Notification of a Proposal to issue a Certification Memorandum

Certification Aspects of Integrated Modular Avionics

EASA Proposed CM No.: Proposed CM-AS-005 Issue 01 issued 29 April 2015

Regulatory requirement(s): **CS 23.1301, CS 25.1301, CS 27.1301, CS 29.1301**
CS 23.1302, CS 25.1302, CS 27.1302, CS 29.1302
CS 23.1309, CS 25.1309, CS 27.1309, CS 29.1309
CS 23.1322, CS 25.1322, CS 27.1322, CS 29.1322

In accordance with the EASA Certification Memorandum procedural guideline, the European Aviation Safety Agency proposes to issue an EASA Certification Memorandum (CM) on the subject identified below. All interested persons may send their comments, referencing the EASA Proposed CM Number above, to the e-mail address specified in the "Remarks" section, prior to the indicated closing date for consultation.

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.

Log of issues

Issue	Issue date	Change description
01	29.04.2015	First issue.

Table of Content

1. Introduction

1.1. Purpose and scope

The purpose of this Certification Memorandum is to support the airworthiness approval of Integrated Modular Avionics (IMA) systems.

It proposes a way to identify when a system may be considered as an IMA or not.

Finally it suggests supplements to EUROCAE ED-124 as an Acceptable Means of Compliance for the approval of IMA. This Certification Memorandum amends, complements and gives further guidance on the following particular aspects:

- scope of certification credit,
- TSO and ETSO aspects.

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-124	Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations	---	**Error! Reference source not found.**	June 2007
AMC 20-115()	Software considerations for certification of airborne systems and equipment	---	3.1	Latest
ED-80	Design Assurance Guidance for Airborne Electronic Hardware	---	3.1	April 2000
ED-79()	Guidelines for Development of Civil Aircraft and Systems	---	3.1	Latest
ARINC 653	Avionics Application Software Standard Interface	---	1.3 2.2	March 2006

The Agency is also developing:

- ETSO-2C153 for authorisation of IMA modules at part level, through RMT.0456;
- Certification specifications for assembly of ETSO articles providing aircraft functions, into an IMA system, to be included in CS-ETSO Subpart A (ref. RMT.0621); and
- AMC 20-170 offering guidance for integration of IMA at product level, through RMT.0622 (NPA expected in 2015).

1.3. Abbreviations

IMA — Integrated Modular Avionics

EASA — European Aviation Safety Agency

APEX	Application programming interface called APplication EXecutive as per ARINC 653
AMC	Acceptable Means of Compliance (to a certification specification as in CS-25 book 1)
LRU	Line Replaceable Unit
RSC	Reused Software Component

1.4. Definitions

Aircraft Function	The capability of the aircraft that may be provided by the hardware and software of the systems on the aircraft. Functions include flight control, autopilot, braking, fuel management, flight instruments, etc. IMA has the potential to broaden the definition of avionics to include any aircraft function. [ED-124]
Application	Software and/or application-specific hardware with a defined set of interfaces that, when integrated with a platform, performs a function. [ED-124]
Component	A self-contained hardware part, software part, database, or combination thereof that is configuration controlled. A component does not provide an aircraft function by itself. [ED-124]
IMA System	Consists of an IMA platform(s) and a defined set of hosted applications. [ED-124]
Incremental certification	A process for obtaining credit toward certification by accepting that an IMA module, application, and/or off-aircraft IMA system complies with specific requirements. This incremental certification is divided into tasks. Credit granted for individual tasks contributes to the overall certification goal. Incremental certification provides the ability to integrate and accept new applications and/or modules, in an IMA system, and maintain existing applications and/or modules without the need for re-doing certification compliance demonstration.
Interoperable	The capability of several integrated modules to operate together to accomplish a specific goal or function. This requires defined interface boundaries between the modules and allows the use of other interoperable components. To describe this concept in physical terms, an IMA platform may include interoperable modules and components such as physical devices (processor, memory, electrical power, Input/Output (I/O) devices), and logical elements, such as an operating system, and communication software. [ED-124]
Module	A component or collection of components that may be accepted by themselves or in the context of IMA. A module may also comprise other modules. A module may be software, hardware, or a combination of hardware and software, which provides resources to the IMA-hosted applications. Modules may be distributed across the aircraft or may be co-located. [ED-124]
Partitioning and Robust Partitioning	Partitioning is an architectural technique to provide the necessary separation and independence of functions or applications to ensure that only intended coupling occurs. [ED-124] Robust partitioning is a means for assuring the intended isolation in all circumstances (including hardware failures, hardware and software design errors, or anomalous behaviour) of aircraft functions and hosted applications using shared resources. The

objective of robust partitioning is to provide an equivalent level of functional isolation and independence as a federated system implementation. [ED-124]

2. Background

The use of IMA has rapidly expanded in the last two decades and is expected to progress even more in the future in all types of products, parts and appliances. From a regulatory standpoint, there are not yet specific requirements adopted within the current EASA Certification Specifications or in AMC 20 series for the certification aspects of IMA. Additional guidance is hence needed to address specific aspects at application, component, platform, system, and aircraft level.

2.1. IMA overview

IMA is a shared set of flexible, reusable and interoperable hardware and software resources that, when integrated, form a system that provides computing resources and services to hosted applications performing aircraft functions [ED-124]. In other words IMA architecture integrates several aircraft functions on the same platform, provided by different hosted applications that historically have been contained in functionally and physically separated 'boxes' or LRUs.

2.2. IMA characteristics

The purpose of this section is to list key characteristics of IMA to help identifying when it starts to be beneficial following guidance of ED-124.

One difficulty encountered during certification exercises is to assess if the system under consideration is an IMA or not. Defining with precision what is an IMA system is not easy as there are as many possible definitions as there are implemented architectures. Several characteristics of an IMA system may be found either in a single hardware platform having a single APEX and one or several hosted applications, in a more complex system having several platforms working concurrently and communicating together or in a larger system of distributed sub IMA systems. ED-124 Annex D presents some IMA examples:

1. a single LRU platform,
2. a distributed IMA platform,
3. a distributed complex IMA system,
4. a software designed radio platform.

Despite the informative nature of those examples, they may not represent a sufficient subset of IMA systems to help to decide whether or not a system is an IMA. One of the intent of this Certification Memorandum is to proposes a list of IMA characteristics to help the applicant and the certification authority in agreeing on the IMA nature of the system under consideration. When taken individually those characteristics may be addressed in other guidance (like ED-12C or ED-80) and this Certification Memorandum may look inappropriate or over specifying, but when combined with other characteristics, it is getting more difficult to rely solely on a dedicated single guidance. The list of IMA characteristics is compiled from elements found in section 2.3 of ED-124 and complemented as follow:

1	Incremental certification.
2	Multiple applications sharing common platform resources (power, CPU, memory, I/O, buses, etc.).
3	Platform are configurable to allow resources allocation to hosted application's requirements.

4	Robust partitioning of shared resources.
5	Presence of an Application Platform Interface (API) like the ARINC 653 to provide isolation between platform and applications.
6	Different stakeholders in the process, from conceptual design to retirement from service (applicant, system integrator, platform and module suppliers, application suppliers, maintenance organisation).
7	An application may be designed, verified and integrated independently of other applications, platforms or modules.
8	An application is designed to be modular for use on different products.
9	Presence of a shared communication network used as a means for data communication between platforms/modules and/or applications (ARINC 664).
10	Fault management and health monitoring capability.
11	Multiple applications implementing different high-level system or aircraft functions, running in different partitions.

2.3. Use cases

This section presents three typical case studies with associated IMA characteristics taken from existing certification applications that were identified as IMA that can be used as reference.

Case 1: a large distributed system using common platform with several function developed by different stakeholders. All the functions communicate via an ARINC 664 network and contain means, on the platform and in a dedicated function, to detect, isolate and report the faults in the systems or functions. This architecture has the following characteristics of IMA:

- Asks the benefits of incremental certification [1],
- Contains computing modules with identical API (ARINC 653) [3, 4, 5, 7] ,
- Every module may contain several independent aircraft functions [2],
- Several stakeholders in the process (several module suppliers, several module integrator, one system designer, several function suppliers) [6],
- Contains data concentrators [2],
- May be installed on several product [8],
- Presence of a shared communication network [9],
- Central maintenance system with platform BITE [10].

Case 2: a medium distributed system using shareable resources.

This system consists of components that can be integrated by adding or removing elements of the system configuration without any impact on other components. In its certified version, it consists of two displays with two processing units in each and two general purpose computing modules with also two processing units. All computing modules communicate via ARINC 429 or discrete. There is no backbone avionics network. All functions can be installed in any ARINC 653 partition, the limiting factor is the close link between platform and external resources due to lack of common avionics network. This architecture has the following characteristics of IMA:

- Benefits from incremental certification of component / application / system[1],
- Contains computing modules with identical API (ARINC 653) [3, 4, 5, 7],
- Every module may contain several independent aircraft functions [2],
- Several stakeholders in the process (one platform supplier one system designer, but several function suppliers) [6].

Case 3: a display unit with non-display functions.

A display unit (DU) that provides classical “display” functions (like Primary Flight Display / Multi-Function Flight / navigation Display, etc.) and that contains a provision for extension to other applications, completely independent from the already installed ones. All those functions are hosted as applications inside the DU on top of and ARINC 653 compliant operating system, ensuring the robust time and space partitioning.

An applicant may install an API compliant function in the equipment, for example a Synthetic Vision Display (SVS), a surveillance function (like a weather radar, an enhanced aircraft stability function, or any other independent function). This architecture has the following characteristics of IMA:

- Asks the benefits of incremental certification, the already installed function does not have to be reassessed [1],
- Contains several applications sharing the same resources [2, 3, 4, 5, 7],
- Several stakeholders in the process (one system supplier but several function suppliers) [6].

2.4. Characterisation principles

The characteristics listed in section 2.2 and the typical use-cases of section 2.3 show that some characteristics are typical of an IMA when other, despite they are found on other federated architecture, are also encountered often in IMA systems. This led us to consider two categories:

1. The characteristics that are "IMA typical", deemed sufficient alone to characterize the system as IMA and trigger the need for ED-124 guidance. This category includes characteristics [1], [7], [8] and [11]. If one of these characteristics is met, the system should be classified as IMA and the guidance from section 3 of this Certification Memorandum could be followed to facilitate the certification process.
2. The characteristics that are "IMA related" as they are necessary to ensure safe implementation if the system is an IMA but not sufficient alone to define an IMA (these could be also met by a single LRU system). This category includes characteristics [2], [3], [4], [5], [6], [9] and [10]. If one or more of these characteristics are met but none of the characteristics that are IMA typical is met, early discussion should take place between the applicant and the Agency in order to determine whether the system under consideration should be classified as an IMA system or not.

3. EASA Certification Policy

3.1. EASA Policy

3.1.1. Recognition of ED-124

This EASA Certification Memorandum should be used in conjunction with EUROCAE standard ED-124 on ‘Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations’, published in July 2007. ED-124 (equivalent to the RTCA standard DO-297) provides guidance and means of compliance for the development and certification of IMA architectures. These guidance and means of compliances are considered acceptable by EASA for the certification of IMA systems when used with the supplement described in section 3.1.2 of this document, when the system under consideration has been identified as having sufficient IMA characteristics as described in section 2.2.

ED-124 references other EUROCAE documents at their latest version. This may be understood by some applicants as a request to use today ED-79A/ARP 4754A, ED12C, etc. which may be misleading. In the context of this Certification Memorandum it should be understood that document referenced [1] to [8] in ED-124 should use the applicable version in accordance with the certification basis and related guidance material.

Documents referenced [9], [10] and [11] in ED-124 are out of the scope of this Certification Memorandum.

3.1.2. Amendments to ED-124

This Certification Memorandum amends the ED-124 in the following areas:

- Incremental certification process,
- Failure modes and Flight Crew Annunciation and Messaging,
- Specific analysis,
- Configuration data / parameter data item.

3.1.2.1. Incremental certification process

The incremental certification process is the process to certify aircraft systems embedding digital equipment for which EASA agrees to grant some certification credit for the previously qualified component/module, application or system, before that module, application or system is configured and integrated at product level.

This process is presented in document ED-124, but some wording and concepts presented in this section are not compatible with EASA system, in particular:

- The concept of “letter of acceptance” is not feasible in EASA system. The certification credit granted by EASA is only limited to a specific aircraft type certification (TC), or to a subsequent aircraft level certification of a system modification (MOD) or in the frame of a Supplemental Type Certificate (STC). Pending adoption of ETSO-2C153, there is currently no means to benefit from the certification credit granted within a S(TC) in the frame of another product certification project. Nevertheless, it does not prevent the use of previous certification documentation in further projects, as applicable. The applicant remains responsible for the content of the data, it has to be reviewed as being reusable in the context of the new certification exercise.
- The alternate concept of Reusable Software Component (RSC) acceptance as described in ED-124 section 4, table 4 with reference to FAA AC 20-148 is not feasible in EASA context as it makes use of acceptance letter for software parts. It does not prevent the use of previous software certification documentation in further projects, as applicable. The applicant remains responsible for the content of the data, it has to be reviewed as being reusable in the context of the new certification exercise.

3.1.2.2. Failure modes and flight crew annunciation and messaging

Section 3.6.5 of EUROCAE ED-124 deals with how the IMA and, if available, a Health monitoring and Fault Management function, should present the failures annunciation to the crew. CS XX.1322 and associated AMC address also flight crew alerting systems or warning, caution, and advisory lights. In the case where inconsistency between the text in ED-124 and the text in CS XX.1322 and associated AMC would be identified, the text in the CS XX.1322 and associated AMC should prevail.

3.1.2.3. Specific analyses

ED-124 introduces the need for some specific analyses that are necessary to provide confidence in the correct behaviour or the function: in particular, the Worst Case Execution Time (WCET), Robust Partitioning and Usage Domain analyses require particular attention.

In the frame of certification activities, EASA may ask to review those analyses. The level of detail should allow a correct understanding of the platform design, validation and verification activities.

3.1.2.4. Configuration data / parameter data item

IMA configuration data are described in ED-124 section 3.7.1.1 at IMA system level (platform, module) and 3.7.1.2 (Application). Those data are today referenced as Parameter Data Item in ED-12 and should have the same consideration as other element of the software. Depending on how the parameter data item is to be used in the IMA system or application, they need to be defined, managed and documented at their appropriate level (platform, module, application) and follow the ED-12C guidance including the process to ensure mixability and compatibility during post-TC as indicated in ED-124. Particularly, any parameter data item should be assigned the same software level as the software component using it.

3.1.3. Clarification on ED-124

Section 2.2 of ED-124 introduces the notion of composability, where integration of a new application does not invalidate any verified requirements of an already integrated application. Some clarification is needed here, that when composability is used, it means the capability to take credit of the robust partitioning on two aspects:

- during the development of the application itself, credit may be taken on design activities,
- during the verification activities, credit may be taken on integration of the application and on non-impact on other already verified and installed applications.

The applicant strategy on the credit expected “incremental development” and “incremental verification” strategy should be addressed in the IMA plans (e.g., in the IMAVVP).

3.1.4. TSO and ETSO aspects

Today ETSO-2C153 for hardware components of IMA, equivalent to the FAA TSO C153, is still in draft. Therefore no credit can be granted on EASA product certification from TSO C153. It does not prevent the re-use of TSO data package during the installation of IMA components. The applicant remains responsible for the content of the data, it has to be reviewed as being reusable in the context of the new certification exercise.

EASA rulemaking task RMT.0456 is developing an ETSO for future authorisations of IMA platform/ module level independent from aircraft. This Certification Memorandum will be updated accordingly when the ETSO for IMA module is available.

3.2. Who this Certification Memorandum affects

This Certification Memorandum is primarily aimed at applicants for Type Certificates (TC), Supplemental Type Certificates (STC), of any aviation product implementing a system or an equipment having all or partial IMA characteristics as described in [2.2 IMA Characteristics].

It may be of interest to installers, integrators and suppliers of systems, components and applications having full or partial IMA characteristics as described in [2.2 IMA Characteristics].

4. Remarks

1. This EASA Proposed Certification Memorandum will be closed for public consultation on the **10th of June 2015**. Comments received after the indicated closing date for consultation might not be taken into account.

2. Comments regarding this EASA Proposed Certification Memorandum should be referred to the Certification Policy and Safety Information Department, Certification Directorate, EASA. E-mail CM@easa.europa.eu or fax +49 (0)221 89990 4459.

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

   Name, First Name: ROSAY, Cyrille

   Function: Senior Expert Cybersecurity

   Phone: +49 (0)221 89990 4045

   E-mail: cyrille.rosay@easa.europa.eu