardware components. The purpose of this Section is to define specific guidance for certification aspects associated with the use of digital electronic hardware components in airborne systems. ED-80/DO-254 should be applied as the means of demonstrating that the processes used in the design of airborne electronic hardware devices provide a level of development assurance commensurate with the intended use of that device.

Note: Some compliance credit can be claimed for devices from an ETSO Approval provided that ED-80/DO-254 Development Assurance objectives are requested in the relevant ETSO. Aircraft/Engine installation requirements should be met in any case. Early communication with EASA should be made as this section may be applicable for some ETSO equipment (e.g. due to complexity, Integrated Modular Avionics, etc.).

These devices are often as complex as software based systems; hence they need a rigorous and structured development approach to satisfy the applicable functional and safety CS requirements. Simple digital Electronic Hardware components are also addressed by this Section of the Certification Memorandum.

The objectives of ED-80/DO-254 processes, together with the additional considerations of this section of the Certification Memorandum, will need to be satisfied at the device level for those electronic hardware devices classified in accordance with Table 2-1 of ED-80/DO-254 as requiring development assurance levels A, B or C. With the agreement of the responsible certification authority, for those devices requiring a development assurance level C, verification and validation at system or equipment level may be sufficient. For Level D components, the CM clarifications do not apply and the applicant may choose to follow the ED-80/DO-254 guidance or existing development assurance practices provided it can be justified they meet similar objectives.

See also Table 5-1 of ED-80/DO-254, which maps processes to the hardware design life cycle. Hardware Life Cycle data for devices should be issued as recommended by ED-80/DO-254 Appendix A Table A-1, complemented with the considerations of this section of the Certification Memorandum.

8.2. Applicability

The considerations of Section 8 of this Certification Memorandum apply to the following types of digital devices that have development assurance levels A, B, or C.

- Complex ASICs, PLDs: see Section 8.4
- Simple ASICs, PLDs: see Section 8.5

The Development Assurance of COTS and COTS Graphical Processors (CGPs) is outside the scope of this Section of this Certification Memorandum and specific guidelines for COTS and CGPs are provided in Sections 9 and 10.

8.3. Classification and Determination of ASIC/PLD Characteristics

The following characteristics of each ASIC/PLD should be justified and documented in a PHAC:

- the development assurance level, specifically if lower than the development assurance level of the system or equipment in which the device is used,
- Service Experience,
- Assessment of the complexity of the device (functional, physical).

   Note: Section 1.4 provides the definitions for complex and simple electronic hardware.

The following criteria should be addressed when assessing the simplicity/complexity of a device:

- description of the functions of the device
- description of the functional blocks with the type(s) of interfaces and description of the data processing
- independence of blocks
- synchronous or asynchronous design[2]
- number of independent clocks
- number of the basic elements used in the implementation [3]

---

[2] Asynchronous designs are generally more complex than synchronous ones.

[3] Number of macro-cells for an FPGA and gates for an ASIC

- number of state machines and number of states and state transitions per state machine

- independence of the state machines[4]

- number and type of functioning modes[5]

8.4. Complex ASICs/PLDs

8.4.1. Requirements Capture and Validation

All hardware requirements as defined in ED-80/DO-254 Section 10.3.1 (and not only derived requirements) should be identified and validated.

For the creation of requirements, the following guidance should be addressed.

- ED-80/DO-254 Section 5.2 (conceptual design process), 5.3 (detailed design process) and 5.4 (implementation process) recommend that derived requirements should be produced and fed back to the requirements capture process throughout these processes.

- Derived requirements are created from the design data and design decisions as defined in the following sections:

    - ED-80/DO-254 Section 10.3.2.1 "conceptual design data,"

    - ED-80/DO-254 Section 10.3.2.2 "detailed design data".

Note: ED-80/DO-254 recommends that any characteristics (including functional) to be met by a hardware implementation should be identified as requirements.

Completion of the requirements validation processes (ED-80/DO-254 Section 6.1) should be based on defined criteria.

To ensure the completeness and correctness of requirements, all requirements of the device (including the derived requirements) should be reviewed as recommended by ED-80/DO-254 Section 6.3.3.1:

- Requirements completeness assessment: ED-80/DO-254 Section 6.3.3.1 note 1.

- Requirements correctness assessment: ED-80-/DO-254 Section 6.3.3.1 note 2.

Note: Derived requirements for memory address assignments need to be validated, particularly when associated with partitioning concepts for integrated modular architectures.

The requirements validation processes should be documented as required by the hardware control category as defined in ED-80/DO-254 in table A-1 (item 10.1.3).

For levels A and B, the requirements validation processes should be satisfied with independence (independence being defined in ED-80/DO-254).

8.4.2. Verification of Design and Implementation

In this section:

- Verification of the design description stands for verification of the design at code level (e.g. HDL) and thus before Place & Route.

---

[4] Two state machines are dependent if a transition in one state machine is a function of the state(s) of another state machine. In cases involving dependent state machines, the number of possible conditions is much larger and it may be potentially impossible to completely verify all the conditions.

[5] "Reception, storage and transmission" is less complex than "reception, data processing (computations, filtering, extractions…) and transmission".

- Verification of the implementation stands for verification after Place & Route, comprising timing simulation, and verification with the component itself.

8.4.2.1. Verification of the Design Description

a) The correctness of requirements, conceptual design data and detailed design data (including HDL or schematics) should be verified in order to ensure that detailed design data correctly and completely represent the device behaviour specified in the requirements.

b) As recommended by ED-80/DO-254 Section 5.1.2, derived requirements which address the monitoring that unused functions will not interfere with the normal device behaviour should be verified.

Note: Definition of unused function is provided in ED-80/DO-254 section 3.3.1.2.3

c) COTS IP is used, the guidance within the IP specification (including user's manual) should be used to identify specific constraints necessary to properly control the unused functions of the COTS IP. The used interface to the COTS IP should be defined as derived requirements and verified as part of the overall verification activities.

d) If partitioning within the device is used (i.e. separation or isolation of functions or circuits), then partitioning integrity should be demonstrated, verified and documented.

e) For level A & B devices, verification processes should be satisfied with independence (defined in ED-80/DO-254).

f) If a Hardware Description Language (HDL), as defined in ED-80/DO-254, is used, coding standards for a proper use of this language should be defined.

HDL coding standards usually include but are limited to:

- Comment, style and naming rules,

- Traceability information for the HDL files (i.e. inclusion of actual file names, document and requirement references if appropriate),

- Guidelines to ensure the design will synthesize properly,

- Guidelines to exclude or limit the use of certain types of constructs (i.e. Case statements, "If Then" statements, "Do" loops),

- Rules to address the limits of design and verification tools,

- Guidelines for structure within the HDL (separation between different functions, limits on modules size),

- Rules to address technological constraints,

- Guidelines to address specific features (i.e. for synchronous designs, for interfaces with asynchronous signals for management of resets),

- Guidelines to organise the text to improve testability,

- Guidelines to reuse lessons learned from previous developments.

Conformance to those standards should be established.

g) If a Hardware Description Language (HDL), as defined in ED-80/DO-254, is used, an HDL code coverage measurement is an acceptable means to assess the way the HDL code has been exercised during device functional verification by simulation. The HDL code coverage measurement at sub-function level may alleviate the HDL code coverage measurement at device level. The degree of HDL code coverage measurement that should be achieved is as follows:

- For Level A: Decision coverage. (Every point of entry and exit in the HDL code has been invoked at least once and every decision in the HDL code has taken on all possible outcomes at least once),

- For Level A and B: Statement coverage. (Every statement in the program has been invoked at least once),

- Additionally, for Levels A and B in cases involving State Machines: Transition coverage.

The non-covered areas should be analysed and justified with the objective of reaching those coverage criteria.

Note 1: Branch coverage may replace Decision coverage if an assessment is performed to show it provides the same level of confidence.

Note 2: When the coverage is performed by an analysis of the RTL (Register Transfer Level) synthesis, this method should be assessed to show it provides the same expected HDL coverage.

h) In cases where an HDL code coverage tool is used, the above code coverage criteria may differ from the HDL code coverage metrics provided by some of the tools available on the market. For this reason, the applicant should justify how the achieved HDL code coverage as provided by the tool is equivalent to the criteria defined above.

i) If a Hardware Description Language (HDL) is used, an HDL code review against the conceptual design and requirements should be performed.

j) Sometimes, the design verification relies on using an HDL model simulating the behaviour of the expected device. For level A and B devices, the behaviour of this HDL model needs to be validated with regards to the device requirements.

8.4.2.2. Verification of the Implementation

Verification of the implementation is the verification (e.g. post layout simulations) of the detailed design after place and route and of the device itself.

The following considerations should be taken into account by the applicant as being complementary to ED-80/DO-254:

a) To assess at device level the freedom from unacceptable robustness defects, requirements-based testing should be defined to cover normal and abnormal input conditions and normal and abnormal operating conditions (clock frequency variations, power supply levels, voltage variations, temperature variations…). Where necessary and appropriate, additional verification activities, such as analysis and review, may have to be performed to address robustness aspects.

b) The PHAC (or HVP) should define and justify for each level of implementation (Register Transfer Level - RTL, post layout, physical device, board level) the type of planned verification activity (test, simulation, analysis, inspection…).

c) The test cases and procedures should be reviewed to confirm they are appropriate for the requirements to which they trace (see Section 6.2.2(4b) of ED-80/DO-254).

For level A and B devices:

d) Verification strategies should be based on a hierarchical approach, as for the design approach i.e. before integration at device level, sub-functions should be verified against their respective requirements.

When integration of sub-functions is complete, the verification of the overall device behaviour should be performed against the related requirements. Functional robustness should also be assessed at isolated sub-function level. Verification at overall device level and at sub-function level should be documented.

Note: sub-functions are not single gates or flip/flops. Sub-functions are a set of low level hardware gates or flip/flops that contribute together to perform a specific function: for instance, an SDRAM memory controller.

e) An analysis of the process used to perform the synthesis, place and route should confirm that the verification of the design demonstrates the behaviour of the implementation of the device.

f) Any inability to verify specific requirements by test on the device itself should be justified, and an alternative means of development assurance provided.

g) Verification processes should be satisfied with independence (as defined in ED-80/DO-254).

8.4.3. Traceability

Additionally to ED-80/DO-254 (Section 10.4.1 "traceability data" and respective objectives in Table A-1), the applicant should provide for Level A, B and C devices, bi-directional traceability between the system requirements, device requirements, the conceptual design data, the detailed design data and the HDL code.

Note: Note 6 in the table A-1 of the ED-80/DO-254 of Appendix A for DAL/IDAL C stating that "Only the traceability data from the requirements to tests is needed" should be considered as invalid and objectives 6.1.1(1) and 6.2.1(1,2) have to be met.

8.4.4. COTS IP

The rigor of the development processes for any COTS IP used in the design and implementation of ASICs or PLDs should be commensurate with their intended use and should satisfy the applicable functional and safety requirements. COTS IP life cycle data may need to be augmented to satisfy the guidance of ED-80/DO-254 and this CM Section.

If COTS IP is used:

*   COTS IP requirements should be defined and verified as recommended in ED-80/DO-254 and the relevant sections of this CM.

*   COTS IP guidelines (in datasheets, user manuals and errata sheets) should be defined to identify specific constraints necessary to properly control the unused functions of the COTS IP.

*   In addition to the verification that the COTS IP is used as recommended (in datasheets, user manuals and errata sheets), functional robustness verification should be performed to ensure correct interaction within the functions involving the COTS IP.

8.4.5. Configuration Management

•   Configuration Management should be performed at device level and performed as recommended by ED-80/DO-254 Section 7.2.3 "problem reporting, tracking and corrective action" and Section 7.2.4 "change control".

•   The Top Level Drawing to be submitted to the certification authorities should include configuration information to completely identify the configuration of the hardware and the embedded logic. In cases where this information is not available, a Hardware Configuration Index (HCI) should be submitted to the certification authorities to complement the Top Level Drawing on aspects concerning the configuration of the hardware and the embedded logic.

•   The Top Level Drawing may include the Hardware Life Cycle Environment data. In case where this information is not included, a dedicated Hardware Lifecycle Environment Configuration Index (HECI), which identifies the configuration of the life cycle environment for the hardware and embedded logic, should be available for review by the certification authorities. The HCI, HECI and Top Level Drawing facilitate the reproduction of the hardware and embedded logic life cycle environment, embedded logic regeneration, re-verification or embedded logic modification.

8.4.6. Process Assurance

- Process Assurance should be performed as recommended in Section 8 of ED-80/DO-254.

- A Hardware Conformity Review should be defined, performed and documented with the objective of obtaining assurance for the complex device submitted as part of a certification application. This review should determine that:

    1. The hardware life cycle processes are complete.

    2. The life cycle data is complete and developed from device requirements according to the plans

    3. Problem reports have been managed in configuration (see section 13 of this CM)

    4. The Synthesis and place-and-route process is controlled and can regenerate the file downloaded into the device from the detailed design data.

8.5. Simple ASICs/PLDs

The following guidelines apply to Simple Electronic Hardware (SEH) devices according to their DAL/IDAL:

- A comprehensive combination of deterministic tests and analyses should:

    o **For Levels A and B**, demonstrate the expected operation of the device under all possible combinations, permutations and concurrence of conditions of the inputs of the individual logical components (gates or nodes) within the device.

    o **For Level C,** demonstrate the expected operation of the device under all possible combinations, permutations and concurrence of conditions at the pins of the device (i.e. those inputs available external to the packaging of the device). All possible states of any state machines should also be tested.

    o **For Level D**, demonstrate the device satisfies the system or component level requirements specified for the device.

- A verification coverage analysis should ensure that the testing and analyses satisfied the above criteria, confirm the requirements, and are complete.

- Processes such as problem reporting, configuration management, production environment control, etc., help define the SEH device as a configuration controlled component. Therefore, all SEH devices should be under configuration control.

- Partition integrity (separation, isolation of functions or circuits) should be verified and documented, if partitioning or other protection means are used to justify that the device is simple.

In cases where the previous guidelines and particularly the exhaustive physical testing defined above is not feasible or is impracticable, then the applicant can use the guidance defined in ED-80/DO-254 corresponding to the allocated DAL/IDAL of the component.

8.5.1. Documentation

ED-80/DO-254 Section 1.6 states, "The supporting processes of verification and configuration management need to be performed and documented for a simple hardware item, but extensive documentation is not needed."

The list of documentation which should be submitted to the certification authority for SEH is described within §4.5.5 of this Certification Memorandum.

The above documentation can be combined with the other submitted documentation for other SEH or CEH devices. For example, a single PHAC for both simple and complex devices (or multiple SEH devices) may be submitted.

8.6. Additional Considerations

This section is applicable for the development of both Simple and Complex ASICs/PLDs.

8.6.1. Modifiable Aspects of Airborne Electronic Hardware Devices

ED-80/DO-254 does not address the modifiable aspects of a digital device where all or part of the embedded logic can be changed by the end user at any time from an external source without physical modification of the device hardware.

When the logic of a programmed electronic hardware device is intended to be modified in the field, in addition to the ED-80/DO-254 guidance material for the hardware, the applicant should consider the intent of the guidelines of ED-12B/DO-178B Section 2.5 concerning field loadable aspects for software.

When the logic of a programmed electronic hardware device is intended to be modified by the end user (aircraft owner/operator), in addition to the ED-80/DO-254 guidance material for the hardware, the applicant should consider the intent of the guidelines of ED-12B/DO-178B Section 2.4 concerning user-modifiable aspects for software.

8.6.2. Tool Assessment and Qualification

- Assurance compliant with ED-80/DO-254 Section 11.4 should be provided for development and verification tools.

- A claim for credit of relevant tool history, as discussed in ED-80/DO-254 Section 11.4.1 item 5, should be submitted to the Certification Authority in the PHAC.

- ED-80/DO-254 Section 11.4.1 item 4 states: "If a tool is used to assess the completion of verification testing, such as in an elemental analysis, no further assessment is necessary for such tool". Any other particular usage of the output of this type of tool should be reviewed. The adequacy of the tool to address the guidance of this CM (sub-section 8.4.2.1.g) as well as the tool limitations should be documented.

9. Guidelines for Commercial Off-The-Shelf Digital Airborne Electronic Hardware Components

9.1. Purpose

Applicants are proposing to use Commercial Off-The-Shelf Digital Airborne Electronic Hardware components such as Microcontrollers, Controllers or Highly-complex COTS microcontrollers in aircraft/engine airborne systems that have safety implications for their aircraft.

In the EASA Certification Specifications (CS), there are no specific requirements for the certification aspects of COTS airborne electronic hardware components. The purpose of this Section of the Certification Memorandum is to define specific guidance for certification aspects associated with the use of COTS digital electronic hardware components in airborne systems.

These devices are often as complex as software controlled microprocessor-based systems; hence they need a rigorous and structured approach to satisfy applicable functional and safety EASA CS requirements. Simple digital COTS Electronic Hardware components are also addressed by this Section of the Certification Memorandum.

ED-80/DO-254 Section 11.2 states that "the use of an Electronic Component Management Process (ECMP), in conjunction with the design process, provides the basis for COTS component usage". The following section of this Certification Memorandum provides some guidance for an ECMP. Some other guidance exists (e.g. IEC TS62239) which covers part of the activities described below.

In addition to the COTS considerations included in ED-80/DO-254 Section 11.3 (Product Service Experience), some of the following sections of this Certification Memorandum should be considered.

9.2. Applicability

The objectives of the ED-80/DO-254 processes, together with the additional considerations of this section of the Certification Memorandum, will need to be satisfied at the COTS device level for those electronic hardware devices classified in accordance with Table 2-1 of ED-80/DO-254 as requiring development assurance levels A, B or C. For Level D components, the additional guidance of this Section does not apply but the ED-80/DO254 processes are still applicable.

The considerations of this section apply to the following types of digital devices that have DALs/IDALs A, B, C.

- Commercial-Off-The-Shelf (COTS) ICs,

- COTS microcontrollers,

- Highly Complex COTS Microcontrollers.

Software and microprocessors are out of scope of this Section. The development assurance of microprocessors and of the core processing part of the microcontrollers and of highly complex COTS microcontrollers (Core Processing Unit) will be based on the application of ED-12B/DO-178B to the software they host, including testing of the software on the target microprocessor/microcontroller/highly complex COTS microcontroller.

COTS Graphical Processors are out of scope of this Section (see Section 10).

COTS IP is outside the scope of this section (See section 8.4.4).

9.3. Activities for Commercial Off-The-Shelf components (COTS)

The activities to be performed for simple, complex and highly complex COTS are dependent on their complexity, their criticality and the relevance of their Product-Service experience.

Those activities are defined in the following Sections:

- Classification and determination of device characteristics (see Section 9.3.1).

- Device data (see Section 9.3.2).

- Usage domain aspects (see Section 9.3.3).

- Analysis of the errata sheets (see Section 9.3.4).

- Configuration Management (see Section 9.3.5).

- HW/HW and HW/SW integration (see Section 9.3.6).

- Product-Service Experience (see Section 9.3.7).

- Architectural mitigation means (see Section 9.3.8).

- Partitioning issues (see Section 9.3.9).

- Alternative methods (see Section 9.3.10).

The specific activities to be performed for each type of device are identified within the following sections:

- Activities for Simple COTS ICs and Simple COTS microcontrollers (see Section 9.3.11).

- Activities for Complex COTS ICs and Complex COTS microcontrollers (see Section 9.3.12).

- Activities for Highly Complex COTS microcontrollers (see Section 9.3.13).

A summary of the intended activities should be documented in a PHAC. A summary of the outcome of these activities should be documented in a HAS.

9.3.1. Classification and Determination of COTS Device Characteristics

[1]: The applicant should classify and determine the characteristics of each device as follows:

- Its allocated development assurance level,

    Note: The safety process may justify the lowering of the hardware DAL/IDAL at board or at device level by using the appropriate standard (ED-79 (A) / ARP4754 (A) and/or ED-80/DO-254 appendix B §2).

- Its classification into one of the following categories (√) (see the COTS devices definitions in Section 1.4):

Category / COTS Device	Simple	Complex	Highly Complex
COTS IC	√	√	
COTS Microcontroller	√	√	√

- o The classification as simple and complex of the COTS IC or of the COTS microcontroller at least depends on:

    - the description of the functions of the device,

    - the description of the functional blocks of the device with the types of interfaces and a description of the data processing performed,

    - the number and type of functional modes[6],

    As a result of the assessment of the criteria here above, the ability to verify by test on the physical device all the requirements in all configurations is a prerequisite for the classification of a device as simple.

- o If a COTS microcontroller has any of the following characteristics, it should be classified as Highly Complex:

    - more than one Central Processing Unit (CPU) are embedded and they use the same bus (which is not strictly separated or which uses the same single port memory),

    - several controllers of complex peripherals are dependent on each other and exchange data,

    - several internal busses are integrated and are used in a dynamic way (for example, a dynamic bus switch matrix).

9.3.2. Device Data

[2]: The applicant should identify and archive the specific data corresponding to each COTS device. It should at least include the user manual, datasheet, device errata sheet and user manual errata sheet, installation manual (including the hardware/software interface and the explanation of activation/deactivation of COTS functions).

[3]: Design data:

---

[6] "reception, storage and transmission" is less complex than "reception, data processing (computations, filtering, extractions…) and transmission".

- When device design data for the COTS component is available, the applicant should capture and assess that data for consistency with the requirements of the device.

- When the design data for the COTS component is not available for review, the following approach should be documented:

  o The applicant should verify that the manufacturer of the component has a documented quality management process that is applied,

  o The applicant should verify that the manufacturer of the component has a deterministic and repeatable manufacturing process,

  o The applicant should verify that the manufacturer of the component applies an internal component approval process (i.e. there are test procedures with detailed acceptance criteria).

In case of a highly complex COTS microcontroller, if the component manufacturer's public data and training support are not sufficient to address the aspects above, then access to the component manufacturer's private data should be requested and established.

9.3.3. Usage Domain Aspects

[4]: The applicant should determine the usage domain of each COTS device for the intended application and demonstrate that the component is operated within the limits/recommendations established by the manufacturer of the component. The usage domain should identify for example:

- Used functions (e.g. description of each function, configuration characteristics, mode of operation, control and monitoring during normal/abnormal operation),

- Unused functions,

- The means used to deactivate functions,

- External means to control any inadvertent activation of unused functions, or inadvertent deactivation of used functions,

- Means to manage device resets,

- Power-on configuration,

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

- Usage conditions (clock frequency, power supply level, temperature, etc.).

[5]: The applicant should validate the usage domain of the component with respect to safety and system specifications:

- The use of features should be justified and be consistent with the system, hardware, software and safety requirements, particularly when internal device functions are used to ensure that safety objectives are fulfilled,

- The validity of the usage domain should be ensured by a set of verification activities mainly based on:

  o Test (of used functions, verification of support for fault tolerance, effectiveness of unused function deactivation, verification of errata workarounds, validity of the usage conditions defined by the component manufacturer). As test is not always possible, a combination of testing and analysis may be performed.

  o Analysis:

    ▪ Design margin analysis to verify that the implementation of the component takes into account the potential variability of component characteristics,

- ▪ If the component is previously approved, an analysis should be performed to compare the characteristics and usage and to identify the differences between the two usage domains. Any differences should be analysed and justified,

    - ▪ Analysis of the impact of the inadvertent activation of unused functions.

- The determinism of a device (e.g. bus throughput, data latency, WCET, stack activity) should be ensured for the usage domain and device characteristics. Additional assessment may be required for complex architectures (e.g. dependent complex interfaces, multiple internal busses used dynamically, etc.).

- In the case of multi-core processor usage, an assessment of all specific multi-core functionalities or usual CPU functionalities using the multi-core design should be performed. This assessment may include but is not limited to: multi-processing strategy, simultaneous multi-threading, parallel internal bus management and determinism, Very Long Instruction Word (VLIW), Single Instruction Multiple Data (SIMD), Vector processing, internal memory/cache management, software impact on the Operating System and associated middleware, partitioning impact, usage domain impact, external Databus impact, timing requirement impact, safety requirement impact, and impact on the WCET strategy.

9.3.4. Analysis of the Component Manufacturer Errata Sheets

[6]: The applicant should provide evidence to show:

- How the component manufacturer captures and maintains the list of errata and publishes it.

- That the rate of occurrence of new errata from the component manufacturer decreases as a function of time - this is a criterion to determine the maturity of the component.

[7]: The applicant should assess:

- All the errata from the component manufacturer for any potential adverse safety effects on the system. This assessment should comprise:

    - o Justification to show which of the errata are applicable to the specific application of the device,

    - o Justification to show which of the errata are not applicable to the specific application of the device,

    - o Description of the mitigation implemented for each of the applicable errata,

    - o Evidence that the implementations of errata mitigations are covered by relevant requirements and design data.

[8]: The applicant should document their own past experience of usage of the component and the experience they gained as part of the current development, along with any other additional recommendations (e.g. errata workarounds) that should be implemented in order to use the component.

9.3.5. Configuration Management

[9]: The applicant should verify:

- That the component manufacturer manages in configuration (see ED-80/DO-254 §7.1) the device data (see §9.3.2),

- How component changes implemented by the component manufacturer are documented and controlled.

- That the component manufacturer provides the applicant with change description data.

[10]: In cases where a change is made to the component, the applicant should

- Perform a change impact analysis in order to determine which additional verification activities should be conducted.

9.3.6. HW/HW and HW/SW Integration

[11]: The applicant should:

- Perform the associated Verification and Validation activities (see ED-79 / ARP-4754 or ED-79A / ARP-4754A definitions) against the requirements of the component at LRU/board level, and against the hardware/software interface requirements,

[12]: The applicant should:

- Perform an analysis at the device level (based on the identification of the architecture and an assessment of the independence of blocks/pin-outs) so as to refine the failure modes and associated failure rates of the device. (Device failure rates should take into account the coverage of test features embedded in the device),

- Ensure that the performance assessment and functional safety analysis of the device take into account the used configuration of the device,

- When the device can be configured via hardware or software pin-programming, ensure that the programmed configuration that is used (e.g. the register programming status) actually configures the device as expected.

9.3.7. Product Service Experience

[13]: The applicant should document:

- The target market for the COTS component,

- The specific environments (e.g. civil aircraft, military aircraft, space, telecom, automotive, medical, consumer…) in which the operating experience of the component was gained and the related numbers of operating hours,

- The criticality of the usage of the component (e.g. involved in a Catastrophic failure path…),

- The total order of magnitude of the time for which the component has been used (i.e. the number of execution hours and the usage duration in years),

- For DAL/IDAL A, B and C COTS components, the classification of the Product Service Experience as "Sufficient PSE" or "Low PSE" and the justification using the following criteria which use the definitions: <u>Aircraft applications:</u> aircraft operation in flight or on ground **+** board/LRU/system/aircraft tests; <u>Safety applications:</u> Space, airborne military, nuclear, medical, railway, automotive; <u>Other applications:</u> bank, computer, telecom…

  - For components allocated DAL/IDAL A, the Product Service Experience is "sufficient PSE" if one of the following criteria is met (whereas if none of the criteria is met then the Product Service Experience is "Low PSE"):
    - At least 2 years of use **with [**hours of aircraft applications **+** safety applications**] >10^6**,

    - At least 2 years of use **with { [**hours of aircraft applications **+** safety applications**] >10^5 AND [**hours within other applications**] >10^7 }**

  - For components allocated DAL/IDAL B, the Product Service Experience is "sufficient PSE" if one of the following criteria is met (whereas if none of the criteria is met then the Product Service Experience is "Low PSE"):

An agency of the European Union

- At least 2 years of use **with [**hours of aircraft applications **+** safety applications**] >10^5**,

- At least 2 years of use **with { [**hours of aircraft applications **+** safety applications**] >10^4 AND [**hours within other applications**] > 10^7 }**

o For components allocated DAL/IDAL C, the Product Service Experience is "sufficient PSE" if the following criterion is met (whereas if the criterion is not met then the Product Service Experience is "Low PSE"):

- **[**Hours in aircraft applications **+** safety applications **+** other applications**] >10^5**,

- For DAL/IDAL A and B COTS components, the minimum amount of usage is defined as follows:

o At least 2 years use **with** [hours of aircraft applications **+** safety applications **+** other applications] **> 10^6**

DAL/IDAL A and B COTS components with less usage than this minimum amount should not be used.

[14]: The applicant should provide evidence of the stability and maturity of the component taking into account:

- The number of modifications of the device design or implementation,

- The nature of device modifications,

- The rate of occurrence of errata associated with the different versions.

9.3.8. Architectural Mitigation

Results of the common mode analysis should be taken into account in order to show whether:

[15]: Architectural mitigation should be implemented in any case in which one or more instances of the COTS component could cause a Catastrophic failure effect without any other contributing faults occurring.

The results of Common Cause Analysis performed by the applicant should be taken into account. For example, the anomalous behaviour or failure of identical COTS components (common design), implemented in redundant system architecture, should not lead to a Catastrophic failure condition.

Also the Common Cause Analysis performed at Aircraft level may reveal some Hazardous engine/propeller Failure Conditions that lead to a Catastrophic Aircraft Failure Condition. In such a case, this topic [15] should be addressed.

9.3.9. Partitioning Issues

In some products, partitioning is implemented to provide independence between System, Software or Hardware functions. In some cases, a COTS component may be involved in the mechanisms and/or requirements defined to ensure correct spatial and temporal partitioning. However, the design of some COTS components may not be able to ensure robust partitioning.

Note: Refer to several standards (e.g. ED-12B / DO-178B, ED-94B / DO-248B) which define robust partitioning and how it should be specified and implemented.

[16]: When a COTS component is used in an implementation that requires robust partitioning, a partitioning analysis (including spatial and temporal assessments) should be performed to show that the COTS component can provide robust partitioning.

Note: If robust partitioning is not confirmed by the partitioning analysis, a means of mitigation external to the COTS component may need to be implemented.

9.3.10. Alternative Methods

Where alternative methods to those described above are proposed, the applicant should explain their interpretation of the ED-80/DO-254 objectives, describe their proposed alternative methods, and present to the authority at an early stage, their justification of equivalence to ED-80/DO-254 and to this Certification Memorandum.

Examples of alternative methods could be:

- Reverse engineering of a device to generate life-cycle design data, enabling verification activities compliant with ED-80/DO-254,

- For simple COTS or simple microcontrollers, it could be practical to verify each of the functions and the performance of these components at LRU/board level by a combination of deterministic tests and analysis under all foreseeable operating conditions.

9.3.11. Activities for Simple COTS ICs and Simple COTS Microcontrollers

This Section list the activities to be performed for Simple COTS ICs and Simple COTS Microcontrollers, taking into account the corresponding DAL/IDAL.

Simple COTS ICs and Simple COTS Microcontroller / Activities	DAL/IDAL A	DAL/IDAL B	DAL/IDAL C
[1]:	A	A	A
[2]:	A	A	A
[6]:	A	A	
[7]:	A	A	
[15]:	A		

A: Applicable

9.3.12. Activities for Complex COTS ICs and Complex COTS Microcontrollers

This Section list the activities to be performed for Complex COTS ICs and Complex COTS Microcontrollers, taking into account their corresponding DAL/IDAL and Product Service Experience.

Complex COTS ICs and Complex COTS Microcontroller / Activities	DAL/IDAL A		DAL/IDAL B		DAL/IDAL C	
	Sufficient PSE	Low PSE	Sufficient PSE	Low PSE	Sufficient PSE	Low PSE
[1]:	A	A	A	A	A	A
[2]:	A	A	A	A	A	A
[3]:		A		A		

An agency of the European Union

[4]:	A	A	A	A	A	A
[5]:		A		A		A
[6]:	A	A	A	A	A	A
[7]:	A	A	A	A	A	A
[8]:		A		A		
[9]:	A	A	A	A	A	A
[10]:	A	A		A		A
[11]:	A	A	A	A	A	A
[12]:						
[13]:	A	A	A	A	A	A
[14]:		A				
[15]:	A	A				
[16]:	A	A	A	A	A	A

A: Applicable

9.3.13. Activities for highly complex COTS microcontrollers

This Section list the activities to be performed for Highly Complex COTS Microcontrollers, taking into account their corresponding DAL/IDAL and Product Service Experience.

Highly Complex COTS Microcontroller / Activities	DAL/IDAL A		DAL/IDAL B		DAL/IDAL C	
	Sufficient PSE	Low PSE	Sufficient PSE	Low PSE	Sufficient PSE	Low PSE
[1]:	A	A	A	A	A	A
[2]:	A	A	A	A	A	A
[3]:		A		A		
[4]:	A	A	A	A	A	A
[5]:	A	A	A	A		A
[6]:	A	A	A	A	A	A
[7]:	A	A	A	A	A	A
[8]:		A		A		
[9]:	A	A	A	A	A	A
[10]:	A	A		A		A
[11]:	A	A	A	A	A	A
[12]:		A		A		
[13]:	A	A	A	A	A	A
[14]:	A	A		A		
[15]:	A	A				

[16]:	A	A	A	A	A	A

A: Applicable

10. Guidelines for the Usage of Commercial Off-The-Shelf Graphical Processors in Airborne Display Applications

10.1. Purpose

This Section of the Certification Memorandum is related to the use of Commercial Off-the-Shelf (COTS) Graphical Processors (CGPs) (which have been allocated a DAL/IDAL of A, B or C) in airborne display systems that are part of the technical configuration of an aircraft.

NOTE: For Level D components, the additional guidance of this Section does not apply but the ED-80/DO254 processes are still applicable.

These devices represent a different class of devices from the microprocessors being used in critical airborne applications. These COTS devices were originally designed to be used in graphics intensive non-aerospace applications, such as laptop computers and video games. They are able to provide functionality that previously needed to be implemented in software.

However, there are several aspects that justify the need to address specific certification considerations in order to prevent potential design errors that may adversely impact the safe operation of an aircraft system in which a CGP is installed:

- These devices use multiple embedded microprocessors that run asynchronously and a single CGP may contain a total of 30 to 100 million transistors. A CGP cannot, therefore, be considered to be a simple device.

- As for any microprocessor (graphical or not graphical), these CGPs have typically not been developed per ED-80/DO-254.

- It may be impractical to perform verification activities or reverse engineering to make these devices compliant with ED-80/DO-254.

- Due to the very short life-cycle of these components, it may be difficult to use service history to verify that the design is free of design errors.

In general, the use of COTS devices in critical airborne applications causes some difficulties for system designers. Typically, microprocessors (like CGPs) have not been developed to a recognized standard such as ED-80/DO-254 and are excluded from these Sections related to Electronic Hardware Development Assurance and COTS usage (in Section 7 and section 9 of this Certification Memorandum). Hence, it may not be feasible to comprehensively test such a device in a manner that would ensure the device is free of design errors that may adversely impact safe operation of the aircraft system in which it is installed.

The following devices include some of the concerns and issues that could arise when CGPs are used in safety-critical airborne systems:

a. Because CGPs are devices of very high complexity that typically have very short design cycles, there is an increased possibility that they may contain design errors, hardware failures or inappropriate responses to external events (e.g., EMI, high operating temperature) that could result in the undetected display of Hazardously Misleading Information (HMI) to the flight crew. If the resulting erroneous information is not flagged as Invalid Data, it could induce the flight crew to take inappropriate and potentially hazardous action based on that erroneous data, or to not take appropriate action when action is required.

b. Because CGPs are devices of very high complexity that typically have very short design cycles, there is an increased possibility that they may contain design errors which could result in a reduction of

the availability of the display system in which they are incorporated and in the loss of multiple, redundant display systems.

c. CGPs, depending on the type, complexity, and supplier, may exhibit performance variations over the production lifetime of the device. These variations may appear at temperature extremes, over-voltage conditions, or other operating environmental conditions. Alternatively, these variations may not require any extreme operating conditions for their effects to be revealed. These variations could have adverse effects on the display systems in which they are incorporated.

d. Many CGPs contain configurable elements. Some of them may be selectable by loading specific microcode instructions into the device. This capability leads to concerns regarding the configuration control of CGPs installed in display systems.

e. The CGP part numbering, change control process and revision identification scheme used by the individual CGP suppliers may not be known/understood by the applicant. As a result, not every change of a CGP device that is significant to the system in which it is installed may be reflected in the CGP part number. Similarly, variations in manufacturing processes may result in different device characteristics among devices produced in different production runs. These are critical concerns, given that the typical life cycle of these types of devices may be as short as 12 to 18 months.

f. It may be difficult to determine whether a CGP design is such that it includes any functionality that would result in unintended operation of the device under unusual operating conditions or as a result of failures.

g. These devices require substantial graphics software that allows functional applications to draw visual components on the display, such as a software package that implements the OpenGL graphics drivers and applications. The developer of the display system may not be the same company that develops the graphics software. There may be software graphics packages available for these COTS graphical processors that were not developed to ED-12B/DO-178B or other acceptable means of compliance.

h. Establishing a component failure rate for a CGP microprocessor, or a family of microprocessors, may be problematic. Empirical data on the actual failure rates experienced in avionics applications of these devices may be non-existent. An analytical method for determining the expected failure rate of these devices should, therefore, be established, in order to show that the proposed availability rate of the system is adequate for its purpose.

10.2. Use of ED-80/DO-254

COTS Graphical Processors have been developed primarily for a non-aerospace, non-safety critical market. As such, it may be problematic, if not impossible, for an applicant to obtain the required documentation necessary to show compliance with a development assurance process such as the one contained in ED-80/DO-254 Sections 2 to 9. Therefore, reliance on a development assurance process for a CGP as an acceptable means of compliance will likely be very difficult to substantiate.

Nevertheless, ED-80/DO-254 paragraphs 11.2 and 11.3 contain information regarding how a specific COTS device should be chosen for use in an airborne system, and how possible certification credit can be obtained by using the documented service experience of the device. Hence, the applicant should apply the considerations listed in these paragraphs for COTS Graphical Processors devices. Some of the main points made in those sections are summarized below:

1. Electronic component management principles apply to CGP devices. That is, concepts such as the supplier track record, quality control, establishment of device reliability, and the suitability of the device for its intended use should all be taken into account when choosing a CGP.

2. The applicant should have plans to address probable issues such as the lack of CGP device development assurance data, possible variations in device parameters from one production batch

An agency of the European Union

to the next one, and the eventual redesign or complete phase-out of that device by the CGP supplier.

3. Product service experience may be used to substantiate partial development assurance of a CGP device. Non-airborne systems experience of the device may be used if gathered in a similar usage domain and/or critical operating environment. However, data of this nature carries some expectations. Formal documentation (such as specifications, data sheets, application notes, errata sheets, etc.), a formal problem reporting and resolution scheme, a method of determining actual failure rates of the device experienced in the field, etc., should be requirements for obtaining certification credit. If the applicant intends to develop a service experience case to obtain certification credit, they should be aware that this certification credit requires substantiation.

10.3. Additional Considerations for Hazards Identified

This section includes additional considerations that should be considered by the applicant in response to the hazards identified in the background section.

10.3.1. Item a - Hazardously Misleading Information (HMI)

The applicant should show that the CGPs used in the aircraft airborne equipment cannot display HMI, to a level of assurance commensurate with the hazard classification (e.g., Catastrophic, Hazardous, Major) of the HMI in question.

As discussed previously, reliance on a development assurance process, such as the one described in ED-80/DO-254 Sections 2 through 9, as an acceptable means of compliance, is not considered to be practical. It would be extremely problematic for the user of a CGP to obtain documentation from the CGP supplier that would show that the device was developed using ED-80/DO-254, or some equivalent development assurance process.

Additionally, it may be difficult to substantiate a "Service History Experience" proposal for certification credit using the guidelines of ED-80/DO-254 Section 11.3. The latest generation CGPs, although conceptually similar to those devices used in currently certified airborne display systems, have advanced in functionality and complexity to the point that no similarity to devices from earlier generations is apparent. Likewise, it may be difficult to make a case that can be substantiated using non-airborne applications of the device.

Given the points made in the preceding paragraph, the most likely and obvious means to ensure protection against the display of HMI for HW devices incorporating CGPs is:

*   to include architectural mitigation(s) at the equipment level, as identified in ED-80/DO-254 Appendix B Section 3.1, and

*   to include architectural mitigation(s) at the system level, as identified in ED-79/ARP4754 Section 5.4 (or ED-79/ARP4754 Section 5.2),

such that the probability of misleading information being displayed to the flight crew is commensurate with the hazard classification of that event. Architectural mitigation(s) for erroneous operation of any/all CGPs in the system may take many different forms. However, the basic response of any mitigation should be that any misleading information computed by a CGP should be detected and not allowed to be displayed on the displays, or else the displayed data should be flagged as invalid. The mitigation(s) proposed by the applicant should also be independent of the device that is causing the anomalous behaviour.

If any mitigation scheme is proposed that will require pilot recognition of the anomalous behaviour, the applicant should describe the cues (e.g., visual, aural, tactile) on which the pilot recognition depends. The applicant should also describe the testing, such as during flight test or in a flight simulator, which will be used to evaluate pilot recognition of any failure conditions that are not reliably detectable by the design and which could cause or contribute to a hazardous or catastrophic failure condition if the information is accepted by the pilot.

10.3.2. Item b - Multiple display failures due to common failure mode/display system availability

The architecture of a display system should be such that the availability of the displayed critical data complies with the numerical probability required by the safety assessment process. The applicant should demonstrate that a flight deck display system utilizing multiple displays provides the required flight deck display functions to a level of assurance commensurate with the hazard classification (e.g., Catastrophic, Hazardous, Major).

The concern is that a common failure mode error associated with the use of common CGPs across all displays could have a significant impact on the availability of the entire display system. The loss of data on a single display generally has less effect on safety than the simultaneous/cascading loss of the data on all displays. A common cause fault can lead to the loss of data on more than one display.

If architectural mitigation is used for HMI hazards (as identified in Device a), it should not adversely impact the overall availability of the display system in such a manner that the availability requirements of the display system are not met due to a single common cause or a cascading failure. This includes not only faults and design errors within the CGP, but also the hardware supporting the operation of the CGP. Events such as the loss of cooling air, extreme vibration or mechanical "shock", etc., should not cause the loss of multiple displays unless the probability of that event is commensurate with the hazard of the loss of multiple displays.

The Common Mode Analysis should use a checklist similar to that described in ED-135/ARP 4761 K.3.1.1. The output from the review described in ED-135/ARP4761 K.3.1.1 is a list of Common Mode Analysis requirements. The objective is to confirm that the approved design contains the design requirements and production processes to mitigate common cause faults.

The statements regarding common cause faults in this section refer only to faults that would have an effect on the CGP device itself, and the aspects of the design that support the CGP device. It is assumed that the system level common mode analysis has already been accomplished.

10.3.3. Item c - CGP Device Variations during Production Life

There is a possibility that the CGP, during the production lifetime of the device, may exhibit variations or degradations in its performance or operating characteristics. These changes in the operating performance and characteristics of the device could manifest themselves in various ways, including but not limited to the following:

- Changes in the operational environment range (e.g. variation in performance over the expected thermal operation range, or a cascading failure initiated by over-voltage).

- The introduction of a failure mechanism that was not present in the original design of the device.

The applicant should explain the programs/processes that are in place that would directly address the concerns listed in this section. The plan from the applicant to deal with variations in performance and characteristics of the CGP during its production lifetime may include:

- Environmental screening of either specific components or the equipment (e.g. verify that a sample does not contain manufacturing errors).

- Acceptance testing of different productions runs of the same device to determine whether any of the critical performance aspects of the device have changed.

- An in-service program (e.g. post-delivery program for event logging) to analyse actual single-display failure events for their potential to cause or contribute to failures in other installed equipment. This may include design features to support root cause investigation, such as a fault code logging memory feature.

The applicant should identify CGP component variations which could have an adverse impact on the display system, identify appropriate tolerances, and implement display system mitigation(s) to address these variations or component screening to detect out of tolerance components.

10.3.4. Item d - CGP Configurable Devices

Many CGPs contain configurable devices, such as separately loadable microcode or hardware "straps". The applicant should show that the configurable devices of the CGP, such as the loadable microcode, are controlled and that any production/manufacturing errors involving the display system configurable devices, such as option selection hardware strapping, will be detectable by the proposed system operation and monitoring, end device acceptance test, or other applicable check. The applicant is responsible for ensuring the configuration control of the display system and its components. Additionally, in cases where the configurability of a CGP is based on the use of configuration files, the applicant should apply the certification considerations included in the EASA Certification Memorandum related to Software.

10.3.5. Item e - Continued Monitoring of Supplier Data

The applicant should explain their process for continually monitoring supplier data (such as device specifications and errata sheets) for COTS Graphical Processor devices, such that newly discovered problems with the device or instructions for future usage are known to the software and/or hardware design teams and appropriate actions are taken. Specific Change Control procedures, including the associated Change Impact Analysis, should be put in place in order to take into account in the updated design the evolutions of the CGP characteristics and constraints.

Additionally, the applicant should explain their plan for ensuring awareness of any changes to the CGP that may affect the display system certification that could require existing analyses to be reassessed. These include but are not limited to the concerns expressed below:

- Changes in fit, form or manufacturing techniques that may affect the physical layout, mechanical, electrical or thermal characteristics of the CGP.

- Changes or additions in functionality, including those aspects that are not used in the display system application, including firmware, device drivers and libraries.

- Performance enhancements, such as an increased operating frequency.

10.3.6. Item f - Unintended CGP Functionality

The applicant should explain how they intend to demonstrate that the CGP does not contain any functionality, used or un-used, documented or undocumented, in this application, which would cause HMI to be displayed or otherwise affect the integrity of the displayed data.

Note: EASA is aware that it would be extremely problematic to show that a CGP, or any other very complex microprocessor device, does not contain any "undocumented functionality". EASA does not expect the applicant to provide 100% assurance of this point. However, the expectation is that the applicant will have a program that will test the device extensively, and one that will include a large amount of robustness testing, above and beyond the functionality that is expected to be provided by the device. A thorough program of this nature will be taken as evidence that the applicant has made a "best effort" to determine whether the CGP contains any undocumented features or functions that could affect the final design of the display system.

10.3.7. Item g - Open GL Software Drivers

CGPs usually require many complex software drivers that are resident in the main system processor. There are some software packages that may be obtained from third party suppliers which implement OpenGL graphics packages. In any case (whether the software drivers are obtained from the CGP supplier or from a third party), the applicant should demonstrate compliance with ED-12B/DO-178B (or some other acceptable development assurance process) for this software to the appropriate software level as determined by the safety assessment process. The applicant should also address the software level when evaluating their choice of graphics generators and drivers, and developing the design. The same considerations should be applied to loaded microcode in cases where the configurability of the CGP (if any) was based on these means.

10.3.8. Item h - CGP Component Failure Rate

The display system architecture should be such that the availability of the displayed critical data complies with the numerical probability required by the safety assessment process. If the display system fault trees use specific failure rates for CGPs, the applicant should include substantiating data or other appropriate justification for these failure rates. The applicant should work with EASA to determine an acceptable method of calculating an estimated failure rate or determining an appropriate empirical one.

10.4. Certification plan

Each COTS Graphical Processor used in airborne systems should be listed in the Applicant's Certification Plan, including information about the airborne system that incorporates the CGP, the information displayed and the assigned equipment DAL/IDAL. For each CGP that is part of the technical configuration, the certification plan (or some other specific document identified by the applicant) should describe the means selected by the applicant to cover the certification issues addressed in this Certification Memorandum as well as the way in which the information that substantiates the achievement of the certification issues is planned to be presented. Early coordination with EASA of the selected means is recommended in order to reduce program risk.

11. Properly Overseeing Suppliers

11.1. Background

a. Many TC/STC/ETSO applicants have shifted system and hardware development, verification, and certification activities onto their aircraft/engine/propeller system suppliers and sub-tier suppliers. In the past, these suppliers participated in compliance activities only at their respective system, subsystem, or component levels. With airborne systems becoming increasingly more complex and integrated, and suppliers and sub-tier suppliers accepting these new responsibilities, EASA is concerned that their potential lack of expertise could result in incomplete or deficient certification activities.

b. Each responsibility that the applicant delegates to a supplier creates an interface with that supplier that needs to be validated and verified to ensure that the transition from the supplier's processes to the applicant's processes (or vice-versa) is accomplished correctly and accurately. Lack of proper validation and verification of life cycle data at the transition point may result in issues with regard to requirements, problem reporting, changes, etc.

c. Finally, retention of substantiating data, such as hardware life cycle data and other certification and compliance data, is a critical part of the certification process. When this data is retained by a sub-tier supplier, it may not be readily available to us. This may also affect the continued operational safety of the aircraft and its systems, especially with regard to in-service problems (service difficulties), problem resolution (service bulletins), and mandatory evolutions/corrections (airworthiness directives).

NOTE: The aim of this section is to explain EASA's concerns related to supplier oversight, but this section does not create any new needs or expectations in terms of procedures or documentation.

11.2. EASA Certification Policy

11.2.1. Supplier Oversight Aspects in Plans and Procedures

The applicant should create oversight plans and procedures that will ensure all suppliers and sub-tier suppliers will comply with all regulations, policy, guidance, agreements, and standards that apply to the certification program with regards to Hardware aspects of Certification. The applicable publications include, but are not limited to:

(2) EASA Certification Specifications;

(3)   EASA CRIs;

(4)   Applicant DOA procedures, airworthiness representative procedures, and memoranda of agreement;

In addition, coordination should be established between the applicant and the supplier regarding the following aspects:

(5)   Standards, plans, procedures and processes;

(6)   Process assurance plans, procedures, and processes;

(7)   Configuration management plans, procedures, and processes;

(8)   Standards for hardware development (including requirements, design, and coding standards); and

(9)   Process for hardware change impact analysis.

The applicant's planning documents, such as certification plans and Plans for Hardware Aspects of Certification (PHACs), should describe how the applicant will have visibility into their suppliers' and sub-tier suppliers' activities. The applicant should submit these plans for review and approval, preferably early in the program. The applicant should avoid making changes to the plans late in the program. If late changes are unavoidable, the applicant should allow adequate time for review and consideration.

11.2.2. Supplier oversight in the Applicant's plans

The applicant should address the following concerns in a supplier management plan or other suitable planning documents. The plan(s) should address the following areas:

1.   Visibility into compliance with regulations, policy, plans, standards, and agreements: The plan should address how the applicant will ensure that all applicable regulations, policy, plans, standards, CRIs, and memoranda of agreement are conveyed to, coordinated with, and complied with by main and sub-tier suppliers.

2.   Integration management: The plan should address how the system components will be integrated, and who will be responsible for validating and verifying the hardware and the integrated system. The plan should address:

   (a)   How requirements will be implemented, managed, and validated; including safety requirements, derived requirements, and changes to requirements;

   (b)   How the design will be controlled and approved;

   (c)   How the integration test environment will be controlled;

   (d)   How the hardware build and release process will be controlled (reconcile any differences between the supplier's and the applicant's release strategies);

   (e)   What product assurance activities that support the certification requirements will be conducted and who will be conducting them; and

   (f)   The applicant's strategy for integrating and verifying the system, including requirements-based testing and coverage analysis.

3.   Tasks and responsibilities in the oversight of suppliers: The plan should identify who the responsible parties are and what their responsibilities are, who the focal points are, and how their activities will be coordinated and communicated. It should also identify the parties involved in the review and assessment of hardware life cycle data as necessary for the applicant compliance demonstration.

4.   Problem reporting and resolution: The plan should establish a system to track problem reports. It should describe how problems will be reported between the applicant and all levels of suppliers. The problem reporting system should ensure that problems are resolved, and that reports and the

resulting changes are recorded in a configuration management system. The plan should describe how the responsible parties will oversee problem reporting.

5. Integration verification activity: The plan should identify who will be responsible for ensuring that all integration verification activities between all levels of suppliers comply with applicable guidance. It should describe how the responsible parties will oversee the verification process.

6. Configuration management: The plan should describe the procedures and tools to aid configuration management of all hardware life cycle data. It should describe how configuration control will be maintained across all sub-tier suppliers and how the persons responsible for certification will oversee configuration management.

7. Compliance substantiation and data retention: The plan should describe how the applicant will ensure that all supplier and sub-tier supplier compliance findings are substantiated and retained for the program. The plan should address, at minimum, the following certification data:

    (a)   Evidence that compliance has been demonstrated;

    (b)   Verification and validation data; and

    (c)   Hardware life cycle data.

The applicant's supplier management plan (or equivalent plans) should address the concern identified in paragraph 11.1.b. regarding the transition of life cycle data between the applicant's processes and the suppliers' processes. The plan should address the validation and verification of data with regard to all processes, including requirements management, problem reporting, use of standards, change impact, reviews, etc.

12. Oversight of AEH Change Impact Analyses used to Classify AEH Changes as Major or Minor

12.1. Background

ED-80/DO-254, Section 11.1.1, identifies analysis activities to be performed for proposed hardware changes. ED-80/DO-254 also states that re-verification should be accomplished on all hardware changes and areas affected by those changes.

Subpart D of Part 21 addresses the classification of changes to type design as minor or major. Paragraph 21A.91 proposes criteria for the classification of changes to a type design as minor or major.

The purpose of this classification is to determine the certification route to be followed in Part 21 Subpart D (either 21A.95 or 21A.97) or alternatively in Subpart E.

For approved ETSO articles, Subpart O of Part 21 addresses the classification of design changes.

12.2. Procedures

Detailed guidance for the classification of system changes to type design is given in GM 21A.91. However, in GM 21A, there is no detailed guidance on AEH changes classification and the proposal hereafter should be used to classify as major or minor such AEH changes.

Where a change is made to AEH produced in accordance with the guidelines of EUROCAE ED-80/RTCA DO-254, the change should be classified as major if any of the following applies:

1)   The AEH equipment or CBA, determined to be Level A or Level B in accordance with the guidelines, is changed and that change either:

    a)   introduces a new function;

    b)   introduces an aircraft/system functional limitation;

An agency of the European Union

c) requires an update of the certification process;

d) modifies a physical interface of the equipment or CBA;

e) impacts line or base maintenance;

f) involves an IC major change (see below);

or

2) The AEH Integrated Circuit, determined to be Level A or Level B in accordance with the guidelines, is changed unless that change involves only a variation of a parameter value in the HDL code within a range already verified for the previous certification standard;

or

3) The AEH, determined to be level C, is deeply changed (e.g. re-engineering process, introduction of new functions, etc.).

For AEH developed to guidelines other than ED-80/DO-254, the applicant should assess changes in accordance with the foregoing principles.

13. Guidelines on Management of Problem Reports

13.1. Background

Problems related to airborne electronic hardware may surface relatively late in the industrial development process. When these problems do not affect the safety of the aircraft/engine (and compliance with the EASA Certification Specifications has been demonstrated), the applicant may decide to propose for certification airborne software and electronic hardware devices that still have known problems.

For airborne electronic hardware, this situation is covered by ED-80/DO-254, section 10.9.3, as follows:

> *"Hardware status: this section [of the Hardware Accomplishment Summary- HAS-document produced for certification] contains a summary of problem reports unresolved at the time of certification, including a statement of functional limitations."*

Problems may arise due to the methods that are used by the suppliers and sub-tier suppliers of applicants for tracking and reporting problem reports. There may be inconsistencies in the reporting and tracking of problem reports and the tools that are used to track them between the applicant, their suppliers and their sub-tier suppliers. This may make it difficult for the applicant and the certification authority to gain an accurate picture of the number and the severity of the open problem reports across the various groups that are involved.

The use of suppliers and sub-tier suppliers may also result in situations where the sub-tier suppliers do not have sufficient knowledge and visibility of system level requirements and considerations when evaluating problem reports and their effects.

The intent of this section of this electronic hardware Certification Memorandum is to discuss the issues related to Problem Management for airborne electronic hardware.

13.2. Objectives

One of the principal objectives of any airborne electronic hardware development and approval should be to minimise the number and the severity of Open Problem Reports (OPRs) in any airborne electronic hardware release that is proposed for certification. The OPR management principles and assessment guidelines detailed in this section of this Certification Memorandum should not, in any case, be understood as a justification for an applicant to deviate from this prevailing objective.

This section of this Certification Memorandum has three purposes:

1. To clarify the role of the aircraft/engine manufacturer and the equipment supplier in the assessment of limitations of an item of equipment with embedded airborne electronic hardware because of known problems at the time of certification. It should be noted that even if the equipment supplier has sufficient knowledge to explain the functional effect of an OPR on the equipment/device, only the aircraft/engine manufacturer can assess or confirm the potential effect at the system/aircraft/engine level.

2. To facilitate the assessment of the acceptability of a baseline released with Open Problems reports, by defining a harmonized categorization of OPRs and an adequate means of recording the category of an OPR.

3. To clarify the aspects of problem reporting that should be covered in the plans of suppliers and sub-tier suppliers of the applicant.

13.3. Scope

This section of this Certification Memorandum is applicable to all systems containing digital equipment with a DAL/IDAL of A, B or C.

This Section is not applicable to digital equipment of DAL/IDAL D except for equipment containing both DAL/IDAL D items and items of higher DALs/IDALs.

13.4. Terminology

The text in italics in the definitions below is extracted from the glossary of ED-80/DO-254.

- **Problem report**: any of the following features: error, fault, failure, deviation from the rules

- **Error**: *a mistake in requirements, design or implementation*

- **Fault**: *(1) A manifestation of a flaw in hardware due to an error or random event. A fault, if it occurs, may cause a failure. (2) An undesired anomaly in a device.*

- **Failure**: *The inability of a system or system component to perform a required function within specified limits. A failure may be produced when a fault is encountered.* A failure is a manifestation of a fault at system level. But a fault may also remain hidden at system level and have no operational consequences.

- **Failure condition**: *The effect on the aircraft and its occupants both direct and consequential caused or contributed to by one or more failures, considering relevant adverse operational and environmental conditions.* A failure condition is classified according to the severity of its effect as defined in FAA AC25.1309 or AMC 25.1309.

- **Deviation from the rules**: a non-conformity of the development process with the plans, development standards, applicable CRIs. In the particular case where a non-conformity with the plans or development standards is intentional and the plans or development standards are planned to be modified accordingly, such a non-conformity might not be recorded as a problem, but instead be identified and justified in the compliance status of the HAS.

- **Open Problem Report (OPR)**: a problem which has not been corrected at the time the airborne electronic hardware is presented for approval.

13.5. Typology of Open Problem Reports

A logged OPR should be categorized according to the nature and effect of the OPR. One possible way to classify OPRs that is acceptable to EASA is as follows:

- **Type 0**: a problem whose consequence is a failure – under certain conditions - of the system, with a safety impact.

- **Type 1**: a problem whose consequence is a failure – under certain conditions - of the system, having no safety impact on the aircraft/engine. (This needs to be confirmed by the aircraft/engine manufacturer). If agreed between the aircraft/engine manufacturer and the equipment/hardware supplier, this type should be divided into two sub-types:

    o **Type 1A**: a failure with a "significant" functional consequence; the meaning of "significant" should be defined in the context of the related system in agreement between the aircraft/engine manufacturer and the equipment/hardware supplier (for instance a "cockpit effect").

    o **Type 1B**: a failure with no "significant" functional consequences.

- **Type 2**: a fault which does not result in a failure (i.e.: no system functional consequences and the fault is not detectable by the crew in any foreseeable operating conditions).

- **Type 3**: Any problem which is not of type 0, 1 or 2, but which is a deviation from the rules (i.e. the plans or hardware development standards, applicable CRIs). If agreed between the aircraft/engine manufacturer and the equipment/hardware supplier, this type should be divided into two sub-types:

    o **Type 3A:** a "significant" deviation, whose effects could be to lower the assurance that the airborne electronic hardware behaves as intended and has no unintended behaviour.

    o **Type 3B:** a "non-significant" deviation from the methodology (plans) that does not affect the assurance obtained.

13.6. Guidelines on OPR Management

EASA considers that, as far as possible, a root cause analysis should be performed for all OPRs, except in exceptional cases where a root cause analysis is not feasible. Any such infeasibility should be justified. In the cases of Types 0, 1 or 2, this root cause analysis should lead to the identification of the corresponding error (e.g. in the VHDL code) and of any associated methodological deviations. For Type 3 problems, the root cause analysis consists of the identification of the methodological deviation associated with the problem.

All OPRs should be categorized according to the typology of problems defined in this Section, or an equivalent typology. If an equivalent typology is proposed, any new type(s) should correspond to only one of the types (0, 1, 2 or 3) as defined in this section of this Certification Memorandum.

All OPRs should be described in order to substantiate their categorization into adequate types; this description should be recorded.

When previously developed airborne hardware is used, previously existing OPRs should be reassessed in the operational environment of the aircraft/engine to be certified.

In order to avoid decreasing the assurance of the quality of the airborne hardware to be certified due to an increasing number of OPRs, the following objectives should be taken into account and acted upon:

- Limitations should be removed at the earliest opportunity.

- Conformity with the specifications should be restored at the earliest opportunity.

- Any OPR should be rectified within a time period compatible with its assessed consequences.

Per ED-79/ARP4754 section 9.2.2 and ED-79A / ARP 4754A section 5.6.2.4, problem reporting should be managed at the system level.

The following type-based objectives should be taken into account:

- Type 0: such OPRs should be rectified before certification or an adequate means of mitigation (for instance, operating limitations,) should be proposed such that there are no adverse effects on safety at the aircraft/engine level.

- Type 0 and 1: Potential effects should be assessed at the system level and, if necessary, at the aircraft/engine level. If necessary, appropriate limitations should be defined in order to ensure there are no adverse effects on safety.

- Type 1: Any claim that an OPR has no safety impact on the aircraft/engine should be justified; this justification should be recorded.

- Type 2: The justification that the error cannot cause a failure should be recorded. For simple cases, this justification may be a simple statement based on engineering judgement. In some specific cases, this justification may imply that some specific additional validation and/or verification activities need to be performed.

13.7. Contents of the Hardware Accomplishment Summary (HAS)

All OPRs of types 0 to 3 should be recorded in the HAS or the equivalent certification document, along with the following information:

- Supplier's identification of the OPR (configuration management number)

- Type of OPR

- Short description (including a brief summary of the root cause, where available)

- Date when the OPR was opened

- Depending on the typology (section 13.5), scheduled closure date for the OPR

- Brief justification as to why it can be left open

- Means of mitigation to ensure there are no adverse safety effects - if applicable

- Interrelationships between OPRs - if applicable.

Although a limited number of type 2 or 3 OPRs should normally not prevent certification, a large number of type 2 or 3 OPRs, or a lack of action plans for the closure of type 2 and 3 OPRs are general indicators of a lack of hardware assurance. The EASA team may reject a request for certification if the number of remaining OPRs is too high, or if there is no evidence of an adequate action plan to close the OPRs.

13.8. Content of System Certification Summary or Equivalent Document

The System Certification Summary or an equivalent certification document should describe:

- The identification of all type 0 and 1 OPRs and the description of their impact at the system level or, if necessary, at the aircraft/engine level (including, any associated operational limitations and procedures).

13.9. Oversight of Problem Reporting

13.9.1. Problem Reporting and Supplier Plans

In order to ensure that hardware problems are consistently reported and resolved, and that hardware development assurance is accomplished before certification, the applicant should discuss in their hardware Configuration Management Plan, or other appropriate planning documents, how they will oversee their supplier's and sub-tier supplier's hardware problem reporting process. The engineer responsible for certification should review the plans and verify that they address the following to their satisfaction:

1) The plans should describe each of the applicant's supplier's and sub-tier supplier's problem reporting processes that will ensure problems are reported, assessed, resolved, implemented, re-verified (regression analysis), closed, and controlled. The plans should consider all problems related

to hardware, LRUs, CBAs, ASICs/PLDs and COTS used in any systems and equipment installed on the aircraft.

2) The plans should establish how problem reports will be categorized so that each problem report can be classified accordingly. The categories described above should be used.

3) The plans should describe how the applicant's suppliers and sub-tier suppliers will notify the applicant of any problems that could impact safety, performance, functional or operational characteristics, hardware assurance, or compliance.

   a) The applicant may enter such problems into their own problem reporting and tracking system. If so, the plan needs to describe how this is accomplished. If the supplier's problem reporting system is not directly compatible with the applicant's system, the plan needs to describe a process for verifying the translation between problem reporting systems.

   b) The applicant may allow their suppliers and sub-tier suppliers to have access to their own problem reporting system. Doing so may help the applicant ensure that they will properly receive and control their supplier's problem reports. If the applicant allows this, they should restrict who has such access in order to maintain proper configuration control, and their suppliers should be trained on the proper use of the reporting system.

   c) The plans should describe any tools that the applicant's suppliers or sub-tier suppliers plan to use for the purpose of recording action devices or observations for the applicant to review and approve prior to entering them into the applicant's problem reporting system.

   d) The plans should state that suppliers will have only one problem reporting system in order to assure that the applicant will have visibility into all problems and that no problems are hidden from the applicant.

   e) Any problems that may influence other applications, or that may have system-wide influence should be made visible to the appropriate disciplines.

4) The plans should describe how flight test, human factors, systems, software, hardware and other engineers of the appropriate disciplines will be involved in reviewing each supplier's and sub-tier supplier's problem report resolution process. They should also describe how these engineers will participate in problem report review boards and change control boards.

5) The plans should establish the criteria that problem report review boards and change control boards will use in determining the acceptability of any open problem reports that the applicant will propose to defer beyond certification.

   a) These boards should carefully consider the potential impacts of any open problem reports on safety, functionality, and operation.

   b) Since a significant number of unresolved problem reports indicate that the hardware may not be fully mature and its assurance questionable, the applicant should describe a process for establishing an upper boundary or target limit on the number of problem reports allowed to be deferred until after type certification.

   c) Depending on the typology (section 13.5), the plan should establish a means of determining a time limit by which unresolved problem reports deferred beyond certification will be resolved. This applies to problem reports generated by the applicant, suppliers, and sub-tier suppliers.

13.9.2. Reviewing Open Problem Reports

The applicant responsible for certification should be involved in certain decisions related to open problem reports prior to certification and should:

1) Review, as appropriate, any problem reports that are proposed for deferral beyond certification. If he/she has concerns that safety might be impacted, the deferral of specific problem reports may be disallowed.

2) If the supplier is using previously developed hardware, they should ensure that the applicant has reassessed any open problem reports for their potential impact on the aircraft or system baseline to be certified.

3) Ensure that the supplier has considered the inter-relationships of multiple open problem reports and assessed whether any open problem report has become more critical when considered in conjunction with another related problem report.

4) Ensure that the supplier has reviewed any open problem reports related to airworthiness directives, service bulletins, or operating limitations and other mandatory corrections or conditions. The supplier may need help to determine which problems to resolve before certification.

5) Review any open problem reports with potential safety or operational impact to determine if operational limitations and procedures are required before EASA test pilots participate in test flights. Other technical experts should be involved as necessary in making this determination.

6) Ensure that the supplier has complied with ED-80/DO-254, section 10.9.3.

14. Remarks

1. Suggestions for amendment(s) to this EASA Certification Memorandum should be referred to the Certification Policy and Safety Information Department, Certification Directorate, EASA. E-mail CM@easa.europa.eu.

2. For any question concerning the technical content of this EASA Certification Memorandum, please contact:

Name, First Name: Senéchal, Anne

Function: Senior Expert Airborne Electronic Hardware & Project Certification Manager

Phone: +49 (0)221 89990 4372

E-mail: Anne.SENECHAL@easa.europa.eu