The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Equipement de l'Aviation Civile

INTEGRATED MODULAR AVIONICS (IMA) DEVELOPMENT GUIDANCE AND CERTIFICATION CONSIDERATIONS

ED-124

June 2007

102, rue Etienne Dolet
92140 MALAKOFF, FRANCE
Web Site : www.eurocae.net

Tel : 33 1 40 92 79 30
Fax : 33 1 46 55 62 65
Email : eurocae@eurocae.net

INTEGRATED MODULAR AVIONICS (IMA) DEVELOPMENT GUIDANCE AND CERTIFICATION CONSIDERATIONS

ED-124

June 2007

TABLE OF CONTENTS

FOREWORD VI

EXECUTIVE SUMMARY VII

CHAPTER 1 INTRODUCTION 1
1.1 PURPOSE 1
1.2 SCOPE 1
1.3 BACKGROUND 2
1.4 RELATIONSHIP TO OTHER DOCUMENTS 2
1.5 REFERENCES 3
1.6 HOW TO USE THIS DOCUMENT 3

CHAPTER 2 INTEGRATED MODULAR AVIONICS OVERVIEW 5
2.1 IMA DESIGN AND CERTIFICATION TERMINOLOGY 5
2.1.1 IMA Design Terminology 5
2.1.2 Certification Terminology 7
2.2 ARCHITECTURAL CONSIDERATIONS 8
2.3 KEY CHARACTERISTICS 8
2.3.1 Platforms and Hosted Applications 9
2.3.2 Shared Resources 10
2.3.3 Robust Partitioning 11
2.3.4 Application Programming Interface (API) 11
2.3.5 Health Monitoring and Fault Management 11
2.4 STAKEHOLDERS 12
2.4.1 Certification Authority 12
2.4.2 Certification Applicant 12
2.4.3 IMA System Integrator 13
2.4.4 Platform and Module Suppliers 13
2.4.5 Application Supplier 13
2.4.6 Maintenance Organization 13

CHAPTER 3 GENERAL DEVELOPMENT CONSIDERATIONS 14
3.1 IMA SYSTEM DEVELOPMENT PROCESS 15
3.1.1 IMA Platform Development Process 15
3.1.2 Hosted Application Development Process 17
3.1.3 IMA System Development Process 17
3.2 IMA SYSTEM RESOURCE ALLOCATION ACTIVITIES 19
3.3 AIRCRAFT SAFETY AND SECURITY 20
3.4 DEVELOPMENT ASSURANCE AND TOOL ASSURANCE 20
3.5 PARTITIONING AND RESOURCE MANAGEMENT ACTIVITIES 20
3.5.1 Design for Robust Partitioning 22
3.5.2 Partitioning Analysis 23
3.6 HEALTH MONITORING AND FAULT MANAGEMENT 25
3.6.1 Components and Aspects to be Monitored 25
3.6.2 Health Determination of Each Application 26

3.6.3 Health Determination of the IMA System as a Whole 26
3.6.4 Response to Each Type of Failure 26
3.6.5 Flight Crew Annunciation and Messaging 26
3.6.6 Control of Maintenance Actions and Reporting 27
3.6.7 Redundancy Management 27
3.6.8 Single Event Upset (SEU) Faults 28
3.7 IMA SYSTEM CONFIGURATION MANAGEMENT 28
3.7.1 Configuration Data 29
3.8 GUIDANCE ON USE OF SHARED DATABASES 30
3.9 MASTER MINIMUM EQUIPMENT LIST (MMEL) 30
3.9.1 Design Considerations for MMEL 30
3.9.2 Approval Considerations for an MMEL 30
3.10 HUMAN FACTORS CONSIDERATIONS 31
CHAPTER 4 CERTIFICATION TASKS 33
4.1 OVERVIEW OF THE CERTIFICATION PROCESS 33
4.2 TASK 1 – MODULE ACCEPTANCE 35
4.2.1 Module Acceptance Objectives 35
4.2.2 Module Acceptance Data 36
4.2.3 Module Acceptance Plan (MAP) 36
4.2.4 Module Requirements Specification (MRS) 38
4.2.5 Module Validation and Verification (V&V) Data 39
4.2.6 Module Quality Assurance (QA) Records 40
4.2.7 Module Configuration Index (MCI) 40
4.2.8 Module Acceptance Configuration Management (CM) Records 40
4.2.9 Module Acceptance Accomplishment Summary (MAAS) 40
4.2.10 Module Acceptance Data Sheet (MADS) 41
4.2.11 Module Problem Reports 42
4.2.12 Additional Module Acceptance Life Cycle Data 42
4.3 TASK 2 – APPLICATION ACCEPTANCE 42
4.3.1 Application Acceptance Objectives 43
4.3.2 Application Acceptance Data 43
4.4 TASK 3 – IMA SYSTEM ACCEPTANCE 44
4.4.1 IMA System Acceptance Objectives 44
4.4.2 IMA System Acceptance Data 44
4.4.3 IMA System Certification Plan (IMASCP) 45
4.4.4 IMA System Validation and Verification Plan (IMASVVP) 46
4.4.5 IMA System Configuration Index (IMASCI) 46
4.4.6 IMA System Accomplishment Summary (IMASAS) 47
4.4.7 Other IMA System Life Cycle Data 47
4.5 TASK 4 – AIRCRAFT INTEGRATION OF IMA SYSTEM (INCLUDING V&V) 47
4.5.1 Aircraft Integration Objectives 48

4.5.2 Aircraft-level IMA System Compliance Data 48
4.5.3 Aircraft-level IMA System Certification Plan (IMASCP) 49
4.5.4 Aircraft-level IMA Validation & Verification Plan..... 49
4.5.5 Aircraft-level IMA System Configuration Index (IMASCI)..... 49
4.5.6 Aircraft-level IMA System Accomplishment Summary (IMASAS)..... 49
4.5.7 Other Aircraft-level Data..... 49
4.6 TASK 5 – CHANGE..... 50
4.6.1 Changes to IMA System Modules, Resources and Applications..... 50
4.6.2 Change Objectives..... 50
4.6.3 Change Management Process..... 50
4.6.4 Change Impact Analysis (CIA)..... 52
4.6.5 Change Data..... 53
4.7 TASK 6 – REUSE OF MODULES OR APPLICATIONS..... 53
4.7.1 Objectives of the Reuse Process..... 53
4.7.2 Reuse of a Software Module or Application..... 54
4.7.3 Reuse of a Complex Electronic Hardware Module or Application 54
4.7.4 Reuse of Environmental Qualification Test Data..... 55
4.7.5 Reuse of a Module that Contains Software and Hardware..... 55
4.7.6 Reuse Compliance Data..... 55
CHAPTER 5 INTEGRAL PROCESSES..... 57
5.1 SAFETY ASSESSMENT..... 57
5.1.1 Responsibilities of the Certification Applicant..... 57
5.1.2 Responsibilities of the IMA System Integrator..... 58
5.1.3 Responsibilities of the IMA Platform Supplier..... 58
5.1.4 Responsibilities of the Application Supplier..... 58
5.1.5 Safety Assessment Activities..... 59
5.2 SYSTEM DEVELOPMENT ASSURANCE..... 63
5.2.1 Software Guidance..... 63
5.2.2 Electronic Hardware Guidance..... 63
5.2.3 Integration Tool Qualification..... 63
5.2.4 Shared Design Assurance..... 64
5.2.5 IMA System Configuration Management..... 64
5.2.6 Environmental Qualification Testing (EQT)..... 64
5.3 VALIDATION..... 65
5.4 VERIFICATION..... 66
5.5 CONFIGURATION MANAGEMENT (CM)..... 68
5.5.1 IMA System Configuration Management Plan..... 68
5.5.2 Configuration Control..... 69
5.6 QUALITY ASSURANCE (QA)..... 69
5.7 CERTIFICATION LIAISON..... 70
5.7.1 Certification Liaison Process..... 70

5.7.2 Means of Compliance and Planning Data 70
5.7.3 Development Life Cycle Data 71
5.7.4 Compliance Substantiation 72
5.7.5 Life Cycle Data Submittals 73
5.7.6 Certification Liaison Process When Changes Are Made 74
5.7.7 Certification Liaison Process For Reuse of Modules 74

CHAPTER 6 CONSIDERATIONS FOR CONTINUED AIRWORTHINESS OF IMA SYSTEMS 75
6.1 TRAINING 75
6.2 MAINTENANCE 75
6.3 POST-CERTIFICATION MODIFICATIONS 76

ANNEX A OBJECTIVE TABLES 77

ANNEX B GLOSSARY OF TERMS 86

ANNEX C LIST OF ABBREVIATIONS AND ACRONYMS 96

ANNEX D IMA SYSTEM DESIGN EXAMPLES 99
D.1 EXAMPLE 1: SINGLE LRU PLATFORM 99
D.1.1 Purpose of this example 99
D.1.2 Definition of platform and modules 99
D.1.3 Key characteristics of IMA found in this system 100
D.2 EXAMPLE 2: DISTRIBUTED IMA PLATFORM 101
D.2.1 Purpose of this example 101
D.2.2 Definition of platform and modules 101
D.2.3 Key characteristics of IMA found in this system 102
D.3 EXAMPLE 3: IDENTIFYING BOUNDS OF A DISTRIBUTED COMPLEX IMA SYSTEM 104
D.3.1 Purpose of this example 104
D.3.2 Definition of platform and modules 104
D.3.3 Key characteristics of IMA found in this system 104
D.4 EXAMPLE 4: SOFTWARE DESIGNED RADIO EXAMPLE 106
D.4.1 Purpose of this example 106
D.4.2 Definition of platform and modules 106
D.4.3 Key characteristics of IMA found in this system 107

LIST OF WORKING GROUP 60 MEMBERS 108

LIST OF FIGURES

Figure 1: Chapters and their relationships	4
Figure 2: Relationship of IMA design terms	6
Figure 3: Example of a typical design highlighting potential shared resources	14
Figure 4: IMA system certification tasks illustration	33
Figure 5: Planning data for IMA system	71
Figure 6: Life cycle data for IMA system	72
Figure 7: Compliance summaries for IMA	73
Figure D-1: Configured single LRU platform	100
Figure D-2: Distributed modular platform	101
Figure D-3: Common module structure	102
Figure D-4: Distributed complex IMA system	104
Figure D-5: Fault reporting hierarchy	105
Figure D-6: SDR IMA platform architecture	106

LIST OF TABLES

Table 1: Key IMA platform characteristics	9
Table 2: Key application characteristics	10
Table 3: Relationship among integration activities and acceptance tasks	19
Table 4: Overview of IMA certification tasks	34
Table 5: Overview of typical validation activities	66
Table 6: Overview of typical verification activities	67
Table 7: CC1/CC2 definition	69
Table 8: Life cycle data to be submitted to certification authority	73
Table A-1: IMA module/platform development process (Task 1) objectives	77
Table A-2: Hosted application development and acceptance (Task 2) objectives	79
Table A-3: IMA system-level development and acceptance (Task 3) objectives	80
Table A-4: Aircraft-level integration (Task 4) objectives	82
Table A-5: Change (Task 5) objectives	84
Table A-6: Module or application reuse (Task 6) objectives	85

FOREWORD

1. This document, jointly prepared by EUROCAE Working Group 60 and RTCA Special Committee 200, was accepted by the Council of EUROCAE on 30 June 2007.

2. EUROCAE is an international non-profit making organization. Membership is open to manufacturers and users in Europe of equipment for aeronautics, national civil aviation administrations, trade association and, under certain conditions, non-European members. Its work program is principally directed to the preparation of performance specifications and guidance documents for civil aviation equipment, for adoption and use at European and world-wide levels.

3. The findings of EUROCAE are resolved after discussion among its members and in cooperation with the RTCA Inc., Washington DC, and/or the Society of Automotive Engineers (SAE), Warrendale PA, USA, through their appropriate committees.

4. EUROCAE Performance Specifications and Guidance Documents are recommendations only; EUROCAE is not an official body of the European Governments. Its recommendations therefore are not valid as statements of official policy unless adopted by a particular government or conference of governments.

5. Copies of this document may be obtained from:

EUROCAE

102 rue Etienne Dolet

92240 MALAKOFF

France

Tel: 33 1 40 92 79 30

Fax: 33 1 46 55 62 65

Email: eurocae@eurocae.net

Web Site: www.eurocae.net

EXECUTIVE SUMMARY

The use of Integrated Modular Avionics (IMA) is rapidly expanding and is found in all classes of aircraft. In recognition of this rapid growth EUROCAE established Working Group 60 (WG-60) and RTCA established Special Committee 200 (SC-200) to jointly develop a document that could be used as guidance in the design, development, and application of IMA. Participants in the development of the document included government, industry, and academic personnel.

IMA is a shared set of flexible, reusable, and interoperable hardware and software resources that, when integrated, form a platform that provides services, designed and verified to a defined set of safety and performance requirements, to host applications performing aircraft functions.

This document provides guidance for IMA developers, integrators, applicants, and those involved in the approval and continued airworthiness of IMA systems. It provides specific guidance for the assurance of IMA systems as differentiated from traditional federated avionics.

The development of this document is based on earlier EUROCAE/RTCA documents, for example EUROCAE ED-12/RTCA DO-178, Software Considerations in Airborne Systems and Equipment Certification and EUROCAE ED-80/RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware. Concepts from other EUROCAE and RTCA documents, as well as SAE and ARINC documents, also guided the document preparation.

CHAPTER 1

INTRODUCTION

1.1 PURPOSE

This document contains guidance for Integrated Modular Avionics (IMA) developers, application developers, integrators, certification applicants, and those involved in the approval and continued airworthiness of IMA systems in civil certification projects. The guidance describes the objectives, processes, and activities for those involved in the development and integration of IMA modules, applications, and systems to incrementally accumulate design assurance toward the installation and approval of an IMA system on an approved aviation product as differentiated from traditional federated aviation system architectures.

IMA system concepts are presented, including the platform and modules, and their relationships to the hosted applications and avionics functions used in an aircraft installation. This includes the description of how the developers and integrators can accumulate incremental acceptance of the modules, platform, and application integration which will provide a means for applicants to achieve design assurance of an IMA system on an approved aviation product.

During the IMA system development the certification applicant for a Type Certificate (TC) or Supplemental Type Certificate (STC) program should develop an effective system of communication among the module and platform developers and system integrators. This is especially important when these suppliers are from different companies. Otherwise, there may be a misunderstanding of the implementation during final integration and approval of the IMA system installation.

Six tasks define the incremental acceptance of IMA systems in the certification process:

- Task 1: Module acceptance.
- Task 2: Application software or hardware acceptance.
- Task 3: IMA system acceptance.
- Task 4: Aircraft integration of IMA system - including Validation and Verification (V&V).
- Task 5: Change of modules or applications.
- Task 6: Reuse of modules or applications.

Approval of an IMA system installation may be based on the accumulation of incremental acceptance, culminating in the complete design assurance needed to demonstrate that the installed system and functions comply with the applicable regulations and guidance.

The incremental acceptance, if appropriate, may be granted in the form of an acceptance letter, stamped type design data, or other means for the specific project.

1.2 SCOPE

This document is applicable to all parties involved in the development, integration, verification, and validation of IMA systems. The guidance in this document is focused on IMA-specific aspects of design assurance. As such it relies on other recognized documents that provide additional guidance on overall aircraft certification, system development, software assurance, and hardware assurance.

As defined in this document, IMA is described as a shared set of flexible, reusable, and interoperable hardware and software resources that, when integrated, form a platform that provides services, designed and verified to a defined set of requirements, to host applications performing aircraft functions. Key IMA and certification terms are described in Section 2.2 and in the glossary.

The primary industry-accepted guidance for satisfying airworthiness requirements for IMA components is included in Section 1.5. The ability to obtain incremental acceptance of individual items of the IMA platform (including the core software) and hosted applications enables the reduction of follow-on certification efforts without compromising system safety.

This document describes application properties as they relate to their integration with a platform; however, it does not address the specific functionality of applications nor specific Technical Standard Order (TSO)/European Technical Standard Order (ETSO) requirements, Minimum Operational Performance Specifications (MOPS), or Minimum Aviation System Performance Specifications (MASPS).

1.3 BACKGROUND

The evolution of software and microelectronics technology enables the introduction of new aircraft functions, new capabilities, and increased levels of complexity. The need to perform these complex functions necessitates the use of high-performance computing platforms that can host multiple applications on a single processor or a distributed network of processors.

Aircraft functions are increasingly being implemented by electronic systems. IMA is a means to accommodate this increase and reduce the number of units per aircraft. Additional benefits are reduced weight and volume of aircraft systems and equipment.

The IMA platform should be capable of providing robust partitioning and other protection means that allow multiple applications to share a platform and its resources, or to support functions distributed across a fault-tolerant network. An IMA platform may be provided by the system integrator or by a third party supplier. Likewise, IMA applications may be provided by the platform supplier or third party suppliers.

Economic factors, including the needs to provide cost-effective upgrade paths, introduce new operational capabilities (e.g., CNS/ATM functions), fast and efficient maintenance, and to avoid premature obsolescence are the primary incentives for the IMA concept. In light of this background, this document describes a set of processes and guidance to be used for the development and certification of IMA systems.

1.4 RELATIONSHIP TO OTHER DOCUMENTS

In addition to the airworthiness regulations and requirements, various national and international standards for software, avionics, complex electronics, and safety are available. In some communities, compliance with these standards may be required. However, it is outside the scope of this document to invoke specific national or international standards, or to propose a means by which these standards might be used as an alternative or supplement to this document.

Where this document uses the term “standards” it should be interpreted to mean the use of project-specific standards as applied to the aircraft systems, equipment, and engines. Such standards may be derived from general standards produced or adopted by the applicant for their certification activities.

1.5 REFERENCES

The latest version of the following documents apply:

[1] EUROCAE ED-14 / RTCA DO-160, Environmental Conditions and Test Procedures for Airborne Equipment.

[2] EUROCAE ED-12 / RTCA DO-178, Software Considerations in Airborne Systems and Equipment Certification.

[3] EUROCAE ED-76 / RTCA DO-200, Standards for Processing Aeronautical Data.

[4] EUROCAE ED-77 / RTCA DO-201, Industry Requirements for Aeronautical Information.

[5] EUROCAE ED-94 / RTCA DO-248, Final Report for Clarification of DO-178B "Software Considerations in Airborne Systems and Equipment Certification".

[6] EUROCAE ED-80 / RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware.

[7] EUROCAE ED-79 / SAE ARP4754, Certification Considerations for Highly Integrated or Complex Aircraft Systems.

[8] SAE ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

[9] Federal Aviation Administration (FAA) AC 20-148, Reusable Software Components.

[10] FAA TSO-C153, Integrated Modular Avionics Hardware Elements.

[11] FAA Order 8110.49, Software Approval Guidelines.

[12] ARINC 615A, Software Data Loading.

[13] ARINC 653, Avionics Application Software Standard Interface.

[14] ARINC 664, Aircraft Data Network.

NOTE: *When FAA Advisory Circulars are referenced, they are intended as material that may supply topics and areas for the applicant to consider. All requirements should be coordinated with the applicant's local certification authority.*

1.6 HOW TO USE THIS DOCUMENT

This document is intended to be used by the international aviation community. To aid in such use, references to specific national regulations and procedures are minimized. Instead, generic terms are used. For example, the term "certification authority" is used to mean the organization or person granting approval on behalf of the country responsible for aircraft and/or engine certification. Where a second country or a group of countries validates or participates in this certification, this document may be used with due recognition given to bilateral agreements or memoranda of understanding among the countries involved.

This document recognizes that the guidance herein is not mandated by law, but represents a consensus of the aviation community. Therefore, use of the word "shall" is avoided. The word "should" is used to describe the method required to adhere to this document, but it is recognized that alternative methods to those described herein may be acceptable.

The document is structured to introduce the reader to IMA and highlight the attributes of IMA that affect the development, acceptance, and installation approval of IMA systems on aircraft.

The document consists of the following chapters:

- Chapter 1 gives the reader an overview of this document.
- Chapter 2 introduces the concept of IMA and highlights the system, hardware, and software characteristics.
- Chapter 3 provides a description of IMA-specific development and integration guidelines.
- Chapter 4 provides guidelines for the acceptance of IMA and describes the relationship to the approval of the installed IMA system.
- Chapter 5 describes integral processes for IMA development.
- Chapter 6 includes guidelines for continued airworthiness of IMA systems.

Figure 1 illustrates the relationships of these chapters.

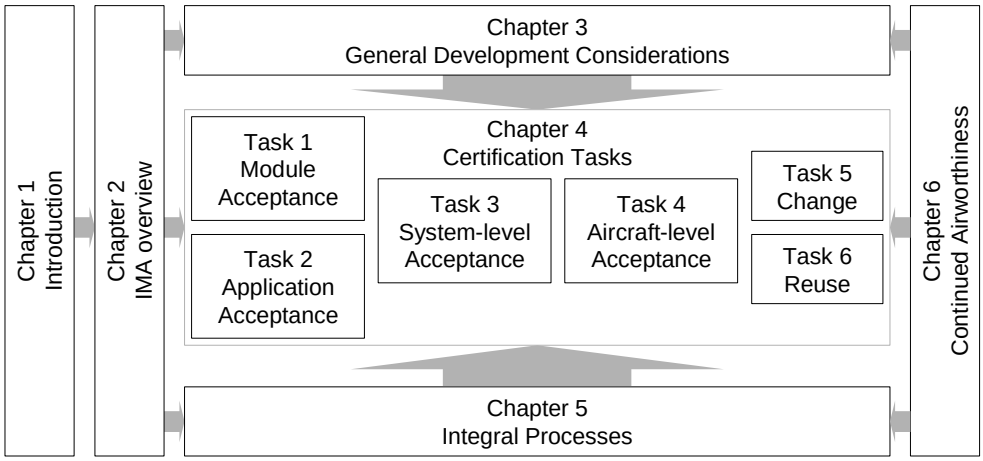

FIGURE 1 : CHAPTERS AND THEIR RELATIONSHIPS

At the end of the document the following annexes are included:

- Annex A summarizes the objectives to be satisfied to demonstrate compliance with this document. Objectives are listed in tables, using a summary of the tasks described in Chapters 3 and 4.
- Annex B is the Glossary of Terms. Note that some terms have a specific meaning in this document.
- Annex C is the list of acronyms and abbreviations used in this document.
- Annex D contains IMA examples.

NOTE: *Annexes A through C are considered normative; Annex D is informational only.*

CHAPTER 2

INTEGRATED MODULAR AVIONICS OVERVIEW

This chapter provides a description of an IMA system. It introduces terminology that applies to IMA and describes the relationship of terms. Key characteristics are introduced to acquaint the reader with the IMA concept.

2.1 IMA DESIGN AND CERTIFICATION TERMINOLOGY

The design, certification, and IMA terms needed to understand this document are described below. In some cases, the description of these terms expands upon the definitions included in the glossary and may be used in a slightly different fashion than in traditional aviation design and guidance material.

2.1.1 IMA Design Terminology

The following terms are used to describe IMA systems. These terms are identical to those defined in Annex B, expanded to provide more understanding of the terms as they apply to IMA design.

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.

Application - Software and/or application-specific hardware with a defined set of interfaces that, when integrated with a platform, performs a function.

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.

Core Software - The operating system and support software that manage resources to provide an environment in which applications can execute. Core software is a necessary component of a platform and is typically comprised of one or more modules.

IMA System – Consists of an IMA platform(s) and a defined set of hosted applications.

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.

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.

Partitioning - An architectural technique to provide the necessary separation and independence of functions or applications to ensure that only intended coupling occurs. The mechanisms for providing the protection in an IMA platform are specified to a required level of integrity.

Platform - Module or group of modules, including core software, that manages resources in a manner sufficient to support at least one application. IMA hardware resources and core software are designed and managed in a way to provide computational, communication, and interface capabilities for hosting at least one application. Platforms, by themselves, do not provide any aircraft functionality. The platform establishes a computing environment, support services, and platform-related capabilities, such as health monitoring and fault management. The IMA platform may be accepted independently of hosted applications.

Resource - Any object (processor, memory, software, data, etc.) or component used by an IMA platform or application. A resource may be shared by multiple applications or dedicated to a specific application. A resource may be physical (a hardware device) or logical (a piece of information).

Reusable - The design assurance data of previously accepted modules and applications may be used in a subsequent aircraft system design with reduced need for redesign or additional acceptance.

Figure 2 shows the relationships between many of these terms.

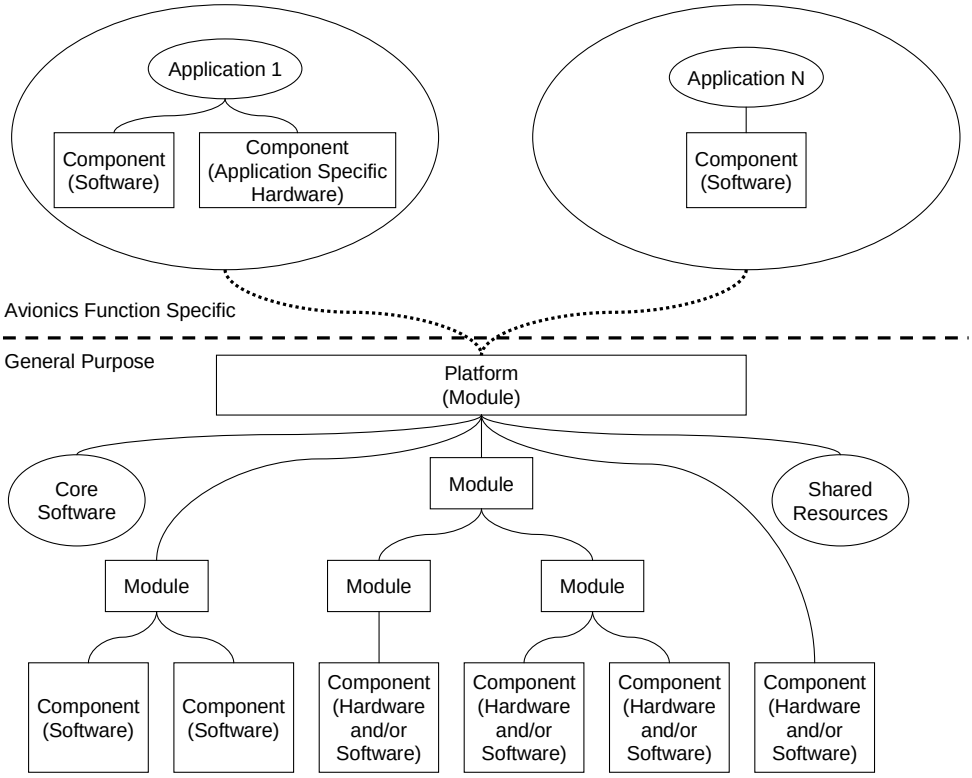

FIGURE 2 : RELATIONSHIP OF IMA DESIGN TERMS

2.1.2 Certification Terminology

A primary purpose of this document is to provide a means of compliance for IMA systems seeking acceptance, approval, and certification of their installation on an aircraft. To accomplish this it is important to understand the certification terminology. The primary certification terms relevant to IMA are defined below:

Certification - Legal recognition by a certification authority that a product, service, organization, or person complies with the requirements. Such certification includes the activities of technically checking the product, service, organization, or person, and a formal recognition of compliance with the applicable regulations and airworthiness requirements by issuance of a certificate, license, approval, or other documents as required by national laws and procedures. In particular, certification of a product includes:

a. the certification applicant process of assessing the design of a product and demonstrating to the certification authority that it complies with the applicable regulations and a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety;

b. the process of assessing products to ensure they conform with the approved type design for that product;

c. the certification authority process of finding compliance and the issuance of a certificate required by national laws to declare that compliance and/or conformity has been found with standards in accordance with items a or b above.

TSO Authorization - Legal recognition by the certification authority that a system, equipment, or part satisfies the TSO requirements and minimum specification applicable for that equipment. This term is equally applicable to European TSO (ETSO) authorizations.

Acceptance – Acknowledgement by the certification authority that the module, application, or system complies with its defined requirements. Acceptance is recognition by the certification authority (typically in the form of a letter or stamped data sheet) signifying that the submission of data, justification, or claim of equivalence satisfies applicable guidance or requirements. The goal of acceptance is to achieve credit for future use in a certification project.

Approval – The act or instance of giving formal or official acknowledgement of compliance with regulations. In the context of IMA there are typically two forms of approval:

a. approval of submitted life cycle data by the certification authority (usually demonstrated by issuance of a stamped and signed data item or a letter),

b. installation approval by the issuance of an aircraft or engine type certificate and/or airworthiness certificate.

Incremental acceptance - A process for obtaining credit toward approval and certification by accepting or finding that an IMA module, application, and/or off-aircraft IMA system complies with specific requirements. This incremental acceptance is divided into tasks. Credit granted for individual tasks contributes to the overall certification goal. Incremental acceptance 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-acceptance.

2.2 ARCHITECTURAL CONSIDERATIONS

An IMA system architecture is composed of one or more platforms and includes interfaces to other aircraft systems and users (for example, flight crew, maintenance personnel, etc.). The allocation of aircraft functions should be addressed in the IMA system architecture to ensure that applicable availability, integrity, and safety requirements are satisfied. Some of the primary considerations are listed and described below:

a. Availability considerations

- Functional performance – allocation of hosted aircraft functions (Section 3.2) to the IMA system architecture.
- Resource management – allocation of IMA platform resources, control of shared and dedicated resources, and protection of IMA platform resources used by multiple hosted aircraft functions or applications (Section 3.5).
- Reliability and maintainability – impact on Master Minimum Equipment List (MMEL), aircraft dispatchability, repair, replacement, and ease of performing maintenance activities to ensure continued airworthiness (Section 3.9).
- Health monitoring – monitoring the condition of the system and operational and maintenance concerns (Section 3.6).

b. Integrity considerations

- Design assurance, IMA safety and protection features, fault detection and partitioning - ability to protect hosted functions and applications to ensure independence and to prevent unintended interactions while using shared resources (Section 3.5).

c. Safety considerations

- Safety assessment - ensure appropriate architecture, design assurance, failure protection, address common mode and impact of combinational failures of aircraft functions, and airworthiness (Section 5.1).

d. Fault management, fault reporting, and recovery actions – detecting and identifying faults, failures and anomalous behavior, and providing appropriate responses (Section 3.6).

e. Composability considerations

- An IMA platform is composable if integration of a new application will not invalidate any verified requirements of an already integrated application.
- In a composable architecture, system requirements follow from requirements allocated to IMA applications. An IMA platform with well defined interface boundaries may be composable with respect to partial acceptance of integrated applications. Robust partitioning is one step toward this goal (Section 3.5.1).

2.3 KEY CHARACTERISTICS

The key characteristics of IMA platforms and hosted applications influence the IMA system architecture, the detailed system design, and, ultimately, the IMA platform and system acceptance process. Sections 2.3.1 through 2.3.5 summarize the characteristics of IMA platforms that affect the certification process.

2.3.1 Platforms and Hosted Applications

Two primary building blocks of an IMA system are the platform and the hosted applications. The key characteristics for the IMA platform are provided in Table 1.

TABLE 1 : KEY IMA PLATFORM CHARACTERISTICS

Key IMA platform characteristics	Description
Platform resources are shared by multiple applications	Integration implies sharing of resources. An IMA platform is able to host multiple applications through partitioning and other protection capabilities provided by it (e.g., HIRF/IEL, power supply, Built-In-Test).
An IMA platform provides robust partitioning of shared resources	This characteristic ensures that shared platform resources are available to the hosted applications as needed, and that those resources are protected from any anomalous behavior of the applications using them. IMA platform resource management ensures that only specified, intentional usage, interactions, and interfaces are allowed by the platform and applications sharing the resources. Robust partitioning will ensure that any hosted application or function has no unintended effect on other hosted applications or functions.
An IMA platform only allows hosted applications to interact with the platform and other hosted applications through well defined interfaces	An IMA platform is a general purpose computing platform able to host one or more aircraft functions or applications. As such, platform behavior may be verified independent of specific applications (e.g., it may be shown to meet its module requirement specification). The IMA platform is viewed as a separately accepted component of an IMA system. This characteristic is necessary to isolate changes between the platform and hosted applications. The intent is to allow modification of the IMA platform with minimum impact on the hosted applications, and changes to applications with minimum impact on the platform. The platform provides documented (and verified) Application Programming Interfaces (API) to allow applications access to platform services and resources.
Shared IMA platform resources are configurable	IMA platform resources are configurable to support the resource requirements of hosted applications.

The key characteristics for IMA hosted applications are provided in Table 2.

TABLE 2 : KEY APPLICATION CHARACTERISTICS

Key Application Characteristics	Description
An application may be designed independent of other applications and obtain incremental acceptance on the IMA platform independently of other applications	Hosted applications may be individually verified on the platform without the full suite of intended applications. The incremental acceptance for each hosted application can be used to support the accumulation of credit toward approval of the IMA system installation on the aircraft.
Applications can be integrated onto a platform without unintended interactions with other hosted applications	As the different applications reach completion and are verified individually, they should be integrated on the platform as a complete suite of hosted applications. Interactions between applications should be verified.
Applications may be reusable	Application modularity and portability may enable and facilitate use on different projects and products.
Applications are independently modifiable	Each application is modifiable with little or no impact on other applications and platform resources and modules. Any impacts should be identified and coordinated with the affected components.

2.3.2 Shared Resources

IMA systems may host several applications that share resources. For example, resources may be shared by the method of access time. This applies to processing resources and hardware. Each shared resource has the potential to become a single point failure that can affect all applications using that resource. Accordingly, appropriate mitigation techniques should be applied as determined by the system safety assessment process.

Processing resource refers to a physical element that may contain Central Processing Unit(s) (CPU), memory and associated interfaces. Memory is capable of storing machine-readable computer programs and associated data. The IMA hosted applications will communicate using shared resources provided by the IMA platform (for example, I/O devices, data buses, shared memory, etc.). A resource or portion of a resource can be allocated per unit time (for example, processor cycles or communication bandwidth).

The IMA platform provides resource management capabilities for shared resources, as well as health monitoring and fault management capabilities to support the protection of shared resources. IMA systems may have multiple electrical power sources that are shared.

2.3.3 Robust Partitioning

Robust partitioning is a means for assuring the intended isolation of independent aircraft functions and applications residing in IMA shared resources in the presence of design errors and hardware failures that are unique to a partition or associated with application-specific hardware. If a (different) failure can lead to the loss of robust partitioning then it should be detectable and appropriate action taken. The objective of robust partitioning is to provide the same level of functional, if not physical, isolation and protection as a federated implementation. This means robust partitioning should support the cooperative coexistence of core software and applications hosted on a processor and using shared resources, while assuring unauthorized or unintended interference is prevented. Robust partitioning should meet the following information guidelines in ED-94/DO-248 (Ref. [5], Section 4.1.4.5):

- A software partition should not be allowed to contaminate the code, I/O, or data storage areas of another partition.
- A software partition should be allowed to consume shared processor resources only during its allocated time.
- A software partition should be allowed to consume only its allocation of shared I/O resources.
- Failures of hardware unique to a software partition should not cause adverse effects on other software partitions.

Robust partitioning is a means for assuring the intended isolation and independence in all circumstances (including hardware failures, hardware and software design errors, or anomalous behavior) 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 (i.e., applications individually residing on separate Line Replaceable Units (LRU)). This means robust partitioning supports the cooperative coexistence of applications using shared resources, while assuring that any attempted unauthorized or unintended interaction is detected and mitigated.

The platform robust partitioning protection mechanisms are independent of any hosted applications, that is, applications cannot alter the partitioning protection provided by the platform.

2.3.4 Application Programming Interface (API)

An API defines the standard interfaces between the platform and the hosted applications and provides the means to communicate between applications and to use I/O capabilities. ARINC 653 (Ref. [13]) Parts 1 and 2 provide an avionics standards for an application programming interface and the related services. ARINC 653 Part 3 provides a standardized test specification to demonstrate compliance to ARINC 653.

2.3.5 Health Monitoring and Fault Management

Health monitoring and fault management (HM/FM) functions deserve special attention due to the integration of multiple applications and resource sharing. IMA systems manage platform faults, hardware failures, partitioning violations, and errors and anomalous behavior of hosted applications, including common mode faults and cascading failures. The methods used to manage platform faults are independent of the hosted applications. Fault management consists of detecting faults, failures and errors, correctly identifying them when they occur and performing the appropriate response. Guidance for fault management and fault reporting is included in Section 3.6.

The IMA platform provides health monitoring and fault management capabilities for the platform and hosted applications. The IMA system may have to provide higher level (aircraft function) health monitoring and fault management capabilities to support availability and integrity requirements.

2.4 STAKEHOLDERS

The assignment of roles and responsibilities is necessary, and should address the entire IMA system life cycle from conceptual design to retirement. These assignments may be based on the underlying IMA system architecture and should include the responsibility for selecting and providing tools. These assignments should be stated in the IMA system project plans, such as the IMA System Certification Plan and supporting lower-level plans.

This section identifies the typical data provided in support of the development, approval, and continued operational safety of IMA systems installed on aircraft. The responsibility for certain activities, data generation, and for demonstrating compliance should be coordinated, communicated, and resolved among the stakeholders as early as possible in the program. Data is accumulated to support incremental acceptance of IMA modules and hosted applications.

While a single group or organization may be able to perform all of the activities described (with the exception of the certification authority), it is anticipated that there will be multiple organizations involved. Certification applicants are strongly encouraged to coordinate their plans with the certification authority as early as possible and to maintain coordination throughout the IMA system development.

Where a failure or fault impacts common IMA components used across projects and aircraft products, there should be a process in place that provides information to be provided to all users of the common components. This process should have communications, not only to the users, but also to the certification authority and those responsible for continued operational safety of the aircraft product. There should be clear and well-defined communications paths and procedures to follow for recording the decisions made, the rectification path, and the agreement for any certification authority actions.

2.4.1 Certification Authority

The certification authority is the organization(s) granting approval on behalf of the state(s) responsible for aircraft and/or engine certification.

2.4.2 Certification Applicant

The applicant is responsible for demonstrating compliance to the applicable aviation regulations, and is seeking a Type Certificate (TC), Amended TC (ATC), Supplemental Type Certificate (STC) or Amended STC (ASTC). The applicant is responsible for generating and validating all aircraft-level requirements and their allocation to subsystems, providing installation instructions for the configured IMA system, integrating it with other aircraft systems, and, where appropriate, installing it on the aircraft. The applicant is ultimately responsible for ensuring that the installed IMA system and the aircraft comply with applicable regulations and are airworthy.

The applicant will perform the necessary development activities to define aircraft-level functions to be implemented and the necessary V&V activities on the system after it is installed in the aircraft. The applicant is also responsible for continued airworthiness (see Chapter 6).

NOTE: *The applicant is not required to perform the actual installation of the IMA system on the aircraft but is still responsible for the items described above.*

2.4.3 IMA System Integrator

The IMA system integrator performs the activities necessary to integrate the platform(s) and hosted applications to produce the IMA system. Typical data developed during IMA system integration includes:

a. The system configuration consisting of the number, type, and specific versions of modules and hosted applications.

b. The shared resource allocation and configuration tables for the integrated IMA system.

c. Results of IMA system V&V, including performance data for the IMA system, consistent with the allocated requirements.

2.4.4 Platform and Module Suppliers

The IMA platform and module suppliers provide the processing hardware and software resources, including the core software. Development and configuration tools are provided to support use of the IMA platform or module. Typical data developed during platform and module development includes:

a. Specification of the interfaces to the IMA platform and modules.

b. Specification of the shared resource allocation and configuration tables.

c. Required resources and configuration data for the IMA platform, including core software.

d. Results of module and/or platform V&V, including performance data, consistent with allocated requirements.

2.4.5 Application Supplier

The application supplier develops the hosted application and verifies it on the IMA platform. The application supplier should ensure that any hardware or software resources that are unique to the hosted application meet the integrity and availability requirements consistent with the assigned failure condition classification, as determined by the aircraft safety assessment. Typical data developed during application development includes:

a. Specification of external interfaces required by the application.

b. Required resources and configuration data for the hosted application.

c. Results of application/platform integration V&V, including performance data, consistent with allocated requirements.

2.4.6 Maintenance Organization

The maintenance organization follows the approved procedures received from the certification applicant to keep the IMA system and the aircraft in an airworthy condition. Additional information relating to continued airworthiness is provided in Chapter 6.

CHAPTER 3

GENERAL DEVELOPMENT CONSIDERATIONS

The development of an IMA system is based on an IMA platform containing hardware and software that are common and can be shared by the hosted applications. Figure 3 shows an example of a typical design highlighting potential shared resources. The shaded areas identify the modules that may be shared.

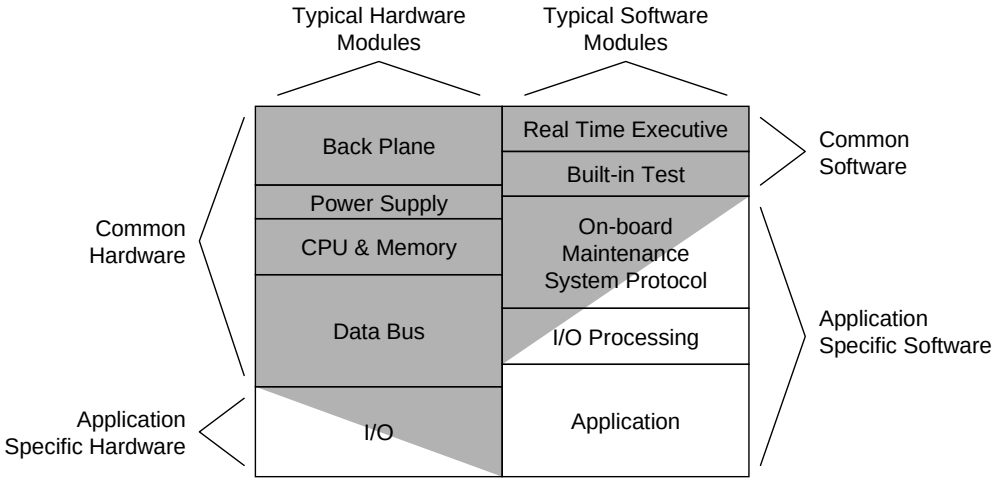

FIGURE 3 : EXAMPLE OF A TYPICAL DESIGN HIGHLIGHTING POTENTIAL SHARED RESOURCES

An IMA development process should ensure the following:

a. Aircraft functions allocated to a specific IMA system are consistent with the design of the system (Section 3.2).

b. Aircraft safety and security requirements allocated to a specific IMA system are identified and have been satisfied by the IMA system design. This should include assignment of system development assurance, hardware design assurance, and software levels. These levels are determined by the aircraft-level safety assessment to support aircraft functions implemented by hosted applications and supporting availability and integrity requirements, as well as any requirements for tool assessment and qualification (Sections 3.3 and 3.4).

c. Behavior of any hosted application is prevented from adversely affecting the behavior of any other application or function by the design of the IMA platform. The platform has robust partitioning, resource management, and other protection means appropriate to the aircraft functions and hosted applications (Sections 3.5 and 3.8).

d. Health monitoring, failure reporting process, and fault management functions are provided for the platform to meet specified requirements of the hosted applications and IMA system (Section 3.6).

e. Configuration management for the IMA platform, applications, integrator, and certification applicant are established and maintained (Section 3.7).

f. IMA system dispatch requirements are implemented and verified. (Section 3.9)

g. Human factors requirements pertaining to the IMA system are implemented and verified. (Section 3.10)

3.1 IMA SYSTEM DEVELOPMENT PROCESS

The overall development process for an IMA system should follow a structured process, such as ED-79/ARP 4754 (Ref. [7]). The IMA system development process should consider the primary characteristics of IMA: flexible, reusable, and interoperable. These characteristics influence the development process which should address, as a minimum:

a. The IMA platform – Definition of reusable, sharable modules and resources (including application programming interfaces and health monitoring strategy).

b. The hosted applications – Definition of the interfaces and system contracts to allow a given hosted application to reside on the given platform.

c. The IMA system – Integration of the specific set of hosted applications onto a given IMA platform(s).

The process outlined here supports the reuse of the IMA platform and hosted application development data on another aircraft program.

The following terms will be used when outlining the development process (these terms supplement those in Section 2.1):

- ***IMA platform*** consists of the IMA modules and core software without any aircraft functions or applications installed.
- ***IMA platform architecture*** refers to the means of structuring, connecting and combining IMA modules to support the requirements of the hosted applications and aircraft functions.
- ***IMA system*** consists of the IMA platform(s) and the hosted applications.
- ***IMA system architecture*** consists of the IMA platform(s), connections and components required to meet the requirements of all of the hosted applications and aircraft functions.

3.1.1 IMA Platform Development Process

The IMA platform may be defined and developed separately from the specific aircraft functions and the hosted applications. If this can be achieved, it may be possible for the data developed for an IMA platform to be reusable with a different set of hosted applications.

One of the primary goals of IMA is to develop an IMA platform that can be reused on different aircraft and with different hosted applications. A reusable IMA platform should be developed using the process objectives described below. The module acceptance process is further described in Chapter 4.

a. Plan and define the IMA platform. The definition should include:

   1. The architecture definition, which contains the type and general function of the various IMA modules, resources and components, and how they will interact (e.g., distributed vs. centralized architecture).

   2. An approach for integrating hosted applications, both hardware and software, onto the IMA platform.

   3. An IMA platform acceptance approach.

   4. An IMA system certification approach that includes support for hosted applications and stakeholder roles and responsibilities for developing compliance data.

   5. A list of platform services to be provided to the hosted applications.

   6. The intended level of aircraft function availability and integrity needed, platform capabilities to support it, and methods for supporting it.

7. The health management and fault management approaches (excluding the actual external interfaces, as this will be dependent on the aircraft HM and crew alerting systems).

8. The platform and IMA system configuration management approaches.

b. Define the IMA platform requirements, including:

1. Safety capabilities:

i. identification of the top level platform failure events that could affect hosted applications.

ii. definition of the acceptable failure rates (reliability requirements of platform hardware modules) associated with each failure event.

iii. development of guidance for use of the above data in meeting the availability and integrity requirements of an aircraft and potential hosted functions.

iv. definition of the safety requirements, including robust partitioning, health monitoring, fault management, resource management, other safety features and other protection means.

2. Performance capabilities.

3. Configuration management approach.

4. Environmental conditions under which the platform modules are intended to operate. Where modules share a common environment, such as a cabinet with common power or a common data bus, a definition of the conditions for the common environment should also be described.

5. Fault management and reporting approach and requirements, including considerations for: fault tolerance, fault isolation to modules, and detection and isolation of single failures (for example, failures resulting in loss of capability, such as internal power source failures, redundant inter-module communication channels, and other similar resources should be considered).

6. Detailed requirements for each aspect of the concept definition.

7. IMA platform architecture which has been defined and verified to the required safety capabilities.

c. Develop and implement the IMA platform design. The software and hardware development processes should follow ED-12/DO-178 (Ref. [2]) and ED-80/DO-254 (Ref. [6]), respectively, along with any regulatory supplemental documents, at the appropriate level to meet the required safety requirements. Additionally, common cause analysis (CCA) should be performed and qualitative failure analysis for the various top level events defined for the platform should be developed.

d. Verify and validate the IMA platform addressing the following activities:

1. Perform environmental qualification testing to the specified environmental conditions.

2. Perform a partitioning analysis and verification testing; verify other protection capabilities and safety features (i.e., resource management, health monitoring, fault management, built-in test (initial and continuous), etc.).

3. Complete the CCA.

4. Complete the numerical analysis showing that implementation meets the reliability requirements and capabilities.

5. Address modules sharing an environment and resources together. Non-IMA modules sharing the same environment should also be addressed. If there are only IMA modules sharing the environment and the configuration of modules is fixed, then the combined partial environmental qualification can be achieved prior to full integration on an aircraft.

e. Obtain IMA platform acceptance using the module acceptance approach described in Chapter 4. The module acceptance data described in Chapter 4 and Chapter 5 should be developed and submitted or made available. All IMA platform requirements should be validated and verified. Traceability between the requirements, implementation, and verification activities should be developed and maintained.

3.1.2 Hosted Application Development Process

Development of hosted applications follow the same development processes as used in non-IMA systems, but should address these objectives:

a. Identify IMA platform resources to be used (part of interface definition).

b. Quantify required IMA platform resources (part of interface definition).

c. Map hosted application safety assessment to IMA platform safety assessment and capabilities (i.e., Preliminary System Safety Assessment (PSSA), Functional Hazard Assessment (FHA), and Common Cause Analysis (CCA)).

d. Define HM/FM requirements for the hosted application and define interactions with IMA platform HM/FM functions.

e. Identify dedicated resources peripheral to the IMA platform (for example, application-specific hardware).

f. Specify environmental qualification level for dedicated resources.

g. Integrate application onto the platform and perform software/platform integration testing.

h. Assess human factors requirements against IMA platform performance.

3.1.3 IMA System Development Process

The IMA system development process should address the following objectives:

a. Identify aircraft functions, including functional, performance, safety, availability, and integrity requirements.

b. Allocate IMA platform resources to the aircraft functions considering the aircraft-level FHA, resource requirements (interface specifications), safety capabilities of the IMA platform, and MMEL considerations. Determine what hosted applications or aircraft functions need isolation and/or protection from other hosted applications and functions and other protection mechanisms or safety features needed.

c. Develop the IMA system architecture, addressing the following aspects:

1. Develop IMA System Certification Plan (Section 4.4.3) based on aircraft requirements, hosted applications, and the IMA system certification approach.

2. Determine the quantity, quality, and type of IMA platform modules and resources needed to meet all application requirements, including functional, performance, safety, availability, integrity, and redundancy requirements.

3. Determine any aircraft function requirements driven by the capabilities of the IMA platform modules, for example:

    1. Availability requirements beyond those available from a single IMA module or platform which could drive the application to be hosted on multiple modules and/or platforms.

    2. Applications using multiple modules should determine application redundancy management requirements.

    3. Integrity requirements beyond those available from an IMA module or platform that could drive the hosting of multiple instances of the application and/or data that may be compared to achieve the necessary integrity.

4. Perform a Preliminary System Safety Assessment (PSSA) for each hosted application using the IMA platform safety requirements.

5. Evaluate the aircraft effects from the combination of platform, hosted applications, and shared resource failures.

6. Identify changes required to the allocation of IMA platform resources to correct any issues identified from the individual and combined PSSA activities.

d. Implement the IMA system, including the following activities:

    1. Develop the applications and perform partial verification.

    2. Integrate all applications onto the platform and perform IMA system validation and verification activities.

    3. Develop initial IMA system failure analysis using IMA platform top-level events as basic events for the hosted application failure analyses.

    4. Evaluate the combination of IMA platform component failures affecting hosted applications which could lead to aircraft level effects, and adjust the allocation and/or application implementation as necessary. It should be noted that IMA platform component failures should have a unique top level event.

    5. Perform aircraft ground and flight testing to validate assumptions in the SSA, requirements and environmental definitions.

e. Integrate, validate, verify, and obtain acceptance of the IMA system (off aircraft). Specific configuration of applications in the IMA system should be shown to meet their requirements (including performance, redundancy management, and IMA platform interface requirements). Analyses for each hosted application should be developed to show it complies with its FHA. Additionally, the hosted application analyses should be combined into an IMA system hardware quantitative analysis that shows that the combined events satisfy the aircraft level safety and reliability requirements.

f. Where appropriate, integrate, validate, verify, and obtain acceptance of the IMA system installed on the aircraft.

The integration activities and the relationship to the acceptance tasks are shown inTABLE 3. The activities are general and can be scaled appropriately to align with the size of development. The acceptance process of IMA is described by six tasks (also refer to Chapter 4).

TABLE 3 : RELATIONSHIP AMONG INTEGRATION ACTIVITIES AND ACCEPTANCE TASKS

Integration Activity	Acceptance Tasks	
Integrate components and/or modules to form a platform	Task 1	Module and/or platform acceptance
Integrate a single application with the platform	Task 2	Application acceptance (software and/or hardware)
Integrate multiple applications with the platform(s) and one another	Task 3	IMA system acceptance
Integrate IMA system with aircraft and its systems	Task 4	Aircraft integration
Identify changes and their impacts, and need for re-verification	Task 5[1]	Change
Identify and use IMA components on other IMA systems and installations	Task 6[1]	Reuse

3.2 IMA SYSTEM RESOURCE ALLOCATION ACTIVITIES

The aircraft functional and performance requirements influence the allocation of IMA hosted functions. In addition to the specific aircraft functions, several issues may need to be addressed including provisions for computing resource availability, application-specific I/O resources, network bandwidth, and meeting the safety, integrity and reliability requirements. Platform services performed on behalf of a specific application should occur within the resource constraints of that application.

a. Processing throughput for an IMA system should address the required execution time of the applications, the context switch times, the platform overhead, and the overall processing requirements. For example, any service performed on behalf of an application should be executed in its allocated time and not during the time allocated to another application. This would include services provided by the platform, such as resource management, health monitoring, fault management, partitioning enforcement, and other active protection means.

b. The amount of computing resource and network bandwidth should address overhead (including partitioning enforcement, processing, and data bus jitter and traffic) associated with context switching, data scheduling, and other constraints.

c. Satisfying the safety requirements for the aircraft, the IMA platform and hosted applications define the integrity and availability requirements of the functions allocated and the configuration of the IMA system. The IMA system architecture should be capable of supporting the highest level of integrity and availability for the aircraft functions and hosted applications.

[1] Integration aspects of Tasks 5 and 6 are performed at the aircraft or system-level and may include Task 1 - 4 activities

3.3 AIRCRAFT SAFETY AND SECURITY

Safety requirements should be addressed in the IMA system requirements. These requirements drive the system configuration and the allocation of functions and hosted applications to IMA resources, and establish the independence, availability, and integrity requirements for those hosted applications contributing to the aircraft functions. Additional safety considerations are addressed in the safety assessment process described in Section 5.1. Requirements derived from the safety assessment and the security analysis are distinguished from functional requirements.

Security requirements should be addressed at the aircraft-level safety assessment (see Section 5.1.5.8). IMA mechanisms may be used to address security concerns.

3.4 DEVELOPMENT ASSURANCE AND TOOL ASSURANCE

The IMA system and components should be designed and developed to the highest assurance levels needed to support the safety, integrity, and availability requirements of the aircraft functions and hosted applications intended for the IMA system as determined by the IMA system safety assessment. This may be difficult to determine for a "general purpose" IMA platform intended to be used on multiple aircraft types with unknown sets of aircraft functions and hosted applications. Therefore, to reduce the risk for a specific aircraft type and configuration of hosted applications, the IMA system developer may want to develop their system to a specific assurance level.

Both the IMA platform user's guide for hosted applications and the interface specification, describing the IMA platforms interface requirements with external systems, should be complete and unambiguous. Since the aircraft functions and hosted applications on an IMA system may originate from multiple suppliers, the IMA platform user's guide should be available to all application suppliers.

Tools provided by the IMA platform developer and used to develop and/or verify compliance to the interface specifications may need to be qualified. For example, certain tools used to generate or verify configuration tables or verify robust partitioning may need to be qualified by the IMA platform developer and/or system integrator, but should not need to be qualified by the application developers.

3.5 PARTITIONING AND RESOURCE MANAGEMENT ACTIVITIES

A primary goal of IMA is to integrate and host multiple aircraft functions and applications on one or more computing platform(s) while ensuring that any one aircraft function is not able to affect another function in an undefined or unacceptable way. Furthermore, failures of the mechanisms that enforce and maintain this independence should be detectable and mitigated to ensure the required levels of safety and integrity.

The criteria for "unacceptable" can be determined only through safety assessment. This requires analyzable mechanisms for behavioral containment and isolation between the aircraft functions and hosted applications. One such technique is commonly known as partitioning and is defined in ED-12/DO-178 (Ref. [2]) as follows:

"Partitioning is a technique for providing isolation between functionally independent software components to contain and/or isolate faults and potentially reduce the effort of the software verification process."

Partitioning within an IMA system should allow independent applications to share resources without any unintended interactions. While the concept of partitioning is used in many commercial computer-based systems, the usual implementations would not provide the degree of protection needed in safety-related systems. Thus, "robust partitioning" is defined to distinguish partitioning for IMA systems.

The characteristics of robust partitioning are:

a. The partitioning services should provide adequate separation and isolation of the aircraft functions and hosted applications sharing platform resources. Partitioning services are the services provided by the platform that define and maintain the independence and separation between partitions. These services ensure that the behavior of functions or applications within a partition cannot unacceptably affect the behavior of functions or applications in any other partition. These services should prevent any adverse effects on the aircraft of the simultaneous undetected corruption of all the functions and applications' partitions sharing the affected resources.

b. The ability to determine in real-time, with an appropriate level of confidence, that the partitioning services are performing as specified consistent with the defined level of safety.

c. Partitioning services should not rely on any required behavior of any aircraft function or hosted application. This implies that all protection mechanisms required to establish and maintain partitioning are provided by the IMA platform.

NOTE: *Other protection mechanisms (e.g., higher level fault detection and resolution, application-specific safety monitoring, or error detection and correction capabilities) may be IMA hosted as part of a hosted application, or may be hosted on other aircraft systems.*

These characteristics should be compatible with the required reliability and integrity levels identified in the aircraft safety assessment. The analysis of these characteristics may be done at the aircraft platform or IMA system integration level.

Dedicated resources are resources allocated by design exclusively to a given application or application function within a partition. An important characteristic of dedicated resources is that the failure of a dedicated resource only affects the application or partition to which it is dedicated. Typical examples of dedicated resources are dedicated memory, specialized hardware, and software logical resources, such as dedicated buffers.

Shared resources are resources that are used by multiple partitions. Therefore, independence or isolation of the application functions in one partition from those in another is needed (e.g., protection of one function from failures or anomalous behavior of another). An important characteristic of a shared resource is that a failure of that resource affects all the applications and partitions using that resource. Different architectures may designate the same resource as either dedicated or shared.

Partitioning analysis and design should conform to two principles. First, the dedicated resources assigned to one partition can never be affected by or affect the operation of an application or application function in any other partition. Second, the use of shared resources by one partition cannot unacceptably affect, as shown by a safety assessment, the operation of an application or application function in any other partition sharing that resource.

An IMA execution environment should ensure that all hosted applications operate in a manner equivalent to operation in a federated system architecture. Each hosted application should have total independence with respect to any other application being co-hosted with it. The platform should guarantee the allocation of necessary resources to all hosted applications, regardless of the operation or errors in other hosted applications.

The design of an IMA system and its associated architecture is determined by many factors (e.g., system issues requiring redundancy, common cause failure considerations, and so on). This section addresses only those aspects of design and architecture related to partitioning. The inability of the IMA system to guarantee partitioning in the presence of hardware failures or software errors may require specific flight crew action or maintenance action. Such actions can be determined only by considering the actual aircraft functions and hosted applications and are beyond the scope of this document. Nevertheless, any mechanism potentially involved

in failures of the IMA system to guarantee partitioning and the effects of those failures on aircraft functions and hosted applications should be identified and provided to the system development and safety assessment processes. In some cases, an IMA system developer may provide specific safety properties independent of any application, such as fail-passive or fail-operational architectures, providing additional constraints and protection that could simplify the overall system safety assessment, verification of robust partitioning and other protection features, and demonstration of compliance.

3.5.1 Design for Robust Partitioning

The design for partitioning in an IMA platform is an iterative process. The proposed design should be analyzed to ensure that the criteria identified in Section 3.5 have been satisfied. If deficiencies are detected, then the architecture should be revised until the criteria can be shown to be satisfied. While the approaches used will be dependent on the specific implementation, some generic guidelines are provided within this section.

All of the dedicated and shared resources should be identified. All propagation paths to those resources where any unintended interaction may occur should be determined. These propagation paths may be the result of hardware failures, hardware design errors, or software design errors. They may also be the result of normal execution. Once propagation paths have been determined, containment boundaries should be established and validated to prevent undesirable interaction between partitions through these propagation paths. Robust partitioning services should provide the protection of the dedicated and shared resources. Failure of these partition services may lead to the generation of unintended failure propagation paths. Example propagation paths are:

a. A faulty partition allows an application to write to a memory location to which another partition assumes it has exclusive access.

b. A common shared communication channel is caused by a faulty partition to deny service to another partition.

c. Processor execution time is denied by one partition to another.

d. A shared flash memory file system is corrupted by a faulty partition.

e. Cache memory on a CPU is not flushed on context switch to a new partition.

f. A faulty partition causes an event to occur at a time, or in a sequence, which differs from what is expected by another partition.

In some cases, more than one containment boundary may be needed for a given propagation path. In others, a single containment boundary may protect more than one propagation path.

The allowed interactions and interfaces between partitioned functions as supplied by the partitioning services should be specified completely. A complete interface definition will facilitate the analysis of propagation paths. Strict adherence and enforcement of the interface specifications between partitions should apply to IMA platforms to avoid unintended behavior.

Partitioning mechanisms should be consistent with IMA system integrity, availability and reliability requirements. IMA system design should satisfy the highest levels of these requirements while recognizing the implications of the combination of hosted applications and aircraft functions.

3.5.2 Partitioning Analysis

A partitioning analysis should demonstrate that no application or sub-function in a partition could affect the behavior of a sub-function or application in any other partition in an adverse manner. All propagation paths between partitions should be identified. The effects of each propagation path should be documented. The mitigation of unacceptable interactions at containment boundaries should be identified. Fault tree analysis, formal methods, and other techniques may be employed. The partitioning analysis should be addressed in the context of the aircraft system safety assessment to include any probability of multiple failure requirements. Alternatively, the analysis may make assumptions about these requirements. Partitioning analysis should address plans, procedures and requirements for how the partitioning and other protection schemes will be verified and validated.

The following sections describe what a partitioning analysis should contain.

3.5.2.1 Top-level Partitioning Property

The requirements allocated to the top-level partitioning properties should be based on the aircraft safety assessment. This part of the analysis should state the main property or properties that are needed to establish that robust partitioning has been achieved and maintained. These may be stated as either a positive property or a property that prevents an undesirable effect.

3.5.2.2 Decomposition of Partitioning Properties

This part of the analysis is a decomposition of the top-level properties to lower level properties that must be achieved to satisfy the top-level properties. The lower level properties may be further decomposed until the lowest level property is reached that can be shown to be fully satisfied by one or more design features of the platform.

NOTE: *An example of decomposition of the top-level property (no application affects the behavior of an application in any other partition in an adverse manner) could be as follows: No application function in one partition can*

a. access memory of any another partition in an adverse manner,

b. affect the timing of any another partition in an adverse manner, or

c. adversely affect the resources used by any other partition.

The above three properties satisfy the top-level property. Other means could be used. In addition, the memory protection can be considered a lowest-level property if there is a design feature that uses a Memory Management Unit (MMU) and a set of configuration files for setting up the MMU that guarantee that the memory allocated to a partitioned function is only accessed by that function.

3.5.2.3 Life Cycle Data

For every design feature related to the lowest level property traceability to life cycle data and associated verification data should be provided. If design features and associated life cycle data are part of another verification process, then only traceability to the design feature and associated requirement is needed.

3.5.2.4 Partitioning Vulnerability Assessment

For each partitioning property a vulnerability assessment should be conducted which examines all potential actions of external system and human interfaces as well as the effects of hardware failures when required by the safety assessment or hazard analysis.

NOTE: *Because the configuration files may be outside of the control of the platform designer, one vulnerability would be that an error in the configuration files could result, for example, in overlapping memory regions between partitioned functions. This would require a mitigation that would result in a requirement for the IMA system integrator to provide verification data that there are no overlapping memory regions.*

3.5.2.5 Potential Sources of Error

The potential sources of errors that should be included in a partitioning analysis are unique to each system analyzed. While there is no comprehensive list of issues that should be addressed, the following list represents some potential sources of design errors that could impact the partitioning analysis.

a. Interrupts and interrupt inhibits (software and hardware).

b. Loops (for example, infinite loops or indirect non-terminating call loops).

c. Real-time correspondence (for example, frame overrun, interference with real-time clock, counter/timer corruption, pipeline and caching, deterministic scheduling).

d. Control flow (for example, incorrect branching into a partitioned or protected area, corruption of a jump table, corruption of the processor sequence control, corruption of return addresses, unrecoverable hardware state corruption (for example, mask and halt)).

e. Memory, input, and/or output contention.

f. Sharing of data flags.

g. Software traps (for example, divide by zero, unimplemented instruction, specific software interrupt instructions, unrecognized instruction, and recursion termination).

h. Hold-up commands (e.g., performance hedges).

i. Loss of input or output data.

j. Corruption of input or output data.

k. Corruption of internal data (for example, direct or indirect memory writes, table overrun, incorrect linking, calculations involving time, corrupted cache memory).

l. Delayed data.

m. Program overlays.

n. Buffer sequence.

o. External device interaction (for example, loss of data, delayed data, incorrect data, protocol halts).

There is an iterative process between the partitioning analysis and the different design steps for the system. The analysis is complete when all partitioning properties have been satisfied and verified, and all identified vulnerabilities have been mitigated and have associated verification data.

3.6 HEALTH MONITORING AND FAULT MANAGEMENT

Health monitoring and fault management (HM/FM) functions should be provided with recognition that the IMA platform may support a collection of diverse aircraft functions. The IMA platform should provide basic health monitoring and fault management capabilities for IMA platform modules. These capabilities should be independent of the hosted applications.

a. Health monitoring should address both operational and maintenance concerns.

b. Strategies for the following example issues may be developed:

c. Identification of components and aspects to be monitored.

d. Health determination of each application.

e. Determination of the health of the IMA system as a whole.

f. Response to each type of failure or anomalous behavior.

g. Flight crew annunciation and messaging.

h. Control of maintenance actions and reporting.

i. Redundancy management.

j. Single event upsets.

3.6.1 Components and Aspects to be Monitored

Health monitoring is that part of the IMA platform responsible for detecting, isolating, containing, and reporting failures that could adversely effect applications using the IMA platform resources, or the resources themselves. This function should detect faults in the shared resources used by the hosted applications. However, some resources dedicated to applications may also be monitored by the IMA platform. For example, memory dedicated to an application partition may be monitored by the IMA platform rather than the application.

Faults in the shared resources could adversely impact all of the applications using those resources. The system architecture should be designed to promote the detection of faults at the lowest possible architectural level, ideally at the component level. This will reduce the potential for ambiguity. This can be done with self-monitoring, platform monitoring, or a combination thereof. Faults are generally detected by their symptoms potentially leaving some ambiguity about which component actually failed. The smaller the ambiguity group is for a fault, the easier it is to define policies for resolving it safely at the IMA system level. Sound architectural choices can frequently reduce the ambiguity to a single isolation region.This is an important consideration when determining responsibility for the detection of faults in the IMA platform. This is even more important with respect to the IMA platform robust partitioning services. Failures of these services can directly affect the ability to maintain that separation and independence. If detection of failures in these services requires hosted application participation, it becomes nearly impossible to isolate these failures to the partitioning mechanisms. For this reason, the health monitoring of the partitioning services should be performed by the IMA platform.

The IMA platform should monitor the health of its services and interfaces.

3.6.2 Health Determination of Each Application

The application supplier should identify potential failure modes of the application. In particular, any application failure modes which require action by the platform should be identified. For example, this may include partition restart, shutdown, or other platform-specific actions.

HM facilities to record, monitor, and manage failures affecting the platform should be provided. This includes the facilities for applications to record and announce maintenance conditions and failures. The application supplier may also provide application-level health monitoring capability specific to their application. This information, independent of the approach used, should be identified and integrated into the overall IMA system health monitoring strategy.

3.6.3 Health Determination of the IMA System as a Whole

The health determination for the IMA system should address IMA platform-level failure conditions and the potential for partitioning failures and application failure modes that are not addressed within the application. An integrated HM strategy should be defined and documented. This strategy should be coordinated with the IMA system safety assessment.

The integrated HM strategy should also define:

a. The means to identify systemic failures and report the conditions to the hosted applications and other platform services.

b. Rules governing partition restart and shutdown.

c. Rules for degraded operations, if applicable.

d. Guidelines to support the MMEL.

e. IMA system health status reporting, content and frequency.

3.6.4 Response to Each Type of Failure

In addition to detection and isolation of faults, the ability to report and contain faults is needed. Reporting refers to internal logging, indicating to hosted applications and platform services, indicating to the flight crew, and indicating to the maintenance crew the existence of the fault or failure. Fault containment refers to the response taken to keep a failure from affecting anything external to the containment area. This subsection focuses on the containment of faults. Reporting of faults will be covered later.

All detectable faults within an IMA platform should have a response determined. Failures within an application which do not affect IMA platform resources are the responsibility of the application. The application should provide the correct response to these failures including providing health status of the application. Any attempts by the application to violate platform partitioning services should be monitored and detected by the IMA platform and appropriate action taken by the platform. The IMA platform response to these faults may be configurable.

The ability to contain faults to an isolation zone greatly facilitates the integration of hosted applications on an IMA platform. This assumes that partitions are all fault containment zones and that platform services are also fault containment zones.

3.6.5 Flight Crew Annunciation and Messaging

In general, IMA systems should be treated no differently than traditional federated systems with respect to flight crew annunciation and messaging. Within the framework of flight alerts and maintenance message systems, the focus for the flight crew is function availability. Although maintenance systems provide information on aircraft maintenance aspects and aircraft dispatch (MMEL) with a degree of correlation to improve the efficiency and efficacy of the maintenance reports, it is the responsibility of the flight alert/warning systems to provide the primary source of information to

assist the flight crew in their decision-making process. This is achieved through systems monitoring with respect to a centralized alerting and warning function, including messages and aural alerts. The flight alert/warning systems, in conjunction with items such as the MMEL, provide the flight crew and maintenance personnel with the information essential to determine the dispatch status of the aircraft.

However, given the status of the IMA system as a whole, and the individual components and hosted applications, certain types of status may need to be annunciated to the crew with respect to system degradation. Flight alert/warning systems may selectively inhibit some warnings to reduce the effects from cascading failures; typically, however, all failures and system degradation and reconfiguration actions are reported.

The appropriate faults, failures, and errors to be logged, reported, or displayed to the flight crew should be determined. These notifications may be restricted to failures from which the system cannot recover (e.g., a hardware failure), failures resulting in degraded performance or a degraded mode, failures that can reduce the safety margins of the aircraft or system (e.g., loss of redundancy or integrity), potential unsafe conditions or notification of loss of functionality. The IMA system fault messages displayed to the flight crew should be analyzed to ensure they are unambiguous and have appropriate priorities assigned to them. Displayed messages and aural alerts should be provided in a clear and prioritized manner to the crew.

3.6.6 Control of Maintenance Actions and Reporting

Maintenance personnel need to be able to analyze health monitoring data, identify system components that have failed or exhibited anomalous behavior, and determine the most appropriate maintenance actions (e.g., defer, test, repair, replace, etc.).

The level of integration, interdependency, and complexity of an IMA system may result in unique and more numerous potential failure modes (for example, all functions affected by the loss of a single shared resource) than federated system architectures. Power supply transients, cascading failures, or failures affecting shared resources can result in multiple functions and hosted applications failing simultaneously, and multiple failures, warning, alert or caution messages being logged and annunciated to the flight crew. Although many of the features described can be attributed to traditional federated systems, particular emphasis should be placed on fault correlation with respect to Built-In Test Equipment (BITE) fault reporting within IMA systems to reduce fault propagation and distinguish between platform-related versus application-related issues.

In general, the maintainability of airborne systems should also be considered in conjunction with the safety, reliability, and supportability objectives for the aircraft. Analysis of these interrelated objectives may also identify unique aspects of preventative maintenance actions.

3.6.7 Redundancy Management

Redundancy is used to improve both the reliability and availability of an aircraft function. An IMA platform and/or system may include mechanisms to support management of redundancy for hosted applications. Redundancy management policies should be established for the IMA system. Where possible, redundancy should be managed independent of the hosted applications to support separate analysis and development of applications and platforms.

Some hosted applications may require application-specific redundancy management. For these the IMA system should provide correct and consistent information about the health of the platform resources, as well as the health of other modules with which the application interacts.

3.6.8 Single Event Upset (SEU) Faults

IMA systems host aircraft functions and applications in a computer environment using shared resources, such as electrical power, computer processing, memory, and data buses. This means there is a potential for an SEU in a shared resource to adversely affect multiple different aircraft functions, applications, and partitions. The IMA platform design and fault management strategy should address the potential for SEU and provide appropriate recovery capabilities.

3.7 IMA SYSTEM CONFIGURATION MANAGEMENT

The certification applicant should provide a robust and easily maintainable configuration management system for the operator of the aircraft. The IMA platform developer should provide capabilities and means for the certification applicant to determine the configuration of the IMA system, platform, modules, resources, functions and hosted applications and databases. The IMA system is composed of multiple, general-purpose, shared resources that may be labeled in a traditional manner or using electronic part numbering. The role and actions of the operator in maintaining the configuration of the aircraft and IMA system should be simple and verifiable. Procedures should be provided to the operator to simplify the task and minimize the likelihood of operator errors and mistakes when maintaining the IMA system. The operator should be provided with the means to verify that the configuration of the aircraft and IMA system is consistent with the certified configuration and conforms to its type design.

Issues to be addressed:

a. Extent of configuration data required for IMA system software and hardware part numbers.

b. Configuration data as controlled configuration items.

c. Coherence among configuration data.

d. User-modifiable hardware, databases, and software without certification authority oversight.

e. The ability to retrieve part numbers from modules and applications for conformity inspections.

f. Multiple, selectable configurations (option selectable modules).

g. Field-loadable modules (hardware, software, databases).

h. Maintenance of configuration data after modification.

i. Configuration practices to provide a means to verify:

- all hardware part numbers and serial numbers installed in the system,
- all hardware modification status indicators,
- the identity of all software (hosted applications and core software) part numbers installed in the system,
- the identity of all configuration data installed in the system,
- the identity of all database files installed in the system,
- all hardware, software, and database file part numbers are correct for the specific aircraft, and
- compatibility of the mix of IMA modules, resources, and hosted applications, especially relative to field loadable components.

3.7.1 Configuration Data

Both the IMA system and the hosted applications should maintain configuration data in the system. These sets of configuration data are aircraft certification compliance items (type design data) and should be included in the certification data packages. These configuration data should be shown to be traceable to the application or module requirements from which they were derived. Verification of the correctness of these files may be shown by a combination of review, analysis, and testing.

The IMA system should manage the field loading of the hosted applications and their configuration data. The IMA system may use information in these files to determine correct configuration of the application, its resource needs, or its status. The design and assurance of the configuration data used by the hosted applications is the responsibility of the application developers and can be achieved independently of the IMA system design and assurance activities.

3.7.1.1 IMA System Configuration Data

There are configuration data unique to IMA systems that are subject to specific certification guidance. For example, it is expected that IMA systems will include configuration data for scheduling applications and allocating resources. This data could be implemented as a set of configuration tables or files established at build time or as separately loadable data.

Configuration data described and discussed in this section is used by the IMA system to:

a. define or select the correct configuration for the aircraft IMA system in its installation.

b. enable configuration control and support conformity inspection of the IMA system, platform, modules, resources and applications.

c. activate or deactivate modules, resources, or functions, e.g., adaptation of the software to several aircraft configurations using option-selectable software or data.

d. define the allocation of IMA system resources to the hosted applications.

e. define the allocation and characteristics of inter-partition communication ports.

f. define other parameters that affect the integrated system (e.g., schedule, performance, module part numbers).

The IMA system configuration data may be dependent on each other. Such a set of configuration data can be considered to make up a single overall configuration for the IMA system. This overall configuration may be controlled as a single end item for which certification data is provided.

3.7.1.2 Application Configuration Data

Other types of configuration data may be used by the hosted applications on the IMA system to:

a. activate or deactivate functions or application-specific resources (e.g., adaptation of the software to several aircraft configurations using option-selectable software, of the hosted applications).

b. adapt the application to the aircraft configuration.

c. provide data to the hosted applications.

3.8 GUIDANCE ON USE OF SHARED DATABASES

Databases are included in aircraft systems to provide static read-only data to the applications. IMA systems may require read-write databases. These databases may be installed as a shared resource or dedicated to a specific application.

IMA system hosted databases may be functionally identical to the databases used with traditional federated systems. The industry accepted guidance for satisfying airworthiness requirements for aeronautical databases are provided in existing documents, such as ED-76/DO-200 (Ref. [3]) and ED-77/DO-201 (Ref. [4]).

Shared databases may be viewed as another shared resource managed by the IMA platform. Shared resources are discussed in Section 3.5. Corruption of shared databases should be addressed by the IMA system health monitoring and fault management function.

3.9 MASTER MINIMUM EQUIPMENT LIST (MMEL)

IMA systems may host and interface with many aircraft systems. With the introduction of these highly integrated systems, the traditional approach of independently addressing aircraft systems, LRUs, or functions is more difficult and may not be possible. The highly integrated nature of an IMA system results in failure modes, resource management, health monitoring, fault management, and other design considerations which may be very different from a typical federated system architecture and strategies.

3.9.1 Design Considerations for MMEL

The MMEL, where required, should be part of the IMA system design and requirements so that fault management and redundancy management can be analyzed and incorporated into the IMA system design. MMEL allowances should be determined with appropriate consideration given to the criticality of IMA system functions and applications, and the effects of the failures upon these systems, functions and shared resources. MMEL allowances should be based on the aircraft-level functional hazard assessment and system safety assessment, and should consider any impact on other functions that share resources with the failed component, resource or function. Any proposed MMEL allowance should continue to demonstrate compliance with the applicable regulations.

When either the FHA or SSA requires the IMA system module, function, or application to be disabled or isolated until appropriate maintenance actions have been taken to correct the failure, then a means of disabling or isolating the failed component should be provided. Where a failed component is not required to be disabled or isolated and may be able to be recovered or reactivated, it should be shown that it cannot be recovered or reactivated in an unsafe condition or have any adverse effect on any other system or function of the aircraft or aircraft safety margins. Functional tests may be required when analysis is not practical to confirm fault isolation and management, recovery actions, redundancy management, degraded operational modes, etc. and to verify that a fault in one or more systems or functions has no adverse or unforeseen cascading effects on other systems or functions.

3.9.2 Approval Considerations for an MMEL

The maintenance and operational requirements for dispatching the aircraft under MMEL allowance should include the appropriate safety justification and procedures that are based on the design considerations of Section 3.9.1. The MMEL should be submitted to the applicable regulatory authority with the supporting data, justifications, and procedures.

3.10 HUMAN FACTORS CONSIDERATIONS

The increased level of integration and complexity introduced by IMA systems has the potential to introduce different interdependencies and interactions between aircraft systems and the flight crew and maintenance personnel than exist in traditional federated system architectures. Human factors issues should be addressed in the IMA system design, with particular emphasis on the identification of performance requirements, functional interactions, pilot interface, displayed information, fault management and crew alerting, degraded operational modes, and the potential for cascading failures. Similarly, the human factors aspects for the continued airworthiness process should be addressed in IMA system design.

Human factors requirements for flight crew and maintenance personnel should be developed as part of the IMA system requirements. A plan to address human factors requirements should be developed early in the program and should include the corresponding methods for complying with those requirements. The human factors requirements for an IMA system may be developed by analyzing the tasks that will be performed by the users (flight crew and maintenance personnel), and the resulting user interfaces to perform those tasks. Analyses used to validate that the design will meet flight crew and maintenance personnel requirements and help system designers meet those user needs may include prototyping, human-in-the-loop testing, user validation, and other methods. The user performance requirements (e.g., response times, duration, load, feedback, etc.) that will be experienced by the flight crew under normal, abnormal, and emergency conditions should be identified and addressed in the design of an IMA system. Design features of the IMA system may need to be modified based upon the results of the human factors analysis of tasks and user interface issues.

The following items, where applicable, should be addressed:

a. Direct user interfaces, such as flight deck interfaces, maintenance interfaces, support crew interfaces, automation or human interaction (e.g., autopilot and other aircraft interfaces).

b. Information processing, displayed information and system information processes.

c. Human information processing – the ability of users to easily understand and act on available information.

d. Standardization (e.g., procedures, tasks, language, symbols, colors, information).

e. System and human performance and response time, including time to do tasks, refresh rates, and consideration of human limitations and potential for error.

f. Automation monitoring and explanation to humans.

g. Health and operational status monitoring and human interaction.

h. Multiple failure and alert messages – should be displayed in a clear and prioritized manner.

i. Fault resolution actions by the flight crew: allowed and disallowed actions in flight.

j. Design for maintainability (e.g., fault management and recording).

k. Design for the full range of human actions and performance that can be encountered.

l. Design system to minimize training and simplify maintenance.

m. Ongoing identification, tracking, and resolution of design issues throughout the development life cycle of the IMA system.

The human factors requirements and the corresponding methods for compliance should be included in the certification plans described in Sections 4.4.3 and 4.5.3.

The human factors requirements are derived from the aircraft and IMA system requirements. To ensure that all of the requirements have been satisfied, traceability should be established between the aircraft and IMA system requirements, including human factors requirements. Verification of the implementation of these requirements should be accomplished by a combination of reviews, analyses, and testing activities.

CHAPTER 4

CERTIFICATION TASKS

This section addresses the IMA system certification considerations with regard to compliance with the applicable regulations, and the functional, performance, and safety requirements defined for the system.

4.1 OVERVIEW OF THE CERTIFICATION PROCESS

An important aspect of the certification process for IMA systems is to obtain incremental acceptance of and certification credit for IMA platforms, modules, and/or hosted applications, cumulating in IMA system installation approval on an aircraft product, and resulting in issuance of the product certificate.

Typical development processes are divided into six tasks that define the incremental acceptance activities for the certification process for IMA systems:

- Task 1: Module acceptance
- Task 2: Application software/hardware acceptance
- Task 3: IMA system acceptance
- Task 4: Aircraft integration of IMA system – including validation and verification
- Task 5: Change of modules or applications
- Task 6: Reuse of modules or applications

The six tasks are illustrated in Figure 4 and will serve as a structure for the remaining sub-sections of this section. Some of these tasks may be concurrent and in some projects some tasks may not be applicable. A subsection is dedicated to each task.

The initial acceptance of a module, application, or IMA system should occur in the framework of an aircraft or engine certification program (TC) or modification project (STC). That is, IMA acceptance can only be proposed in the context of an actual certification project.

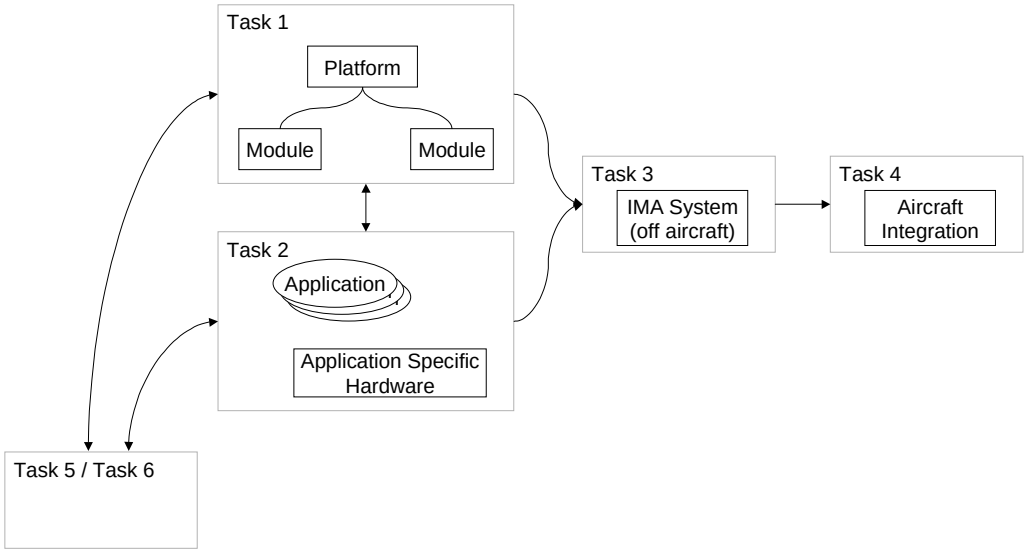

FIGURE 4 : IMA SYSTEM CERTIFICATION TASKS ILLUSTRATION

Table 4 provides a summary and overview of the certification tasks, their references in this document, and the typical means of acceptance. In some cases the compliance data may be approved (with a stamp or letter) prior to issuance of an acceptance letter, which may occur later in the certification project after integration, i.e., at or near the certification date of the aircraft product.

The life cycle data to be generated for each task is represented in the appropriate referenced section and Annex A tables (as shown in column 2 of Table 4). In many cases, stakeholders may have pre-existing processes or may package their data differently. If alternate titles or packaging is used, the stakeholder should develop a document mapping to demonstrate that all the applicable data is available.

TABLE 4 : OVERVIEW OF IMA CERTIFICATION TASKS

Task	Reference/ Objectives	Example means of granting acceptance
Task 1: Module acceptance	Section 4.2 Table A-1	Acceptance letter[2] or stamped data sheet Stamped or approved module acceptance data package RSC acceptance letter (Software only as defined in AC 20-148, Ref. [9]) TSO-C153 authorization letter (Hardware only as defined in Ref. [10])
Task 2: Application acceptance	Section 4.3 Table A-2	Acceptance letter[2] or stamped data sheet RSC acceptance letter (Software only as defined in AC 20-148, Ref. [9]) Stamped or approved IMA platform-hosted application compliance data package
Task 3: IMA system acceptance	Section 4.4 Table A-3	Accepted or approved compliance data package
Task 4: Aircraft integration of IMA system – including V&V	Section 4.5 Table A-4	TC, STC, ATC, ASTC
Task 5: Change of modules or applications	Section 4.6 Table A-5	Same as Task 1 if change of module Same as Task 2 if change of application (both depend on significance of change, aspects of Tasks 3 and 4 may need to be performed also)
Task 6: Reuse of modules or applications	Section 4.7 Table A-6	Same as Task 1 if reuse of module Same as Task 2 if reuse of application (both depend on similarity of reuse environment, aspects of Tasks 3 and 4 may need to be performed also)

[2] Contents of acceptance letter would be similar to the RSC acceptance letter described in AC 20-148, i.e., it should fully describe the content and limitations of the accepted task.

4.2 TASK 1 – MODULE ACCEPTANCE

The purpose of module acceptance within the overall certification process is to demonstrate the module characteristics, performance, and interfaces to obtain incremental acceptance of the module. This is accomplished by providing documented evidence (acceptance and/or compliance data) for the benefit of the other IMA system acceptance tasks and for potential reuse as addressed in Section 4.7. Acceptance of a module can only be performed in the context of the aircraft and/or engine certification program or modification project.

The module acceptance process allows an applicant to gain incremental acceptance for individual components of the IMA platform (e.g., processing module, core software services (e.g., operating system, health monitoring function, fault management function), power module, interface module) toward gaining acceptance of the IMA platform. The platform itself may also be accepted as a module, which typically contains multiple other modules.

4.2.1 Module Acceptance Objectives

The objectives of the module acceptance process are:

a. Plan the acceptance tasks to meet all of the applicable certification requirements. Ensure other stakeholders agree with the acceptance plans.

b. Develop specifications for the module and demonstrate compliance with the Module Requirements Specification (MRS) (where the module supplier may develop the MRS based on assumptions for the intended use). Assumptions for intended use should be documented in the MRS and validated during the verification and validation process.

c. Demonstrate compliance of resource intrinsic properties, such as time and space partitioning, fault management, health monitoring, other safety features, determinism, latency, resource management, resource configuration, and application parameters. The usage domain properties should be predefined within the boundaries of the usability of resources.

d. Verify compliance of resource properties with established requirements in terms of the MRS, such as performance, interfaces, services, safety, fault management, and robustness (fault tolerance).

e. Develop the core software (e.g., operating system, API, and core services) and/or hardware, as relevant to the module and show compliance to the applicable guidance and regulations.

f. Develop and make available the module acceptance data for certification authority acceptance.

g. Provide users of the module with the necessary information to properly use, integrate and interface with the module (e.g., user's guide, module data sheet and interface specifications).

h. If the module is a platform, integrate the platform modules.

i. Assess and qualify, as needed, tools used in the development and verification of the module.

j. Implement quality assurance, configuration management, integration, validation, verification, and certification liaison for the module acceptance.

k. Provide users with the necessary information so that they can properly manage the configuration of the module. Modules should contain a means for the users to determine their configuration (e.g., physical part number), electronic part number/version, core software identifiers, and when that module has changed.

l. Define, specify, assess, and qualify, as needed, module supporting tools to be provided to and used by module users. If shared tools are used, develop an approach for sharing the tool data (e.g., user's guide, tool qualification data, tool specifications).

m. If reuse is a desired outcome for the module development, reuse should be addressed during the development of the module (see Section 4.7).

4.2.2 Module Acceptance Data

The module acceptance process should follow a systematic approach. There should be plans, requirements, and evidence of compliance with these plans and requirements. The following subsections define the module life cycle data needed for module acceptance and the typical contents of each data item.

Section 5.7 describes the data to be submitted to the certification authority. The process for gaining acceptance of the module acceptance data should be coordinated and agreed with the certification authority.

NOTE: *If the developer decides to gain acceptance for the hardware using TSO-C153, this authorization may be used to provide a subset of the acceptance data.*

4.2.3 Module Acceptance Plan (MAP)

The MAP is the primary means used by the module developer to present to the certification authority their plan for obtaining incremental acceptance for their module. It should address all aspects relevant for their specific module, including module development, verification, configuration management, quality assurance, and demonstration of compliance. The MAP should establish the basis for the module acceptance, and facilitate use of the module in the IMA system project. The MAP should address:

a. System overview (if applicable): This section provides an overview of the system in which the module will operate, including a description of its potential hosted applications and functions and their allocation to the hardware and software, the architecture, processor(s) used, hardware/software interfaces, and safety features.

b. Module overview: This section briefly describes the module functions with emphasis on the proposed safety and partitioning concepts, for example, resource management, redundancy, dissimilar design, fault tolerance, and timing and scheduling strategies.

c. Acceptance criteria: This section provides a summary of the criteria to be applied to the module to ensure that it will be acceptable for its intended use and function within the system. This includes the proposed software level(s), hardware design assurance level(s), hardware reliability data, hardware environmental qualification level(s), and/or credit sought for the module. This section should also address any safety objectives and safety-related requirements allocated to the module, known effects of the module on the IMA system safety assessment, and architectural and other features supporting any portion of the safety analysis, partitioning, or other protection strategies.

d. Module life cycle: This section defines the module development life cycle to be used, explains how the objectives of each life cycle process (requirements, design, implementation, verification) will be satisfied. Also specified are the organizations and stakeholders to be involved, the organizational roles and responsibilities, the system life cycle processes, and certification liaison process responsibilities. The development process, configuration management process, quality assurance process, and verification processes should also be addressed in the MAP.

e. Module life cycle data: This section specifies the module life cycle data that will be produced and controlled by the life cycle processes. Also described are the relationship of the data to each other or to other data defining the system, the module life cycle data to be submitted to the certification authority (module acceptance data and/or module compliance data), the form of the data, and the means by which module life cycle data will be made available to the certification authority. If alternate titles or packaging is used, the stakeholder should develop a life cycle data mapping to demonstrate that all the applicable data is available.

f. Schedule: This section should provide the certification authority with visibility of the activities of the module life cycle processes so reviews can be planned.

g. Tool qualification(s): This section describes the methods for assessing the tools used in the development, verification, configuration, integration, and loading of the module, identifies those to be qualified with references to tool qualification plans, and provides rationale for those used in the development that will not be qualified. It describes the functionality and means of qualification of all tools that may be provided to module users to support development, configuration generation, loading of applications and configurations, performance, and verification. This section should identify the tools that are intended to be shared with other module and application developers and integrators.

h. Module reuse: If the module is being developed for reuse (see Section 4.7), the MAP should address the following aspects:

- Justification for reuse suitability, i.e., what aspects of the module make it suitable for reuse
- List of data to be supplied to the applicant to be used as type design data and support module acceptance for their project.
- Prior credit being claimed for the module and the further activities to complete and satisfy the new objectives.
- Plans for addressing common reuse issues.
- Development of data to support reuse, such as: interface definition data, documented usage domain, safety assumptions or failure conditions, user's guide, limitations, instructions for completing any partial credit, etc.
- Applicable guidance for the reusable application, e.g., AC 20-148 (Ref. [9]) and/or Chapter 12 of Order 8110.49 (Ref. [11])

i. Additional considerations: This section describes specific features that may affect the module acceptance process, for example, alternative methods of compliance, tool qualification, reconfigurable modules, COTS software and/or hardware, and product service history. Refer to ED12/DO-178 (Ref. [2]) and ED-80/DO-254 (Ref. [6]) for additional guidance.

NOTE: *The MAP may be divided into multiple documents, such as a development plan, a configuration management plan, a quality assurance plan, and a verification plan, if desired. Likewise, the MAP may reference other plans (see Figure 5).*

4.2.4 Module Requirements Specification (MRS)

The Module Requirements Specification (MRS) defines the requirements and design criteria for the module that will be integrated into an IMA system. This MRS should include the following types of information:

a. Description of the module requirements, with attention to safety-related requirements, protection requirements, and potential failure conditions.

b. Functional and operational requirements under each mode of operation. This should define the functional and performance capabilities of the module, as described below:

- Functional capabilities: This information provides the user with a description of functionality the module performs. Of particular importance are descriptions of the functionality that externally affects users of the module.
- Performance capabilities: This information includes the performance capabilities of the module that are needed by the user for interfacing and integrating purposes (examples of such information are accuracy and resolution, timing characteristics, capacities, and limits).

c. Safety capabilities: This should include information necessary for users to develop and analyze the system to ensure module use in the system will comply with safety requirements. It also includes intended criticality, failures and malfunctions, fault probabilities, software levels and hardware design assurance level(s), assumptions, flight crew alerts and system messages, maintenance checks), installation limitations, independence and isolation requirements, environmental limitations, and requirements for resource management, health monitoring, fault management, robust partitioning, and other protection means.

d. Interface requirements: This should include protocols, formats, input/output, frequency of inputs, frequency of outputs, and allowed interfaces with other modules.

e. Interface definition: This should include all information needed by a user to interface and use the module. Examples are: data buffer layouts, voltages, pin signal definition, data transfer protocols (runtime/maintenance/loading, data integrity encoding/decoding, memory map layouts, timing, synchronization signals, interrupt definitions, electronic configuration data, partitioning boundary set-up information, API definition). Additionally, the definition should include information regarding any abnormal states the data and control interfaces can assume, such as invalid data conditions, test modes, initial conditions, and reset modes.

f. Fault management and health monitoring requirements.

g. Resource management: The strategy for managing each resource and its limitations, the margins, and the method for measuring those margins.

h. Scheduling procedures and inter-processor/inter-task communication mechanisms, including time-rigid sequencing, preemptive scheduling, and interrupts.

i. Requirements for robust partitioning, including identification of allowed interactions between module partitions and requirements for the methods and means of preventing partition breaches, detecting partition violations, and recovering from partition violations.

j. Description of the module and its component, whether they are new or previously developed or accepted, and, if previously developed or accepted, reference to their previous baseline.

k. Description of deactivated features or mechanisms (for future reconfiguration), if appropriate.

l. Where modules use software and/or hardware requirements and design data, the software and hardware data should contain the information described in ED-12/DO-178 (Ref. [2]) Sections 11.9 and 11.10 and ED-80/DO-254 (Ref. [6]) Section 10.3. The data may be referenced, rather than repeated.

m. Physical and installation definition: This includes physical and installation-specific information necessary (e.g., ED-14/DO-160 (Ref. [6])), for the system integrator to integrate the module with other modules and the IMA system.

4.2.5 Module Validation and Verification (V&V) Data

Module V&V data is the evidence of the completeness, correctness, and compliance of the module with its requirements, as defined in the MRS. It provides assurance that the module has been developed to its requirements, correctly produced, validated and verified, and the acceptance criteria has been achieved. Data includes procedures and results for module reviews, analyses, simulation, and testing. Module V&V includes at least the following data:

a. Module V&V plan, which may be part of the MAP and/or the IMA system V&V plan.

b. Software verification cases, procedures, and results (see ED-12/ DO-178, Ref. [2], Sections 11.13 and 11.14), as appropriate to the software level when software is part of the module.

c. Traceability data, review and analysis procedures and results, test procedures and results, and test acceptance criteria (see ED-80/DO-254, Ref. [6], Sections 10.4 and 10.5), as appropriate to the design assurance level when complex hardware is part of the module.

d. Data, which includes the environmental qualifications form, level(s) of testing, test plan, test procedures, and results of the tests (see ED-14/DO-160, Ref. [1]). Not all testing can typically be done at the module level. Certain types of tests can only be done when the module is integrated within the system and/or aircraft.

e. Module integration V&V cases and procedures, when modules are integrated. These include at least the following:

- Review and analysis procedures: Details, supplementary to the description in the V&V plan, which describes the scope and depth of the review or analysis methods to be used.
- Test cases: The purpose of each test case, set of inputs, conditions, expected results to achieve the required coverage criteria, and the pass/fail criteria.
- Test procedures: The step-by-step instructions for how each test case is to be set up and executed, how the test results are evaluated, and the test environment to be used.

f. Module integration V&V results should document the following:

- For each review, analysis, and test indicate each procedure that passed or failed during the activities and the final pass/fail results.
- Identify the configuration item or version reviewed, analyzed, or tested.
- Include the results of tests, reviews, and analyses, including coverage analyses and traceability analyses.

g. Module traceability data. Module traceability establishes a correlation between the requirements, detailed design, implementation, and verification data that facilitates configuration control, modification, and verification of the module.

4.2.6 Module Quality Assurance (QA) Records

The results of the module QA process activities are recorded in QA records. These may include QA review or audit reports, meeting minutes, records of authorized process deviations, and conformity review records.

4.2.7 Module Configuration Index (MCI)

The MCI identifies the configuration of the module and the module life cycle environment. This index is written to aid reproduction of the module, including its life cycle environment, and should include:

a. The module description and configuration.

b. Each component of the module at the next lower level of assembly.

c. Previously developed modules, if used.

d. Module life cycle data, including module acceptance data and module compliance data.

e. Archive and release media.

f. Instructions or drawings for building the module.

g. Identification of the module life cycle environment.

h. Identification of the development and verification tools used to develop and verify the module, including reference to tool qualification data.

i. Identification of the test environment used to verify the module.

j. Data integrity checks, if used.

4.2.8 Module Acceptance Configuration Management (CM) Records

The results of the module CM process activities are recorded in CM Records. Examples include configuration identification lists, baseline or library records, change history reports, archive records, and release records.

4.2.9 Module Acceptance Accomplishment Summary (MAAS)

The MAAS for the module is the primary data item for showing compliance with the MAP. The MAAS should include:

a. Same information as in the MAP (see Section 4.2.3) and any deviations from the MAP.

b. Module characteristics: This section states the timing and memory margins, resource limitations, additional constraints, and the means of measuring each characteristic. This section may be a summary of the module data sheet (see Section 4.2.10).

c. Module identification: This section identifies the module configuration by part number and version.

d. Change history: If applicable, this section includes a summary of module changes with attention to changes made due to failures and anomalous behavior, and identifies changes from the module life cycle processes since the previous acceptance.

e. Module status: This section contains a summary of problem reports unresolved at the time of acceptance, including justification and a statement of functional limitations.

f. Compliance statement: This section includes a statement of compliance with the applicable objectives for this task as defined in Table A-1 of Annex A and this section, the module acceptance criteria, and a summary of the methods used to demonstrate compliance with criteria specified in the module plan(s). This section also addresses additional rulings and deviations from the plans and this document.

g. Remaining activities: This section includes a description of activities that the user and/or integrator will need to address to successfully and safely use the module.

4.2.10 Module Acceptance Data Sheet (MADS)

The MADS is provided to users, integrators, certification applicants, and certification authorities. It should include the following items, as appropriate:

a. Module description and intended use and functionality.

b. Module part number(s) including modification and revision status.

c. Reference to the final Module Configuration Index (with revision status).

d. Software level(s) and hardware design assurance level(s).

e. Environmental qualification test levels achieved.

f. Physical connection information for hardware (e.g., internal data bus interfaces, mating connectors, I/O connector and external data bus and interface requirements, mounting and handling requirements, inter-module interfaces and connections, grounding and shielding provisions, separation and isolation provisions).

g. Power requirements and dissipation.

h. Size and weight.

i. Special installation information including:

- software loading procedures
- required platform cabinet or electronic equipment rack model number(s) (for modules)
- grounding and shielding requirements
- mounting requirements (including orientation in aircraft)
- clearance requirements
- air flow and cooling requirements
- sub-assembly installation and mounting requirements (if applicable)
- separation and isolation provisions
- any other information needed by the user, installer or integrator

j. Limitations.

k. Continued airworthiness information, including any information for continued airworthiness that the user or installer should address.

l. Safety assessment information that may affect installation.

m. Tool requirements as applicable for software development, verification, and system configuration. Reference to the user's guide may also be included on the data sheet.

n. Any additional related acceptance data, such as acceptance letters, data approval letters, etc. should also be referenced.

o. Usage domain of the module.

4.2.11 Module Problem Reports

Module problem reports are a means to identify and record the resolution to errors, failures, and anomalous behavior of the module, process non-compliance with module plans, and deficiencies in module life cycle data. Module problem reports should include:

a. Identification of the configuration item and/or the module life cycle process activity in which the problem was observed.

b. Identification of the configuration item(s) to be modified or a description of the process to be changed.

c. A problem description that enables the problem to be understood and resolved.

d. A description of the corrective action taken to resolve the reported problem.

e. Verification of the corrective action (solution).

4.2.12 Additional Module Acceptance Life Cycle Data

In addition to the life cycle data discussed in 4.2.3 through 4.2.11, the following life cycle data should be addressed, as appropriate:

a. Supporting data: ED-12/DO-178 (Ref. [2]), ED-80/DO-254 (Ref. [6]), and ED-14/DO-160 (Ref. [1]) data that supports the module acceptance.

b. Safety assessment analysis/reports to support the overall aircraft safety assessment and IMA system safety assessment processes.

c. Tool data: Tools used for the development and verification of the module may need to be verified or qualified. In addition, the module developer may provide tools to the integrator or certification applicant to use to integrate or verify the integration of the module. Verification of tools should be documented in verification results. If qualification is needed, tool qualification data should be developed (see ED-12/DO-178, Ref. [2], Section 12.2).

d. Development standards (e.g., coding, requirements, and design) used to develop, design, and implement the module.

e. User's guide: This includes all information for users, integrators, and certification applicants to successfully interface or integrate the module. The guide should define the usage domain for which the module acceptance data are valid. The information should include recommendations and examples for correct use. In addition, the guide should highlight any warnings or limitations for integrating or interfacing the module to avoid potential incorrect or unintended use.

4.3 TASK 2 – APPLICATION ACCEPTANCE

An application is software and/or application-specific hardware with a defined set of logical interfaces that, when integrated with a platform, performs an aircraft function or part thereof. The main goal of application acceptance within the overall IMA system acceptance process is to demonstrate that the application complies with the applicable regulations and requirements allocated by IMA system design, performs within the module limitations, and provides the characteristics and performance as specified. Another goal is to provide acceptance data and compliance evidence for the benefit of the integration of the application in the IMA system and its potential reuse on subsequent projects (see Section 4.7). A process for accepting the application life cycle data (e.g., acceptance letter, stamped data, data approval letter) should be coordinated with the certification authority.

Software and/or hardware applications intended for future reuse should be developed using available guidance such as AC 20-148 (Ref. [9]), ED-12/DO-178 (Ref. [2]), and ED-80/DO-254 (Ref. [6]).

NOTE: *Section 5.7 describes the data to be submitted to certification authority.*

4.3.1 Application Acceptance Objectives

The objectives of the application acceptance process are:

a. Demonstrate that the application performs its intended function and satisfies applicable regulations while properly utilizing the appropriate platform resources and interfacing with other modules and/or applications.

b. Define the platform resources required by the application.

c. Verify that the application uses the platform resources in accordance with the appropriate module requirements specification, interface specifications and module/platform user's guide.

d. Ensure that other acceptance and approval activities are addressed as appropriate.

e. Develop the necessary application life cycle data. This data may be organized in a way to support future application reuse.

f. Validate and verify the operation of the application when integrated on its target IMA platform.

g. Maintain configuration control and ensure properly configured tools and modules are used for the development, integration, and verification processes.

h. If reuse is desired for the application, it should be addressed during the application development.

4.3.2 Application Acceptance Data

The application acceptance process will typically involve compliance with ED-12/DO-178 (Ref. [2]), ED-80/DO-254 (Ref. [6]), and ED-14/DO-160 (Ref. [1]). Therefore, the associated life cycle data should be produced and organized to support the IMA system acceptance objectives, and, in particular, to support IMA system integration and certification of the IMA system on the aircraft, and to show that the application functions correctly within the platform and module requirements and limitations.

In addition to the previously specified life cycle data, additional data may be needed for application acceptance or demonstration of compliance, depending on the nature of the IMA system installation on the aircraft. For example, interface specifications and usage domain analysis data may be required to ensure that the application is compatible with the platform.

If reuse of the application is desired (see Section 4.7), the Plan for Software Aspects of Certification (PSAC) or the Plan for Hardware Aspects of Certification (PHAC) for the application should address the following aspects:

a. Justification for reuse suitability, what aspects of the application make it suitable for reuse.

b. List of data to be supplied to the certification applicant to be used as type design data to support certification and reuse.

c. Credit being claimed for the application (full, partial, or none), and activities for the users to complete to achieve full credit for all objectives.

d. Plans for addressing common reuse issues.

e. Development of data to support reuse, for example: interface definition data, documented usage domain, safety assumptions or failure conditions, user's guide, limitations, instructions for completing any partial credit, application data sheet (similar to the module data sheet described in Section 4.2.10), environmental qualification, etc.

f. Applicable guidance for the reusable application, e.g., AC 20-148 (Ref. [9]) and/or Chapter 12 of Order 8110.49 (Ref. [11]).

g. Plans for how guidance in Section 4.7 (Task 6) will be addressed.

h. Plans for how a problem reporting system will be developed to support future reuse.

4.4 TASK 3 – IMA SYSTEM ACCEPTANCE

The main goal of IMA system acceptance is to demonstrate that the integrated modules, hosted applications, and the platform continue to perform their intended functions and do not adversely affect other hosted applications or modules. The activities may be performed on or off the aircraft. For off-aircraft activities, a major goal is to perform V&V activities that can be applied toward the overall aircraft certification effort. The level of certification credit obtained for the particular off-aircraft V&V should be coordinated in advance with the certification authority.

The delineation between Tasks 3 and 4 will vary significantly by project. Therefore, the life cycle data for Tasks 3 and 4 may be combined or allocated as appropriate. Any life cycle data not addressed in Task 3 should be completed in Task 4.

4.4.1 IMA System Acceptance Objectives

The objectives of the IMA system acceptance process are:

a. Plan the IMA platform and system activities with the intent of using the integration, validation, and verification for aircraft-level certification credit.

b. Consolidate the resource requests from applications to be integrated and generate a final IMA system configuration using defined tools and processes.

c. Verify proper interaction between all applications, modules, and platform resources, including robustness testing, correct resource allocation and management, correct redundancy management, no adverse impact on performance of individual applications, and satisfaction of safety, health monitoring, fault management, partitioning, and protection requirements.

d. Demonstrate compliance with appropriate regulations, guidance, and requirements.

e. Demonstrate that the configuration of IMA system is correct and approved processes are followed.

f. Perform integration and V&V activities on the IMA system.

g. Develop IMA system acceptance and compliance data.

h. Evaluate module and application problem reports to determine their impact on the IMA system, and take appropriate action.

4.4.2 IMA System Acceptance Data

The IMA acceptance process should use a structured approach. The acceptance process for the IMA system should be documented in an IMA System Certification Plan (IMASCP) and an IMA system V&V plan. The V&V results, system restrictions, limitations and tools used should be documented in the IMA System Accomplishment Summary (IMASAS). The IMA system configuration index should define the compatibility between modules and hosted applications at the IMA system- and aircraft-levels.

Before submitting to the certification authority, the acceptance data should be reviewed and accepted by the certification applicant. Sections 4.4.3 through 4.4.7 describe the IMA system acceptance data to be generated and their typical contents.

4.4.3 IMA System Certification Plan (IMASCP)

The IMASCP should include, as a minimum:

a. A functional and operational description of the IMA system including the modules, resources, platforms, and hosted applications that compose the IMA system. This description should establish the functional, physical, and interface relationships between the modules, resources, platforms, hosted applications, and any other external systems and functions (e.g., interfaces with non-IMA system functions).

b. A statement of the relationship of the IMASCP to any other relevant certification (aircraft certification plan) and acceptance plan(s). If alternate titles or packaging is used, the stakeholder should develop a life cycle data mapping to demonstrate that all the applicable data is available.

c. A summary of the PSSA, reliability requirements, and assurance level allocations for the system, hardware, and software, and assumptions of the FHA (aircraft hazards, IMA functional hazards, failure conditions, and classifications). Also, a description of the IMA system fault tolerance, fail-safe design features, and reversion capabilities (e.g., resource management, fault management, health monitoring, failure recovery, degraded modes, comparators and voting planes, redundancy, and functional isolation and independence capabilities).

d. A description of any new or novel design features that are planned to be used in satisfying the safety objectives and complying with the regulations.

e. High-level description of human factors issues (see Section 3.10).

f. The IMA system certification basis including any special conditions, exemptions, deviations, or equivalent level of safety proposals.

g. Identification of field-loadable software or hardware, option-selectable software or hardware, and user-modifiable software and the parties responsible for loading, modifying, and verifying the software loads, option selections, and user (operator) modifications.

h. Proposed acceptance and approval means for the IMA system, i.e., the certification approach for system, hardware, and software. The proposed methods of showing compliance with the certification basis, including an outline of the anticipated development assurance processes (safety assessment, development, validation, verification, configuration management, quality assurance, and certification liaison). This should include a description of how objectives of this document will be satisfied. Sections 5.5.1 and 5.6 provide details on IMA system configuration and quality assurance plans; these plans may be included in or referenced by the IMASCP.

i. Description of integration activities.

j. Any additional compliance means should be described and justified. If using previously developed or accepted software or hardware (reuse), this may include compliance methods for change impact analyses, usage domain analyses, module or application reuse, etc.

k. A list of the compliance and acceptance data to be submitted to the certification authority and the data to be retained under configuration control, along with a description or sample of data formats.

l. The approximate sequence and schedule for acceptance, approval, and certification events with their interdependencies.

m. List of roles and responsibilities for all stakeholders involved in the IMA system development, acceptance, integration, installation, and certification (see Section 2.4).

n. Identification of the key personnel or specific organization(s) responsible for acceptance and certification coordination.

o. Description of how problem reports from modules and applications will be evaluated for impact on the IMA system.

4.4.4 IMA System Validation and Verification Plan (IMASVVP)

The IMASVVP should include or provide references to the following kinds of information:

a. Description of how different modules, resources, platforms, and hosted applications are integrated into the IMA system.

b. Description of the methods and procedures to be applied for V&V of the IMA system.

c. Description of how fault tolerance, fail-safe design, and reversion features and functions will be verified and validated.

d. Data to be recorded during the V&V activities for the IMA system, such as summaries, review results, analyses, simulation, bench test results, integrated system laboratory test results, or investigations.

e. Description of how SSA assumptions, system safety features, and system resource allocations and management will be validated and verified.

f. How the status of V&V activities will be maintained or managed, especially when changes are made to requirements or resource allocation.

g. Description of the pass/fail criteria for each V&V activity.

h. Roles and responsibilities associated with the V&V activities.

i. A schedule of key V&V activities with a description of their interdependencies.

j. A description of the degree of independence of the development and verification activities.

For completeness and consistency the integration, validation, and verification activities should be coordinated with all involved stakeholders.

4.4.5 IMA System Configuration Index (IMASCI)

The IMASCI should include the following information and/or provide references to other data containing this information:

a. Identification of the physical location within the IMA system of hardware and software components.

b. Configuration identification of each IMA system component.

c. Configuration indices for the development, integration, and V&V environments.

d. Operational or maintenance procedures and limitations that are integral to the IMA system.

e. Any system design features or capabilities provided to establish IMA system safety under the applicable regulations should be identified.

f. Interconnection and inter-relationship of IMA platforms and hosted applications.

g. Interfaces (e.g., buses, dedicated links, etc.) with other aircraft systems.

h. Information describing permissible interchangeability and/or intermixability of alternate items, if applicable.

i. Identification of qualified tools and their associated tool qualification data.

j. Reference to IMA system component configuration indices.

k. Instructions for loading, verifying, and maintaining proper IMA system configuration and conformance to the IMA system and aircraft type design.

4.4.6 IMA System Accomplishment Summary (IMASAS)

The IMASAS should include the following information, as a minimum:

a. The same information as included in the IMASCP (in Section 4.4.3) and a description of any deviations from the plan, including rationale to substantiate the deviation.

b. List of all open problem reports with a brief description (including justification as appropriate) of their impact on IMA system functionality and/or aircraft safety, operations, maintenance, or limitations.

c. Identification of the IMA system components, including part numbers and versions.

d. Summary of changes made if the IMA system is based on a previously approved IMA system baseline.

e. Statement of any required limitations.

f. A statement of compliance to the airworthiness regulations, this guidance, and any other applicable guidance.

g. List of data that demonstrates compliance of the IMA system for installation approval and aircraft certification (including reference to or listing of acceptance and compliance data for all modules, applications, and the IMA system).

4.4.7 Other IMA System Life Cycle Data

a. V&V records and results for all system-level activities.

b. Configuration management records.

c. Quality assurance records.

d. Safety assessment analyses and report(s).

e. Problem reports.

f. IMA system requirements and design data, which may be part of the aircraft requirements.

g. Tool qualification data as defined in ED-12/DO-178 (Ref. [2]) or ED-80/DO-254 (Ref. [6]).

4.5 TASK 4 – AIRCRAFT INTEGRATION OF IMA SYSTEM (INCLUDING V&V)

The final IMA system installation, integration, and V&V activities are similar to those that would be conducted on a federated system architecture, demonstrating that each aircraft function and hosted application functions as intended, supports the aircraft safety objectives, and complies with the applicable regulations. However, during the installation activities, the interactions between hosted applications relative to the provided aircraft functions should be verified and validated during aircraft ground and flight testing. Also, the interactions, interfaces, and connections between the IMA system and other aircraft systems should be verified and validated. Any IMA system life cycle data not addressed in Task 3 should be completed as part of Task 4.

The V&V activities are described in more detail in Sections 5.3 and 5.4.

4.5.1 Aircraft Integration Objectives

The objectives of the IMA aircraft integration process are:

a. Plan the activities for installation, integration, validation, and verification of the IMA system on the aircraft.

b. Demonstrate compliance with intended functionality and requirements, using laboratory, appropriate analyses, ground, and flight tests.

c. Verify IMA system resource management, fault tolerance and management, health monitoring, degraded modes, and reversion capabilities.

d. Demonstrate compliance to the regulations appropriate for the aircraft and/or engine certification basis.

e. Evaluate repercussion of specific anomalies, such as a loss or malfunction of multiple applications or of entire shared resources.

f. Perform V&V activities to address module failure modes affecting several hosted applications (intra-module analysis); common failure modes on module level affecting several hosting applications (inter-module analysis); and failure modes affecting multiple aircraft systems. Back up systems and mitigation means should also be addressed.

g. Address human factors issues regarding multiple aircraft functions failure and anomalous behavior especially under abnormal operating conditions and degraded modes (see Section 3.10).

h. Perform High Intensity Radiated Fields (HIRF) and Indirect Effects of Lightning (IEL) testing with regard to multiple aircraft functions failure and anomalous behavior, as required.

i. Verify proper interaction and interfaces between all IMA platforms, including their resources and hosted applications, and ensure there is no adverse impact on the performance of individual applications, modules, or any other aircraft systems.

j. Verify the failure effects of each IMA module and resource affecting more than one hosted application in the IMA system safety assessment.

k. Develop aircraft-level IMA system compliance data for acceptance by the certification authority.

l. Develop an aircraft-level safety assessment that addresses all failure effects of the IMA systems, including the integration and interdependencies with aircraft systems and functions. It may not be necessary to address any failure effects of IMA modules that affect only a single application, provided it can be shown that the safety assessment of the IMA system using that single application fully addresses those failure effects. These assessments should address generic and cascade failures, including possible failure combinations.

m. Install the IMA system on the aircraft.

4.5.2 Aircraft-level IMA System Compliance Data

IMA system approval on the aircraft should use a structured approach. The aircraft-level IMASCP should be developed as a high-level document that provides the certification basis and proposed means of compliance for the installation of the IMA system on the aircraft, demonstration of compliance with the regulations, and approval of the installation and certification of the aircraft. The aircraft-level IMASCP may be part of the aircraft certification plan. The IMA system integration and V&V processes at the aircraft-level should use a structured approach as outlined in Sections 5.3 and 5.4. The integration and V&V process for the IMA system on the aircraft should be documented in an aircraft-level IMASVVP. The V&V and integration plans may be included in the aircraft-level IMASCP, if appropriate. The configuration of the IMA system should be documented in the aircraft-level IMA system configuration index.

The results and compliance data should be documented in the aircraft-level IMASAS. The typical content of these life cycle data items is described below (in Sections 4.5.3 through 4.5.7).

4.5.3 Aircraft-level IMA System Certification Plan (IMASCP)

The aircraft-level IMASCP should include the same type of information as listed in Section 4.4.3.a through 4.4.3.n, plus the following information:

a. Plan for performing aircraft-level safety assessment related to the IMA system.

b. Plan for development of instructions for continued airworthiness related to the IMA system.

NOTE: *If there will be only an aircraft-level IMASCP, the above information should be included in this plan. If there will be a system-level and an aircraft-level IMASCP then the information above can be covered on system-level, on aircraft-level, or on both levels based on planned activities.*

4.5.4 Aircraft-level IMA Validation & Verification Plan

The aircraft-level V&V plan should include the same type of information listed in Section 4.4.4.a through 4.4.4.j, plus the following information:

a. Address single and multiple common mode failures which could effect continued safe operation of the aircraft.

b. Actions to measure the aircraft and flight crew responses to abnormal operational conditions, degraded modes, and failure modes.

c. Actions to verify and validate the intended functions of the aircraft.

d. Actions to verify and validate that the IMA system does not perform unintended functions.

NOTE: *If there is only an aircraft-level V&V plan, all information listed above should be included in this plan. If there are system-level and aircraft-level V&V plans, then the listed information above can be covered on system-level, on aircraft-level, or on both levels based on planned activities.*

The integration and V&V activities should be coordinated with all involved stakeholders for consistency and understanding of their roles and responsibilities in the installation approval process.

4.5.5 Aircraft-level IMA System Configuration Index (IMASCI)

The aircraft-level IMASCI should include the same type of information as listed in Section 4.4.5, plus any other data needed for the installation, integration, validation, and verification of the IMA system on the aircraft.

4.5.6 Aircraft-level IMA System Accomplishment Summary (IMASAS)

The aircraft-level IMASAS should include the same kinds of information as listed in Section 4.4.6, with aircraft-level details.

4.5.7 Other Aircraft-level Data

a. V&V records and results, including ground and flight test results, and human factors assessments.

b. Configuration management records.

c. Quality assurance records.

d. Safety assessment report(s). The IMA safety assessment process should use a systematic process as defined through ED-79/ARP4754 (Ref. [7]) and result in the following safety activities: FHA, PSSA, SSA, and CCA.

e. Problem reports.

f. Installation instructions, including data loading procedures.

g. Aircraft-level environmental testing plans (e.g., HIRF and IEL) and results.

h. Instructions for continued airworthiness.

i. IMA system requirements and design data.

j. Tool qualification data, as defined in ED-12/DO-178 (Ref. [2]) or ED-80/DO-254 (Ref. [6]).

k. MMEL, if required.

4.6 TASK 5 – CHANGE

4.6.1 Changes to IMA System Modules, Resources and Applications

Changes to IMA system components will likely occur throughout the life cycle of the IMA system. A change may involve modification to resources, modules or hosted applications, including addition, deletion, repair, or modification of IMA system components. In some cases, components may be changed in the modules to address obsolescence, reliability, etc. without affecting the functionality of the IMA system. There are a variety of types of changes that may occur, such as a new application being hosted on the IMA platform, modification to an existing hosted application, new supporting software and processing hardware, a modification to existing supporting software or hardware, or addition of new network infrastructure. Changes will require re-acceptance or approval by the certification authority.

4.6.2 Change Objectives

A primary objective of the IMA system development and acceptance process is to minimize the impacts of an IMA system component change on the IMA system and aircraft certification. Only the changed module(s) and/or application(s) could require re-acceptance or re-approval when considering installation, safety, operational, functional, and performance issues. The main goal of the change process within the IMA system is to bound changes in such a way that their effects are known and can be fully verified and validated. The objectives of the change process are to:

a. Develop a change management process and coordinate it with all stakeholders. The process should identify how the various levels of developers, suppliers, integrators, and certification applicants will coordinate and address changes.

b. Perform changes using the approved change management process.

c. Conduct and document the change impact analysis.

d. Re-integrate the changed component into the IMA system. Perform all necessary verification, validation, and integration activities (including regression analysis and testing) to obtain acceptance of the modified module or application and to ensure that the change has no adverse impact on affected, but unchanged modules and applications.

e. Maintain configuration control of all life cycle data related to the change.

4.6.3 Change Management Process

The change management process should be documented at all appropriate levels (aircraft, IMA system, platform, application, and module) with identification of interrelationships between different levels. If multiple stakeholders are involved, there will likely be multiple change processes for the specific levels of the system, e.g., the applicant, IMA system integrator, module developer, and application developer would each need a defined change management process that is coordinated with the change process of other stakeholders. The process should address, at a minimum:

a. ***Propose changes.*** The first step of the change process is to identify the proposed change(s) and reasons for the change. Typically a number of changes are proposed at the same time to optimize the change effort. These changes should be documented in a consistent manner (e.g., engineering change request, software change request, problem report, or similar manner). The proposed changes may include requests to fix errors, to add new features, to modify existing features, etc.

b. ***Perform an initial change impact analysis.*** Each proposed change should be analyzed to determine the potential impact on the functionality and performance of the component, on other components that use or interface with the component to be changed, and on IMA system and aircraft functionality, performance and safety. Section 4.6.4 further addresses the change impact analysis process. Typically, an initial analysis is performed early in a change proposal process, but may be modified after the change is implemented to ensure that the original performance, safety, and resource constraints have not been compromised.

c. ***Develop an implementation strategy.*** Once a change has been authorized, an implementation strategy should be developed and executed. The implementation strategy should specify the change process, life cycle data to be updated, activities to be implemented, verification activities to be performed, resources needed, schedules to be applied, etc. The specific roles and responsibilities of the various developers, integrators, and applicants should be clearly defined in the implementation strategy. The implementation strategy should be documented in the appropriate plan(s) and coordinated with the certification authority prior to implementing the change(s).

d. ***Implement the changes to the agreed implementation strategy.*** The implementation of changes should follow the documented plans. Many developers desire to implement multiple changes at the same time. It is difficult to determine the correctness of each change and to perform a thorough change impact analysis and regression testing, if concurrent changes are made to the baseline. However, changes can be implemented simultaneously, as long as each change is incorporated individually into an existing baseline. To assure correctness of each change or combination of changes, the changes should be verified both individually and collectively for their impact on the IMA system and aircraft.

e. ***Implement change control and problem reporting.*** Changes should be made using a controlled process. Problem reports should be documented and addressed.

f. ***Verify the changes.*** Once the changes have been implemented, they should be verified. Verification includes reviews, analyses, and tests.

g. ***Integrate the changed item.*** The changed item should be integrated and verified in the IMA system.

h. ***Finalize the change impact analysis.*** Early in the change process it may be difficult to fully evaluate the impact of changes. Therefore, once the changes have been implemented and verified, the change impact analysis should be finalized to ensure that its impact has been fully assessed and addressed (see Section 4.6.4).

i. ***Follow the procedures.*** Stakeholders should follow the configuration management and part numbering procedures as defined in Section 5.5.

4.6.4 Change Impact Analysis (CIA)

When a change is made to the IMA system a change impact analysis should be performed and should include an evaluation of the impact of the change on the original system safety assessment and aircraft-level safety. The change impact analysis should determine whether the change could adversely affect safe operation of the system or product, and other components impacted by the change.

The following are examples of areas that could have an adverse impact on safety or operation:

a. Safety-related information is changed. For example:

- Previous hazards, as identified by the system safety assessment.
- Failure condition classification(s), as identified by the system safety assessment.
- Software levels or hardware design assurance levels, particularly if the new software level or hardware level is more severe than the previous level.
- Safety-related requirements, as identified by the system safety assessment.
- Safety margins are reduced.
- Validity of the environmental qualification test results is affected.
- V&V methods or procedures are modified.

b. Operational or procedural characteristics of the aircraft are changed in a manner that could adversely affect flight safety or operations as a result of the change. For example:

- Aircraft operational or airworthiness characteristics.
- Flight crew procedures.
- Increased pilot workload.
- Situational awareness, warnings, cautions, or alerts.
- Displayed information to make flight decisions.
- Assembly and installation requirements.
- Changes that affect equipment interchangeability and/or intermixability with other equipment.
- Certification maintenance requirements are changed or added.

c. New functions or features are added to the existing system functions that could adversely impact aircraft safety, functionality, performance, or operations.

d. Processors, interfaces, and other hardware components or the environment are changed in such a way that safety, functionality, performance, or operations could be adversely affected. See ED-12/DO-178 (Ref. [2], Section 12.1.3), and ED-80/DO-254 (Ref. [6], Sections 11.1.3 and 11.1.3).

e. Life cycle data, such as requirements, code, and architecture are significantly changed in a way that could adversely affect safety, functionality, performance, or operations.

f. Performance, integration, and development issues due to shared resource changes that could adversely affect safety, functionality, performance, or operations.

Since there are various levels of development and integration in an IMA system, changes to accepted modules, hosted applications, IMA platforms, the IMA system, and changes at the aircraft level should be addressed.

Changes should be coordinated with all stakeholders and the impact on the aircraft should be addressed, as discussed above.

Changes to any software or hardware should be reflected in the appropriate life cycle data affected by the change and verification activities conducted to assure that no adverse effects are introduced during the change.

4.6.5 Change Data

The module developer, application developer, integrator, and/or applicant should obtain approval or acceptance of the following data for a changed module or application:

a. CIA, as described in Section 4.6.4.

b. Change management plan, which describes the change management process (see Section 4.6.3). The change management plan may be included in an updated MAP, PSAC, PHAC, and associated software or hardware plans.

c. V&V plan, records, and results to demonstrate appropriate regression analysis and testing.

d. Modified life cycle data. The life cycle data described for module acceptance or application acceptance should be updated as required by the change and documented in the MCI, Software Configuration Index (SCI), and/or Hardware Configuration Index (HCI) (i.e., Top-Level Drawing). That is, all changes to life cycle data should be completed and documented in the appropriate configuration index.

e. Updated accomplishment summary for the module or application.

f. Maintenance and change history records.

4.7 TASK 6 – REUSE OF MODULES OR APPLICATIONS

IMA systems are composed of modules and applications that can be used in many different configurations. Reuse involves the use of certification credit (i.e., full, partial, none) for modules and/or applications in a subsequent installation. This subsection focuses on the reuse of module acceptance data (i.e., data in Sections 4.2.2 through 4.2.12) or application acceptance data (i.e., data in Section 4.3.2). The goal is to reuse acceptance data without reassessing the data itself but rather to assess its suitability for and integration into the new installation.

4.7.1 Objectives of the Reuse Process

The main goal of reuse is to be able to use module or application life cycle data that has been previously assured and accepted, with minimal need for oversight by the certification authority. Reuse should be planned during the initial development process. Modules are accepted with the intent of being reused in multiple systems. Once the module or application has been accepted, the objectives of the reuse process are to:

a. Ensure that the module or application life cycle data is unchanged from what was previously accepted.

b. Ensure that the limitations, assumptions, etc. documented in the module or application acceptance data sheet are addressed in the subsequent installation.

c. Analyze the suitability of the module or application for reuse by performing a usage domain analysis to ensure that the module or application is being reused in the same way it was originally intended and accepted. A usage domain analysis includes V&V that the subsequent installation characteristics fall within the usage domain.

d. Evaluate any open problem reports of the module or application to ensure that the problem does not adversely impact safety, functionality, performance, or operations.

e. Integrate the module or application into the subsequent installation and verify its proper functionality in the IMA system.

f. Submit necessary plans and data to the certification authority and users.

4.7.2 Reuse of a Software Module or Application

If the module to be reused is software only, the original acceptance should have documented which objectives of ED-12/DO-178 (Ref. [2]) were satisfied fully, partially, or not at all (see Sections 4.7.1, 4.2.3h, 4.3.2, and AC 20-148 (Ref. [9])). Objectives that are not satisfied by the software developer should be completed by the platform integrator, system integrator, or certification applicant. For the reuse in the subsequent installation, the following items should be assured:

a. The software life cycle data was previously approved or accepted by the certification authority.

b. The software life cycle data being considered for reuse has not changed since its previous approval.

c. The software level(s) of the software application(s) or module(s) is the same or less severe than the software level of the initial acceptance.

d. The interfaces to the application or module remain the same, for example, range and data type of inputs to the application or module are within the range or equivalent to its accepted predecessor.

e. The application or module being reused is resident on the same target computer and used in the same way operationally as it was for the previous acceptance. If a different target computer is used, portability and re-verification of target dependencies should be performed.

f. Equivalent software/hardware integration testing and system testing were conducted on the target computer and system as in the previous acceptance. If a different target computer is used, software/hardware integration testing should be performed for the subsequent installation.

g. Software has been shown to (1) have no adverse effect on the system safety, performance, or functionality, and (2) have no adverse effect on the subsequent operational capability.

h. All open problem reports and in-service problems associated with the software to be reused should be analyzed to ensure that there are no safety or operational issues.

i. The integration of the software application or module into the IMA system satisfies all of the applicable ED-12/DO-178 (Ref. [2]) objectives.

4.7.3 Reuse of a Complex Electronic Hardware Module or Application

If the module to be reused is Complex Electronic Hardware (CEH) that was required to satisfy the objectives of ED-80/DO-254 (Ref. [6]), each objective should have been evaluated by the hardware developer to determine what was satisfied fully, partially, or not at all. Objectives that are not met by the hardware developer should be completed by the platform integrator, system integrator, or certification applicant.

IMA systems frequently reuse CEH. If CEH is reused, the following items should be assured:

a. The CEH life cycle data being considered for reuse has not changed since its initial acceptance.

b. The CEH design assurance level (DAL) is the same or less severe than the DAL of the initial acceptance.

c. The interfaces to the CEH remain the same (for example, range and type of inputs to the hardware are within the range or equivalent to its accepted predecessor).

d. The CEH being reused interfaces with other hardware and software in the same way and is used in the same way operationally as it was for the initial acceptance. If interfaces are different or it is being used in a different way, environmental qualification testing and re-verification of interface and/or functional dependencies will be required.

e. Equivalent integration testing and system testing were conducted on the target environment and system as in the initial acceptance.

f. The CEH has been shown to (1) have no adverse effect on the new system safety, performance, or functionality, and (2) have no adverse effect on the new operational capability.

g. All open problem reports and in-service problems associated with the CEH to be reused should be analyzed to ensure that there is no safety, performance, functional, or operational issues.

h. The integration of the CEH into the IMA system satisfies all of the applicable ED-80/DO-254 (Ref. [6]) objectives.

4.7.4 Reuse of Environmental Qualification Test Data

If the module to be reused is hardware, either complex or simple, the reuse of environmental qualification test data (ED-14/DO-160, Ref. [1]) should be evaluated. The similarity of the environment and module usage should be evaluated to determine if it can be reused or what additional testing (if any) will be needed. That is, if the previous EQT results are still valid for the current installation, or if some testing needs to be repeated at a level consistent with the current intended installation environment.

Environmental qualification data may be reused when it is shown to be appropriate to the new installation environment and configuration. See Section 5.2.6 regarding which types of environmental qualification tests may be performed at module level, platform level, system level, or aircraft level.

4.7.5 Reuse of a Module that Contains Software and Hardware

The guidance in Sections 4.7.2 through 4.7.4 should be followed for a module that contains both software and hardware.

4.7.6 Reuse Compliance Data

This section describes the data that should be available or developed to reuse a previously accepted module or application.

4.7.6.1 Initial Accepted Life Cycle Data

The following data from the initial development and acceptance should be provided:

a. Evidence of the initial module or application acceptance data described in Sections 4.2.2 through 4.2.12 and Section 4.3.2 that support design assurance.

b. Module or application data sheet and summary of problem reports.

c. Installation procedures, user's guide, interface specifications, etc.

4.7.6.2 Subsequent Acceptance and Integration Data

The applicant, module/application developer, or system integrator seeking acceptance on a subsequent IMA system should develop the following data when integrating the reused module or application:

a. Life cycle data for the subsequent acceptance and integration, which includes a reused module or application, should be developed to comply with the applicable certification requirements for the subsequent installation and this guidance.

b. V&V records should include results from reviews, analyses, and testing (verification and validation) of the re-integration of the module or application into the subsequent IMA platform, system, and aircraft configuration, including an usage domain analysis. The usage domain analysis includes:

- Assumptions made by the module or application developer regarding the subsequent use, installation configuration, and V&V to be conducted by the integrator.
- Analysis of the impact of reusing a module or application in the subsequent platform, system, and installation configuration.
- Analysis of the subsequent system impact on the module or application.
- Analysis that the interfaces of the subsequent system integration are consistent with the usage domain and interface specification of the module or application.

CHAPTER 5

INTEGRAL PROCESSES

5.1 SAFETY ASSESSMENT

Due to the high level of integration inherent in IMA systems, it is recommended that applicants use ED-79/ARP 4754 (Ref. [7]) and ARP 4761 (Ref. [8]), or acceptable alternatives. The process should consider the following, as a minimum:

a. Isolation, separation, and independence to prevent interference to safety-critical functions by functions of lower failure conditions severity (e.g., partitioning, resource management, fault management, and containment).

b. Protection to prevent single failures and foreseeable combinations of failures that could adversely affect multiple functions simultaneously (e.g., independence, redundancy, health monitoring and fault management, and safety monitoring).

c. A preliminary FHA should be performed at the aircraft and IMA system levels to assess the intended functionality, characteristics, and capabilities of the IMA architecture.

d. Examination of the architectural design and safety-related capabilities of the IMA platform and the constraints imposed on the aircraft functional allocation and hosted applications. For example, requirements for application independence, partitioning, protection, redundancy, resource needs, interface communications, performance, network access, and/or dedicated links to aircraft sensors and actuators will be produced. The result of this examination should be an IMA PSSA.

e. Examination of the behavioral issues of the IMA platform. This includes details such as a health monitoring, resource management, and fault management capabilities provided by the platform and the types of available failure recovery or containment.

f. Examination of the performance details within the IMA platform to ensure it will satisfy the performance requirements of the hosted application(s).

While a single stakeholder may be able to perform all of the activities described above, it is anticipated that these will be distributed among multiple stakeholders. A typical allocation of responsibilities is provided in the following sections.

5.1.1 Responsibilities of the Certification Applicant

The certification applicant is responsible for aircraft-level system safety assessment processes and ensuring that the IMA system, platform, modules, and hosted applications will satisfy the aircraft safety, integrity, and reliability requirements. The certification applicant will be responsible for the consolidation of the results of IMA system safety assessment performed by the IMA system integrator, platform and module developers, and application developers; and ensuring their SSA results are consistent with the aircraft safety assessment.

The certification applicant should address:

a. Single failures and combination of failures between the IMA system and other aircraft systems.

b. Common cause and cascading failures (refer to Section 5.1.5.4).

c. The impact of the IMA-specific SSA results on demonstration of compliance with the applicable regulations, operations, and the continued airworthiness of the aircraft.

d. Network security.

e. Any other relevant safety data.

5.1.2 Responsibilities of the IMA System Integrator

The IMA system integrator will be responsible for consolidation of the results of system safety assessments performed by the IMA platform, module, and application suppliers; and ensuring their SSA results are consistent and compatible with the IMA SSA. As part of the integration and V&V processes, the IMA system integrator should ensure that the behavior and safety-related properties of the IMA system components are consistent with the IMA SSA requirements. This process should include verifying the PSSA/SSA results with testing of the resource management, health monitoring, fault management, and other protection features of the platform and system (e.g., redundancy management, cross channel comparators, reversion strategies), and should be performed at multiple levels of integration.

5.1.3 Responsibilities of the IMA Platform Supplier

The IMA platform supplier should perform a detailed platform safety assessment. The results from this assessment should be used in the consolidation and integration of Sections 5.1.1, 5.1.2, and 5.1.4. These analyses should examine IMA platform-specific features and capabilities to support the hosted applications, IMA system, and aircraft installation that include robust partitioning, resource management, health monitoring, fault management, input/output (network communications), performance, and other architectural and protection features provided by the platform.

The IMA platform supplier will be responsible for the common mode failure analysis of the IMA platform. This common mode failure analysis should be coordinated with the application developers and the IMA system integrator to support the IMA system and aircraft-level safety assessments.

Platform safety assessment data, resource management guarantees, and fault management and health monitoring features should be made available to other stakeholders for their use in the application safety assessment, the IMA system safety assessment, and the aircraft safety assessments.

The platform supplier may need to gather input from multiple component or module developers in order to complete the IMA platform safety assessment tasks.

5.1.4 Responsibilities of the Application Supplier

The application supplier should perform a detailed PSSA for the application, and specify the safety features, performance, and interface requirements for that application. As part of the PSSA they should also specify assumptions that the application is making with regard to the platform on which the application will be hosted, and their needs for resource management, health monitoring, fault management, failure responses, etc. The subsequent IMA system-level and aircraft-level safety assessments will verify these assumptions and requirements as part of their activities. The PSSA results will be used in the consolidation, evaluation, and integration activities (see Section 5.1.2, 5.1.3, and 5.1.5.3). The application supplier should ensure that the behavior and properties of the application are consistent with specific system and aircraft safety requirements.

5.1.5 Safety Assessment Activities

The following safety assessment activities should be addressed during the various phases of the IMA system development.

5.1.5.1 Functional Hazard Assessment (FHA)

The intended functions of the IMA system should be identified and evaluated for their impact on aircraft safety. A FHA should be conducted at the aircraft and system levels to determine and classify the failure conditions and effects associated with both the loss and malfunction of each function provided by the IMA system. The hazards associated with the simultaneous loss or malfunction of multiple functions provided by the IMA system should also be identified and classified. In addition, the loss and malfunction of functions provided by the IMA system should be addressed in combination with the loss and malfunction of related functions provided by other aircraft and engine systems to ensure that common mode failures are addressed (see Section 6.1 of ED-79/ARP-4754, Ref. [7]).

5.1.5.2 Preliminary System Safety Assessment (PSSA)

a. Based on the failure condition classifications determined by the FHA, the proposed design and architecture of the IMA system components should be evaluated by a PSSA to determine that the system development assurance level and safety requirements identified in the FHA will be achieved.

b. The PSSA should establish the number (redundancy), isolation and independence features, software levels, hardware design assurance levels, and reliability of each component of the IMA system, including the power supplies, communication interfaces, displays, and controls that are required to protect the aircraft from the effects of random hardware failures. The system development assurance levels necessary to protect the aircraft and engine from failures and combinations of failures, and design errors in the hardware and software of each component should be determined. Unless measures are provided to protect an IMA cabinet or rack (or other co-located modules) from common-cause failures (such as an electrical fire), all of the functions provided by a single IMA cabinet or rack (or other co-located modules) should be assumed to fail as the result of a single failure. All functions that use any single hardware element should be assumed to fail as the result of a single failure or combinations of failures. The PSSA should identify the fail-safe design techniques and fault tolerance requirements as applicable for the aircraft type. When addressing failures or other events, consequential or cascading effects should also be addressed.

c. The software levels should be determined for all platform-provided software and hosted software applications in compliance with the FHA requirements.

d. The hardware design assurance levels should be determined for all platform-provided and application-specific hardware devices in compliance with the FHA requirements.

e. PSSA should identify specific safety requirements for hardware and software components including failure containment, partitioning, independence, redundancy, health monitoring, etc. and specific verification strategies (see Section 6.2 of ED-79/ARP-4754, Ref. [7]).

5.1.5.3 System Safety Assessment (SSA)

A systematic, comprehensive evaluation of the applications hosted by the IMA system as installed in the aircraft should be conducted to show that the relevant safety requirements identified in the PSSA have been met. This evaluation may include bench, ground, and flight tests to ensure assumptions made in the PSSA are correct and validated. The SSA combines the results of a number of different analyses and tests to verify the safety of the overall system, as installed. The SSA should be conducted as described in ARP 4761 (Ref. [8]). A typical SSA includes:

a. A system description, including functions and interfaces.

b. A list of failure conditions.

c. The classification of each failure condition.

d. Qualitative analysis of each failure condition.

e. Quantitative analysis of each failure condition, as required.

f. The results of common-cause analyses.

g. Confirmation that any cascading failures and/or single failure affecting multiple systems have been addressed.

h. Laboratory, simulator, and aircraft test procedures and results, as appropriate, that substantiate flight crew recognition and response to failure conditions.

i. Verification that any failure modes of lower integrity functions that could adversely affect higher integrity (more critical) functions are prevented.

j. Confirmation that all software has been developed to the appropriate software level identified in the PSSA.

k. Confirmation that CEH has been developed to the hardware design assurance levels identified in the PSSA.

l. Verification that all safety-related requirements of the hardware and software have been implemented correctly (see Section 6.3 of ED-79/ARP-4754, Ref. [7]).

5.1.5.4 Common Cause Analysis for IMA Systems

For IMA systems, where resources are shared between multiple aircraft-level functions and hosted applications which are conceptually independent, Common Cause Analysis (CCA) at the aircraft level is required because a single causal event can directly (or indirectly) contribute to simultaneous adverse effects. Additionally, cascading failures should be part of this analysis.

The methods of the CCA need not change from the traditional one, but it should be applied at a higher level in the hierarchy of aircraft systems. It should now be applied to the collection of systems (and the aircraft functions they perform) that are implemented by an IMA system and its components. This may mean that the analysis needs to be performed by the certification applicant, rather than by the IMA system integrator, platform developer, or application developer. It should be performed when the configuration of the IMA system is finalized and may need to be repeated if functions are added to the IMA system following initial certification. It may also include traditional analyses of redundant systems, which are implemented in whole or in part by the IMA system.

The CCA will involve these three analyses (see ED-79/ARP-4754, Ref. [7], and ARP-4761, Ref. [8]):

a. Common Mode Failure Analysis.

b. Particular Risks Assessment.

c. Zonal Safety Analysis.

5.1.5.5 Failure Mode Analysis

This section discusses analyses of generic IMA platform components, the types of data expected to be produced by these analyses, and the integration of results at the application, platform, IMA system integration, and aircraft levels. These integration activities are required to demonstrate the safety of the IMA system. The higher levels of analyses should be based upon the results of the lower levels.

5.1.5.5.1 IMA Components Failure Mode Analysis

The analyses of IMA components (modules, platforms, resources) determine what effects component failure modes will have on the hosted applications, other IMA modules, the platform, the IMA system, and the aircraft and/or engine. In order to accomplish this failures of the components should be identified and how these failures manifest themselves should be determined. In other words, under known failure conditions or causal events, how does the component deviate from its required operation and intended function(s), and what is the impact on other modules, hosted applications, the IMA system and aircraft functions.

For random failures, this is typically accomplished by evaluating piece-part failures and determining the effects on the component operation. In some cases, these effects may be viewed simply from the component boundaries; however, if applications or other components interact internally with the component, the effects should be defined at these interface boundaries. For components that provide common services or resources for multiple other components or applications, the interface boundaries can be difficult to isolate and determine the potential effects on them. For causal events, the focus of failures and effects need only be to those aspects of the component that are vulnerable to the causal event.

In some cases, it may not be feasible to begin the analyses at the piece-part level components because of lack of visibility at that level (e.g., an off-the-shelf power conditioning module). For these cases, worst-case assumptions (e.g., loss of function, unintended functionality) should be assumed about the components and their failure modes.

Without knowledge of the hosted applications or aircraft usage of the components it is difficult to determine the failure effects. Assumptions can be made about possible installations and usage to make estimates of the severity of the failure. The assumptions and failure modes identified at this level should be provided as input to the next level of analysis.

5.1.5.5.2 IMA Platform Failure Mode Analysis

In analyzing the IMA platform, the IMA modules and components are combined in the absence of applications. The failure modes and effects of the individual IMA components are now analyzed within the context of the platform architecture and interfaces to determine how they manifest themselves at the platform boundaries. As with the component analyses, the focus is on how the platform may vary from its defined behavior.

Since most hosted applications will be interacting with components internal to the platform, the effects at the internal interfaces should also be determined and evaluated. Additionally, failures stemming from the loss or degradation of shared resources should be assessed in this analysis.

5.1.5.5.3 Applications Failure Mode Analysis

The application failure mode analyses consider each individual application. If there is any hardware that is not part of the platform, but is used to support a hosted application, this hardware should be analyzed in a similar manner as described in Section 5.1.5.5.1. The only difference is that hosted applications typically have portions of the aircraft FHA associated with them (at least those providing an aircraft-level function) and a better analysis of the severity of the failure effects for these components can be determined.

Each application should be assessed within the context of the target platform and architecture without interference from other hosted applications. Both application and platform failure modes should be analyzed to determine how they manifest themselves at the application boundaries, that is, how the application deviates from its intended function and performance. If each application is functionally independent of other applications, then only those effects at the boundaries may need to be analyzed.

NOTE: *If applications are not functionally independent, then their dependencies and interfaces should be analyzed to identify combinations of failures, and cascading failures.*

5.1.5.5.4 IMA System Failure Mode Analysis

This activity analyzes the failure modes of an IMA system, considering the previous analyses (for the components, modules, platform, and applications) as input. The results of the analysis become an input to the aircraft-level failure mode analysis.

The IMA system failure mode analysis considers the hosted application interactions and couplings with other applications and shared resources of the platform(s), and the IMA system. Application interactions should address both normal and unintended interference between applications and shared resources. Single and multiple failures of applications and resources should be examined and IMA system-level failure effects are determined.

If an IMA system consists of multiple platforms, potential interactions between these platforms should also be addressed and failure modes determined.

5.1.5.5.5 Aircraft Level Failure Mode Analysis

The component, hosted application, IMA platform, and IMA system failure mode analyses results are used in the aircraft-level failure mode analysis. It is this analysis that finally consolidates all the predicted failure effects and modes from the lower level analyses, and confirms that they are appropriate for the IMA system(s) installation and operation on the aircraft. Any erroneous assumptions of the lower level analyses should be detected and corrected during the aircraft-level failure mode analysis. Additionally, interactions with other aircraft systems should be addressed at the aircraft-level.

5.1.5.6 Fault Management, Health Monitoring, and Redundancy Management

The fault management, health monitoring, and redundancy management considerations in Section 3.6 should be implemented in the design and considered in the safety assessment process. Failure modes of these capabilities should be addressed in the failure mode analyses for the platform and system, and possibly for the aircraft.

5.1.5.7 Partitioning Analysis

A partitioning analysis should be provided as input to the failure analyses, and the failure modes of partitioning violations addressed in the failure mode analyses for the platform and system. Section 3.5.2 provides specific guidance regarding this analysis.

5.1.5.8 Network Security

A breach in IMA system network security may adversely impact aircraft safety. Therefore, failure modes of the IMA system network security should be addressed as part of the aircraft-level safety assessment. Examples of threats to network security are: data content integrity (alteration of data value contents), data source integrity (impersonation), and data latency and other denial-of-service attacks. This document may be used in combination with other guidance material for network security certification issues.

5.2 SYSTEM DEVELOPMENT ASSURANCE

This section describes key areas of system development assurance, which include software guidance, hardware design assurance, shared design assurance, IMA system configuration management, and environmental qualification.

5.2.1 Software Guidance

Software used in IMA systems should be developed using the guidance of ED-12/DO-178 (Ref. [2]) or another acceptable means of compliance to the appropriate software level(s). Certification policy and guidance should be addressed when considering key IMA system software aspects of certification, such as software reuse, user-modifiable software, field-loadable software, and database integrity. In addition, specific aircraft programs may have additional software policy or guidance that is applicable for the IMA system to be installed.

5.2.2 Electronic Hardware Guidance

If the IMA system contains CEH devices whose functions cannot feasibly be comprehensively verified by test and/or analysis, the CEH devices should be developed using the guidance of ED-80/DO-254 (Ref. [6]) or other acceptable means of compliance to the appropriate level of hardware design assurance. Certification policy and guidance should be addressed when considering key IMA system hardware aspects of certification, such as field-loadable hardware, environmental qualification testing, hardware module acceptance, aircraft personality modules, hardware configuration files, etc. In addition, specific aircraft programs may have additional hardware policy or guidance that is applicable for the IMA system to be installed.

Field-modifiable hardware may be used within an IMA system; for example, programmable logic devices may be modified through external means. Since ED-80/DO-254 (Ref. [6]) does not currently contain guidance for such implementations, the current guidance on field-loadable software (for example, Section 2.4 and 2.5 of ED-12B/DO-178B, Ref. [2]) may be applied.

5.2.3 Integration Tool Qualification

ED-12/DO-178 (Ref. [2]) and ED-80/DO-254 (Ref. [6]) provide guidance on verification and development tools used for software and hardware development, respectively. In the IMA system development, there may be additional tools used for integration, such as tools used for:

a. Generation and/or verification of configuration files and resource allocations.

b. Setting up and verifying partitioning protection and other IMA system safety and protection features, such as redundancy management, reversion, health monitoring, fault management, flight crew alerts, etc.

c. Verifying the configuration of the IMA system and its intra-platform and inter-platform data communication.

d. Verifying correct usage of interfaces with other aircraft systems and sensors.

An integration tool should be evaluated to determine if it is a development tool (produces an item that will be implemented in the IMA system) or a verification tool (verifies an item that will be implemented in the IMA system). If the tool output is not fully verified, it may need to be qualified. The tool qualification approach should be based on ED-12/DO-178 (Ref. [2]) Section 12.2.

5.2.4 Shared Design Assurance

In IMA systems, it is likely that design assurance of modules will depend on design assurance activities of other modules that may be developed by another organization. The methods by which the completion of design assurance is achieved will depend upon the contractual relationships between the various stakeholders. The plans (e.g., MAP, PSAC, PHAC) should address the means used to demonstrate complete design assurance, including shared responsibilities.

5.2.5 IMA System Configuration Management

Section 3.7 provides guidance on IMA system configuration management. The configuration management approach should be supported by the system safety assessment process and data included in the appropriate life cycle data (e.g., software requirements, design, etc.), verified and validated, and configuration and change controlled.

5.2.6 Environmental Qualification Testing (EQT)

The flexibility and reconfigurable nature of IMA systems can lead to a large number of hardware and software configurations to be considered for the environmental qualification tests. This flexibility of configurations, as well as the need to enable hardware module EQT without the hosted application(s), are the primary aspects of IMA system and hardware environmental qualification that differ from a federated system EQT. The extent to which the EQT may be done at lower levels is highly dependent on specific aspects of the module(s) in question, as well as their installed environment. EQT of IMA system modules and hardware should be performed to the appropriate levels as defined in ED-14/DO-160 (Ref. [1], or other acceptable means) as determined by the assumed or intended aircraft installation and operational environments.

The guidelines below outline some of the concerns that should be addressed. The IMA platform developer and/or system integrator should develop a comprehensive EQT plan that defines how the environmental qualification testing will be performed and the pass/fail criteria. This plan should receive engineering approval from the certification applicant.

The environmental qualification credit that can be taken at the module level is dependent on:

- Definition of the environment in which the module will reside (this should address expected combinations of modules and their contribution to this environment, as well as the contribution of the aircraft environment).
- Definition of effects the module can contribute to its environment.
- Definition of the module reaction to specific events, such as HIRF and lightning. (IMA systems using these modules should be designed to appropriately accommodate these defined module reactions.)

Module-level environmental qualification does not replace further qualification at higher levels of integration; however, the environmental qualification at higher levels of integration should validate the subset of environmental requirements imposed on the individual modules. If applicable, the application supplier should provide a justification that the application presents an acceptable behavior under environmental conditions considering the module reactions defined either in the MRS or in the module user's guide. In addition, specified behavior of the IMA platform (including during EQT conditions) should be made available to allow the hosted application developers to design to the platform reaction. If these reactions are properly defined in the MRS, the applications can base their design on those performance characteristics without necessarily needing to know the environmental conditions that drive those reactions.

The guidance for environmental qualification testing of hardware modules is described below:

a. The hardware module developer should specify the assumed or intended environment and applicable environmental test categories and levels of ED-14/DO-160 (Ref. [1]), supplemented with additional requirements, if necessary, such that tests are representative of expected conditions that modules may be subjected to in the actual aircraft installation.

b. The developer should specify the module performance requirements for each applicable test procedure in ED-14/DO-160. The developer may elect to specify a different set of pass and/or fail criteria, and/or test tolerances at environmental extremes, if appropriate. Once the applicable ED-14/DO-160 test conditions and categories have been specified, the hardware module developer should write a EQT plan by which testing will be conducted. It may be necessary to combine modules during testing to more closely represent the actual environment and operating conditions.

c. If a developer desires to qualify a hardware module for multiple categories of an EQT, then all applicable tests should also be performed for those categories.

d. The module or platform configurations should include the appropriate interfacing electrical and mechanical connectors, including shielding, back shells, and strain relief, intended for the cabinet or rack and modules. The equipment configuration should include interfacing wires and cables specified by the installation procedures in ED-14/DO-160.

e. If the hardware module can be loaded with software to perform aircraft functions or host software applications, then the developer should use the hosted application software or special purpose test software to demonstrate correct operation of the hardware module functions. The developer should verify, validate, and control the configuration of the modules and software to ensure the validity of the testing.

f. Some developers may prefer to use a worst-case environmental qualification testing to qualify the modules for a variety of installations. Such an approach may be proposed to the certification authority. However, the results of testing and any limitations should be well documented, such that future users and the certification authority can judge the validity of the testing as applicable to the desired installation.

g. Data buses used in IMA systems may have special electromagnetic compatibility concerns which will depend on the data bus specifications for pulse rise-times, bus speed, bus topology, and interconnection schemes. These concerns and any environmental effects that may be a source of common mode failures should be addressed in the EQT plan, as applicable.

5.3 VALIDATION

The validation process should ensure that the IMA system requirements are correct and complete. This section provides a framework for IMA system validation and supplements ED-79/ARP-4754 (Ref. [7]).

The objectives of validation are to:

a. Ensure the completeness and correctness of all levels of the IMA system requirements, including modules, hosted applications, platform(s), and IMA system requirements. Each level of requirements within the hierarchy should be validated prior to validating the next lower level.

b. Evaluate the IMA system architecture and functional allocation of hosted applications.

c. Ensure that the partitioning protection is robust, in terms of processor throughput time and usage, memory allocations, I/O devices and buses, and other shared resources. Ensure redundancy, resource management, health monitoring, and fault management requirements are correct and complete for the overall IMA system.

d. Ensure compatibility with safety, integrity, and reliability requirements of each application hosted on the IMA system.

e. Evaluate data coupling and control coupling between modules and applications.

f. Ensure both normal and degraded operations are considered, and their potential impact on aircraft safety identified.

Table 5 demonstrates the allocation of validation activities for the various tasks.

TABLE 5 : OVERVIEW OF TYPICAL VALIDATION ACTIVITIES

Task	Validation Activities (Items to be Validated)
1 – Module and/or Platform Validation	– Allocation of IMA platform requirements to IMA core software and modules – Robust partitioning requirements – Determinism requirements
2 – Application Validation	– Allocation of applications to aircraft functions – Functional allocation of requirements to application-specific hardware (dedicated resources) and software
3 –IMA System-level Validation	– Allocation of IMA system requirements to IMA platforms and applications hosted on each platform – Allocation of applications to IMA processors – Allocation of IMA resources to applications – I/O requirements to IMA resources
4 – Aircraft-level Validation	– Validation of the allocation of requirements to the IMA system from the aircraft-level requirements

In the case of the IMA platform, it is possible to have a scenario where the IMA platform requirements are generated from a set of generic requirements and assumptions based on aircraft knowledge. Then later, the platform will be applied to a specific aircraft. At that time, the generic IMA platform requirements and assumptions should be traced and validated to the actual aircraft requirements to complete the validation of the IMA system requirements.

5.4 VERIFICATION

The verification process should ensure that the implementations of specified requirements for the IMA system have been met. This section provides a framework for IMA system verification and supplements ED-79/ARP4754 (Ref. [7]).

The objective of verification is to ensure that all levels of requirements are properly and completely implemented, and that the means to ensure this are correct. The verification process ensures that all levels of requirements are complete, traceable, accurate, verifiable, and unambiguous. Verification may initially be performed in a simulated representative target computer and environment (usually during development to ensure it will work when the platform becomes available); however, the activity cannot be completed without verification on the target platform. In a situation where application and platform are developed concurrently, it is recognized that initial application verification process described by ED-12/DO-178 (Ref. [2]) may be performed in a “host” computer (simulated representative) environment prior to the availability of the target platform. In this circumstance, partial acceptance credit may be granted for completion of those processes, if the developer can substantiate that those verification procedures and results are valid for the target computer and environment.

Table 6 demonstrates the allocation of verification activities for the various tasks.

TABLE 6 : OVERVIEW OF TYPICAL VERIFICATION ACTIVITIES

Task	Verification activities (items to be verified)
1 – Module and/or Platform Verification	– Module(s) implementation complies with its physical, installation, functional, performance, interface (API), and safety-related requirements – Conformance of modules and core software, when integrated to form a platform, with the platform requirements – Platform physical characteristics, as appropriate – Platform characteristics, including services (API) such as, robust partitioning, network services, data communication, resource management, health monitoring, fault management, etc. – Capability of the platform to provide protection of shared resources for hosted applications – Platform configuration and means of maintaining and verifying the configuration
2 – Hosted Application Verification	– Application meets all its requirements in the target module and platform – Application configuration – Application uses its allocation of shared resources correctly
3 – IMA System-level Verification	– Applications meet their requirements on the target platform and system – Configuration of the modules, platforms, and hosted applications, and means to maintain the configuration – Allocation of shared resources for modules, platforms, and hosted applications – Interfaces and interactions between applications, between module resources and applications, between modules, and between platforms – Platform(s) implementation, when integrated to form an IMA system, with the IMA system requirements – IMA system functionality and performance – IMA system behavior for normal and abnormal (degraded) modes – Integrated applications, modules, and their platforms; and the allocation of shared resources, including functional interactions, inter-process communications, temporal interactions, etc. – Final configuration of the IMA system and means to maintain it
4 – Aircraft-level IMA System Verification	– IMA system installed on the aircraft meet its requirements – IMA system physical characteristics – IMA system interactions and interfaces with other aircraft systems – IMA system behavior for normal and abnormal (degraded) modes – Functional, performance, and safety requirements of the aircraft (ground and flight tests)

5.5 CONFIGURATION MANAGEMENT (CM)

This section addresses configuration management (CM) of the IMA system life cycle data and life cycle environment. CM of the installed IMA system is addressed in Sections 3.7 and 5.2.5.

The IMA system life cycle should manage and maintain:

a. Configuration of components, modules, resources, platforms, hosted applications, and IMA systems;

b. Life cycle data; and

c. Tools and environments used to develop, verify, and validate the IMA system.

ED-12/DO-178 (Ref. [2]) identifies CM guidance for software (e.g., core services and hosted applications) and should be used for software in IMA systems. ED-80/DO-254 (Ref. [6]) identifies CM guidance for electronic hardware and should be used for electronic hardware in IMA systems. A comparable CM process in accordance with ED-79/ARP-4754 (Ref. [7]) should be implemented for modules, platforms, resources, and the overall IMA system(s).

5.5.1 IMA System Configuration Management Plan

The IMA System Configuration Management Plan (IMASCMP) should be developed and should describe the configuration management processes, procedures, and activities to be used for the IMA system, as appropriate for the required development assurance level of the system, to demonstrate compliance. The IMASCMP should define the generic configuration items (e.g., modules, resources, platforms, interfaces, hosted applications, databases, configuration files, data, etc.) to be placed under configuration management, how changes to these items will be controlled, and the IMA system configuration accounting methods that will be used to define the configuration of the IMA system baselines at specific milestones throughout the life cycle. One or more CM plans may be developed to address the multiple components of the IMA system: modules, resources, applications, platforms, IMA system(s), and aircraft installation. Alternatively, a joint plan may be used to address all the components.

The IMASCMP should contain the following information, as a minimum:

a. A description of the IMA system for which the CM process is being applied.

b. A description of the CM process organization(s) for the IMA system and installation, the roles and responsibilities of various stakeholders, data under CM, data organization, supplier control, and interfaces to other entities.

c. A description of the CM environment to be used, including procedures, tools, methods, standards, organizational responsibilities, and interfaces.

d. A description of the CM process activities, such as, configuration identification, baselines, traceability, configuration control, change management, status accounting, generation of configuration index, archival and retrieval process, etc.

e. The transition criteria for the CM process.

f. A description of the data produced by the CM process, including CM records, control categories, the IMA Configuration Index and the IMA Life Cycle Environment Configuration Index.

g. A description of how CM and control of the modules, resources, platforms, applications, interfaces, IMA system, and aircraft installation will be maintained during development, installation, in-service, and maintenance activities throughout the service life of the IMA system.

h. A description of the robust and easily maintainable means of verifying that the IMA system configuration installed on the aircraft is the approved configuration conforming to the type design, especially for post-certification modifications.

5.5.2 Configuration Control

Life cycle data can be assigned to one of two categories: Control Category 1 (CC1) and Control Category 2 (CC2). CC1 and CC2 refer to the configuration management controls placed on life cycle data. CC2 objectives are a subset of the CC1 objectives. The definition of CC1 and CC2 for software are contained in Section 7.3, Table 7-1, of ED-12B/DO-178B. These are also referred to as Hardware Control Categories 1 and 2 (HC1 and HC2) in Section 7.3, Table 7-1 of ED-80/DO-254 (Ref. [6]). TABLE 7 below summarizes the definition of CC1 and CC2. A comparable level of configuration control should be applied to IMA system life cycle data and should be described in the IMASCMP. Annex A tables provide general CC1/CC2 guidelines for the IMA life cycle data. For some systems (e.g., lower level systems) the amount of configuration control may be less stringent, if justified in the IMASCMP.

TABLE 7 : CC1/CC2 DEFINITION

CM Process Objective	**CC1**	CC2
Configuration Identification	x	x
Baselines	x	
Traceability	x	x
Problem Reporting	x	
Change Control - integrity and identification	x	x
Change Control – tracking	x	
Change Review[3]	x	
Configuration Status Accounting[3]	x	
Retrieval	x	x
Protection against Unauthorized Changes	x	x
Media Selection, Refreshing, Duplication	x	
Release	x	
Data Retention	x	x

5.6 QUALITY ASSURANCE (QA)

Highly integrated and complex systems like IMA systems present many opportunities for development errors and undesirable, unintended effects. At the same time, it is not practical to develop a finite test suite for IMA systems which conclusively demonstrates that there are no development errors present. Since these errors are generally not measurable and suitable numeric methods for characterizing them are not available, other qualitative means should be used to establish that the IMA system can satisfy regulations and safety and functional requirements with minimal likelihood of design errors causing unacceptable events. Thus, for highly integrated and complex systems development assurance is relied upon to reduce the likelihood of errors in the system.

A QA process in accordance with ED-79/ARP-4754 (Ref. [7]) should be implemented for both the IMA system and the modules within the system. QA personnel are responsible for monitoring the development to ensure that:

a. approved plans, standards, policies, and procedures are followed,

b. appropriate life cycle data is produced, and

c. the resulting implemented IMA system has been developed and verified using structured, rigorous processes appropriate for the development assurance level of the IMA system.

[3] These items vary slightly between ED-80/DO-254 and DO-178B/ED-12B.

ED-12/DO-178 (Ref. [2]) identifies QA requirements for software and should be used for software in IMA systems. ED-80/DO-254 (Ref. [6]) identifies process assurance requirements for electronic hardware and should be used for electronic hardware in IMA systems. The QA process should ensure that development and verification activities are performed in compliance with the approved plans, standards, and procedures. The QA process should address all levels of IMA system development (e.g., module, platform, application, IMA system, and aircraft installation).

An IMA System Quality Assurance Plan (IMASQAP) should be developed and should describe the quality and process assurance processes and activities to be used for the IMA system as appropriate for the development assurance level of the system and to demonstrate compliance. One or more QA plans may be developed to address the multiple levels of system development or a joint QA plan may address all the levels of the IMA system development.

The IMASQAP should contain at least:

a. A description of the QA environment, including scope, organizational responsibilities and interfaces, standards, procedures, tools, and methods.

b. A statement of the QA authority, responsibility, and independence, including the approval authority for IMA system components. QA should have a level of independence that gives them enforcement authority.

c. The QA activities that are to be performed, including QA methods, evidence of QA involvement, preparation of QA records, transition criteria, etc.

d. The process for evaluation and implementing corrections.

e. A definition of the records to be produced by the QA process.

NOTE: *"Quality assurance" is called "process assurance" in ED-80/DO-254 (Ref. [6]) and ED-79/ARP-4754 (Ref. [7]).*

5.7 CERTIFICATION LIAISON

5.7.1 Certification Liaison Process

The certification liaison process establishes communication and understanding between the applicant and the certification authority throughout the IMA system life cycle to assist in the acceptance and certification process.

Typical contents of life cycle data have been described throughout this document. However, it should be noted that life cycle data may be packaged and titled as appropriate for the project but should still address the contents prescribed in this document. If alternate titles or packaging is used, the stakeholder should develop a document mapping to demonstrate that all the applicable data is available.

5.7.2 Means of Compliance and Planning Data

To implement the certification liaison process the applicant proposes a means of compliance that defines how the development of the IMA will satisfy the certification basis. The IMASCP (see Sections 4.4.3 and 4.5.3), the Module Acceptance Plan (see Section 4.2.3), the PSACs, and PHACs define part of the IMA system context of the proposed means of compliance. These plans also state the system development assurance level, software level(s), hardware level(s), and environmental qualification testing levels, as determined by the system safety assessment process and the planned installation environment and aircraft. The applicant should:

a. Submit the IMASCP, IMASAP, PSACs, PHACs, EQT plans, and other requested data to the certification authority for review at a point in time when the effects of changes are minimal, that is, when they can be managed within project constraints.

b. Resolve issues identified by the certification authority concerning the proposed means of compliance and plans for the IMA aspects of certification.

c. Obtain agreement with the certification authority on the IMASCP, IMASAP, PSACs, PHACs, EQT plans, flight test plans, and other plans.

Figure 5 illustrates the typical planning data.

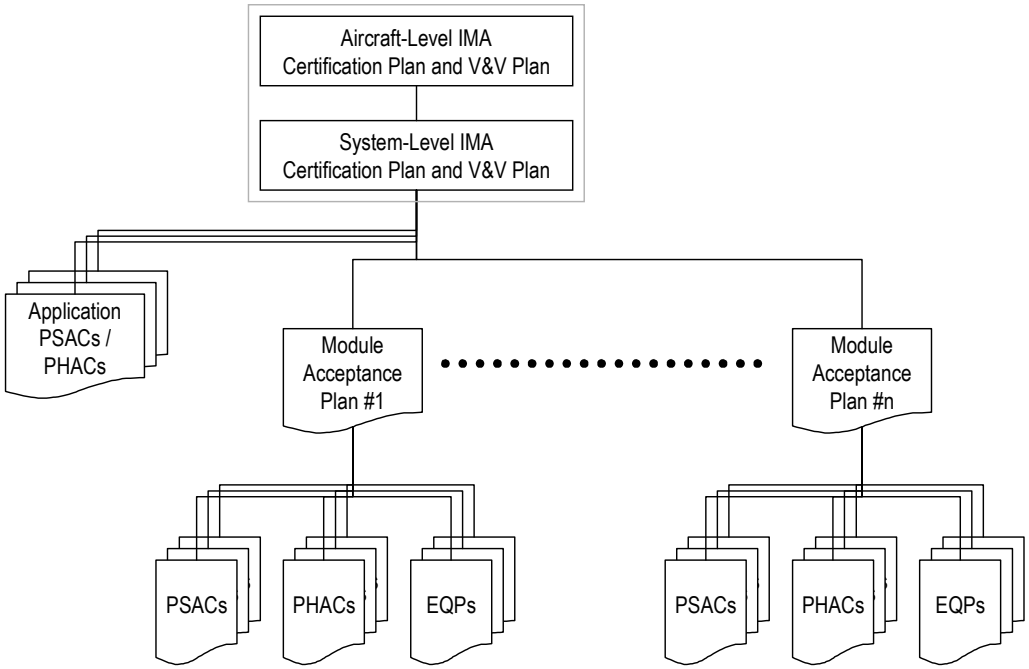

FIGURE 5 : PLANNING DATA FOR IMA SYSTEM

5.7.3 Development Life Cycle Data

Throughout the development of the IMA system and installation on the aircraft life cycle data will be developed. These data should be made available to the certification authority upon request:

a. Module Acceptance Data (see Sections 4.2.2 through 4.2.12), including all MRSs, module V&V results, module QA records, module CM records, module problem reports, and additional Module Acceptance Data (Section 4.2.12).

b. Hosted Application data (see Section 4.3.2).

c. IMA system data (see Sections 4.4.2 through 4.4.7).

d. Aircraft-IMA system integration data (see Sections 4.5.2 through 4.5.7).

Figure 6 provides an overview of the life cycle data for an IMA system. All data should be available to certification authority. Table 8 illustrates the life cycle data to be submitted to certification authority.

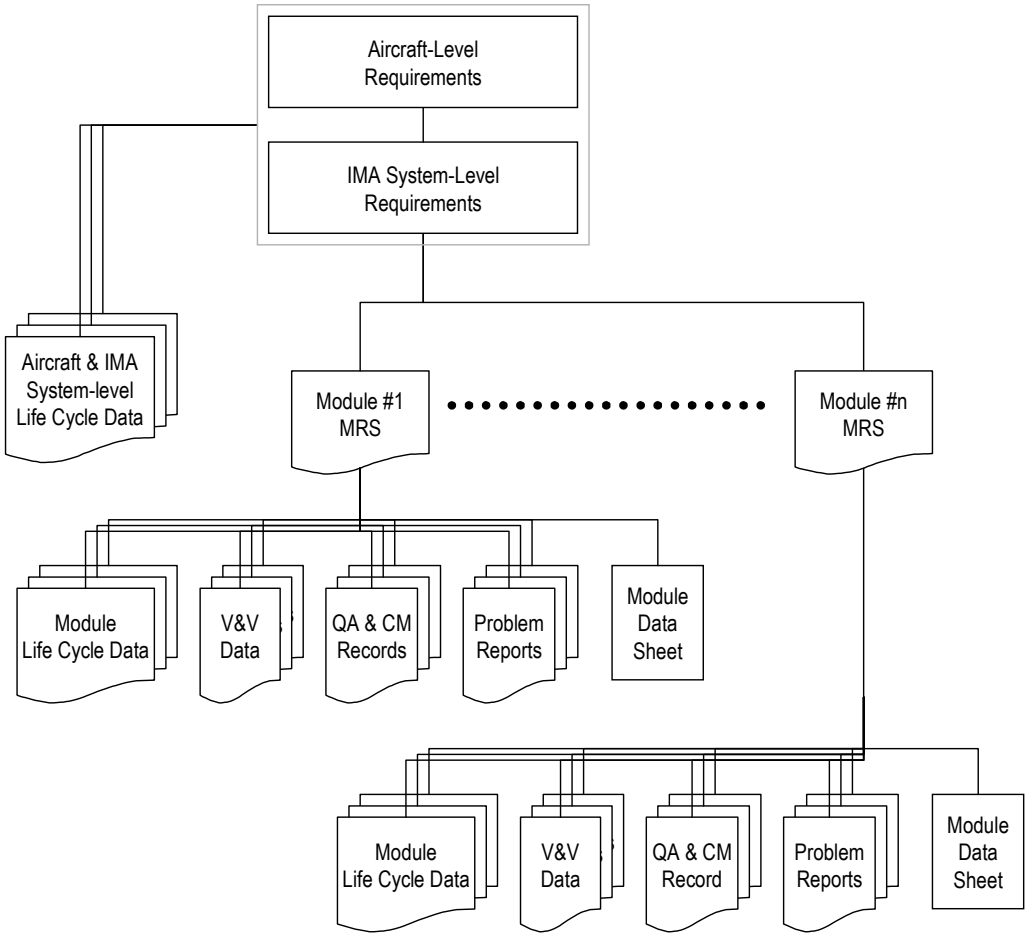

FIGURE 6 : LIFE CYCLE DATA FOR IMA SYSTEM

5.7.4 Compliance Substantiation

The applicant provides evidence that the IMA system development processes satisfy the plans, and should demonstrate that the aircraft and installed IMA system complies with all applicable regulations. Certification authority reviews may take place at the applicant's facilities or the developer's facilities. This may involve discussions with the applicant or its developers. The applicant arranges these reviews of the activities of the life cycle processes and makes IMA system life cycle data available, as needed. The applicant should:

a. Resolve issues raised by the certification authority as a result of its reviews.

b. Submit the System-Level and/or Aircraft Level IMA System Accomplishment Summaries, MAASs, SASs, HASs, module acceptance data sheets, MCIs, SCIs, HCIs (i.e., top-level drawings), EQT reports, aircraft installation data, aircraft ground and flight test results, and the Aircraft-Level and/or System Level IMA System Configuration Index(es) (may be included in the compliance report) to the certification authority. The data to support the modules, platforms, and hosted applications should be addressed in the IMA system compliance.

c. Submit or make available other data or evidence of compliance requested by the certification authority.

Figure 7 illustrates a typical compliance data tree.

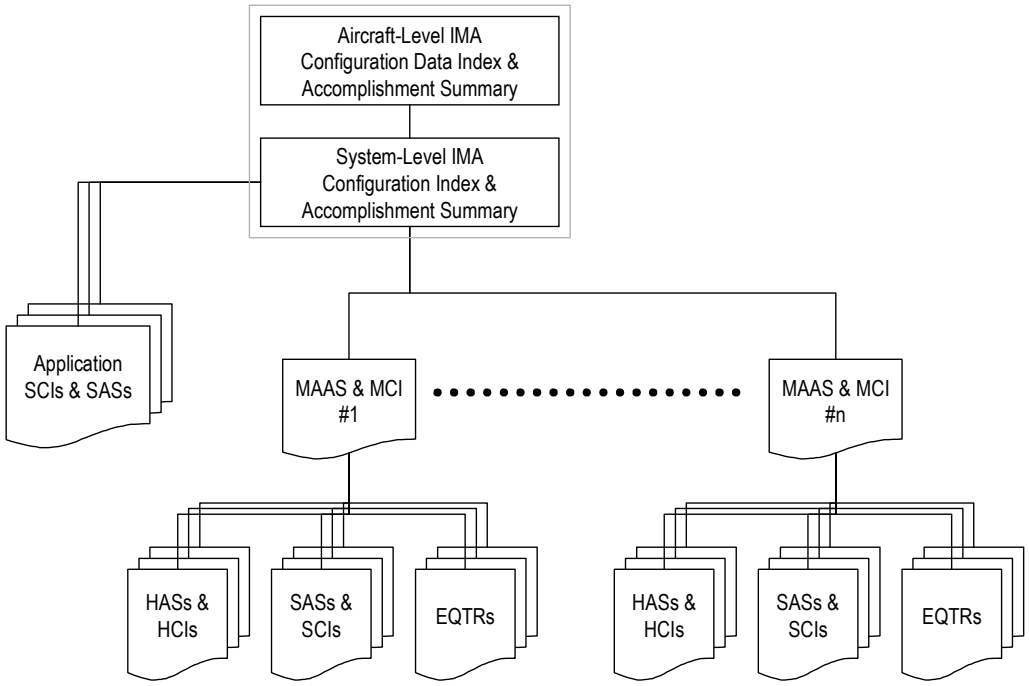

FIGURE 7: COMPLIANCE SUMMARIES FOR IMA

5.7.5 Life Cycle Data Submittals

Table 8 summarizes the typical IMA system life cycle data that is submitted to the certification authority. These data items may be combined and/or distributed across multiple documents as appropriate, and should be specified in the higher level IMA System Certification Plans. The certification authority may request additional data, as needed.

TABLE 8 : LIFE CYCLE DATA TO BE SUBMITTED TO CERTIFICATION AUTHORITY

Life Cycle Data Item	Ref.	Task 1	Task 2	Task 3	Task 4
Module Acceptance Plan (MAP)	4.2.3	X			
Module Configuration Index(es) (MCI)	4.2.7	X			
Module Acceptance Accomplishment Summary (MAAS)	4.2.9	X			
Module Acceptance Data Sheet	4.2.10	X			
Plans for Software Aspects of Certification (PSACs)	4.2.12.a 4.3.2	X	X		
Plans for Hardware Aspects of Certification (PHACs)	4.2.12.a 4.3.2	X	X		
Software Configuration Indices (SCIs)	4.2.12.a 4.3.2	X	X		
Hardware Configuration Indices (HCIs) (i.e., Top-Level Drawings)	4.2.12.a 4.3.2	X	X		

Life Cycle Data Item	Ref.	Task 1	Task 2	Task 3	Task 4
Software Accomplishment Summary(ies) (SAS)	4.2.12.a 4.3.2	X	X		
Hardware Accomplishment Summary(ies) (HAS)	4.2.12.a 4.3.2	X	X		
Safety Assessment Analysis/Report(s)	4.2.12.b			X	X
Hosted Application Acceptance Data Sheet	4.3.2		X		
IMA Certification Plan (system- and aircraft-level)	4.4.3 4.5.3			X	X
IMA Verification and Validation Plan (system- and aircraft-level)	4.4.4 4.5.4			X	X
IMA Configuration Index (system- and aircraft-level)	4.4.5 4.5.5			X	X
IMA Accomplishment Summary (system- and aircraft-level)	4.4.6 4.5.6			X	X
Environmental Qualification Test (EQT) Plan	Ref. [1]	X	X	X	X
Environmental Qualification Test (EQT) Reports	Ref. [1]	X	X	X	X

5.7.6 Certification Liaison Process When Changes Are Made

When a change to an approved module or hosted application is proposed, a change impact analysis (CIA) should be performed and documented as described in Section 4.6.4. The CIA and other planning documents that address the change should be submitted to the certification authority as early as possible to obtain agreement. Changes should not be implemented until agreement is obtained. All data affected by the change should be updated in compliance with the plans. After the change is made, as a minimum, the data listed in Section 5.7.5 which is affected by the change should be submitted to the certification authority.

NOTE: *The certification authority may request additional documentation to support the change, such as verification planning.*

5.7.7 Certification Liaison Process For Reuse of Modules

When a module or hosted application acceptance package is proposed for reuse, as described in Section 4.7, the data identified in Section 4.7.6 should be submitted to the certification authority.

CHAPTER 6

CONSIDERATIONS FOR CONTINUED AIRWORTHINESS OF IMA SYSTEMS

This section provides guidance for continued airworthiness of IMA systems related to training, maintenance, and post-certification modifications of aircraft with IMA systems installed. Although this guidance is not specific only to an IMA system, the increased level of integration, interdependency, and complexity has the potential to introduce new areas of concerns when maintenance and modification procedures are conducted. Therefore, the guidance for continued airworthiness becomes of greater concern than in a federated system architecture and should be thoroughly addressed in the initial design of an IMA system, as well as in the continued airworthiness process.

6.1 TRAINING

To maintain the continued airworthiness of an IMA system, maintenance personnel and appropriate flight operations personnel should receive training for the specific IMA system.

During the development of an IMA system, a human factors assessment should be performed to address the practicalities of operations with the system in normal and degraded configurations and in recovery situations (see Section 3.10). Training should ensure that flight operations personnel understand the effects of degraded mode operations, cascading failures, multiple messages, and aural alerts.

Cascading failures in an IMA system have the potential to hide the primary cause of failure, and the required flight crew actions may not always be obvious. Therefore, training for the flight crew of well-defined processes for failure identification, recovery actions (if appropriate), and failure reporting is required.

The reporting by the flight crew of IMA system failures or anomalous behavior and the retrieval of fault diagnostic reports (see Section 3.6.5) are important for maintenance. These reports should be accurate and complete and should reference the applicable fault codes.

Due to the increased integration, interdependency, complexity, and potential for latent and cascading failures (which can be very difficult to isolate and may not always be obvious to determine by traditional methods), the training of maintenance personnel is very important to the continued airworthiness of an IMA system. The information and procedures provided to the maintenance personnel (i.e., instructions, fault diagnosis, repairs, verification, confirming the IMA configuration after maintenance work, etc.) should be well planned, accurate, complete, and easy to understand. For example, identification and diagnosis of faults or failures in an IMA system may be difficult due to cascading or latent failures, which may hide the primary cause of failure. Therefore, the training required for fault identification and correction should be thorough and comprehensive, and may be more encompassing for an IMA system than for a federated system architecture.

6.2 MAINTENANCE

For continued airworthiness, flight operations, and maintenance, the IMA system should be capable of displaying the status, version, and currency of the loaded software and data. The configuration of the components of the IMA system should be available to make repairs and perform any tests or inspections to determine conformance of the system to the approved type design.

Since software can be loaded independently from hardware on the aircraft, the operator should establish a process for maintaining and recording the IMA system configuration (identification and revision status of hardware and software components and modules). This information should be current and maintained as part of the aircraft records.

When loading field-loadable hardware or software, there should be a robust process established to ensure correct and complete loading, to confirm the hardware or software loaded is approved, and to verify the upload has not been corrupted (e.g., verification with an appropriate data transfer integrity check). This process should include checks before and after loading into the IMA system and to annunciate any failures of the loading. The operator should also be able to confirm the compatibility and intermixability of hardware and software loads with other components.

A human factors analysis (see Section 3.10) of the maintenance interface and procedures should be included in the IMA system design data. Clear and unambiguous fault identification and diagnostic procedures should be addressed in the maintenance manuals. The IMA system should provide a means to detect and identify failures to facilitate maintenance of the system.

6.3 POST-CERTIFICATION MODIFICATIONS

Modifications to an IMA system after initial certification should reference the design data and certification criteria established by the certification applicant. This also applies where the applicant is not the original certification applicant. Post-certification modifications should include reviews of the human factors assessment (both flight crew and maintenance procedures - see Section 3.10), the safety assessment (see Section 5.1), and certification requirements of the installation for changes that have an impact on the certified aircraft configuration and type design.

Due to the increased level of integration, interdependency, and complexity of an IMA system, post-certification modifications should be developed and accomplished with consideration to the impact on the aircraft safety assessment, IMA system safety assessment, and aircraft certification basis. When a modification is proposed, a change impact analysis should be performed (see Section 4.6.4). This change impact analysis should determine whether the proposed change could adversely affect safe operation and continued airworthiness of the IMA system, aircraft, or engine.

An area of particular concern with an IMA system is when there is a failure that results in numerous failure or alert messages being displayed (see Section 3.6) and/or aural alerts occurring simultaneously. These messages should be displayed in a clear and prioritized manner. The priority of aural alerts should be established (i.e., status, caution, warning, immediate pilot action). In a post-certification modification, these prioritization hierarchies should be analyzed for continued airworthiness compliance and to minimize flight crew workload. Under no circumstances should a flight crew be expected to determine the priority of these messages and alerts and the order in which they should be addressed, because this could lead to an unacceptable delay in dealing with failures and may result in an unacceptable safety of flight situation.

ANNEX A

OBJECTIVE TABLES

The objectives are used to plan and ensure that the installed IMA system complies with the guidance of this document. Objectives should be addressed during the planning process of the aircraft certification program (e.g., Aircraft and/or IMA System Certification Plans, Platform Acceptance Plan, Module Acceptance Plan, Hosted Application Acceptance Plans). Since multiple stakeholders will typically be involved in the acceptance and certification efforts, the plans should clearly delineate who is responsible for achieving each objective. Plans should also indicate the roles and responsibilities of each stakeholder when more than one stakeholder is involved in the satisfaction of an objective and how compliance with that objective will be demonstrated and by whom. Evidence of compliance with these objectives (full, partial, or none) should be provided in the compliance documentation (e.g., Aircraft-Level and System-Level IMA System Accomplishment Summaries, Platform/Module Accomplishment Summaries, Hosted Application Accomplishment Summaries).

The "Objective" column provides the certification objectives of this document that should be met during IMA system development. The "Doc Ref" column refers to a section(s) in this document where more explanation of the objective is available. The "Life Cycle Data Description" refers to the data that typically satisfies the objective. The "Life Cycle Data Reference" column refers to a section(s) where more explanation or data content description are provided.

NOTE: *Control Categories (CC) CC1/CC2 is provided as general guidelines in these tables (see Section 0). For some systems, platforms, modules, or applications, the amount of configuration control may be less stringent, if justified in the IMASCMP (e.g., lower levels of design assurance).*

TABLE A-1 : IMA MODULE/PLATFORM DEVELOPMENT PROCESS (TASK 1) OBJECTIVES

ID	Objective	Doc Ref	Life Cycle Data Description	Life Cycle Data Reference	Control Category
1	Module/platform development and acceptance life cycle, and associated processes are planned and implemented consistently with the guidance of DO-160, DO-178, DO-254 and this document.	4.2.1a 3.1.1a	Module/Platform Acceptance Plan	4.2.3	CC1
2	Module/platform requirements specifications are defined, traceable, and verifiable.	4.2.1b 3.1.1b	Module/Platform Requirements Specifications	4.2.4	CC1
			Traceability Data	4.2.5	CC2
3	Module/platform design is documented and addresses the IMA unique failure modes, safety analysis, and functionality.	3.1.1c,d 4.2.1b,c 5.1	Module/Platform Design Data	4.2.4	CC1
			Module/Platform Failure Analyses and Safety Analyses	4.2.12b	CC1

4	Verification and development tools are assessed and qualified, as needed.	4.2.1i 3.4 5.2.3	Module/Platform Tool Qualification Data	4.2.12c	CC2 or CC1[4]
5	Partitioning ensures that the behavior of any hosted application is prevented from adversely affecting the behavior of any other application or function.	3.5 3.1.1c,d 4.2.1c,d 5.1, 5.3, 5.4	Partitioning Analysis Data	4.2.4j	CC1
			V&V Data	4.2.5	CC2
			Failure Analyses and Safety Analyses	4.2.12b	CC1
6	Compliance with module requirements, resource requirements, etc. is demonstrated.	3.1.1d,e 4.2.1c 4.2.1d 4.2.1e	Module/Platform V&V Data	4.2.5	CC2
7	Ensure module users have the information needed to integrate and interface the module.	4.2.1g,k,l 3.4	Module/Platform Acceptance Data Sheet	4.2.10	CC1
			Interface Specifications	4.2.4f	CC1
			Module/Platform User's Guide	4.2.12e	CC2
8	Platform integration is complete.	4.2.1h 3.1.1d 5.3, 5.4	Platform Integration, Verification, and Validation Data	4.2.5	CC2
9	Health monitoring and fault management functions of the IMA platform are provided and documented for use by the hosted applications and the IMA system.	4.2.1c 3.6 5.1.5.5 5.1.5.6	Platform Requirements Specification	4.2.4f	CC1
10	Quality assurance, configuration management, integration, validation, verification, and certification liaison for the module/platform are implemented and completed.	4.2.1f,j,k 5.3 to 5.7	Module/Platform QA Records	4.2.6	CC2
			Module/Platform CM Records	4.2.8	CC2
			Module/Platform V&V Data	4.2.5	CC2
			Module/Platform Acceptance Accomplishment Summary	4.2.9	CC1
			Module/Platform Configuration Index	4.2.7	CC1
			Module/Platform Problem Reports	4.2.11	CC2

[4] Control category for tool qualification data is defined in ED-12/DO-178 (Ref. [2]) or ED-80/DO-254 (Ref. [6]).

TABLE A-2: HOSTED APPLICATION DEVELOPMENT AND ACCEPTANCE (TASK 2) OBJECTIVES

ID	Objective	Doc Ref	Life Cycle Data Description	Life Cycle Data Reference	Control Category
1	Acceptance plans for the hosted applications are complete, identify the IMA platform resources to be used and address IMA system unique aspects of the life cycle development and verification processes.	3.1.2a,b	Hosted Application PSAC/PHAC	4.3.2[5]	CC1
2	Compliance of applications to the appropriate guidance (software ED-12/DO-178, and hardware DO-254/ED-12) is demonstrated and appropriate life cycle data is developed.	3.1.2g 4.3.1d,e	Hosted Application Life Cycle Data[4]	4.3.2[5]	[5]
3	Platform resources required by the hosted application are defined. Application safety, health monitor/fault management, environmental qualification, resources outside the platform, and human factors aspects are defined as required.	4.3.1b 3.1.2c,d,e,f,h	Hosted Application Life Cycle Data[4]	4.3.2[5]	CC1[5]
4	Application is integrated on the platform.	4.3.1f	Hosted Application Life Cycle Data[4]	4.3.2[5]	[5]
5	Proper use of resources allocated to the application by the integrator are verified.	4.3.1c	Verification and Validation Results	4.3.2	CC2
6	Compliance of hosted applications on the target computer and environment is demonstrated.	4.3.1a	Complete Hosted Application Life Cycle Data Package[4]	4.3.2[5]	[5]
7	Configuration control is maintained and ensures properly configured tools, applications and modules are used for the development, integration, and verification processes.	4.3.1g	CM Plans, Procedures, and Records[4] Configuration Indices	4.3.2[5]	[5]
8	If reuse credit is desired for the application, it is addressed during the development of the application.	4.3.1h	Application PHAC, PSAC	4.3.2[5]	[5]

[5] Assurance processes, life cycle data, and appropriate control category(ies) is defined in ED-12/DO-178 (Ref. [2]) for software applications and ED-80/DO-254 (Ref. [6]) for hardware applications (HC1 or HC2)

TABLE A-3 : IMA SYSTEM-LEVEL DEVELOPMENT AND ACCEPTANCE (TASK 3) OBJECTIVES

ID	Objective	Doc Ref	Life Cycle Data Description	Life Cycle Data Reference	Control Category
1	IMA system activities are planned with the intent of using the integration, validation, and verification for aircraft-level certification credit.	3.1.3c 4.4.1a 5.5 5.6	IMA System Certification Plan	4.4.3	CC1
			IMA System CM Plan	5.5.1	CC1
			IMA System QA Plan	5.6	CC1
			IMA System V&V Plan	4.4.4	CC1
2	IMA system safety assessments and analyses are complete.	3.1.3b,d 4.4.1c 5.1.5	IMA Safety Analysis(es) and Report(s)	4.4.7d	CC1
3	The IMA system architecture is defined and documented.	3.1.3c	IMA System Requirements and Design Data	4.4.7f	CC1
4	Integration, verification, and validation activities are performed on the IMA system.	3.2 3.1.3e,f 4.4.1f	IMA System V&V Data	4.4.7a	CC2
5	Health monitoring, failure reporting, and fault management functions are provided for the platform to meet the requirements.	3.6 4.4.1b	IMA System Verification and Validation Results	4.4.7a	CC2
			IMA System Requirements & Design Data	4.4.7f	CC1
6	Configuration management and quality assurance for the IMA system are established and maintained.	3.7 4.4.1c, d 5.5 5.6	IMA System Certification Plan	4.4.3h	CC1
			IMA System CM Plan	5.5.1	CC1
			IMA System QA Plan	5.6	CC1
			IMA SystemCM Records	4.4.7b	CC2
			IMA System Configuration Index	4.4.5	CC1
			Problem reports	4.4.7e	CC2
7	Allocation of shared resources is established and verified.	3.2 3.5 4.4.1b	IMA System Requirements and Design Data	4.4.7f	CC1
			IMA System V&V Results	4.4.7a	CC2
8	Design and configuration tools are developed and assured to the level of assurance required to support the IMA system.	3.4 4.4.1b 5.2.3	Tool Qualification Data	4.4.7g	[6]
9	If required, IMA system is designed to support the MMEL requirements.	3.9 5.1.5	IMA Safety Analysis(es) and Report(s)	4.4.7d	CC1

[6] Control category as defined in ED-12/DO-178 (Ref. [2]) or ED-80/DO-254 (Ref. [6]).

ID	Objective	Doc Ref	Life Cycle Data Description	Life Cycle Data Reference	Control Category
10	Human factors issues are addressed in the IMA system design.	3.10	IMA System Requirements and Design Data	4.4.7f	CC1
11	IMA system design assurance activities are completed.	3.1.3e,f 4.4.1d,g	IMA System Configuration Index	4.4.5	CC1
			IMA System Accomplishment Summary	4.4.6	CC1
			Additional IMA System Data	4.4.7f,g [7]	CC1
			Additional IMA System Data	4.5.7a,b,c,d	CC2
12	Module and application problem reports are evaluated at the system level, and system-level problem reporting is established.	4.4.1h	IMA System Problem Reports	4.4.7e	CC2
			IMA System Certification Plan	4.4.3o	CC1

[7] Control category for tool qualification data (section 4.4.7g) is defined in ED-12/DO-178 (Ref. [2]) or ED-80/DO-254 (Ref. [6]).

TABLE A-4 : AIRCRAFT-LEVEL INTEGRATION (TASK 4) OBJECTIVES

ID	Objective	Doc Ref	Life Cycle Data Description	Life Cycle Data Reference	Control Category
1	Aircraft IMA System installation, integration, verification, and validation activities are planned.	4.5.1a	Aircraft-level IMA System Certification Plan	4.5.3	CC1
			Aircraft-level IMA V&V Plan	4.5.4	CC1
			Aircraft-level IMA CM Plan	5.5.1	CC1
			Aircraft-level QA Plan	5.6	CC1
2	Compliance is demonstrated for intended functionality, performance and safety requirements, using laboratory, ground, and flight tests, and appropriate analyses.	4.5.1b	V&V Results	4.5.7a	CC2
3	IMA system resource management, fault tolerance and management, health monitoring, degraded modes and reversion capabilities are verified.	4.5.1c 3.1.3f	V&V Results	4.5.7a	CC2
4	Compliance is demonstrated to the regulations appropriate for the aircraft and/or engine certification basis.	4.5.1d	Aircraft-level IMA Accomplishment Summary	4.5.6	CC1
			Aircraft-level IMA Configuration Index	4.5.5	CC1
5	Repercussions of specific anomalies are evaluated, such as a loss or malfunction of multiple applications or of entire shared resources, latent failures, and cascading failures.	4.5.1e 5.1.5	Safety Analysis(es) and Report(s)	4.5.7d	CC1
			V&V Results	4.5.7a	CC2
6	V&V activities are performed to address module failure modes affecting several hosted applications (intra-module analysis); common failure modes on module level affecting several hosting applications (inter-module analysis); and failure modes affecting multiple aircraft systems. Back up systems and mitigation means should also be addressed.	4.5.1f 3.1.3f 5.1.5	Safety Analysis(es) and Report(s)	4.5.7d	CC1
			V&V Results	4.5.7a	CC2
7	Human factors issues are addressed with regard to multiple aircraft functions failure, pilot workload and anomalous behavior, and normal and emergency operational procedures.	3.10 4.5.1g	Aircraft-level IMA System Certification Plan	4.5.3	CC1
			V&V Results	4.5.7a	CC2

8	High Intensity Radiated Fields (HIRF) and Indirect Effects of Lightning (IEL) testing is performed with regard to multiple aircraft functions failure and anomalous behavior, as required.	4.5.1h 5.2.6	Aircraft-level Environmental Test Plans	4.5.7g	CC1
			Aircraft-level Environmental Test Results	4.5.7g	CC2
9	Proper interaction is verified between the IMA system and other aircraft systems.	4.5.1i	Aircraft-level IMA System Certification Plan	4.5.3	CC1
			Aircraft-level IMA System V&V Plan	4.5.4	CC1
			V&V Results	4.5.7a	CC2
10	Aircraft-level certification data for the IMA system is completed.	4.5.1k	Aircraft-level IMA System Configuration Index	4.5.5	CC1
			Aircraft-level IMA System Accomplishment Summary	4.5.6	CC1
			Additional Aircraft-level Data	4.5.7d,f,g[8], h,i,j	CC1
			Additional Aircraft-level Data	4.5.7a,b,c,e ,g[8]	CC2
11	An aircraft safety assessment that addresses any failure modes of an IMA system is developed.	4.5.1j,l 5.1.5	Safety Analysis(es) and Report(s)	4.5.7d	CC1
			V&V Results	4.5.7a	CC2
12	IMA system is installed and integrated on the aircraft.	4.5.1 5.3 5.4	V&V Results	4.5.7a	CC2
			Installation Instructions	4.5.7f	CC1
13	If required, the MMEL is developed to address the aircraft-level dispatch requirements.	3.9	Master Minimum Equipment List (MMEL)	4.5.7k	CC1
14	Continued airworthiness of an IMA system is maintained.	6.1 6.2	Aircraft-level IMA System Configuration Index	4.5.5	CC1
			Instructions for Continued Airworthiness	4.5.7h	CC1

[8] Control category for tool qualification data (section 4.5.7g) is defined in ED-12/DO-178 (Ref. [2]) or ED-80/DO-254 (Ref. [6]).

TABLE A-5 : CHANGE (TASK 5) OBJECTIVES

ID	Objective	Doc Ref	Life Cycle Data Description	Life Cycle Data Reference	Control Category
1	Change management process is developed and coordinated with all stakeholders.	4.6.2a 4.6.3 6.3	Change Management Plan	4.6.5b	CC1
2	Change impact analysis is conducted and changes are made and documented.	4.6.2b,c 4.6.4 6.3	Change Impact Pnalysis	4.6.5a	CC1
3	The changed module or application is re-integrated into the IMA system. All necessary verification, validation, and integration activities (regression analysis and testing) are performed.	4.6.2d 6.3	V&V Plan	4.6.5c	CC1
			V&V Results	4.6.5c	CC2
			Modified Life Cycle Data (including Configuration Indices)	4.6.5d	[9]
			Updated Accomplishment Summary	4.6.5e	CC1
			Change History and Maintenance Records	4.6.5f	CC2
4	Configuration control of all life cycle data related to the change is maintained.	4.6.2e 6.3	Modified Life Cycle Data (including Configuration Indices)	4.6.5d	[9]
			Updated Accomplishment Summary	4.6.5e	CC1
			Change History and Maintenance Records	4.6.5f	CC2

[9] The specific life cycle data description, reference, and control category depends on what is being modified and may vary for each instance of reuse.

TABLE A-6 : MODULE OR APPLICATION REUSE (TASK 6) OBJECTIVES

ID	Objective	Doc Ref	Life Cycle Data Description	Life Cycle Data Reference	Control Category
1	Module or application life cycle data is ensured to be unchanged from what was previously accepted.	4.7.1a	MAAP, PSAC, PHAC, or other appropriate plan proposing the reusable module or application	4.7.6[10]	[10]
2	Limitations, assumptions, etc. are documented in the module or application acceptance data sheet and are addressed in the subsequent installation.	4.7.1b	Acceptance Data Sheet	4.7.6[10]	[10]
			Verification Results of Subsequent Installation	4.7.6[10]	CC2
			Accomplishment Summary of Reused Module or Application	4.7.6[10]	CC1
3	Usage domain analysis is performed to ensure that the module or application is being reused in the same way it was originally intended.	4.7.1c	V&V Results	4.7.6[10]	[10]
4	Open problem reports of the module or application are evaluated to ensure that no problem adversely impacts safety, functionality, performance, or operations.	4.7.1d	Problem Reports Analysis Results	4.7.6[10]	[10]
5	Reusable module or application that was previously accepted is integrated, verified and validated in the new installation.	4.7.1e	Integration Procedures	4.7.6[10]	[10]
			V&V results	4.7.6[10]	[10]
6	Submit necessary data to the certification authority.	4.7.1f	Initial Accepted Life Cycle Data	4.7.6[10]	[10]
			Subsequent Acceptance Life Cycle Data	4.7.6[10]	[10]
			V&V Records	4.7.6[10]	[10]
			Accomplishment Summaries	4.7.6[10]	[10]

[10] The specific life cycle data description, reference, and control category depends on what is being reused and may vary for each instance of reuse. For reuse of modules and applications see Section 4.7.

ANNEX B

GLOSSARY OF TERMS

Acceptance	Acknowledgement by a certification authority that the module, application, or system meets its defined requirements.
Adverse	Action, impact or behavior determined by the safety assessment process as being unacceptable or detrimental.
Aircraft Function	A capability of the aircraft that is provided by the hardware and software of the systems on the aircraft.
Airworthiness	The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function.
Analysis	An evaluation based on decomposition into simple elements.
Anomalous behavior	Behavior that is inconsistent with specified requirements.
Applicable requirements	Mandatory criteria for acceptance as established by a certification authority for the type of aircraft, engine, airborne system or equipment, or component thereof under consideration.
Applicant	A person or organization seeking approval from the certification authority.
Application	Software and/or application-specific hardware with a defined set of interfaces that when integrated with a platform(s) performs a function.
Application software	The part of an application implemented through software. It may be allocated to one or more partitions.
Application-specific hardware	Hardware dedicated to one application.
Approval	The act or instance of giving formal or official acknowledgement of compliance with regulations.
Assembly	A number of parts, subassemblies, or any combination thereof, joined together to perform a specific function.
Assessment	An evaluation based upon a defined engineering approach.
Assumptions	Statements, principles, and/or premises offered without proof.
Assurance	The planned and systematic actions necessary to provide adequate confidence and evidence that a product or process satisfies given requirements.
Authority	The organization or person responsible within the state (country) concerned with applicable requirements. A matter concerned with aircraft, engine, or propeller type certification or equipment approval would normally be dealt with by the certification authority; matters concerned with continuing airworthiness might be dealt with (by what would be referred to as) the airworthiness authority.
Availability	Probability that an item is in a functioning state at given point in time.

Baseline	The approved, recorded configuration of one or more configuration items, that serves as the basis for further development, and is changed only through change control procedures.
Cabinet	A physical package containing one or more IMA components or modules, that provides partial protection from environmental effects (shielding) and may enable installation and removal of those component(s) or module(s) from the aircraft without physically altering other aircraft systems or equipment.
Cascading Failure	A propagation of failure(s) that were not isolated or mitigated.
Certification	Legal recognition by the certification authority that a product, service, organization or person complies with the requirements. Such certification comprises the activity of technically checking the product, service, organization or person and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval or other documents as required by national laws and procedures. In particular, certification of a product involves: (a) the process of assessing the design of a product to ensure that it complies with a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety; (b) the process of assessing an individual product to ensure that it conforms with the certified type design; (c) the issuance of a certificate required by national laws to declare that compliance or conformity has been found with standards in accordance with items (a) or (b) above.
Certification Authority	Organization or person responsible for granting approval on behalf of the nation of manufacture.
Certification credit	Acceptance by the certification authority that a process, product or demonstration satisfies a certification requirement.
Change control	The systematic evaluation, coordination, approval or disapproval and implementation of approved changes in the configuration of a configuration item after formal establishment of its configuration identification or to baselines after their establishment.

NOTE: *This term may be called configuration control in other industry standards.*

Code	The implementation of particular data or computer program in a symbolic form, such as source code, object code or machine code.
Commercial Off-The-Shelf (COTS) software	Commercially available applications sold by vendors through public catalogue listings.
Common Cause Analysis	Generic term encompassing zonal analysis, particular risk analysis, and common mode analysis.
Common Mode Failure	An event which simultaneously affects a number of elements otherwise considered to be independent.
Compiler	Program that translates source code statements of a high level language into object code.

Complexity	An attribute of systems or items which makes their design and/or operation difficult to comprehend.
Compliance	Successful performance of all mandatory activities; agreement between the expected or specified result and the actual result.
Component	A self-contained hardware or software part, database, or combination thereof that may be configuration controlled.
Computer	A device or group of devices that performs a data processing function.
Configuration Control	See Change Control.
Configuration identification	The process of designating the configuration items in a system and recording their characteristics.
Configuration index	The approved documentation that defines a configuration item.
Configuration item	1) One or more hardware or software components treated as a unit for configuration management purposes. 2) Software life cycle data treated as a unit for configuration management purposes
Configuration management	A discipline applying technical and administrative direction and surveillance to (a) identify and record the functional and physical characteristics of a configuration item, (b) control changes to those characteristics, and (c) record and report change control processing and implementation status.
Configuration status accounting	The recording and reporting of the information necessary to manage a configuration effectively, including a listing of the approved configuration identification, the status of proposed changes to the configuration and the implementation status of approved changes.
Conformance	Demonstrable adherence to a set of mandatory requirements.
Containment	The property of the IMA system, module, or component to prevent the propagation of errors or cascading failures. Containment also identifies the collection of all bounds relevant to a specific application.
Control coupling	The manner or degree by which one software component influences the execution of another software component.
Core Software	The operating system and support software that manage platform resources to provide an environment in which an application can execute.
Criticality	Indication of the hazard level associated with a function, hardware, software, etc., addressing abnormal behavior of this item alone, or in combination with external events.
Data coupling	The dependence of a software component on data not exclusively under the control of that software component.

Deactivated code	Executable object code (or data) which by design is either (a) not intended to be executed (code) or used (data), for example, a part of a previously developed software component, or (b) is only executed (code) or used (data) in certain configurations of the target computer environment, for example, code that is enabled by a hardware pin selection or software programmed options.
Demonstration	A method of proof of performance by observation.
Dependability	The dependability of a system is that property of the system which allows reliance to be justifiably placed on the service it delivers.
Determinism / deterministic	The ability to produce a predictable outcome generally based on the preceding operations. The outcome occurs in a specified period of time with some degree of repeatability.
Development assurance	All of those planned and systematic actions used to substantiate, at a level of confidence, that development errors have been identified and corrected such that the system satisfies the applicable certification basis and its requirements.
Domain	A grouping of items into areas that share a common interest or characteristics.
European Technical Standard Order (ETSO) Authorization	Legal recognition by the certification authority that a system, equipment, or part satisfies the ETSO requirements and minimum performance specification, and authorization to manufacture that item.
Fail passive	The property of a system to recognize that a fault has occurred and transition into a passive state to avoid adverse affects on the system operation.
Failure	The inability of a system or component to perform a required function within specified limits. A failure may be produced when a fault is encountered.
Failure condition	The effect on the aircraft and its occupants, both direct and consequential, caused or contributed to by one or more failures.
Failure effect	A description of the operation of an item as the result of a failure.
Failure mode	The way in which a failure of an item occurs.
Fault diagnosis	The ability to positively identify the cause of a fault from recorded fault, failure, error or anomalous behavior events.
Fault tolerance	The built-in capability of a system to provide continued execution in the presence of a limited number of hardware or software faults.
Federated system	Aircraft equipment architecture consisting of primarily line replaceable units that perform a specific function, connected by dedicated interfaces or aircraft system data buses.
Formal methods	Descriptive notations and analytical methods used to construct, develop and reason about mathematical models of system behavior.

Function	A named capability that performs a specific task.
Function hazard assessment	A systematic, comprehensive examination of aircraft functions to identify and classify failure conditions of those functions according to their severity.
Guidelines	Recommended procedures for complying with regulations.
Hardware	An item that has physical being. Generally refers to such items as line replaceable units or modules, circuit cards, and power supplies.
Hardware/software integration	The process of embedding the software into the target computer.
Integrated Modular Avionics	A shared set of flexible, reusable, and interoperable hardware and software resources that, when integrated, form a platform that provides services, designed and verified to a defined set of safety and performance requirements, to host applications performing aircraft functions.
Incremental acceptance	A process for obtaining credit toward approval and certification by accepting or finding that an IMA module, application, and/or off-aircraft IMA system complies with specific requirements. Credit granted for individual tasks contributes to the overall certification goal.
Independence	1) Separation of responsibilities which ensures the accomplishment of objective evaluation. - For software verification process activities, independence is achieved when the verification activity is performed by a persons(s) other than the developer of the item being verified, and a tools(s) may be used to achieve an equivalence to the human verification activity. - For the software quality assurance process, independence also includes the authority to ensure corrective action. 2) A design concept that ensures that the failure of one item does not cause a failure of another item. Initialization A sequence of actions which bring the system or component thereof to a state of operational readiness.
Inspection	1) An examination of an item against a specific standard. 2) The examination and testing of supplies and services, including when appropriate, raw materials, components, intermediate assemblies and services, to determine whether they conform to specified requirements.
Integral process	A process which assists the system, software or hardware development processes and other integral processes and, therefore, remains active throughout the life cycle. The integral processes are the verification process, the quality assurance process, the configuration management process, and the certification liaison process. Integration Gathering a number of separate components to form a single implementation.

Integrity	A qualitative measure of the assurance that a system, hardware or software will function correctly and timely to defined requirements, typically achieved by applying a defined, rigorous development process to the design, implementation and verification of that item to an appropriate assurance level.
Interchangeability	The ability to substitute one item for another within a system and have the system perform to its specification.
Interoperability	The capability of several modules to operate together to accomplish a specific goal or function.
Intermixability	The capability to intermix software and/or hardware of different versions and/or modification standards.
Library	Set of common software functions or resources usable by one or more different applications.
Maintainability	The attribute of dependability with regard to the ease of performing maintenance actions. In a quantified way, it is the measure of the interruption of the service if a failure appears, and the ease of identifying the failure and performing the correct repair action. An useful estimator associated with this measure is the MTTR (Mean Time To Repair).
Malfunction	The occurrence of a condition whereby the operation is outside specified limits.
Means of compliance	The intended method(s) to be used by the applicant to satisfy the requirements stated in the certification basis for an aircraft, engine or propeller.
Memory device	An article of hardware capable of storing machine-readable computer programs and associated data. It may be an integrated circuit chip, a circuit card containing integrated circuit chips, a core memory, a disk, or a magnetic tape.
Message	A continuous block of data with a defined length which is transported by the system (either by the communication network or within a module).
Master Minimum Equipment List (MMEL)	A controlled list which identifies which equipment and systems are necessary for an aircraft to be allowed to be dispatched. A unit is described in the MMEL as ”GO”, if it is not required, and ”NO GO”, if it is required. As a consequence, a unit which has failed and is a MMEL NO GO must be repaired or replaced before the aircraft can be dispatched.
Module	A component or collection of components that may be accepted by themselves or in the context of an IMA system. 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 system hosted applications.
Network	A term used to refer to one or more physical communications links used for the same purpose.
Object code	A low-level representation of the computer program not usually in a form directly usable by the target computer but in a form which includes relocation information in addition to the processor instruction information.

Operating system (OS)	1) The same as executive software. 2) The software kernel that services only the underlying hardware platform. 3) Software that directs the operations of a computer, resource allocation and data management, controlling and scheduling the execution of computer hosted applications, and managing memory, storage, input/output, and communication resources.
Operational capability	A function or group of functions that provides an aircraft capability visible to the flight crew or other personnel.
Part number	A structured set of numbers, letters or other characters used to identify an aircraft part or configuration item.
Particular Risk	Risk associated with those events or influences that are outside the system(s) and item(s) concerned, but which may violate failure independence claims.
Partition	An allocation of resources whose properties are guaranteed and protected by the platform from adverse interaction or influences from outside the partition.
Partitioning	An architectural technique to provide the necessary separation and independence of functions or applications to ensure that only intended coupling occurs.
Platform	A module or group of modules, including core software, that manages resources in a manner sufficient to support at least one application.
Portability	The ease with which a software can be transferred from one computer, hardware, software or platform environment to another with no or minimal change to the software to operate correctly in the subsequent environment.
Preliminary System Safety Assessment (PSSA)	A systematic evaluation of a proposed system architecture and its implementation, based on the Functional Hazard Assessment and failure condition classification, to determine safety requirements for all components in the architecture.
Processing resources	The physical item which contains a CPU, memory and associated interfaces, which constitute an independent processing unit.
Processor	A device used for processing digital data.
Product service history	A contiguous period of time during which an aircraft, product or part thereof is operated within a known environment and during which failures are recorded.
Redundancy	Multiple replicas and/or versions of a function with the same or dissimilar specifications that use the same types of input and produce the same or similar outputs that can be compared to gain confidence in the output results.
Redundant	Multiple means incorporated to accomplish a given function 1) Distinction is made between the following redundant architecture principles: - similar redundancy (the multiple means are of the same type) - dissimilar redundancy (the multiple means are of different types)

	- temporal redundancy (redundancy given by repetition of the operation) 2) The operation of redundant architecture may be classified as follows: - active redundancy (multiple means are routinely in operation and participating in carrying out the task) - passive redundancy (the additional means participate in carrying out task only in case of malfunction or failure) - warm passive redundancy (the additional means are always switched on) - cold passive redundancy (the additional means are switched on only in case of malfunction or failure)
Reliability	1) The quantitative attribute and measure of dependability with regard to the continuity of the service. In a quantified way, it is the conditional probability that the system or component thereof has survived in a specified environment untill the time t, given that it was operational at time 0. A frequently used estimator associated with this measure is the MTFF (Mean Time to First Failure). 2) The probability that a component will perform a required function under specified conditions, without failure, for a specified period of time.
Requirement	An identifiable element of a specification that can be validated and against which an implementation can be verified.
Resource	Any object (processor, memory, software, data, etc.) or component used by a processor, IMA platform, core software, or application. A resource may be shared by multiple applications or dedicated to a specific application. A resource may be physical (a hardware device) or logical (a piece of information).
Reuse	The subsequent use of unaffected, previously approved system hardware or software assurance data.
Safety	The attribute of dependability with regard to the non-occurrence of or recovery from failures and other conditions that could cause unacceptable operational events of an aircraft, engine or component thereof.
Security	The attribute of dependability with regard to the prevention of corruption or unauthorized access to and/or handling of information.
Simulation	All the elements (executables, configuration files, test sets) defining a functional model which can be handled by a user.
Simulator	A device, computer program, system component(s) or environment that accepts the same inputs and produces the same output as a given target device, application, system component or environment.
Software	Computer programs and, possibly, associated documentation and data pertaining to the operation of a computer system.
Software change	A modification in source code, object code, executable object code, or its related documentation from its previous baseline.
Software integration	The process of combining code components.

Software life cycle	1) An ordered collection of processes determined by an organization to produce a software product. 2) The period of time that begins with the decision to produce or modify a software product and ends when the product is retired from service.
Software product	The set of computer programs and associated documentation and data designated for delivery to a user. In the context of this document, this term refers to software intended for use in an IMA system and its associated software life cycle data.
Software tool	A computer program used to help develop, test, analyze, produce or modify another program, its documentation or data. Examples are an automated design tool, a compiler, test tools and modification tools.
Specification	A collection of requirements which, when taken together, constitute the criteria that define the functions and attributes of a system, a component thereof, or an interface.
Standard	A rule or basis of comparison that provides both guidance in and assessment of the performance of a given activity or the content of a specified data item.
Structure	A specified arrangement or interrelation of parts to form a whole.
System	A collection of hardware and software components organized to accomplish a specific function or set of functions.
System architecture	The interfaces and the structure of the hardware and software selected to implement the system requirements.
System Safety Assessment (SSA)	A systematic, comprehensive evaluation of the implemented system to show that the relevant safety-related requirements are satisfied.
Target computer	The processor and resources that will execute a computer program in its intended target hardware.
Target computer environment	The target computer and all its support hardware, software and systems needed to function in its actual aircraft environment.
Test	A single or suite of procedure(s) to prove correct functionality and performance using stated objective criteria with pass or fail results.
Test procedure	1) A set of actions that exercises a system or component to verify that it satisfies specified requirements and to detect errors. 2) Detailed instructions for the set up and execution of a given set of test cases, and instructions for the evaluation of results of executing the test cases.
Tool qualification	The process necessary to obtain assurance for a software tool within the context of a specific aircraft system.

Traceability	1) The evidence of an association between items, such as between process outputs, between an output and its originating process, or between a requirement and its implementation. 2) The characteristic by which requirements at one level of a design may be related to requirements at another level.
Transition criteria	The minimum conditions defined by the planning process to be satisfied to enter another process.
Technical Standard Order Authorization	Legal recognition by the certification authority that a system, equipment, or part satisfies the TSO requirements and minimum performance specification, and authorization to manufacture that item.
Unintended Function	A function that is visible at the aircraft level and was neither intended nor a predicted (foreseeable) fault condition in the PSSA.
Usage domain	A declared set of characteristics for which it can be shown that: 1) The module is compliant to its functional, performance, and safety requirements as defined in the Module Requirements Specification. 2) The module meets all the assertions and guarantees regarding its defined allocate-able resources and capabilities. 3) The module performance is fully characterized, including fault and error handling, failure modes, and behavior during adverse environmental effects.
Validation	The process of determining that the requirements are the correct requirements and that they are complete. The system development process may use requirements and derived requirements in system validation.
Verification	1) The evaluation of an implementation of requirements to determine that they have been met. 2) The evaluation of the results of a process to ensure correctness and consistency with respect to the inputs and standards provided to that process.
Zonal Safety	The safety standard with respect to installation zones, potential hazards and environmental conditions associated with those zones, interference between systems or from external events, and potential maintenance issues.

ANNEX C

LIST OF ABBREVIATIONS AND ACRONYMS

AC	Advisory Circular
AMOC	Acceptable Means of Compliance
AMJ	Advisory Material - Joint
APP	Application
API	Application Programming Interface
ARINC	Aeronautical Radio Incorporated
ARP	Aerospace Recommended Practice
ASTC	Amended Supplemental Type Certificate
ATC	Amended Type Certificate
ATM	Air Traffic Management
BIT(E)	Built-In Test (Equipment)
CCA	Common Cause Analysis
CEH	Complex Electronic Hardware
CIA	Change Impact Analysis
CM	Configuration Management
CMA	Common Mode Analysis
CNS	Communication, Navigation and Surveillance
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CS	Certification Specification
DO	RTCA Document
EASA	European Aviation Safety Agency
ED	EUROCAE Document
e.g.	For example
EQTP	Environmental Qualification Test Plan
EQT	Environmental Qualification Test
ETSO	European Technical Standard Order
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FHA	Functional Hazard Assessment
FLS	Field-Loadable Software
FM	Fault Management
HAS	Hardware Accomplishment Summary
HF	High Frequency

HIRF	High Intensity Radiated Field
HM	Health Monitor
H/W	Hardware
ICAO	International Civil Aviation Organization
ICAW	Instructions for Continued Airworthiness
i.e.	That is
IEEE	Institute of Electrical and Electronic Engineers
IEL	Indirect Effects of Lightning
IMA	Integrated Modular Avionics
IMAS	Integrated Modular Avionics System
IMASAS	Integrated Modular Avionics System Accomplishment Summary
IMASCI	Integrated Modular Avionics System Configuration Index
IMASCMP	Integrated Modular Avionics System Configuration Management Plan
IMASCP	Integrated Modular Avionics System Certification Plan
IMASQAP	Integrated Modular Avionics System Quality Assurance Plan
I/O	Input and/or Output
JAA	Joint Aviation Authority
JAR	Joint Aviation Requirement
LRU	Line Replaceable Unit
MAP	Module Acceptance Plan
MMEL	Master Minimum Equipment List
MMU	Memory Management Unit
MAAS	Module Acceptance Accomplishment Summary
MADS	Module Acceptance Data Sheet
MRS	Module Requirements Specification
MTTR	Mean Time To Repair
MTFF	Mean Time to First Failure
OS	Operating System
PHAC	Plan for Hardware Aspects of Certification
PSAC	Plan for Software Aspects of Certification
PSSA	Preliminary System Safety Assessment
QA	Quality Assurance
RSC	Reusable Software Component
SAE	Society of Automotive Engineers
SATCOM	Satellite Communication
SAS	Software Accomplishment Summary
SCI	Software Configuration Index
SEU	Single Event Upset
SI	System Integrator
SSA	System Safety Assessment

STC	Supplemental Type Certification
S/W	Software
TC	Type Certification
TSO	Technical Standard Order
UMS	User-Modifiable Software
V&V	Validation and Verification

ANNEX D

IMA SYSTEM DESIGN EXAMPLES

This annex contains examples of various system designs. Each example shows how some subset of the IMA characteristics may be implemented in a typical design. These examples are supplied for information only.

D.1 EXAMPLE 1: SINGLE LRU PLATFORM

D.1.1 Purpose of this example

This example illustrates the sharing of computational and I/O resources within a single Line Replaceable Unit (LRU). Key IMA characteristics include:

- Hosting of multiple applications.
- Sharing of processing, memory, and I/O within the LRU and sharing of a network.
- Platform configuration data and data loading.
- Defined API between the platform and hosted applications.

At one level, this example illustrates a single platform providing core computational resources. At another level, this example illustrates a module to be used within a larger IMA platform.

D.1.2 Definition of platform and modules

The platform for this example is a single LRU that provides shared computational resources and hosts multiple software applications. These resources include the CPU (Central Processing Unit), MMU (Memory Management Unit), FPPU (Floating Point Processing Unit), co-processors, specific hardware mechanisms to support robust partitioning, physical memory, access to the aircraft network and I/O channels. A configuration table determines the specific purpose of a LRU. The LRU is field loadable, e.g. ARINC 615A. The core software provides an ARINC 653 API to ensure portability and robust partitioning of applications.

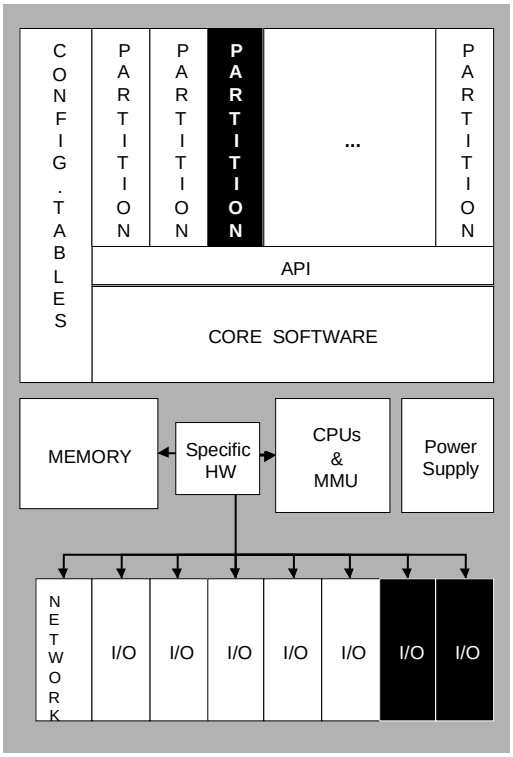

FIGURE D-1 : CONFIGURED SINGLE LRU PLATFORM

Figure D-1 shows a typical design of a single LRU platform containing:

- Hardware: CPU, MMU, network interface and I/O
- Software: Core software and partitioned application software
- Configuration tables: partition definition, network port allocation, I/O mapping

D.1.3 Key characteristics of IMA found in this system

This LRU may be independently accepted as a platform providing core computational resources for multiple avionics functions. It may be accepted as a stand-alone platform, or as a module for use within a larger IMA system.

In order to isolate multiple partitions within this platform, the platform-specific hardware (MMU, watchdog timers, etc.) provides the core software with the ability to manage shared memory space, shared processing time, and access to shared I/O. The core software manages multiple software partitions, and provides robust partitioning between applications.

Other things to note are the robust partitioning of the network interface when integrated with other platforms by a deterministic profile of ARINC 664 to meet bandwidth limitations and the mitigation of network failures by replication of the channels.

The LRU is adapted to ensure the CPU time, memory and I/O requirements of each software application. Embedded configuration tables provide this configuration capability which, together with the core software, can activate or de-activate appropriate software functions or provide adequate parameters to the core software.

Another key characteristic is a high level of internal fault/failure detection.

D.2 EXAMPLE 2: DISTRIBUTED IMA PLATFORM

D.2.1 Purpose of this example

This architecture example illustrates how a fault-tolerant, distributed platform for real-time applications can be established based on robust partitioning of the communication network resource. Based on a strict TDMA (Time Division Multiple Access) pattern the communication platform provides robust partitioning either between LRUs (on a sub-system bus, distributed throughout the aircraft) or between LRMs (on a backplane bus, within a cabinet). The platform is designed to provide a robustly partitioned communication service to hosted applications, even in the event of a single, arbitrary software or hardware fault within any of the applications or the communication network itself.

The platform allows for the assembly of an application-specific, fault-tolerant network from a set of standard, configurable hardware boards (top-level, combined HW/SW modules of the platform) linked using a partitioned fault-tolerant digital communication network as shown in Figure D-2.

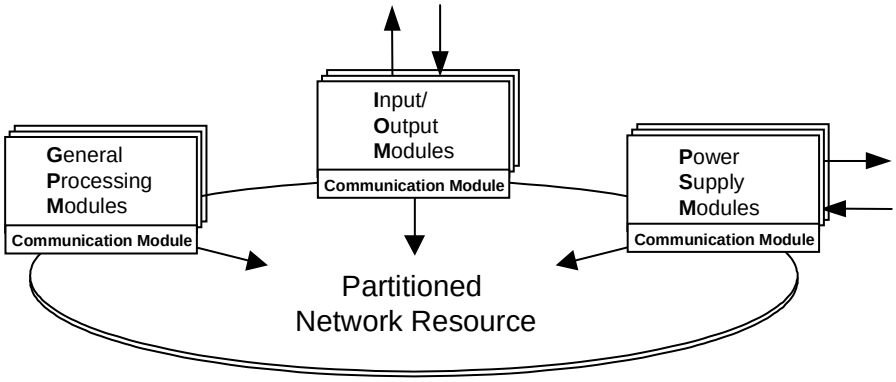

FIGURE D-2 : DISTRIBUTED MODULAR PLATFORM

D.2.2 Definition of platform and modules

The platform in this example consists of three standard hardware boards (see Figure D-2), each designed to provide a defined set of functions when assembled in accordance with the modular system architecture:

- The General Processing Module (GPM).
- The Power Supply Module (PSM).
- The I/O Module (IOM).

Each of these boards could be instances of a Single LRU platform as discussed in Example 1.

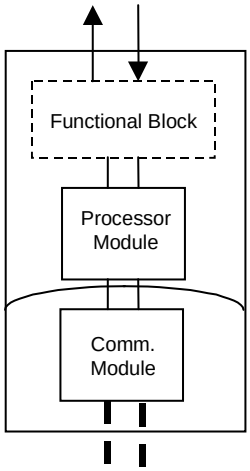

FIGURE D-3 : COMMON MODULE STRUCTURE

In this example, all boards share a common structure (see Figure D-3), containing:

- a Processor Module (potentially partitioned as described in Example 1).
- a Communications Module (robust partitioning of communication resource).
- a functional block (application-specific to each of the hardware board).

The platform also uses *core software components*, which provide a uniform API to applications:

- a real-time operating system module (potentially partitioned as in Example 1).
- a fault management.
- a health-monitoring component.

Using this general platform, one or several applications can be integrated, using multiple instances of the basic modules interfacing with the core software components as required. This architecture and its modules is highly composable: Applications based on this platform can be developed independently of each other according to strict interface definitions supported by the partitioning mechanism. The resulting integration effort is usually minimal.

D.2.3 Key characteristics of IMA found in this system

Sharing of resources, Robust Partitioning:

The distributed platform is designed to provide robust partitioning at the communication level. It is based on a synchronous, redundant data bus to establish this property. Access to the communication channels is enabled by a dedicated communication module, which autonomously executes a static communication schedule. The proper operation of these modules is further monitored by independent guardian units deployed in the network. These units only grant a module access to the shared communication resources at their assigned times. A partitioning analysis using formal correctness proofs, as well as validation and verification by testing shows, that arbitrary node failures can be tolerated with such an architecture: The distributed platform will isolate a single fault in any hosted application (hardware or software fault) and prevent any interference with the configured (hard real-time) communication activities of another application.

Hosting of multiple applications, Re-qualification impact:

Since the partitioning requirements of the distributed platform have been developed to meet Level A (ED-12/DO-178 (Ref. [2])), multiple applications of varying levels of criticality can be implemented independently and integrated on the platform. A time-triggered communication module supports a precisely defined interface in the time as well as in the value domain for all communication on the network. This interface can be frozen early in the design. Subsequently individual applications can then be implemented according to this interface specification. Interactions with other applications can be simulated based on precisely the same interface specification that will be used in the final system. Integration will thus not change the interface properties in terms of timing and values of the platform, when another application is integrated on the platform. The verified service of previously integrated applications should, therefore, not suffer any impact by the integration or modification of an additional application on the platform.

API between platform and applications:

The applications are provided with a simple, configurable, state message based API to with well-defined and verifiable timing and value properties to the fault management and health management components of the platform.

Platform configuration data:

The platform is configured with configuration tables for the operating system component, the communication module, the fault management and health management component.

Fault Management, Health monitoring:

While communication faults are dealt with by the robust partitioning mechanisms, node failures can be masked by active replication of applications on redundant hardware modules. The communication module of the platform provides a redundant, deterministic message transmission service. Built on this basic service, redundant modules may be integrated on the platform. Applications are relieved from fault management by a core software component available for this purpose. It also reports health information about hardware modules and application components hosted by them.

D.3 EXAMPLE 3: IDENTIFYING BOUNDS OF A DISTRIBUTED COMPLEX IMA SYSTEM

D.3.1 Purpose of this example

This example identifies boundaries of a distributed complex IMA system and presents considerations for fault management and reporting. Figure D-4 provides an example of a distributed complex modular avionics system.

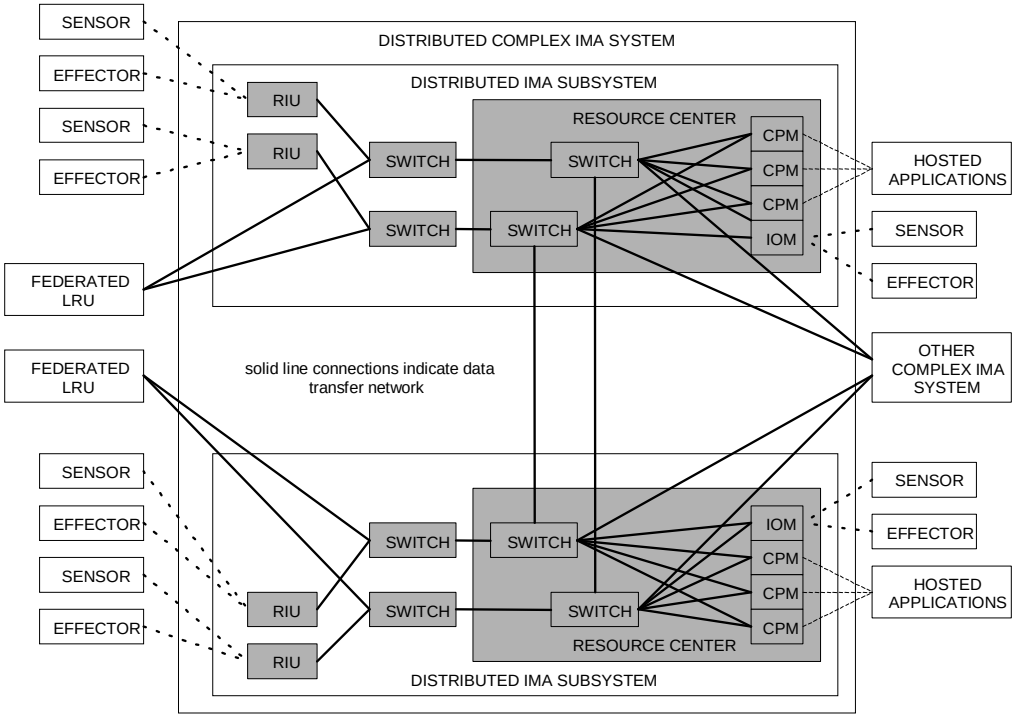

FIGURE D-4 : DISTRIBUTED COMPLEX IMA SYSTEM

D.3.2 Definition of platform and modules

The main architectural elements of the system are the computing resources, data transfer network, and remote I/O Units. The network consists of the network switches located both remotely in the aircraft and at resource centers, the end node interfaces, and the underlying transport protocol. The RIU (Remote I/O Unit) and IOM (I/O Module) are similar devices where one is located remotely and the other at the resource center. Each of these modules could be instances of single LRU platforms as discussed in Example 1. As a point of clarity, Figure D-4 does not imply a specific implementation of functional interface. There are a number of ways aircraft systems can use the distributed, complex MA system resources. The actual methodology of resource utilization for a particular aircraft system or function will be dependent on the requirements of that system or function.

D.3.3 Key characteristics of IMA found in this system

Fault Management, Health monitoring

One element of significant interest is flight deck effects in the presence of failures within the distributed, complex MA system. The situation can be decomposed into a condition where a cascading set of failures are reported by the distributed, complex MA system, multiple applications hosted on the CPM, and possibly by other distributed, complex MA systems or federated systems. As one begins to look at issues such as this, it becomes necessary to look at a hierarchy for information that is reported to the flight deck and or logged for maintenance action.

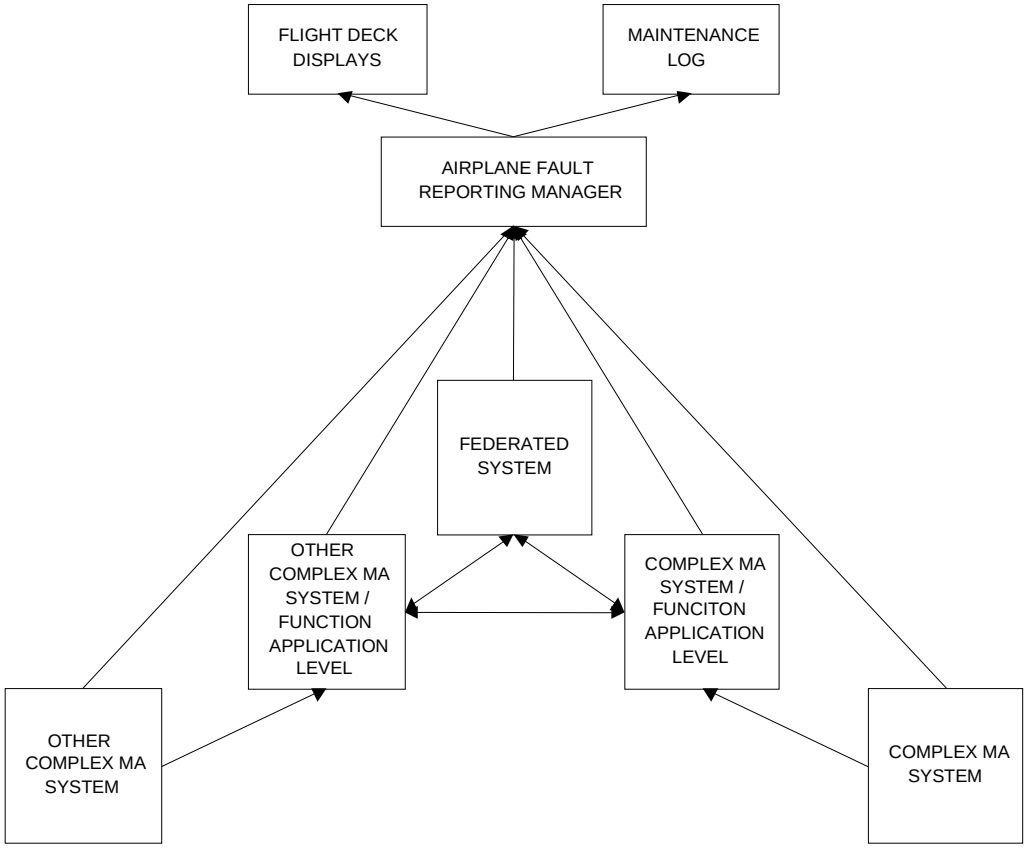

FIGURE D-5 : FAULT REPORTING HIERARCHY

Figure D-5 is presented to show a possible hierarchy of fault reporting and management. The intention of this figure is to illustrate the following.

- There are complex interactions between MA systems, aircraft system functions and MA hosted applications and federated systems that in time of failure will result in multiple failure indications. Left unchecked this will produce an increase in workload for the flight crew and confusion for maintenance personnel.
- There is a need to provide functionality that correctly determines the messages, alerts and affects that appear on the flight deck and the messages that appear in maintenance logs.
- The aircraft-level fault reporting functionality is not part of a particular complex MA System.

D.4 EXAMPLE 4: SOFTWARE DESIGNED RADIO EXAMPLE

D.4.1 Purpose of this example

This example illustrates a software designed radio (SDR) platform architecture. Radios include 8.33 kHz and Mode S transponders, for example. It is expected that different companies in different time frames will develop these platforms and the applications implementing these radios.

This SDR platform concurrently supports many different radios within broad frequency bounds from a large available collection of radio applications. A detailed specification is developed to accommodate re-hosting of applications that has the flexibility to satisfy special requirements of radio functions.

This example illustrates two levels of robust partitioning; reconfiguration using applications stored in memory, use of high performance interfaces to satisfy specific demanding interface requirements, and architecturally compatible interfaces for less demanding requirements.

D.4.2 Definition of platform and modules

The architecture consists of an intra-platform logical bus and several channel modules, as shown in Figure D-6. This intra-platform bus includes physical and logical interfaces to the channels, core processing and memory, system health monitor, and system configuration data. A general-purpose data communications module accommodates application rehosting[11]; a high performance data communications interface is provided for those instances where the general-purpose module is inadequate, i.e., tight real-time control is needed.

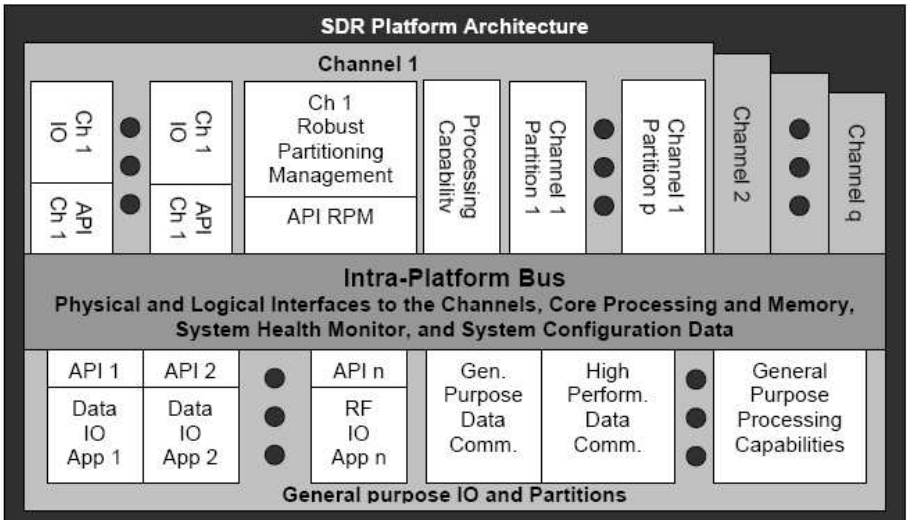

FIGURE D-6 : SDR IMA PLATFORM ARCHITECTURE

Common modules and applications, with their corresponding APIs, are included in the basic platform and are accepted with the platform. These may include Ethernet or ARINC 429, RF signal interfaces, and audio frequency interfaces.

A platform has several channel modules that are robustly partitioned from one another. A channel module conceptually supports a single radio function, but this is not a requirement. A channel includes modules that provide data and radio frequency I/O applications and APIs, multiple general purpose processing capabilities, and a robust partition monitor that monitors the applications, APIs, and general purpose processing partitioning.

[11] The common object request broker architecture (CORBA) may be used as an approach

D.4.3 Key characteristics of IMA found in this system

Robust partitioning – Into Channels

The partitioning into channels simplifies implementation of multiple radio functions. The allocation of a radio function on the platform is independent of the channel assignment because each of the channels has the same resource requirements. The architecture specifies robust partitioning of the channel resources.

In every case, channel operation and control is through the intra-platform bus. There is no specification that only one radio is accommodated on a channel at one time, but this is recognized as the conceptual norm. Channel sharing is possible and some radios may require more than one channel.

Robust partitioning – Within a Channel

A channel is separated into partitions. The separate partitions in a channel module allow parts of the radio transmit or receive processing to be performed totally isolated from one another. The military, for example, may apply this feature for classified and unclassified data separation. Multiple I/O modules support multiple RF and data ports for reception, transmission, data, and control.

Reconfiguration Using Applications Stored In Memory

A collection of available radio applications may be stored in memory with the general purpose processing capability. These stored radios applications may be made operational by providing the needed channel space, loading the radio application from memory into the partition, updating the system configuration, and activating the radio.

Data Communication – High Performance And General-Purpose Interfaces.

The general-purpose data communications interface is used whenever possible to increase application re-hostability. The high performance interfaces are used when the general-purpose interface cannot satisfy the performance requirements of the radio.

LIST OF WORKING GROUP 60 MEMBERS

Chairman	EVELEENS	Rene	NLR
Secretary	BROWN	David	AIRBUS UK
	ANDERS	Peter	AIRBUS Deutschland GmbH
	BAKER	Kirk	FAA
	BARANES	Sophie	DGAC/SFACT
	BARBAGELATA	Serge	EUROCOPTER
	BAUER	Brigitte	THALES AVIONICS
	BENICH	Chris	HONEYWELL
	BERTHON	Guy Andre	THALES AVIONICS
	BIRKEDAHL	Byron	HONEYWELL
	BLUMENSTEIN	Dieter	DIEHL AEROSPACE GmbH
	BREUNIG	Jeff	ICF Consulting
	BRODEGARD	William	Ryan International Corporation
	BROWN	John	ROLLS-ROYCE
	BYRUM	Jim	CESSNA
	CANOVI	Len	HONEYWELL
	CARETTE	Philippe	LABINAL
	CHELINI	James	VEROCEL
	CONMY	Philippa	UNIVERSITY OF YORK
	CROKER	John	DCS Corporation
	CROSS	Joe	RAYHTEON
	DENZEL	Paul	BOEING
	DEVARASETTY	Krishna	GOODRICH AVIONICS SYSTEMS Inc
	DEWALT	Mike	CERTIFICATION SERVICES Inc
	DODDS	Graham	AIRBUS UK
	DONOVAN	Colleen	FAA
	DOPPELBAUER	Kurt	TTTECH
	DRISCOLL	Kevin	HONEYWELL
	DUFF-COLE	Chris	CAA/SRG
	EARL	Malcolm	BAE SYSTEMS
	FERRELL	Tom	FAA Consulting
	FERRELL	Uma	FAA Consulting
	GALLAWAY	Glen	FAA
	GAYRAUD	Pierre	THALES AVIONICS
	GUY	John	NATS
	HAYHURST	Kelly	NASA
	HILL	David	HONEYWELL
	HOLLINGER	Kent	MITRE
	HOLLOWAY	Michael	NASA
	HORTON	Olly	BAE SYSTEMS
	HUTCHESSON	Stuart	ROLLS-ROYCE
	JACKSON	Robert	RAYHTEON
	JANSSON	Leif	SAAB AVIONICS
	JESKE	Rolf	AIRBUS
	KALMBACH	Joern	AIRBUS Deutschland GmbH
	KILGORE	Charles	FAA
	KRODEL	Jim	PW
	KROHN	Patrick	UNIVERSAL AVIONICS SYSTEMS CORPORATION
	LEE	Douglas	TRANSPORT CANADA
	LEWIS	John	FAA

LIVACK	Gary	FAA
MAIER	Reinhard	TTTECH
MANGAN	Joseph	COANDA AEROSPACE
MAZUK	Dan	ROCKWELL COLLINS
MCCLAIN	Tom	AFFSA/XRC
McGOOKEY	Jeff	SMITHS AEROSPACE
MINER	Paul	NASA
NAROTAM	Matt	BOEING
NEWTON	Ian	BAE SYSTEMS
NICHOLSON	Mark	UNIVERSITY OF YORK
NICKUM	Jim	MITRE
NORDSIECK	Arnold	BOEING Commercial Aiplane Co.
NORRIS	John	ELDEC Corporation
OVENS	Norm	ROCKWELL COLLINS
PARKER	Ted	HONEYWELL
PARKINSON	Paul	WINDRIVER
PENNY	John	CAA/SRG
PERI	Robin	SMITHS AEROSPACE
PERRY	Robin	SMITHS AEROSPACE
PIVETTA	Enrico	DIEHL AEROSPACE GmbH
PRIZASNUK	Paul	ARINC AEEC
PRUIETT	Jay	SMITHS AEROSPACE
PURWANTORO	Yudi	UNIVERSITY OF YORK
REEVE	Tammy M.	PATMOS ENGINEERING SERVICES
RETKO	Eric	SMITHS AEROSPACE
RIERSON	Leanna	FAA
ROBINSON	Dave	FAA
RUANA	Rudy	RTCA, Inc.
RUSHBY	John	SRI INTERNATIONAL
RYBECKY	Jiri	AIRBUS CONSULTANT
SCHROEDER	Brian	CESSNA
SCHWARZ	Martin	TTTECH
SEVERSON	Michael	BELL HELICOPTER
SHIMIN	Gu	CARERI
SHOEN	Dave	BOEING
SINGLETON	Joe	FAA
SKAVES	Peter	FAA
SMITH	Bernald	SOARING SOCIETY OF AMERICA
SPITZER	Cary	AVIONICON
STRUCK	Will	FAA
TAFRESHI	Mohammad	BOEING
TAHIR	Abdul	ADVISO INC
TAMBURRO	Giuliana	ENTE NAZIONALE PER L'AVIAZIONE CIVILE (ENAC)
THEDFORD	William	HASCOM AFB
TROMEUR	Daniel	DGA/CEAT
WADE	Matt	FAA
WALLEN	Dave	FAA
WALLINGTON	Andy	SMITHS AEROSPACE
WEALE	Denis	SMITHS AEROSPACE
WHISTON	Paul	HIGH INTEGRITY SOLUTIONS LTD
WORCESTER	Tom	HONEYWELL