RTCA有限公司
1828 L St. NW., Suite 805
华盛顿 DC 20036

综合模块化航空电子系统(IMA)
开发指南与认证考虑

RTCA DO-297
2005 年11月8日

由SC-200编制

本文件的拷贝可以从下面地址获得

RTCA, Incorporated
1828 L St. NW., Suite 805
Washington, DC 20036

电话: 202-833-9339
传真: 202-833-9434
网址: www.rtca.org

要获得价格和订购信息请和RTCA公司联系

译者序

综合模块化航空电子系统（IMA），在开发、验证和认证等过程中与联合式的航空电子系统有很大的区别，特别是IMA系统的综合过程，需要有更多的参与者更细的阶段划分。于是RTCA的特别委员会SC-200于2005年发布了RTCA/DO-297《综合模块化航空电子系统(IMA)开发指南和认证考虑》，对IMA系统开发和认证过程的参与者进行了定义，对IMA系统综合阶段及其工作任务进行了规定。

在IMA系统的综合过程中，每个模块或组件都要以假设、限制和配置的形式加以约定，特别是IMA的系统综合工作。这就需要更清晰地确定参与者的角色和职责、各项活动的约定与目标，以及分级综合与增量认证的方法等。

在RTCA/DO-297发布之后，美国联邦航空管理局(FAA)组织研究了实时操作系统与组件在IMA系统中进行综合的有关问题，主要包括：

- 确定IMA系统在开发、验证、以及认可和批准过程中所需要的角色；
- 追溯支持取证的证据，包括有部分符合目标与全部符合目标；
- 定义、追溯和验证IMA系统模块与部件所需承担的全部义务或约定；
- 通过分级综合与增量认可方法，支持模块和部件的配置控制；
- 建立并验证严密的强分区和其它平台服务。

本译文的目的是在IMA系统的开发和认证过程中，帮助工业界和认证机构了解IMA系统开发和批准的活动和要求。

本译文由中国航空工业集团公司六三一所孔德岐研究员、中国航空工业集团公司三O一所黄永葵研究员和朱晓飞工程师翻译，由六三一所田莉蓉研究员和张学宏研究员校对。由于译者水平有限，译文中难免有错误之处，敬请斧正。

前　言

本文件由RTCA的特别委员会(SC-200)和EUROCAE的工作组60联合编制，并于2005年11月8日由RTCA的项目管理委员会(PMC)批准。

RTCA公司是一个非盈利的社团组织，它为了公众利益，推进航空和航空电子系统中的先进技术与科学。该组织作为联邦咨询委员会行使职责，并就当今航空界的有关议题建议寻求共识。RTCA的目标包括但不限于以下内容：

- 通过技术需求的方式，把航空系统的用户和供应商联系在一起，以使政府和工业界满足他们的共同目标和责任；
- 随着航空界不断追求安全性、系统能力和系统效率的提高，需要对航空界面临的系统技术问题进行分析并提出建议的解决方案；
- 针对相关技术的应用寻求共识，以实现用户和供应商的要求，包括开发能支持航空界的电子系统和设备的最低操作性能标准；
- 基于国际民航组织与国际通信联盟及其它适当国际组织的立场，帮助开发适当的技术资料。

组织的建议经常用作政府和私营机构决策的基础，也作为联邦航空局技术标准规定的基础。

由于RTCA不是美国政府的正式机构，其建议不能作为正式的政府政策声明，除非美国政府组织或对这些建议相关的事项有法令权限的机构给出明确的声明。

目 录

摘　要

综合模块化航空电子系统（IMA）使用的（范围）正在迅速扩大，且已应用在各类飞机中。基于这种快速增长（的情况）的认识，RTCA设立了特别委员会200（SC-200），同时EUROCAE建立了工作组60（WG-60），（两个组织）联合编制了一份用于指导IMA设计、开发和应用的文件。参与该文件编制的人员有政府、工业界和学术界的人士。

IMA 是一组灵活的、可重用的、可互操作的共享硬件和软件资源，当把这些资源综合在一起时，可以构建一个平台，该平台能提供各种服务来执行飞机功能的宿主应用，而这些服务按一组确定的安全和性能需求进行设计和验证。

本文件为 IMA 的开发者、综合者、（认证）申请人，以及在 IMA 系统的批准和持续适航中涉及到的人员提供指南。由于和传统的联合式系统不同，它还为 IMA 系统的（设计）保证提供指导。

本文件是基于 RTCA/EUROCAE 早期文件编制的，例如，RTCA DO-178/EUROCAE ED-12《机载系统和设备合格审定中的软件考虑》和 RTCA DO-254/EUROCAE ED-80《机载电子硬件的设计保证指南》。其它 RTCA 和 EUROCAE 文件，以及 SAE 和 ARINC 文件中的概念，也在本文件的编制过程中起到了指导作用。

第1章　简介

1.1　目的

本文件用于为IMA平台开发者、应用开发者、综合者、（认证）申请人以及在民机适航工程中IMA系统的批准和持续适航中所涉及到的人员提供指南。由于（IMA）不同于传统的联合式系统架构，对于参与开发和综合IMA模块、应用以及系统人员，本指南描述了目标、过程和活动，以使设计保证不断递增，直至IMA系统在已批准的航空产品上得到批准和安装。

本文档给出了IMA系统的概念，包括平台和模块、以及它们与宿主应用的关系，和与装在飞机上使用的航电功能的关系。这包括描述开发者与综合者如何能够进行模块、平台和应用综合的增量认可，它为申请人提供了一种使批准安装在航空产品上的IMA系统达到设计保证的方法。

在IMA系统开发期间，型号取证（TC）或补充型号取证（STC）项目的认证申请人要在模块和平台的开发者与系统综合者之间建立一种有效的沟通系统。当这些供应商来自不同的公司时，这种沟通系统就特别重要。否则在最后综合时以及在IMA系统安装批准时的实施过程中就会产生误解。

在认证过程中，IMA系统增量认可确定了六项任务：

－任务1: 模块认可；

－任务2: 应用软件或硬件认可；

－任务3: IMA系统认可；

－任务4: IMA系统的飞机综合-包括验证和确认 (V&V)；

－任务5: 模块或应用的更改；

－任务6: 模块或应用的重用。

IMA系统的安装批准可以基于累积式的增量认可（方式），最终完整的设计保证要证实所安装的系统和功能要与适用的规章和指南一致。

如果增量认可适用的话，可以通过认可信件的形式获取批准（承认），且要标记型号的数据，对于特殊项目可采用其它方式。

1.2 范围

本文件适用于IMA系统开发、综合、验证和确认的各方参与者，本文件中的指导重点

是有关IMA特有方面的设计保证。因此，它也依赖于其它公认的文件，这些文件对整个飞机的认证、系统开发、软件保证和硬件保证能够提供更多的指导。

就像本文之前所定义的那样，IMA是一组灵活的、可重用的、可互操作的共享硬件和软件资源，当把这些资源综合在一起时可以构建一个平台，该平台能提供各种服务来执行飞机功能的宿主应用，而这些服务是按一组确定的安全和性能需求进行设计和验证。关键的IMA和认证术语在2.2节和术语表中描述。

在第1.5节中给出了工业界公认的有关IMA组件满足适航要求的主要指南。获得IMA平台（包括核心软件）和宿主应用的单项增量认可的能力可以减少后续的认证工作量，而不会损失系统的安全性。

本文件只描述那些与平台综合有关的应用属性，既不涉及特定的应用功能，也不涉及特定的技术标准规定（TSO）/欧洲技术标准规定（ETSO）的要求、最低操作性能规范（MOPS）或最低航空系统性能规范（MASPS）。

1.3 背景

软件和微电子技术的发展为飞机带来了新的功能、新的能力，同时也增加了复杂程度。要执行这些复杂功能需要使用高性能的计算平台，这种计算平台能够在单个处理器上或分布式网络处理器上宿主多个应用。

由电子系统实现的飞机功能正在不断地增加，IMA是一种能够适应这种功能增加并且能减少每架飞机上设备数量的方法。另外还具有减少飞机系统和设备重量与体积的优势。

IMA平台应该能提供健壮分区隔离和其它保护措施，这些措施允许多个应用共享一个平台以及平台上的资源，还支持飞机功能在某一容错网络上分布。IMA平台可以由系统综合者或者由第三方供应商提供。同样，IMA的应用也可以由平台供应商或者第三方供应商提供。

经济因素是实现IMA概念的主要动力，这些因素包括要求提供费效性（好的）升级途径、引入了新的操作能力（例如，CNS/ATM功能）、快速有效的维护以及避免采用不成熟的（技术和器件）带来的过时问题等。根据这一背景情况，本文将描述一组用于开发和认证IMA系统的过程和指南。

1.4 与其它文件的关系

除了适航规章和要求外，软件、航空电子系统、复杂电子系统和安全性方面的各种国家和国际标准都是可用的。在有些团体机构中，要求符合这些标准。但对特定的国家标准或国际标准的引用，或者建议以某种方式使这些标准作为本标准的替代或补充，都不属于本文档件的范围。

在本文中凡使用“标准”一词的地方，都应理解为飞机系统、设备和发动机上项目使

用的特定标准。这样的标准可以从申请人所采用或产生的用于认证活动的通用标准派生出来。

1.5 参考资料

使用下列文件的最新版本：

[1] RTCA DO-160 / EUROCAE ED-14 机载设备的环境条件和测试程序；

[2] RTCA DO-178 / EUROCAE ED-12 机载系统和设备认证中的软件考虑；

[3] RTCA DO-200 / EUROCAE ED-76 航空数据处理标准；

[4] RTCA DO-201 / EUROCAE ED-77 航空信息的工业要求；

[5] RTCA DO-248 / EUROCAE ED-94 说明DO-178B的最终报告；

[6] RTCA DO-254 / EUROCAE ED-80 机载电子硬件的设计保证指南；

[7] SAE ARP4754 / EUROCAE ED-79 高度综合或复杂飞机系统的认证考虑；

[8] SAE ARP4761 民用机载系统和设备进行安全性评估过程的指南和方法；

[9] FAA AC 20-148 可重用的软件组件；

[10] FAA TSO-C153 IMA的硬件部件；

[11] FAA Order 8110.49 软件批准指南；

[12] ARINC 615A 软件数据加载；

[13] ARINC 653 航空电子系统应用软件标准接口；

[14] ARINC 664 飞机数据网络。

注意：当引用FAA咨询通告时，是期望他们作为资料，为认证申请人提供要考虑的主题和范围。所有的要求都要与认证申请人当地的认证机构协调。

1.6 如何使用本文件

本文件预期的适用对象是国际航空界。为了有助于本文档的使用，应尽可能少地引用特定的国内规章和程序，而使用通用的术语来替代。例如“认证机构” 一词是指代表国家负责飞机和/或发动机批准的组织或个人。在有第二个国家或一组国家确认或参与这种认证的情况下，本文件可以用于对双边协议的承认，或在多个国家中作为谅解备忘录。

本文件承认这里的指南内容不是法律所强制的，而是航空界所达成的共识。因此，要避免使用“应（shall）”一词。而在本文件中使用“应该（should）”一词来表达要求的方式 ，但要认识到，在这里对这些描述（表述）使用替代的方法是可以接受的。

本文件采用结构化的方法向读者介绍IMA，并着重强调那些影响开发、认可，以及IMA系统在飞机上安装批准的IMA属性。

本文件由下列章节构成：

－第1章，文件概述；

－第2章，IMA概念介绍，着重强调系统、硬件和软件的特性；

－第3章，描述IMA的特有的开发与综合指南；

－第4章，对IMA的认可提供指南，并描述它们与批准所安装IMA系统的关系；

－第5章，描述IMA开发的完整过程；

－第6章，提供IMA系统持续适航指南。

图1 描述了这些章节之间的关系。

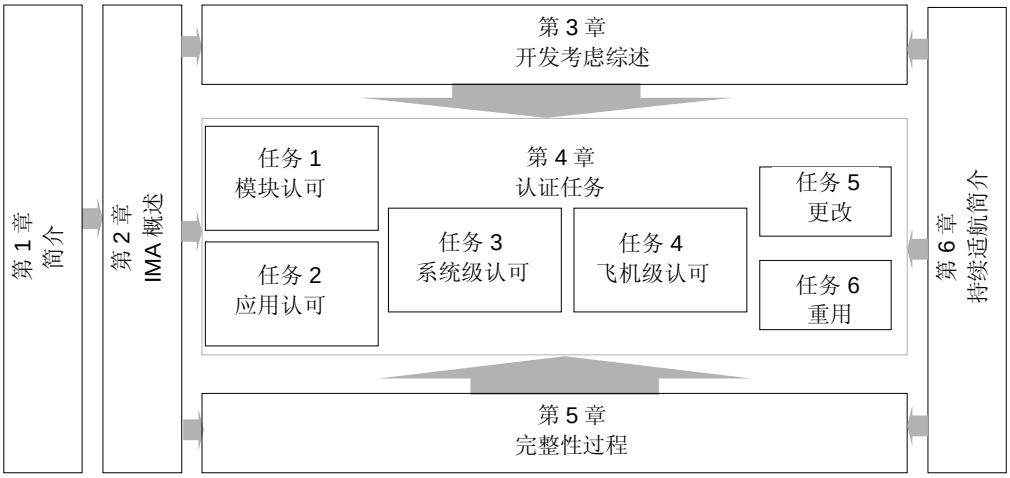


图1　各章及其之间的关系

本文件包含了以下附录：

－附录A 总结了需要满足的目标，以证明能符合本文件的要求。通过对第3章和第4章中所描述任务的总结，以表格形式列出应达到的目标。

－附录B 术语表。注意，有些术语在本文件中有特殊的含义；

－附录C 本文件中所用到的符号与缩写词；

－附录D 给出了一个IMA的例子。

注意：附录A到附录C认为是规范性内容，附录D只是资料性内容。

第2章　综合模块化航空电子系统概述

本章对IMA系统进行描述，介绍用于IMA的术语并描述了这些术语之间的关系，为了使读者了解的IMA概念介绍了一些关键特性。

2.1　IMA设计与认证的术语

要了解本文件需要描述以下在设计、认证和IMA方面的术语，对于有些情况，这些术语的详细描述在术语表中的进行，并且与传统的航空（设备）设计和指南材料相比，在使用风格上略有差异。

2.1.1　IMA的设计术语

下列术语用于描述IMA系统，这些术语与附录B中所定义的是等同的，此处对这些术语的解释进行了扩充以便将它们用于IMA设计时更易于理解。

飞机功能（Aircraft Function）——由飞机上系统的硬件和软件提供给飞机的能力。这些功能有飞行控制、自动驾驶仪、刹车、燃油管理、飞行仪表等。为了能包括飞机的任何功能，IMA可能会扩展航空电子系统的定义。

应用（Application）——软件和/或定义有一组接口的专用硬件，当（这些软硬件）与某个平台综合后能执行一种功能。

组件（Component）——一个自身含有硬件部件、软件、数据库，或其组合（的构件），且受配置管理的控制。组件本身不能提供飞机功能。

核心软件（Core Software）——管理（平台）资源的操作系统和支持软件，以提供一种环境，在这种环境中能够执行应用。核心软件是平台必需的组件，通常由一个或多个模块组成。

IMA系统（IMA System）——由IMA平台和一组规定的宿主应用组成。

可互操作的（Interoperable）——几个综合在一块的模块一起运行来完成某个规定目标或功能的能力。这要求在模块之间定义接口边界，并允许使用其它可互操作的组件。为了在物理方面描述这一概念，IMA平台可以包括可互操作的模块和组件，如物理器件（处理器、存储器、电源、输入输出（I/O）器件），逻辑元件（如操作系统）和通信软件。

模块（Module）——一个组件或一组组件，这些组件可在它们内部或IMA环境中被接纳。一个模块也可以包括其它模块。一个模块可以是软件、硬件或软件和硬件的组合，这些软硬件能为IMA的宿主应用提供资源。模块可以分布于整个飞机或集中放在一起。

分区（Partitioning）——一种结构化的技术，它为功能或应用提供必要的隔离和独立

性，以保证只发生预期的耦合。这种在IMA平台中提供保护的机制是专门对需要有完整性等级（的情况）设立的。

平台（Platform）——一个模块或一组模块，包括核心软件，这种核心软件能足以支持至少一个应用的方式来管理资源。IMA的硬件资源与核心软件是这样设计和管理的，它能为至少一个宿主应用提供计算、通信和接口的能力。平台本身并不提供任何的飞机功能。平台只是建立了一个计算环境，能够支持服务，并提供与平台相关的能力，如健康监控和故障管理。IMA平台可以独立于宿主应用被认可。

资源（Resource） ——由IMA平台或应用使用的任何对象（如处理器、存储器、软件、数据等）或组件。资源可以由多个应用共享也可以由特定的应用专用，它可以是物理的（一个硬件设备），也可以是逻辑的（一段信息）。

可重用的（Reusable）——先前认可模块和应用的设计保证数据可以用于后续飞机系统的设计，能够减少所需要的重复设计或新增认可过程。

图2 给出了这些术语之间的关系。

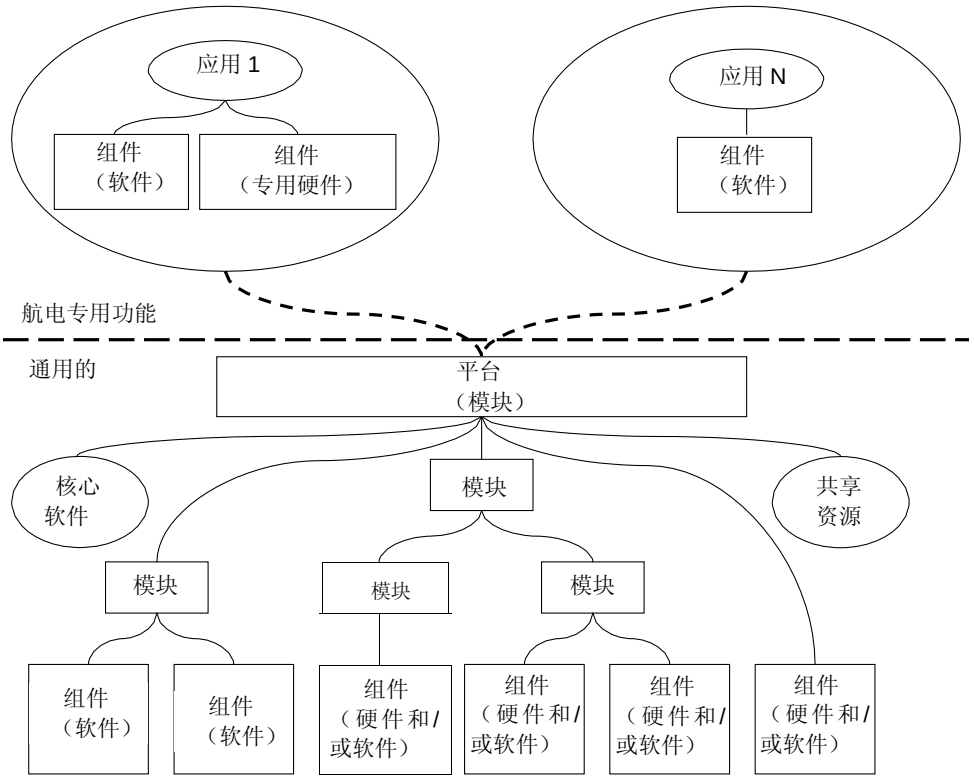


图2　IMA设计术语的关系

2.1.2 认证术语

本文件的主要目的是为IMA系统进行认可、批准以及IMA系统在飞机上的安装认证，提供一种符合性方法。为了达到这一目的，了解认证术语非常重要。以下列出了与IMA有关的主要认证术语：

***认证*（*Certification*）——**由认证机构对某一产品、服务、组织或个人就符合要求的情况给出的正式（法律）承认。这种认证包括对产品、服务、组织或个人进行的技术检查活动，并通过颁发国家法律或程序所要求的证书、许可证、批文或其它文件，正式地承认其符合适用的要求。具体来说，产品的认证包括：

a. 认证申请人评估产品设计的过程，并向认证机构证明产品符合适用的规章以及该型产品所适用的一组标准，以证明（产品达到了）可接受的安全级别；
b. 为确保产品符合批准的型号设计所进行的产品评估过程；
c. 认证机构寻找符合性证据的过程，并依照国家法律要求颁布证书，以声明所发现的一致性和/或符合性（的材料）与上述a或b两条的标准是一致的。

***技术标准规定授权*（*TSO Authorization*）——**由认证机构对系统、设备或部件满足TSO的要求以及设备适用的最低规范给出的合法承认。该术语等同于欧洲TSO (ETSO)管理机构。

***认可*（*Acceptance*）——**认证机构对模块、应用或系统符合其规定要求的承认。认可就是由认证机构对所提交的数据、证据或等价声明满足适用的指南或要求，给出的正式承认（通常以信件或盖章的数据单等形式）。认可的目的是对认证项目未来的使用提供信任。

***批准*（*Approval*）——** 对符合规章给出正式或官方承认的行为或过程。对于IMA这种情况通常有两种批准形式：

a. 由认证机构对所提交的生命周期数据给出的批准（通常通过在数据资料上盖章和签字或用信件来进行证明）；
b. 通过发布飞机或发动机型号认证和/或适航认证来批准安装。

***增量认可*（*Incremental acceptance*）——**获得信任的一种过程，这一过程要通过认可或证实IMA模块、应用和/或未安装在飞机上IMA系统符合特定要求来进行批准或认证。增量认可过程有几项工作任务，通过获得单独任务的信任，最终实现整个系统认证的目标。增量认可能在IMA系统中提供综合与接纳新应用和/或新模块的能力，并能维持现有的应用和/或模块，而不需要重新认可。

2.2 结构考虑

IMA系统是由一个或多个平台组成的，并包括有能连接飞机其它系统和用户（如，飞行机组、维护人员等）的接口。飞机功能的分配应纳入IMA系统架构中来考虑，以确保能都满足适用的可用性、完整性和安全性的要求。下满列出一些主要的考虑内容：

a. 可用性考虑
   - 功能性能——将宿主于飞机上的功能（见3.2节）分配到IMA系统架构上；
   - 资源管理——分配IMA平台的资源，控制共享资源和专用资源，保护由多个宿主的飞机功能或应用（见3.5节）所用的IMA平台资源。
   - 可靠性和维护性——对主要最少设备清单（MMEL）、飞机的派遣率、维修、替换，以及为确保持续适航性（见3.9节）进行便于维护活动等的有影响方面。
   - 健康监控——对系统状态以及操作运行与维护的重点进行监控。

b. 完整性考虑
   - 设计保证、IMA安全性和保护特性、故障探测和分区——保护宿主功能和应用的能力，当使用共享资源时确保独立性并防止受到非预期的影响（见3.5节）。

c. 安全性考虑
   - 安全性评估确保适当的架构、设计保证、失效保护、解决共模和飞机功能组合失效的影响，以及适航性（见5.1节）。

d. 故障管理、故障报告与恢复活动——进行故障、失效和异常行为的检测与识别，并提供适当的响应（见3.6节）。

e. 组合性考虑
   - 在综合新的应用时，对于已经综合过的应用，如果不会使任何已验证过的需求失效，则IMA平台就是可组合的。

   - 在可组合的架构中，系统需求来自于分配给IMA应用的需求，有良好接口边界定义的IMA平台可以与已综合过应用的部分认可对应地组合在一起，健壮分区隔离是迈向这一目标的第一步（见3.5.1节）。

2.3 关键特性

IMA平台与宿主应用的关键特性影响IMA系统架构、详细系统设计，并最终影响IMA平台与系统的认可过程。第2.3.1节到2.3.5节总结了影响认证过程的IMA平台的特性。

2.3.1 平台与宿主应用

IMA系统的两个主要构件块就是平台与宿主应用。IMA平台的关键特性见表1。IMA宿主应用的关键特性见表2。

表1　IMA平台的关键特性

IMA平台的关键特性	描　述
平台资源可由多个应用共享	综合就意味着要共享资源。通过利用分区和平台提供的其它保护能力（如，HIRF/IEL、供电、BIT）等，IMA平台能够宿主多个应用。
IMA平台能提供共享资源的健壮分区隔离	当需要时，这一特性能确保宿主应用获得共享的平台资源，且这些资源是受到保护的，在应用使用它们时能避免产生任何异常行为。IMA平台的资源管理确保只有已规定的、有预期用途、交互和接口等资源可由平台和应用共享。 健壮分区隔离将确保任意的宿主应用或功能不会受到其它宿主应用或功能的非预期影响。
IMA平台只允许宿主应用通过规定的接口与平台同其它的应用进行相互联系	IMA平台是一个通用的计算平台，能够宿主一个或多个飞机功能或应用。因此，平台的行为可以由独立的专用应用来验证（例如，可以用满足其模块需求规范来证明）。IMA平台可以认为是IMA系统中一个单独认可的组件。 对于隔离平台和宿主应用之间的变化来说，这一特性是必须的。其目的是使IMA平台的修改对宿主应用带来的影响最小，以及应用的更改对平台的影响也最小。 该平台提供已文档化的（且已验证的）应用程序接口（API），以允许各应用能够访问平台的服务和资源。
共享的IMA平台资源是可配置的	为了支持宿主应用对资源的需求，IMA平台的资源要可配置。

表2　IMA宿主应用的关键特性

应用的关键特性	描　述
一个应用的设计可以独立于其它应用，并在IMA平台上能独立于其它应用获得增量认可	宿主应用可以在平台上单独验证，而不需要与全套的预期应用在一起进行。对每个宿主应用的增量认可能够用来支持信任积累，以达到IMA在系统飞机上安装的批准
各种应用可以综合到一个平台上，而不会受到其它宿主应用的非预期影响	随着不同应用的完成和单独的验证，它们作为一套完整的宿主应用，应该在平台上进行综合。应用之间的交互关系也应得到验证。
应用可以是重用的	应用的模块化和移植性能够且方便地用于不同的项目和产品。
应用是可独立修改的	每个应用的可修改，对其它应用和平台资源与模块的影响要非常小或没有影响。任何的影响都应得到识别并要与受影响的组件进行协调。

2.3.2　共享资源

IMA系统可以宿主几个在一起共享资源的应用。例如，可以通过访问时间的方式来共享资源。这种情况适用于处理资源和硬件。每一种共享的资源都可能造成单点失效，这种失效能够影响所有应用使用该资源。因此，要采用由系统安全性评估过程所确定的适当缓解技术。

处理资源是指可能包含有CPU、储存器和相关接口的物理单元。储存器能够存储机器可读的计算机程序和相关数据。IMA宿主应用使用IMA平台提供的共享资源（例如，I/O设

备、数据总线、共享存储器等）来进行通信。某一资源或部分资源可以按照时间单位来分配（例如，处理器的周期或通信带宽）。

IMA平台能对共享资源提供资源管理的能力，还能提供健康监控和故障管理的能力，以支持共享资源的保护。IMA系统可以有多个共享的供电电源。

2.3.3 健壮分区隔离

健壮分区隔离是一种保证各独立飞机功能和应用达到隔离目的的措施，这种功能和应用宿主在IMA的共享资源上，在出现设计错误和硬件故障时，问题能够对应到唯一的分区或与应用相关的硬件上。如果某一（不同的）失效能够导致健壮分区隔离特性丧失，那么这种失效应该是可探测到的，并应采取适当的措施（予以处理）。健壮分区隔离的目的就是提供与联合式等级相同的功能隔离和保护，如果不是指物理隔离的话。这就意味着健壮分区隔离应支持在宿主处理器上共存的核心软件与应用软件相互协同，并使用共享的资源，且要确保避免产生未授权或非预期的交互。健壮分区隔离应满足DO-248/ED-94 (参考资料[5], 第4.1.4.5节)中的下列指南要求:

- 某一软件分区不允许破坏其它分区的代码、I/O或数据储存区；
- 某一软件分区只允许在分配给它的时间段中使用共享资源；
- 某一软件分区只允许使用分配给它的共享I/O资源；
- 唯一对应到某一软件分区的硬件失效，不能对其它软件分区造成不利影响。

对于在所有出错情况下（包括硬件失效、软硬件设计错误或系统行为异常）使用共享资源的各种飞机功能和宿主应用，健壮分区隔离是一种确保实现预期隔离和独立的一种措施。

健壮分区隔离的目的是提供一种与联合式系统（即应用程序各自宿主在分离的LRU中）级别相同的功能隔离和独立性。这就意味着健壮分区隔离应支持使用共享资源的应用软件协同共存，且要确保能够探测到并能化解任何试图进行未授权或非预期的交互。

平台的健壮分区隔离保护机制独立于任何宿主的应用，即，应用不能改变由平台提供的分区保护措施。

2.3.4 应用程序接口(API)

API定义了平台和宿主应用之间的标准接口，且对应用之间的通信和使用I/O的能力提供实现手段。ARINC 653 (参考资料[13]) 的第1和第2部分对应用程序接口和相关服务提供了航电标准。ARINC 653的第3部分提供了证明符合ARINC 653的标准测试规范。

2.3.5 健康监控和故障管理

由于多个应用和共享资源综合在一起，健康监控和故障管理(HM/FM)功能应给予特别

的关注。IMA系统管理着平台的故障、硬件的失效、分区的冲突，以及宿主应用的错误和异常行为，包括共模故障和级联故障。用于管理平台故障的方法与宿主应用是独立的，故障管理由故障、失效和错误的探测、正确地识别（当发生时）以及适当的响应等方面组成。故障管理和故障报告的指南详见3.6节。

IMA平台为平台和宿主应用提供了健康监控和故障管理的能力。IMA系统必须要提供更高级别（飞机功能）的健康监控和故障管理能力，以支持可用性和完整性的要求。

2.4 利益相关方

角色和职责的分配是必要的，并且角色和职责应涉及IMA从概念设计到退役的整个系统生命周期范围。这些角色和职责的分配可基于基本的IMA系统架构，并应包括选择和提供工具的职责，这些角色和职责的指定应该在IMA系统的项目计划中描述，如IMA系统的认证计划，并要能支持低级计划。

对于装在飞机上IMA系统本节确定了一些典型数据，这些数据用来支持IMA系统的开发、批准和持续安全地运行。对于某些活动、数据的产生以及要证明符合性的责任，应尽早地在项目的各利益相关方中得到协调、沟通和解决。为了支持IMA模块和宿主应用的增量认可，需要积累数据。

尽管单一的团组或组织机构可以完成所述的所有活动(除认证机构负责的活动外) ,在此还是希望有多个组织参与。强烈鼓励认证申请人尽早地与认证机构协调它们的计划，并在IMA系统开发的整个过程中保持与认证机构的协调。

不管何处（产生）的失效或故障，要是影响了项目和飞机产品中使用的公共IMA组件，都要在适当的地方设置一个过程将所提供的信息（资料）传给所有使用公共组件的人员。这种信息沟通的过程不仅要对用户，还要对认证机构以及那些负责飞机产品持续安全运行的部门。对于如何记录所做出的决策、重新认证的途径，以及对于认证机构任何活动所达成的协议，都要有清晰和准确定义的沟通渠道与过程。

2.4.1 认证机构

认证机构是这样的组织，它代表国家负责批准飞机和/或发动机的认证。

2.4.2 认证申请人

认证申请人负责对符合适用的航空规章进行证实，并寻求进行型号认证(TC)、修改的型号认证(ATC)、补充的型号认证(STC)、或修改的补充型号认证(ASTC)。认证申请人负责产生和确认所有的飞机级需求，并将他们分配给子系统，负责提供所配置IMA系统的安装说明，负责将IMA系统与飞机的其它系统进行综合，且在适当时，负责将IMA系统安装到飞机上。对所安装的IMA系统和飞机，认证申请人最终负责确保符合适用的规章，且确保

它们具有适航性。

认证申请人要进行必要的开发活动，来定义所要实现的飞机级功能，并在系统安装到飞机上后，再进行必要的验证与确认(V&V)活动。认证申请人还要负责进行持续适航(见第6章)。

注意：认证申请人不需要在飞机上对IMA系统进行实际安装，但仍要对上述条目负责。

2.4.3 IMA的系统综合者

为了把平台和所宿主的应用综合起来形成IMA系统，IMA的系统综合者要进行必要的活动。在IMA系统综合过程中，需要产生的主要数据包括：

a. 系统配置，包括模块和宿主应用的数量、类型与特定版本；

b. 用于综合IMA系统的共享资源的分配和配置表；

c. IMA系统验证与确认（V&V）的结果，包括IMA系统的性能数据、与分配需求的一致性。

2.4.4 平台和模块的供应商

IMA平台和模块的供应商提供处理硬件和软件资源，包括核心软件。为了支持IMA平台和模块的使用，需要提供开发和配置工具，在平台和模块开发过程中，需要产生的主要数据包括：

a. IMA平台和模块的接口规范；

b. 共享资源分配与配置表的规范；

c. IMA平台所需的资源和配置数据，包括核心软件；

d. 模块和/或平台验证与确认（V&V）的结果，包括性能数据、与分配需求的一致性。

2.4.5 应用的供应商

应用的供应商负责开发所宿主的应用，并在IMA平台上对其验证。应用供应商应确保唯一分配给宿主应用的硬件或软件资源能满足完整性和可用性的要求，就像在飞机安全性评估所确定的那样，这些完整性和可用性需求要与失效状态一致。在应用开发中，要产生的主要数据包括：

a. 应用所需的外部接口规范；

b. 宿主应用所需的资源和配置数据；

c. 应用/平台综合验证与确认（V&V）的结果，包括性能数据、与分配需求的一致性。

2.4.6 维护组织

维护组织执行认证申请人获得批准的流程，以保持IMA系统和飞机在适航状态之中。在第6章中提供了有关持续适航的附加信息。

第3章　开发考虑综述

IMA 系统是基于 IMA 平台开发的，该平台包含的软硬件组件是公共的并能由宿主应用共享。图 3 给出了一种典型设计范例，它强调潜在共享资源，阴影区为可以共享的模块。

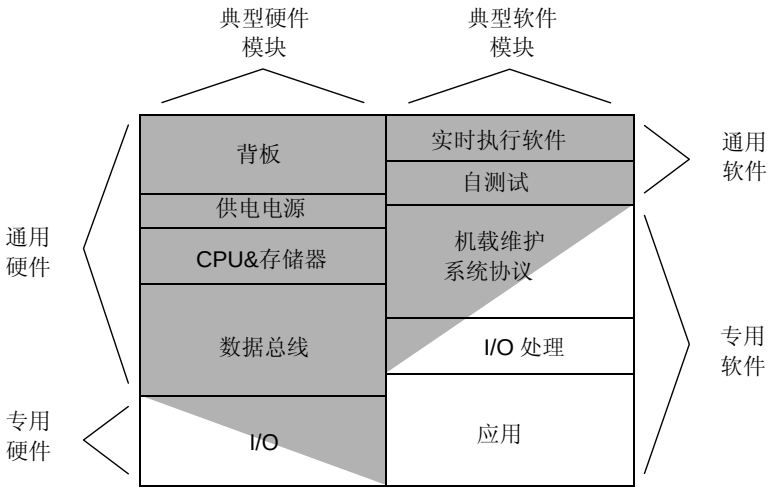


图3　强调有可能共享资源的一种典型设计举例

IMA的开发过程应该确保以下方面：

a. 分配到特定IMA系统的飞机功能要与系统的设计一致（见3.2节）；
b. 分配到特定IMA系统的飞机安全性和信息安全性需求要得到确定，并要通过IMA系统设计来满足，包括指定系统的开发保证、指定硬件的设计保证以及软件的级别。这些级别的确定要通过飞机级安全性评估来进行的，确定这些级别可以支持由宿主应用实现的功能系统，并支持系统的可用性和完整性需求，以及针对工具评估和鉴定的各种需求（见3.3和3.4节）；
c. 通过IMA平台的设计，任何宿主应用的行为都要避免对其它任何应用或功能的行为带来不利的影响。IMA平台具有健壮分区隔离、资源管理以及能适用于飞机功能与宿主应用的其它保护措施，（见3.5和3.8节）；
d. 提供给平台的健康监控、失效报告过程以及故障管理功能，要满足宿主应用和IMA系统所规定的需求（见3.6节）；
e. 建立并维护给IMA平台、应用、综合者和认证申请人使用的配置管理（见3.7节）；
f. 实现和验证分配给IMA系统的需求（见3.9节）；
g. 实现和验证属于IMA系统的人员因素需求（见3.10节）。

3.1 IMA系统的开发过程

IMA系统的整个开发过程应按照结构化的过程进行，例如ARP 4754/ED-79 (参考资料[7])的过程。IMA系统的开发过程应考虑IMA的一些主要特征：灵活性、重用性和互操作性。这些特征影响着那些应该实现的开发过程，这些特征至少有：

a. IMA平台——定义可重用的、可共享的模块与资源 (包括应用程序接口与健康监控策略)；

b. 宿主应用——定义接口和系统的约定，以使某个给定的宿主应用宿主在给定的平台上；

c. IMA系统——把一组特定的宿主应用综合到某个给定的IMA平台上。

这里描述的过程支持IMA平台的重用，和支持宿主应用的开发数据用到其它飞机项目。

在描述开发过程时，将使用下列术语(这些术语是对2.1节术语的补充)：

IMA平台（IMA platform）——由IMA模块和核心软件组成，它们可以没有任何飞机功能或已经安载了应用

IMA平台架构（IMA platform architecture）——构造、连接和组合IMA模块的一些方法，这些IMA模块支持宿主应用和飞机功能；

IMA系统（IMA system）——由IMA平台和宿主应用组成；

IMA系统架构（IMAsystem architecture）——由要求满足宿主应用和飞机功能所有需求的IMA平台、连接和组件组成。

3.1.1 IMA平台的开发过程

IMA平台的定义与开发可以与专用的飞机功能和宿主应用的开发分开进行。如果能分开进行的话，开发IMA平台的数据就可能再次使用（与一组不同的宿主应用在一起）。

IMA的一个主要目标就是开发出一个IMA平台，这种平台能够与不同宿主应用一起重复地用到不同飞机上。一种可重用的IMA平台应利用下列描述的过程目标进行开发。模块的认可过程将在第4章中进行描述。

a. 策划和定义IMA平台，这种定义应包括：
   1) 架构定义，它包含各种IMA模块、资源与组件的类型和一般功能，以及他们是如何交互的(如，是分布式的还是集中式的结构)；
   2) 将宿主应用、软件和硬件综合到IMA平台的方法；
   3) IMA平台的认可方法；
   4) IMA系统的认证方法，它包括支持宿主应用和开发符合性数据的各相关方的角色与责任；

5) 能够提供给宿主应用的一组平台服务；
6) 飞机功能级所期望的可用性与完整性的等级、平台对其支持的能力，以及支持的方法；
7) 健康管理和故障管理的方法(不包括对外部的真实接口，因为这部分接口是依赖于飞机的HM和机组的告警系统)；
8) 对平台和IMA系统进行配置管理的方法。

b. 定义IMA平台的需求，包括：
1) 安全性能力
- 确定顶层平台的失效事件，这种事件能够影响宿主应用；
- 定义与各种失效事件相关的可接受的失效率(对平台硬件模块的可靠性要求)；
- 使用上述数据进行开发的指南，这些数据能满足飞机和潜在宿主应用的可用性与完整性要求；
- 定义安全性的要求，包括健壮分区隔离、健康监控、故障管理、资源管理、其它安全特性与其它保护措施。

2) 性能能力；
3) 配置管理方法；
4) 环境条件，在这种条件下平台模块能按预期情况运行。这里模块共用同样的环境，如机箱有共用的电源、共用的数据总线。对共用环境的定义也应进行描述；
5) 故障管理与故障报告的方法和要求，需要考虑的内容包括：容错、模块的故障隔离以及单点失效的探测与隔离(例如，导致能力丧失的失效，如内部电源的失效，有冗余模块的内部通信通道，以及其它类似资源等都应予以考虑)；
6) 对各部分概念定义的详细需求；
7) IMA平台的结构，这种架构已按照所需要的安全性能力进行了定义和验证。

c. 开发并实现IMA平台的设计。软件和硬件的开发过程应分别按照DO-178/ED-12 (参考资料[2])和DO-254/ED-80 (参考资料[6])进行，同时要符合各类补充规章文件的要求，在相应的安全级别上满足所需的安全性要求。另外，应该进行共因分析(CCA)，并应针对该平台所确定的各种顶层事件进行定量的失效分析。

d. 验证并确认IMA平台，涉及到以下活动：
1) 针对特定的环境条件进行环境鉴定试验；
2) 进行了分区分析和验证试验；验证其它的保护能力与安全性特性(即，资源管理、健康监控、故障管理、启动自测试和连续自测试，等)；
3) 完成了共因分析CCA；
4) 完成了能证明实现满足可靠性需求与能力的数值分析；

5) 解决模块一起共享的环境和资源问题，与非IMA模块共享同一环境的问题也要解决。如果只有IMA模块有共同的环境，且模块的配置是固定的，那么就能在进行机上完全综合前进行部分可组合的环境鉴定。

e. 使用第4章描述的模块认可的方法来获得IMA平台的认可。应该对第4章和第5章中描述的模块认可数据进行开发，并提交或使其能够获得。IMA平台的所有需求应该得到确认和验证。需求、实现和验证等活动之间的追踪性应该得到开发和维护。

3.1.2 宿主应用的开发过程

开发宿主应用遵循的过程与开发非IMA系统使用的过程相同，但应达到这些目标：

a. 确定需要使用的IMA平台资源(包括部分接口的定义)；
b. 量化所需的IMA平台资源(包括部分接口的定义)；
c. 把宿主应用的安全性评估映射到IMA平台的安全性评估和能力上(即，初步的系统安全性评估(PSSA)、功能危害评估(FHA)以及共因分析(CCA))；
d. 定义宿主应用的HM/FM需求，并确定与IMA平台HM/FM功能的交互关系；
e. 确定IMA平台以外的专用资源(例如，专用硬件)；
f. 规定专用资源的环境鉴定等级；
g. 将应用综合到平台上，并进行软件/平台的综合测试；
h. 对照IMA平台的性能，评估人员因素的需求。

3.1.3 IMA系统的开发过程

IMA系统的开发过程应涉及以下目标：

a. 确定飞机的功能，包括功能、性能、安全性、可用性和完整性的需求；
b. 在考虑飞机级FHA、资源需求(接口规范)、IMA平台的安全性能力以及MMEL等情况下，把IMA平台的资源分配到飞机的功能上。确定出哪些宿主应用或飞机功能需要与其它的宿主应用和功能进行隔离和/或保护，并确定出所需的其它保护机制或安全性特性；
c. 开发IMA系统的结构，涉及到以下方面：
    1) 根据飞机的需求、宿主应用以及IMA系统的认证方法，开发（编制）IMA系统的认证计划（见4.4.3节）；
    2) 确定所需IMA平台模块和资源的数量、质量和类型，以便能满足各种应用需求，包括功能、性能、安全性、可用性、完整性和余度的需求；
    3) 确定由IMA平台模块的能力决定的各种飞机功能需求，例如：
        - 对可用性的需求超过了单个IMA模块或平台能够达到的范围，这种情况能促使应用宿主到多个模块或平台上；
        - 使用多个模块的应用应确定应用的余度管理需求

- 对完整性的需求超过了一个IMA模块或平台能够达到的范围，这种情况能使宿主多种实例的应用和/或数据通过比较来达到所需要的完整性。

4) 对于每个要使用IMA平台安全性需求的宿主应用，都要进行初步系统安全性评估(PSSA)；
5) 根据平台、宿主应用和共享资源失效的组合情况，来评估飞机的影响；
6) 对IMA平台资源的分配，确定出所需进行的更改，以解决单独和组合PSSA活动所发现的任何问题。

d. 实现IMA系统，包括进行下列活动：
   1) 开发应用软件，并进行部分验证；
   2) 将所有应用综合到平台上，并对IMA系统进行确认与验证活动；
   3) 利用IMA平台的顶层事件作为宿主应用失效分析的基本事件，进行初始IMA系统的失效分析；
   4) 评估影响宿主应用的IMA平台组件失效的组合情况，这些失效可能会在飞机级产生影响，并在必要时调整资源分配和/或应用的实现。需要注意，IMA平台组件的失效应该是一种独特的顶级事件；
   5) 进行飞机的地面和飞行试验，以确认SSA中的假设、需求和环境定义。

e. 综合、确认、验证（未装在飞机上的）IMA系统并获得认可， 对IMA系统中的特定应用配置，应证明能满足其需求(包括性能、余度管理以及IMA平台的接口需求)，应该对每一种宿主应用进行分析，以表明其符合自己的FHA。另外，对宿主应用的分析应该与IMA系统硬件的定量分析结合起来，通过这种定量分析就能表明事件的各种组合能满足飞机级安全性和可靠性的需求。

f. 适当时，要综合、确认、验证装在飞机上的IMA系统，以获得IMA系统的装机认可。

表3给出了综合活动与认可任务的关系。这些活动都是通用的，并能按照开发的规模进行适当的范围调整。IMA认可的过程有六项任务(参见第4章)。

表3　综合活动与认可任务之间的关系

综合活动	认可任务	
将组件和／或模块综合到一起，形成平台	任务1	模块和／或平台的认可
将单个应用与平台综合到一起	任务2	应用的认可(软件和／或硬件)
将多个应用与平台综合到一起，并进行多个应用的相互综合	任务3	IMA 系统的认可
将IMA系统与飞机及机上系统综合到一起	任务 4	飞机级综合
确定更改及其更改的影响，且需重新验证	任务 5[1]	更改
确定并使用能用于其它IMA系统的IMA组件，并进行安装	任务6[1]	重用

([1] 任务 5 和任务 6 的综合是在飞机级或系统级上进行的，可能还包括任务 1 – 4 的活动)

3.2 IMA系统的资源分配活动

飞机的功能和性能需求会影响IMA宿主功能的分配，除专用的飞机功能外，还有几个问题需要解决，包括计算资源可用性、专用I/O资源、网络带宽的提供，并满足安全性、完整性和可靠性的要求。代表特定应用的平台服务应运行在该应用所限制的资源范围内。

a. IMA系统的处理吞吐量应该达到应用、上下文切换、平台运行管理以及总处理需求所需要的执行时间。例如，代表应用的任何服务应在其分配的时间内进行运行，并且不能占用分配给其它应用的时间。这也包括由平台提供的服务，如资源管理、健康监控、故障管理、分区隔离实施，以及其它有效的保护措施；

b. 计算资源和网络带宽的总量(包括分区隔离实施、处理以及数据总线的抖动和流量)应超过与上下文切换、数据调度以及其它限制相关的要求；

c. 为了满足飞机的安全性需求，IMA平台和宿主应用就要确定分配和配置给IMA系统的功能完整性与可用性的需求。对于飞机功能和宿主应用，IMA系统的结构应能支持最高级别的完整性和可用性。

3.3 飞机的安全性和信息安全

安全性需求应在IMA系统需求中进行讨论。这些需求影响着系统的配置和分配给功能与宿主应用的IMA资源，并对实现飞机功能的宿主应用建立独立性、可用性和完整性的需求。另外对安全性的考虑要在第5.1节中描述的安全性评估过程中进行。从安全性评估和信息安全分析中派生出的需求也不同于功能需求。

信息安全的需求应在飞机级安全性评估中进行讨论(见第5.1.5.8节)。IMA的机制可以用来解决信息安全的问题。

3.4 开发保证与工具保证

IMA系统和组件应该按最高的保证等级的要求进行设计和开发，以支持飞机功能和IMA系统要执行的宿主应用的安全性、完整性和可用性需求，这些需求是由IMA系统的安全性评估所确定的。要确定“通用”IMA平台（的需求）可能是困难的，这种IMA平台会用到多种型号的飞机上，而这些型号飞机的飞机功能和宿主应用都是不定的（不知道的）。因此，为了减小特定飞机型号和宿主应用配置所带来的风险，IMA系统的开发商就想要按某个特定的保证级别来开发他们的系统。

给宿主应用的I MA平台用户指南与接口规范（描述IMA平台与外部系统的接口需求），都应该是完整的和无二义性的。由于飞机功能和IMA系统上的宿主应用可能源于多个供应商，因此，所有的应用供应商都应能得到IMA平台的用户指南。

由IMA平台开发商提供的工具以及用于开发和/或验证符合接口规范的工具可能需要进行鉴定。例如，某些用来产生或验证配置表的工具或验证健壮分区隔离的工具可能需要

由IMA平台的开发商和/或系统综合者进行鉴定，而不需要由应用开发商进行鉴定。

3.5 分区隔离与资源管理活动

IMA的一个主要目的就是把飞机的多个功能和应用综合到一起并宿主到一个或多个计算平台上，同时确保任意一个飞机功能都不会以未规定的方式或不可接受的方式来影响其它的功能。而且，能够强制并维持这种独立性的失效机制应该是可检测的和能进行缓解的，以确保达到所要求的安全性和完整性的等级。

对于“不可接受”的准则只能通过安全性评估来确定。这需要对飞机功能和宿主应用之间有抑制和隔离的行为有分析的机制。这种技术就是通常所说的分区隔离，在DO-178/ED-12 (参考资料[2])中定义如下：

“分区隔离是一种技术，它能在功能独立的软件组件之间提供隔离，以包容和/或隔离故障，并尽可能减少软件验证过程的工作量。”

IMA系统中的分区隔离，在没有任何非预期的影响下，应允许相互独立的应用共享资源。尽管分区隔离的概念已在许多以商用计算机作为基础的系统中得到应用，但通常（实现）都不提供相关安全性系统所需要的保护等级。这样，“健壮的分区隔离”就成了对IMA系统专门规定的分区隔离。

健壮分区隔离的特点有：

a. 分区隔离的服务应当对共享平台资源的飞机功能和宿主应用提供适当的分离和隔离，分区隔离的服务是由平台提供的服务，这种服务定义和维护分区之间的独立性和分离性。这些服务确保在分区内功能或应用的行为不能对其它任何分区功能或应用的行为构成不接受的影响。这些服务应能防止对飞机产生任何不利的影响，而这种不利影响的情况就是对所有功能和应用有影响的共享资源产生同时检测不到的破坏；
b. 有能力确定具有一定信任等级的实时性，这样，分区隔离的服务就能按照与规定安全等级相符合的要求来执行；
c. 分区隔离的服务不应该依靠飞机功能或宿主应用的任何行为来进行，这就是说，建立并维护分区隔离所需的任何保护机制都应由IMA平台来提供。

注意：其它保护机制(例如，高等级故障的检测与分辨、专用的安全性监控，或错误检测与更正能力)可以作为宿主应用的一部分宿主在IMA上，或可以宿主在飞机的其它系统上。

这些特性应与所要求的可靠性和完整性等级相谐调，可靠性和完整性的等级是由飞机

安全性评估所确定出来的。对这些特性的分析可以在飞机平台或IMA系统级别的综合中进行。

在设计中配给分区内某个指定应用或应用功能独占的资源就是专用资源。专用资源的一个重要特征就是它的失效只影响指定使用这些资源的应用或分区。专用资源的一种典型情况就是专用存储器、特定的硬件以及软件逻辑资源，如专用的缓冲器。

由多个分区使用的资源就是共享的资源。因此，把某一分区内应用功能与另一分区的应用功能进行独立或隔离是必要的(例如，一个功能不受另一功能的失效或异常行为的影响)。共享资源的一个重要特性就是它的失效会影响使用该资源的所有应用和分区。不同的架构可以把同一种资源指定成专用的，也可以指定成共用的。

分区隔离的分析与设计应该符合两个原则。第一，指定给某一分区的专用资源绝不能受到其它任何分区应用或应用功能操作的影响，也绝不能影响其它任何分区应用或应用功能的操作。第二，某一分区对共享资源的使用不能对共享该资源的其他分区中应用的运行或应用功能造成不可接受的影响。这种影响是通过安全性评估来说明的。

IMA的执行环境应确保所有的宿主应用在运行方式上等同于联合式系统架构中的方式。每个宿主应用相对于与其一起宿主的其它应用应完全独立的。平台应保证对所有的宿主应用分配必要的资源，不管其它宿主应用的运行是正常还是出错。

IMA系统及其架构的设计由许多决定因素(例如，系统需要冗余的问题、对共因失效的考虑，等等)。本节只讨论与分区隔离有关的设计和结构问题。在出现硬件失效或软件错误情况下，IMA系统不能保证分区隔离可能需要飞行机组人员或维护人员采取特殊的行动。这些行动只能根据飞机实际的功能和宿主应用来确定，这些内容已经超出的本文件的范围。然而，为了保证飞机功能和宿主应用上分区隔离与那些失效的影响，可能涉及IMA系统失效的任何机制，都应被识别出来，并提供给系统开发过程和安全性评估过程。在有些情况下，IMA系统的开发商可能提供与任何应用都无关的特殊安全属性，如，失效静默或失效运行的架构、提供附加的限制与保护，这些能够简化整个系统的安全性评估，简化对健壮分区隔离和其它保护特性的验证以及对符合性的证明。

3.5.1 健壮分区隔离的设计

IMA平台上的分区隔离设计是一个迭代过程。应该对提出的设计进行分析，以确保3.5节中所确定的准则都能得到了满足。如果发现有不足之处，就应修正这种架构，直到能够证明这些准则都得到满足。尽管所采用的方法将依赖于具体的实现，在本节中还是能够提供出一些通用的指南。

对所有的专用资源和共享资源都要进行识别。对这些资源可能会产生非预期影响的所有传播路径都应予以确定。这些传播路径可能产生于硬件失效、硬件设计错误或软件设计错误，这些传播路径也可以产生于正常的执行。一旦确定出了这些传播路径，就要建立并

确认抑制范围，以防止通过这些传播路径在分区间产生非预期的影响。健壮分区隔离的服务应对专用资源和共享资源提供保护。这些分区服务的失效可能导致产生非预期失效的传播路径。传播路径的例子有：

a. 有故障的分区允许某个应用对存储器的某个单元进行写操作，而这个单元是其它分区不能对其进行访问的；
b. 某个有故障的分区会导致共享共用的通信通道不能对其它分区提供服务；
c. 处理器执行时间被拒绝从一个分区交给另一个分区；
d. 一个有故障的分区能毁掉一个共享闪存的文件系统；
e. 在上下文切换到一个新的分区时，CPU上的高速缓存没有得到刷新；
f. 一个有故障的分区会引起某一事件在某一时刻发生或顺序发生，而这种情况不是另一分区所希望的那样。

在有些情况下，对于给定的传播路径，可能需要一个以上的（错误）抑制范围。在另一些情况下，一个单一的（错误）抑制范围可以保护一个以上的传播路径。

在由分区隔离服务所提供的分区隔离功能之间所允许的相互交联和接口应做出完整的规定。完整的接口定义会方便传播路径的分析，在分区间对接口规范的严格坚持并执行要求应在IMA平台上采用，以避免非预期行为的出现。

分区隔离的机制应与IMA系统的完整性、可用性和可靠性的要求相协调。IMA系统的设计应满足这些需求的最高等级，同时要认识到IMA系统包含有各种宿主应用与飞机功能的组合。

3.5.2 分区隔离分析

分区隔离分析应证明在分区中的任何应用或子功能都不会对其它任何分区的某个应用或子功能的行为产生不利的影响。分区之间的所有传播路径都应得到识别，每个传播路径所带来的影响都应在文件中记录。（错误）抑制范围内不可接受交互关系的缓解措施都应得到识别，故障树分析、形式方法和其它技术都会（在分区隔离分析中）用到，分区隔离分析应该在飞机的系统安全性评估中进行，以包括多种失效要求的可能性。换句话说，这种分析可对上述的要求做出假设，分区隔离分析应对如何进行分区隔离作出计划、程序和要求，并要对其它保护机制进行验证和确认。

下面的几节给出了分区隔离分析应包含的内容。

3.5.2.1 顶层分区隔离的特性

分配给顶层分区隔离属性的需求应基于飞机的安全性评估，这部分的分析应该描述需要建立的主要特性和属性，这些特性和属性可以使健壮分区隔离得以实现和维护。这些内容既可以从正面来描述属性，也可以从防止不期望的属性加以描述。

3.5.2.2 分区隔离特性的分解

这部分的分析是由顶层属性到低层属性的分解，这些低层属性是为满足顶层属性而必需要达到的。这些低层属性可以进一步分解，直到最底层的属性，这一过程要能表明平台设计中的一个或多个特性能够得到完全满足。

注意: 一个顶层属性分解的例子 (任何应用决不会对在其它分区中的任何应用行为造成负面的影响)可能按以下步骤进行: 在一个分区中任何应用功能决不能

a. *以某种不利的方式访问其它分区中的任何存储器;*

b. *以某种不利的方式影响其它分区中的任何定时;*

c. *对其它任何分区所用的资源造成不利的影响。*

上述三个特性能够满足顶层的属性，可能还要用到其它的方法。另外，存储器保护可作为最底层的属性来对待，

如果设计特性使用了存储器保护单元(MMU)，且对MMU的设置有一组配置文件，这些配置文件能够确保分配给分区功能的存储器只能由该功能来访问。

3.5.2.3 生命周期数据

对于每个与最底层属性相关的设计特性，对生命周期的数据和相关验证的数据都要能够进行追踪。如果这些设计特性和相关生命周期数据是另一验证过程的一部分，则只需要追踪到这一设计特性和相关的需求。

3.5.2.4 分区隔离的脆弱性评估

对于每个分区隔离的属性，都要进行脆弱性评估。当需要进行安全性评估和危害性分析时，这种评估能检查外部系统和人机接口的所有可能行为，以及硬件失效的影响。

注意：由于配置文件可能超出平台设计者的控制范围，可能存在这样一种脆弱性情况，例如，配置文件中的一个错误可能导致分区功能间的存储器区域覆盖。这就要求有这样一种缓解措施，它要求对IMA系统综合者提供的验证数据不能覆盖存储器区域。

3.5.2.5 可能的错误源

在分区隔离分析中要涉及的可能错误源，对每个要进行分析的系统都是唯一的。尽管不需要列出一套完整的问题清单，但下面列出一些可能的设计错误源都会影响分区隔离的分析。

a. 中断和中断屏蔽(用软件和硬件进行的)；
b. 循环 (例如，无限循环或间接的无法终止的调用循环)；
c. 实时响应 (例如，帧超限、与实时时钟冲突、计数器/定时器损坏、流水线和高速缓存、有确定性的调度)；
d. 控制流 (例如，不正确的分支进入一个分区隔离的或受保护的区域、跳转表受损坏、处理器队列控制的损坏、返回地址的损坏、不可恢复的硬件状态受损坏 (如，屏蔽和停止))；
e. 存储器、输入和/或输出的内容；
f. 共享的数据标记；
g. 软件陷阱(例如，被零除、未实现的指令、专用软件中断指令、不能识别的指令和递归终止)；
h. 停止命令Hold-up commands (例如，性能障碍)；
i. 输入或输出数据的丢失；
j. 输入或输出数据的损坏；
k. 内部数据的损坏(例如，直接或间接的存储器写入、表越界、非正确的链接、包含有时间的计算、受损的高速缓存存储器)；
l. 延迟的数据；
m. 程序重叠；
n. 缓冲顺序；
o. 外部设备的交互(例如，数据的丢失、延迟的数据、不正确的数据、协议停止).

对于系统来说，分区隔离分析和不同设计步骤之间存在一种反复的过程。在这种情况下，即所有的分区隔离属性都能得到满足且所有已确定的脆弱环节都得到了缓解并有相关的验证数据，这种分析才算是完整的。

3.6 健康监控与故障管理

健康监控和故障管理(HM/FM)的功能应能认识到，IMA平台可以支持一组不同的飞机功能。IMA平台应该向IMA平台的模块提供基本的健康监控和故障管理的能力，这种能力应该独立于各宿主应用，健康监控应解决运行与维护两方面关注的问题。

要制定出解决下列问题的策略：

a. 确定需要监控的组件和内容；
b. 对各个应用健康状况的确定；
c. 确定IMA系统整体的健康状况；
d. 对各类失效或异常行为的响应；
e. 对飞行机组的通告与通信；
f. 对维护活动及其报告的控制；
g. 冗余管理；
h. 单个事件的翻转。

3.6.1 需要监控的组件与内容

健康监控是IMA平台负责对失效进行探测、隔离、抑制与报告的部分，这种失效对使用IMA平台资源的应用或者资源本身都会产生不利的影响。这种功能应能检测出宿主应用所用共享资源中的故障。然而，专门用于应用的一些资源也可以通过IMA平台来监控，例如，专门用于某个应用分区的存储器可以由IMA平台来监控，而不是由应用监控的。

共享资源中的故障可能会对使用该资源的所有应用产生不利的影响。系统架构应该设计成能在尽可能低的架构等级上，理想的是在组件等级上，进行检测故障。这将会减少二义性的可能。这种过程可通过自监控、平台监控或某种组合来完成。故障通常是通过征兆来检测的，这可能会对实际发生故障的部件产生一些混淆。对于某一故障，混淆的范围越小，就能越容易地在IMA系统级别上确定出安全的解决手段。选择可靠的架构能够大大减少隔离到单个区域的模糊程度。对于IMA平台中的故障检测，当确定责任时，这是一个重要的考虑方面。对于IMA平台的健壮分区隔离服务来说，这可能更重要。这些服务的失效能够直接影响维护时进行分离和隔离的能力。如果要使用宿主应用来检测这些服务（例程）中的失效，就几乎不可能把这些失效与分区隔离的机制进行隔离。由于这一原因，分区隔离服务的健康监控应该在IMA平台上进行。

IMA平台应该监控其服务和接口。

3.6.2 每个应用的健康情况确定

应用的供应商应确定应用的可能失效模式，特别是要确定对平台有行动要求的应用失效模式。例如，这可能是分区重启动、关闭（关机）或者是其它平台特定的行动。

HM应对记录、监控以及管理影响平台的失效提供方便，这种方便就是能对应用进行记录，并能向应用通告维护的状态与失效情况。应用供应商对特定应用也能在应用级别上提供健康监控的能力，这些内容不依赖所用的方法，就应能将它们识别出来并纳入到IMA系统的总体健康监控策略中。

3.6.3 确定整个IMA系统的健康情况

要确定IMA系统的健康需要讨论IMA平台级的失效状态，并要对在应用中没有讨论过的、可能的分区隔离失效与应用失效模式性进行讨论。对综合在一起的HM策略应进行规定，并记入文件之中，这种HM策略应与IMA系统的安全性评估相协调。

综合在一起的HM策略还要规定以下内容：

a. 确定系统失效的措施，并向宿主应用与其它平台服务报告状态；

b. 控制分区进行重启动和关闭的规则；

c. 若适用的话，给出降级运行的规则；

d. 能支持MMEL的指南；

e. IMA系统健康状况的报告、内容与频度。

3.6.4 各种失效类型的响应

除了能检测并隔离故障外，还需要有报告和抑制故障的能力。报告故障就是对所存在的故障或失效进行内部登记、指示给宿主应用与平台服务、指示给飞行机组或者指示给维护机组。故障抑制就是使失效不要对外部造成任何损坏影响的一种响应，本小节重点是故障抑制，故障报告的内容将在以后进行叙述。

在IMA平台上所有可检测的错误都应该有确定的响应，在某个应用中的那些不会影响IMA平台资源的失效，应该由应用负责处理。该应用要对这些失效提供正确的响应，包括提供应用的健康状态。IMA平台应对应用试图违反平台分区隔离服务的任何行为进行监控与检测，并由平台采取适当的措施，IMA平台对这些故障的响应是可以配置的。

能把故障限制到某个隔离区域的能力，可以极大地方便宿主应用综合到IMA平台上，这里假设分区都是故障抑制的区域，并且平台服务也是故障抑制的区域。

3.6.5 飞行机组的通告与通信

一般来说，在处理飞行机组通告与通信方面， IMA系统和传统的联合式系统应该没有区别。在飞行警告与维护消息系统的框架内，飞行机组关心的重点是功能的可用性。虽然，维护系统提供的是飞机维护方面和飞机派遣(MMEL)的信息，这些信息能以某种正确程度来改进维护报告的效率与效果，但在帮助飞行机组做出决策的过程中，还是飞行提醒/警告系统负责提供主要的信息。通过系统监控相关的中央提醒/警告功能，包括消息提醒和语音提醒，就能完成这一过程。飞行提醒/警告系统连同MMEL清单中的项目一起，能为飞行机组和维护人员提供决定飞机派遣状态的基本信息。

然而，对于IMA系统作为一个整体所给出的状态以及单独的组件与应用所给出的状态，有一些与系统降级相关的状态需要通告给机组人员。飞行提醒/警告系统可以有选择地禁止一些警告以减少来自级联失效的影响，然而，通常来说，对所有的失效和系统降级以及重

新配置的活动都要报告。

哪些故障、失效和错误需要进行登记、报告或显示给飞行机组都要适当地确定出来。那些通知可以只限于这些情况：系统不能恢复的失效(如，硬件失效)、导致性能降级或进入失效模式的失效、可能降低飞机或系统安全边界的失效(如，丧失了冗余或完整性)、可能不安全的状态或功能性丧失的告知。对显示给飞行机组的IMA系统故障信息应该进行分析，以确保它们没有二义性，并给它们指定适当的优先级别，所显示的信息和语音提醒都应该以清晰且有序的方式提供给机组人员。

3.6.6 维护活动与报告的管理

维护人员需要能够分析监控健康的数据，确定出已失效的或已表现出异常行为的系统组件，决定采取最合适的维护活动(例如，延期、测试、修理、替换，等)。IMA系统的综合性、独立性和复杂性等级所导致的潜在失效模式(例如，所有的功能都会受到单个共享资源丧失的影响)，与联合式系统的失效模式相比可能更特殊和更多。电源电流瞬间过大、级联失效或影响共享资源的失效，都能导致多个功能和宿主应用的同时失效，且会有多个被记录和通告给飞行机组的失效、警告、提醒或小心消息。虽然这里描述的许多特性都能借鉴传统的联合式系统，但为了减少故障的传播并区分出故障问题是与平台相关还是与应用相关，需要特别重视纠正由IMA系统自测试设备(BITE)所报告出的故障。

一般来说，机载系统的维护性应该与飞机的安全性、可靠性和保障性目标一起考虑，对这些相关目标的分析也可确定出预防性维护活动的特有方面。

3.6.7 冗余管理

冗余用来改进飞机功能的可靠性与可用性，IMA平台和/或系统可包括有支持管理宿主应用冗余的机制，IMA系统应建立冗余管理的手段，只要有可能，对冗余的管理应该独立于宿主应用，以支持分开进行应用和平台的分析与开发。

有些宿主应用可能需要专用的冗余管理，对于这种情况，IMA系统应该对平台资源的健康以及其它模块的健康提供正确和相协调的信息，而这些信息与应用是交互的。

3.6.8 单事件翻转(SEU)故障

通过使用共享资源，如电源、计算处理、存储器以及数据总线等，IMA系统能在一台计算机环境中宿主若干飞机功能和应用。这就是说，共享资源中发生的SEU可能会对飞机的不同功能、应用和分区产生多种不利影响。 IMA平台设计和故障管理的策略应能解决潜在的SEU问题并提供相应的故障恢复能力。

3.7 IMA系统的配置管理

认证申请人应能为飞机的运营者提供强壮的且易于维护的配置管理系统，IMA平台的

开发者应该为认证申请人提供相关的能力和方法，来确定IMA系统、平台、模块、资源、功能与宿主的应用和数据库的配置。IMA系统由多种通用的共享资源组成，这些资源可以用传统的方式标记，也可以用电子部件编号来标记。在维护飞机和IMA系统的配置过程中，飞机运营者的作用与行为应该简单并可验证。操作过程应该提供给飞机的运营者，以便在维护IMA系统时能简化工作任务并减少操作者的错误和过失。给飞机的运营者应该提供一种方法，以便能验证飞机和IMA系统的配置与所要认证的配置是一致的，且符合型号的设计。

所要涉及的问题有：

a. IMA系统软件和硬件的部件编号所需要配置数据的长度；
b. 作为受控配置项中的配置数据；
c. 配置数据之间的相互性；
d. 用户可修改的硬件、数据库和软件而没有得到认证机构的监管；
e. 有能力从模块和应用恢复出部件的编号，用于一致性检查；
f. 有多种、可选的配置(可选模块的选用情况)；
g. 现场可加载的模块(包括硬件、软件、数据库)；
h. 维护修改后的配置数据；
i. 用于提供验证方法的配置实践：
   - 安装在系统中的所有硬件部件编号和序列号；
   - 对硬件修改的所有状态索引；
   - 安装在系统中所有软件(包括宿主应用与核心软件)部件编号的标识符；
   - 安装在系统中所有配置数据的标识符；
   - 安装在系统中所有数据库文件的标识符；
   - 对于特定的飞机，所有硬件、软件和数据库文件的部件编号都要正确；
   - IMA模块、资源与宿主应用混合在一起的兼容性，特别是与现场可加载有关的部件。

3.7.1 配置数据

IMA系统和宿主应用都应该维护系统中的配置数据。这些配置数据组是飞机认证的符合项(型号设计的数据)并应该包括在认证数据包之中。对这些配置数据要证明它们可以追溯到应用和模块的派生需求上。通过审查、分析和测试等方法的组合可以证明这些文件的正确性得到了验证。

IMA系统应该管理对宿主应用及其配置数据的现场加载，IMA系统可以使用这些文件中信息来确定应用、应用的资源需求或应用状态的正确配置。设计并保证宿主应用所用的配置数据是由应用开发者负责的，并能独立地实现IMA系统的设计与保证活动。

3.7.1.1 IMA系统的配置数据

针对IMA系统的特有配置数据要纳入到具体的认证指南中，例如，IMA系统希望能包括进行应用调度和资源分配的配置数据。这些数据作为一组建立的配置表或文件可在构建时实现，或者作为独立加载的数据来实现。

在本节中所描述和讨论的配置数据，由IMA系统用来：

a. 在IMA系统安装到飞机时，定义或选择IMA系统的正确配置；
b. 使能配置控制，并支持IMA系统、平台、模块、资源和应用的一致性检查；
c. 激活或解除模块、资源或功能，例如，利用有可供选择的软件或数据，使软件适应飞机的几种配置；
d. 确定分配给宿主应用的IMA系统资源；
e. 确定分区内部通信端口的分配情况与特性；
f. 确定影响综合系统的参数(例如，调度、性能、模块的部件号)。

IMA系统的配置数据可以相互依赖，这样就能考虑用一组配置数据来构成一整套IMA系统的配置。这种整套的配置可以作为一个最终要提供的认证数据条目来控制。

3.7.1.2 应用的配置数据

由IMA系统中宿主应用使用的其它类型的配置数据可以：

a. 激活或解除某些功能或专用应用资源(例如，利用可供选择的软件或数据，使软件适应飞机的几种配置，使宿主应用适应) ；
b. 使应用适应飞机的配置；
c. 为宿主应用提供数据。

3.8 共享数据库的使用指南

包括在飞机系统中的数据库给应用提供静态的只读数据，IMA系统可能需要有只写的数据库，这些数据库可以作为共享资源或专门用于某个特定应用在飞机上安装。

宿主在IMA系统的数据库在功能上与传统联合式系统所用的数据库相同。对于能满足适航要求的航空数据库，工业界已接受的指南可由现有的文件提供，如DO- 200/ED-76 (参考资料[3])和DO-201/ED-77 (参考资料[4])。

共享数据库可以看作为另一种受IMA平台管理的共享资源。共享资源在第3.5节中已讨论过。受到破坏的共享数据库应该由IMA系统的健康监控和故障管理功能来处理。

3.9 主要最少设备清单(MMEL)

IMA系统可以宿主飞机的许多系统，并能与之进行接口。要在进行独立工作的飞机系

统、LRU或功能等传统的方式引入这种高度综合化的系统，是更为困难且可能是不可能的。IMA系统的高度综合化特性使得失效模式、资源管理、健康监控、故障管理和其它设计考虑方面，与典型联合式系统的架构和策略有很大的不同。

3.9.1 MMEL的设计考虑

在需要时，MMEL应该成为IMA系统设计与需求的一部分，以便能够对故障管理、冗余管理进行分析并将其与IMA系统设计合并在一起。MMEL的范围应通过考虑以下相关内容来确定：确定给IMA系统功能和应用的危险程度，以及由这些系统、功能和共享资源失效产生的影响。MMEL确定的设备应基于飞机级的功能危害评估（FHA）和系统安全性评估（SSA），并应考虑与失效的组件、资源或功能所共享的资源对其它任何功能的影响。任何所提出的MMEL列表内容应能持续地证实符合适用的规章。

当FHA或者SSA要求对IMA系统的模块、功能或应用进行禁止或隔离时（直到采取适当的维护行动来纠正失效前），则要对失效的组件采取一种禁止或隔离的措施。对于失效组件不需要被禁止或隔离且可恢复或重新启动的情况，应表明在以下情况下不进行恢复或重新启动：在某种不安全的条件下，或者，对飞机的其它系统或功能有不利影响或对飞机安全性边界有不利影响。当不能用分析来确定故障的隔离与管理、恢复活动、冗余管理、降级的操作模式等，而且也不能验证在一个或多个系统中的故障不会对其它系统或功能产生不利影响或产生不可预见的级联影响时，就需要进行功能测试。

3.9.2 MMEL批准的考虑

在MMEL确定的设备中，飞机派遣要求的维护与操作应该包括适当的安全性理由和过程，这些都要基于第3.9.1节的设计考虑。MMEL清单连同有支持的数据、正当的理由和操作的过程等，提交给相应的协调管理机构。

3.10 人员因素的考虑

与现有的联合式系统架构相比，由IMA系统所带来的系统综合程度和复杂程度的增加，可能会在飞机系统和飞行机组与地面维护人员之间产生出与以前不同的相互依赖与交互的关系。人员因素问题应该在IMA系统设计过程中解决，需要特别强调的是要确定出性能需求、功能的交互、与驾驶员的接口、要显示的信息、故障管理和机组告警、降级的操作模式以及可能的级联失效。同样，在持续适航过程中的人员因素问题也应该在IMA系统设计过程中解决。

飞行机组与维护人员对人员因素的要求应该作为IMA系统需求的一部分来处理，达到人员因素需求的计划应该在项目的早期进行编制，且应包括能符合那些需求的对应方法。

通过分析用户(飞行机组与维护人员)要执行的任务以及要产生能执行这些任务的用户接口，可以开发出IMA系统的人员因素需求。用于确认设计能满足飞行机组与维护人员需求的分析，并能帮助系统设计人员实现用户需求的分析，可能包括原型实现、人员在环中的测试（有人参与的测试）、用户确认以及其它方法。在正常、不正常和紧急状态情况下，由飞行机组人员体验的用户行为需求(例如，响应时间、持续时间、负载、反馈等)应该在IMA系统的设计中来确定和实现。根据任务与用户接口方面的人员因素分析结果，IMA系统的设计特性可能需要进行修改。

适用时应讨论下列条款：

a. 直接用户接口，如，飞行座舱接口、维护接口、支持机组人员的接口、自动或人机的交互(例如，自动驾驶员与其它的飞机接口)；
b. 信息处理、要显示的信息和系统信息的处理；
c. 人员要处理的信息——对可得的信息，用户要能容易理解并能采取措施；
d. 标准化(例如，过程、任务、语言、符号、颜色、信息)；
e. 系统与人员的行为和响应时间，包括执行任务的时间、刷新率，以及对人员的限制和可能出错的考虑；
f. 对人员的自动监控与解释；
g. 健康与操作状态的监控，以及人员的交互；
h. 有多条失效和提醒的消息——应以清晰和有优先顺序的方式显示出来；
i. 在飞行过程中允许飞行机组采取的处理故障的行动以及不允许采取的行动；
j. 维护性设计(例如，故障管理与故障记录)；
k. 针对可能遇到的人员行动与能力（性能）的全范围进行设计；
l. 系统设计要能缩短培训并简化维护；
m. 在IMA系统的整个开发生命周期中，识别、追踪并解决设计上的问题。

人员因素需求与对应的符合性方法，应该包含在认证计划中（该计划在第4.4.3和4.5.3节中描述过）。人员因素需求是从飞机和IMA系统的需求派生出来的。为了确保所有这些需求都得到满足，应该在飞机和IMA系统的需求之间（包括人员因素需求）建立追踪性。对这些需求实现情况的验证应该通过审查、分析和测试活动的组合来完成。

第4章　认证任务

本节对IMA系统在认证任务方面的考虑进行讨论，涉及到要符合的适用（适航）规章，以及规定系统功能、性能和安全性方面的需求。

4.1　认证过程概述

IMA系统认证过程的一个重要方面就是通过获得IMA平台、模块和/或宿主应用的增量认可与认证信任，通过积累达到IMA系统在飞机上的安装批准，并直到发布产品认证书。

典型的开发过程分解为六项任务，这些任务规定了IMA系统认证过程的增量认可活动：

- 任务1: 模块认可;
- 任务2: 应用软件/硬件的认可
- 任务3: 系统的认可
- 任务4: IMA系统在飞机上的综合，包括确认与验证
- 任务5: 模块或应用的更改
- 任务6: 模块或应用的重用

这六项任务用图4进行了说明，并作为一种结构用于本节后续的子节中。有些任务是可以并行的，在一些工程中有些任务是不适用的。下面对每项任务都有一小节专门描述。

模块、应用或IMA系统的初始认可应该在飞机或发动机认证项目(TC)或修改项目(STC)的范围内进行。即，IMA的认可只能在某个实际认证项目的相关条件下提出。

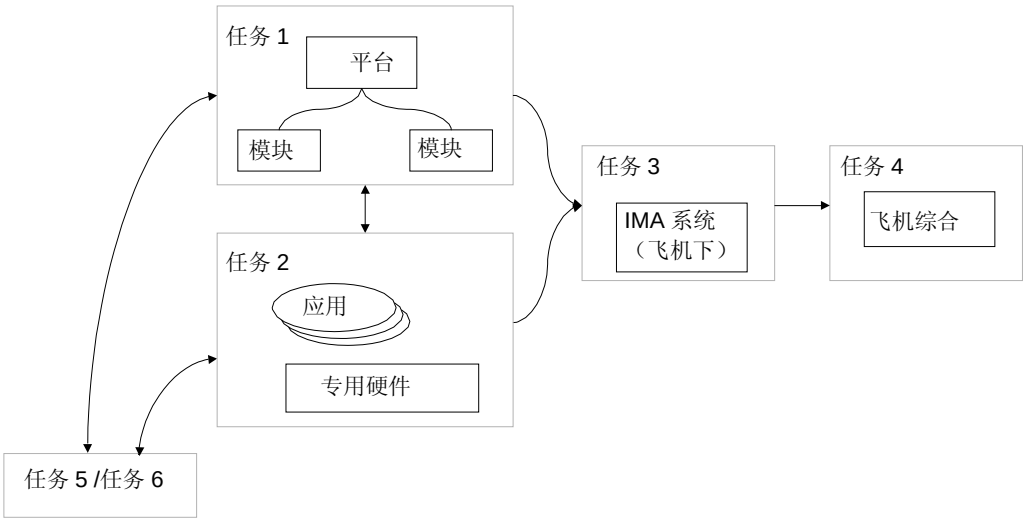


图4　IMA系统认证任务的说明

表4对这些认证任务、它们在本文档中的章节以及典型的认可方法进行了总结和概述。在有些情况下，符合性数据可以在认可信件发布之前获得批准（用盖章或信件的方式），认可信件的发布可能在认证项目完成综合后进行，即在飞机产品取证时或接近取证时。

每项任务需要产生的生命周期数据都列在在适当的引用章节和附录A的表格中(见表4的第2列)。在许多情况下，各利益相关方可以采用事先已有的过程，或者采用不同的过程打包他们的数据。如果要更换标题或重新打包，则该利益相关方应该编制一份映射文档，来证明所有适用的数据都可以得到。

表4　IMA认证任务概述

任务	引用章节/目标	获得认可的方法举例
任务1： 模块认可	4.2节 表A-1	认可信件[2]或盖了章的数据单，盖过章或批准过的模块认可数据包，RSC的认可信件(仅针对AC 20-148参考资料[9]定义过的软件内容)，TSO-C153机构的信件(仅针对参考资料[10]所定义的内容)
任务2： 应用认可	4.3节 表A-2	认可信件[2]或盖了章的数据单，RSC的认可信件(软件仅针对AC 20-148参考资料[9]所定义的软件内容)，盖过章或批准过的IMA平台-宿主应用的符合性数据包
任务3： IMA系统认可	4.4节 表A-3	已认可或批准的符合数据包
任务4： IMA系统在飞机上的综合，包括V&V	4.5节 表A-4	TC, STC, ATC, ASTC
任务5： 模块或应用的更改	4.6节 表A-5	若模块有更改，与任务1相同；若应用有更改，与任务2相同。(两种情况均取决于更改的程度，可能需要开展任务3和任务4的某些活动)
任务6： 模块或应用的重用	4.7节 表A-6	若要重用模块，与任务1相同；若要重用应用，与任务2相同。(两种情况均取决于重用的环境，可能需要开展任务3和任务4的某些活动)

（[2] 认可信件的内容可以类似于AC 20-148所描述的RSC的认可信件，即，它应该描述认可任务的全部内容与限制）

4.2　任务1——模块认可

在整个认证的过程中，模块认可的目的就是要证实模块的特性、性能与接口，以获得模块的增量认可。为了有利于其它IMA系统的认可任务和第4.7节中所讨论的重用，增量认可要通过提供文件化的证据(验收和/或符合性的数据)来完成。模块的认可只能在飞机和/或发动机的认证项目或在修改项目的环境条件下进行。

要获得IMA平台的认可，模块的认可过程允许认证申请人针对IMA平台的单独组件(例如，处理模块、核心软件服务(包括，操作系统、健康监控功能、故障管理功能)、电源模块、接口模块)获得增量认可。平台本身也可以作为一个模块来认可，这种情况通常包含多个其它模块。

4.2.1 模块认可的目标

模块认可过程的目标是：

a. 策划认可的任务，以满足所有适用的认证需求。确保其它利益相关方能够同意这个认可计划；

b. 编制模块的规范，并证实符合模块的需求规范(MRS)（这里模块供应商可以根据设想的目的编制MRS)。设想的目的应该纳入MRS文档中，并在验证和确认过程中要予以确认；

c. 证实资源内在属性的符合性，例如，时间和空间的分区隔离、故障管理、健康监控、其它安全属性、确定性、延迟、资源管理、资源配置以及应用参数等，使用范围的属性应该在资源使用的边界内提前定义；

d. 使用在MRS中确定的需求，例如性能、接口、服务、安全性、故障管理和健壮性(容错)，来验证资源属性的符合性；

e. 针对相关的模块，开发出核心软件(例如，操作系统、API与核心服务)和/或硬件，并证明其过程符合适用的指南与规章；

f. 开发模块认可的数据，并能为认证机构认可提供模块认可的数据；

g. 为模块的用户提供必要的信息（资料），以便能正确地使用模块、综合模块，并与模块进行接口(例如，用户指南、模块的数据手册以及接口规范)；

h. 如果模块就是一个平台，就要综合平台中的模块；

i. 当需要时，对开发和验证模块时所使用的工具进行评价和鉴定；

j. 为了模块的认可，实施质量保证、配置管理、综合、确认、验证以及认证联络；

k. 为用户提供必要的信息（资料），以便他们能正确地管理模块的配置。模块应为用户提供一种方法，以便能够确定模块配置 (例如，物理的部件编号)、电子的部件编号/版本、核心软件的标识符以及模块发生变更的时间；

l. 当需要时，定义、规定、评估和鉴定模块的支持工具，这些工具要提供给模块的用户并由模块的用户使用；如果用到了共享的工具，就要开发出一套方法来共享工具数据(例如，用户指南、工具鉴定的数据，工具的规范)；

m. 如果要想重用模块开发的结果，在模块的开发过程(见第4.7节)中就要解决重用问题。

4.2.2 模块认可的数据

模块认可的过程应该按照系统的方法进行，应该包括计划、需求以及与符合这些计划和需求的证据。在下面几小节中定义模块认可所需要的模块生命周期数据以及各数据项中的典型内容。

第5.7节描述了要提供给认证机构的数据，获得模块认可数据的过程应该与认证机构进行协调，并应征得认证机构的同意。

注意：对使用TSO-C153的硬件，如果开发者决定要获得认可，则要给认证机构提供一个认可的数据子项。

4.2.3 模块认可计划(MAP)

在模块要获得增量认可时，模块开发商要向认证机构提交他们的认证计划，MAP就是所要使用的主要手段。针对特定的模块，MAP应涉及所有的方面，包括模块的开发、验证、配置管理、质量保证以及符合性验证。 MAP应该建立模块认可的基础，并便于在IMA系统项目中使用该模块。MAP应该涉及以下方面：

a. 系统概述(如果适用的话)：这部分对模块将要运行的系统进行概述，包括系统可能宿主的应用和功能，以及分配给它们的硬件和软件、结构、所用的处理器、硬件/软件接口和安全性特性；
b. 模块概述：这部分简要地描述模块的功能，重点强调所提出的安全性和分区隔离的概念，例如，资源管理、冗余、非相似设计、容错以及定时与调度策略；
c. 认可准则：这部分对用于模块的准则进行总结，以确保其预期的使用和在系统中的功能是可接受的，这包括所提出的软件等级、硬件设计保证等级、硬件可靠性数据、硬件环境鉴定等级，和/或找到的模块所信任。这部分还应给出分配到模块上的各项安全性目标以及与安全有关的需求、模块对IMA系统安全性评估的已知影响，以及支持各种安全性分析、分区隔离或其它保护策略的架构与其它特性；
d. 模块的生命周期：这部分定义模块开发要使用的生命周期，解释如何满足生命周期过程的各个目标(需求、设计、实现、验证)，还要对所涉及的组织与利益相关方、组织的角色与责任、系统的生命周期过程以及认证联络过程的责任等做出规定。开发过程、配置管理过程、质量保证过程和验证过程也应该包含在MAP中。
e. 模块的生命周期数据：这部分规定了模块生命周期过程中要产生和控制的生命周期数据，还描述了这些数据之间的关系或者这些数据与定义系统的其它数据之间的关系、描述了要提交给认证机构的模块生命周期数据（模块认可数据和/或模块的符合性数据）、数据的形式，以及能够让认证机构得到模块生命周期数据的途径。如果要更换标题或重新打包，则该利益相关方应该开发出一套对应（映射）的生命周期数据，以证明所有适用的数据都是可获得的。
f. 进度计划：这部分给认证机构提供出模块生命周期过程中明确的活动，以便可以对评审做出计划。
g. 工具鉴定：这部分描述的是对工具进行评估的方法，这些工具是在开发、验证、配置、综合与加载模块中使用的；借助对工具鉴定计划的引用，确定那些要进行鉴定的工具，并对那些用于开发过程而不需要进行鉴定的工具提供合理的理由。这部分

描述鉴定各种工具的功能性和方法，这些工具可提供给模块用户，以支持开发、配置的生成、进行应用和配置的加载、性能（实现）以及验证（的实施）。这部分应确定出预期要同其它的模块和应用开发者与综合者共享的工具。

h. 模块的重用：如果模块要针对能够重用进行开发(见第4.7节)，MAP应该包含以下方面：
   - 给出适合重用的理由，即，模块的哪些方面能使其适宜重用；
   - 要提供给认证申请人的数据列表能够用作为型号设计数据，并能支持其项目的模块认可；
   - 以前声明过的模块信任，以及要进一步完成的活动并要满足新的目标；
   - 制定出能解决公共重用问题的计划；
   - 开发支持重用的数据，例如：接口定义的数据、纳入文件的使用范围、安全性的假设或失效的条件、用户指南、限制、实现部分信任的说明等；
   - 对于可重用应用的应用指南，例如AC 20-148 (参考资料[9])和/或规定8110.49 (参考资料[11]的第12章)。

i. 附加的考虑：这部分描述一些特定属性，这些属性。可能影响模块认可过程，例如，替代的符合性方法、工具的鉴定、可重配置的模块、COTS的软件和/或硬件，以及产品的服务历史。对于附加指南内容请参考DO-178/ED12 (参考资料[2])和DO-254/ED-80 (参考资料[6])

注意：MAP可以分成多个文件，如果想这样做的话，例如有开发计划、配置管理计划、质量保证计划以及验证计划。同样地，MAP可以引用其它计划(见图5)。

4.2.4 模块需求规范(MRS)

模块需求规范(MRS)定义要综合到IMA系统中模块的需求和设计准则。这种MRS应该包括以下类型的信息：

a. 模块需求的描述，要注意与安全相关的需求、保护方面的需求和可能的失效条件；
b. 在各种模式操作下的功能和操作需求，这些需求要定义模块功能和性能的能力，如以下所述：
   - 功能能力：这些内容给用户描述模块能够完成的功能。特别重要的描述是那些影响外部用户的模块功能；
   - 性能能力：这些内容包括模块的性能能力，这些用户需要性能用于接口和综合的目的(这些信息的例子就是精度、分辨率、定时特性、能力和限制)。
c. 安全能力：这部分应该包括用户进行系统开发和系统分析必须要有的内容，以确保模块在系统中的使用能符合安全性要求。这部分还应该包括预期的关键性、失效与

故障、出现故障的可能性、软件等级与硬件设计保证等级、假设条件、飞行机组警示与系统通告消息、维护检查、安装限制、独立性与隔离性要求、环境限制，以及对资源管理、健康监控、故障管理、健壮分区隔离和其它保护措施的要求；

d. 接口需求：这部分应该包括协议、规格、输入/输出、输入的频度、输出的频度，以及所允许与其它模块的接口；
e. 接口定义：这部分应该包括用户与模块对接和用户使用模块时所需要的所有内容。例如有：数据缓冲的设置、电压、引脚信号定义、数据传输协议(运行时间/维护/加载、数据完整性的编码/解码、存储器映像布局、定时时序、同步性信号、中断定义、电子配置数据、分区隔离边界的设置信息、API定义)。另外，还要包括针对各种异常状态确定能够采取的数据和控制接口的相关内容，例如，无效数据的状态、测试模式、初始条件以及复位模式；
f. 故障管理和健康监控的需求；
g. 资源管理：对各种资源进行管理和限制的策略，包括余量以及测量这种余量的方法；
h. 调度过程与处理器内部/任务内部的通信机制，包括严格的时间顺序、抢占式调度和中断；
i. 健壮分区隔离的需求，包括确定在模块分区间能够允许的交互，以及需要能够避免分区破坏、进行分区冲突检测和从分区冲突中恢复的方法与措施；
j. 描述模块及其组件，不管是新的还是以前开发或认可过的（都要描述），且如果是以前开发或认可过的，要引用以前的基线；
k. 如果适用的话，要描述未激活的特性或机制(为以后的重新配置)；
l. 模块在使用软件和/或硬件需求与数据的地方，应该按DO-178/ED- 12 (参考资料[2])第11.9节和第11.10节与DO-254/ED-80 (参考资料[6]) 第10.3节所描述的内容给出软件和硬件的数据，这些数据可以引用，而不需要重复；
m. 物理和安装的定义：它包括物理和特定安装所需要的信息(例如，DO-160/ED-14 (参考资料[6]))，以便系统的综合者能把该模块与其它模块和IMA系统综合在一起。

4.2.5 模块的确认与验证(V&V)数据

模块的V&V数据就是模块的完整性、正确性以及模块符合其需求（与MRS中定义的一样）的证据。它能提供这样的保证：模块是按照其需求开发的、正确地生产出来、已进行了确认和验证并已达到了验收准则。数据包括模块评审、分析、仿真和测试的过程与结果。模块的V&V至少包括以下数据：

a. 模块的V&V计划，它可以是MAP和/或IMA系统V&V计划的一部分；
b. 当软件是模块的一部分时，与软件等级相适应的软件验证用例、过程和结果(见DO-178/ED-12，参考资料[2]，第11.13和11.14节)；

c. 当复杂硬件是模块的一部分时，与硬件等级相适应的追溯性数据、评审与分析的过程与结果、测试试验的过程与结果，以及测试验收的准则(见DO-254/ED-80，参考资料[6]第10.4和10.5节)；

d. 数据，它包括环境鉴定的表格、试验等级、试验计划（大纲）、试验程序和试验结果(见DO-160/ED-14，参考资料[1])。并非所有的试验都能在模块级别上完成，有些类型的试验只能在模块综合到系统内和/或飞机上时才能进行；

e. 模块综合的V&V用例和过程，当综合模块时，至少包括以下数据：

- 评审与分析的过程：对V&V计划补充的详细描述，它们描述用于评审或分析方法的范围与深度；
- 测试用例：每个测试用例的目的、输入的设置、条件、达到所要求的覆盖准则的期望结果以及通过/失败的准则；
- 测试程序：对于如何建立并执行每一个测试用例、如何评估测试结果以及如何使用测试环境进行一步一步的说明。

f. 模块综合的V&V结果应该（用文件）记录以下内容：

- 对每一项评审、分析和测试说明在活动中通过或未通过的每个过程，以及最终的通过/未通过结论。
- 标识经过评审、分析或测试过的配置项目或版本；
- 测试、评审和分析的结果以及覆盖分析和追踪性分析。

g. 模块的追踪性数据。模块的追踪性就是在需求、详细设计、实现以及验证的数据之间建立相关性，它能便于模块进行配置控制、修改和验证。

4.2.6 模块的质量保证(QA)记录

模块QA过程活动的结果要记录在QA记录中，这些记录包括QA的评审或审计报告、会议记录、授权过程派生的记录，以及符合性的评审记录。

4.2.7 模块的配置索引(MCI)

MCI确定了模块的配置和模块生命周期环境，该索引是为帮助模块的再生产编制的，包括模块的生命周期环境，应该包括以下内容：

a. 模块的描述与配置；

b. 模块在更低一级进行组装的每个组件；

c. 以前开发过的模块，如果用到的话；

d. 模块的生命周期数据，包括模块的认可数据和模块的符合性数据；

e. 存档和发布的介质；

f. 制造模块的说明或图纸；

g. 标识模块生命周期环境；
h. 标识用于模块开发和验证的开发和验证工具，包括对工具鉴定数据的引用；
i. 标识用于验证模块的测试环境；
j. 数据的完整性检查，如果用到的话。

4.2.8 模块认可的配置管理(CM)记录

模块CM过程活动的结果要记录在CM记录中，例如包括配置标识清单、基线或库记录、更改历史报告、存档记录以及发布记录。

4.2.9 模块认可的完成总结(MAAS)

模块的MAAS就是能表明符合MAP的主要数据项，MAAS应包括：

a. 与MAP中的内容相同 (见第4.2.3节)，以及从MAP中派生出的内容；
b. 模块的特性：陈述时序和存储器的范围、资源限制、附加的约束以及度量各项特性的方法。这部分内容可以是模块数据手册的总结(见第4.2.10节)；
c. 模块的标识：这部分就是用部件的编号和版本来标识模块；
d. 更改的历史：如果适用的话，这部分要包括模块更改的总结，重点是说明由于哪些失效和异常行为引起的更改，并指明自从上次认可后模块在生命周期过程中的更改；
e. 模块的状态：这部分对认可时尚未解决的问题报告进行总结，包括理由和功能限制的叙述；
f. 符合性说明：这部分描述的是符合附录A表A-1和本节所定义任务的适用目标情况、模块的认可准则以及总结为证实符合模块计划中所确定的准则而采用的方法。这部分还描述附加的规则以及对计划与本文件的偏离情况；
g. 其它的活动：这部分描述的活动就是用户和/或综合者如何能够成功地和安全地使用该模块。

4.2.10 模块认可的数据手册(MADS)

MADS要提供给用户、综合者、认证申请人和认证机构，当适用时，MADS应包括以下条目：

a. 模块的描述及预期的用途与功能；
b. 模块的部件编号，包括修改和修订的状态；
c. 对最终模块配置索引的引用(带有修订的状态)；
d. 软件等级和硬件设计保证等级；
e. 所达到的环境鉴定试验级别；

f. 硬件的物理连接信息(例如，内部数据总线接口、配对的连接器、I/O的连接器以及外部数据总线和接口的需求、安装和操作的需求、模块内部的接口与连接、接地和防护的措施、分离与隔离的措施)

g. 电源需求与功耗；

h. 尺寸与重量；

i. 特殊安装的信息，包括：

- 软件的加载过程；
- 模块要求平台的机箱或电子设备机架的型号编号；
- 接地和防护的需求；
- 安装要求(包括在飞机上的方向)；
- 间隙要求；
- 气流量与制冷要求；
- (如果适用的话)子组装件的安装与装配要求；
- 分离与隔离的措施；
- 用户、安装人员或综合者所需的任何其它信息。

j. 限制；

k. 持续适航的信息（资料），包括用户或安装人员所要用到的各种持续适航信息；

l. 可能影响安装的安全性评估信息；

m. 用于软件开发、验证和系统配置的工具需求，在数据手册中也可引用的用户手册；

n. 任何附加的相关认可数据，例如认可信件、数据批准的信件等也应该能引用；

o. 模块的使用范围。

4.2.11 模块的问题报告

模块的问题报告是一种措施，它识别并记录模块错误、失效和异常行的解决情况、与模块计划不符的过程以及模块生命周期数据中的缺陷。模块的问题报告应包括：

a. 标识配置项目和/或模块生命周期过程的活动，在这些活动中问题能够得以发现；

b. 标识需要修改的配置项目或描述有更改的过程；

c. 使问题能够得到理解和解决的问题描述；

d. 对已报告问题采取纠正行动进行解决的描述；

e. 对纠正行动(解决方案)的验证。

4.2.12 模块认可的附加生命周期数据

除了第4.2.3节到第4.2.11节所讨论过的生命周期数据外，当适用时，还应该包括以下的生命周期数据：

a. 支持数据：支持模块认可的DO-178/ED-12 (参考资料[2]) 数据、DO-254/ED-80 (参考资料[6]) 数据和 DO-160/ED-14 (参考资料[1])数据；
b. 支持整个飞机安全性评估和IMA系统评估过程的安全性评估分析/报告；
c. 工具数据：用于模块开发和验证的工具可能需要进行验证或鉴定，另外，为了进行模块的综合或对综合进行验证，模块开发商可以向综合者或认证申请人提供工具。工具的验证应该记录在验证结果文档中，如果工具需要鉴定的话，需要产生工具鉴定的数据(见DO-178/ED- 12,参考资料[2], 第12.2节)；
d. 用来开发、设计和实现模块的开发标准(例如，编码、需求和设计)；
e. 用户指南：这部分包括用户、综合者和认证申请人为顺利与模块接口或进行模块综合所用的全部信息。该指南应该定义有效使用模块认可数据的范围，指南的内容应包括正确使用（模块）的建议与举例。另外，为了避免可能出现的不正确使用或非预期使用，该指南应该强调模块在综合或接口时的各种警告或限制。

4.3 任务2——应用的认可

应用就是定义有一组逻辑接口的软件和/或专用硬件，当与平台综合时，它能执行飞机的功能或部分功能。在整个IMA系统的认可过程中，应用认可的主要目的就是证明应用符合适用的规章和由IMA系统设计所分配的需求，并能在模块的限制内运行，且提供所规定的特性与性能。另一个目标就是为了有利于在IMA系统中进行应用综合以及可能在其它子项目中重用(见第4.7节)，来提供认可数据和符合性证据。对应用的生命周期数据(例如，认可信件、盖过章的数据、数据的批准信件) 进行认可的过程应该与认证机构协调。

将来预期要重用的软件和/或硬件应用应该使用目前已有的指南进行开发，例如AC 20-148 (参考资料[9])、DO-178/ED-12 (参考资料[2])和DO-254/ED-80 (参考资料[6]).

注意：在第5.7节中描述要提交给认证机构的数据。

4.3.1 应用认可的目标

应用认可过程的目标有：

a. 证明应用能执行其预期的功能，并能满足适用的规章，同时，能正确地使用适当的平台资源并能与其它模块和/或应用进行接口；
b. 确定应用所需要的平台资源；
c. 对应用使用符合相应模块需求规范、接口规范以及模块和/或平台用户指南的平台资源进行验证；
d. 当适用时，确保达到其它认可和批准的活动；
e. 开发必要的应用生命周期数据，这些数据可以通过某种方式组织起来，以支持应用

将来能够重用；

f. 当把应用综合到他的目标IMA平台上时，要确认和验证应用的操作；

g. 在开发、综合与验证过程中，保持配置控制并确保所配置的工具与模块得到正确的使用；

h. 如果想要应用能够重用，就应该在应用的开发过程中来实施。

4.3.2 应用认可数据

应用认可过程通常包括的内容要符合DO-178/ED-12 (参考资料[2])、DO-254/ED-80 (参考资料[6])和DO-160/ED-14 (参考资料[1])的要求，因此，相关的生命周期数据要能够生成并进行组织以支持实现IMA系统的认可目标，特别是对装在飞机上IMA系统，能支持IMA系统的综合与认证，且在平台和模块的需求与限制范围内，要表明应用功能是正确的。

除了前面规定的生命周期数据外，对于应用认可或符合性证明，可能还需要增加其它数据，这取决于IMA系统在飞机上的安装情况。例如，为了确保应用与平台是兼容的，可能还需要有接口规范和使用领域的分析数据。

如果要想应用能够重用(见第4.7节)，应用的软件认证计划(PSAC)或硬件认证计划(PHAC)应包括以下方面的内容：

a. 给出适当的重用理由，应用在哪些方面能使其适合于重用；

b. 要提供给认证申请人的数据清单，要作为型号设计的数据来支持认证和重用；

c. 应用已声明过的信任(全部、部分或没有) ，以及未完全达到所有信任目标用户要进行的活动；

d. 能够达到重用的计划；

e. 支持重用的开发数据，例如：接口定义数据、文件中所列的使用范围、安全性假设或失效状态、用户指南、限制、对部分信任进行完善的说明、应用的数据手册(类似于第4.2.10节所描述的模块数据手册)、环境鉴定等；

f. 可重用应用的适用指南，例如AC 20-148 (参考资料[9])和/或规定8110.49 (参考资料[11]的第12章)；

g. 对如何达到第4.7节(任务6)中的指南做出计划；

h. 对如何开发一种问题报告系统来支持将来的重用做出计划。

4.4 任务3——IMA系统的认可

IMA系统认可的主要目的就是证明综合化的模块、宿主应用和平台能够持续地执行其预期的功能，而不会对其它的模块和应用产生不利影响，这些证明活动可以在飞机上进行也可以在飞机下进行。对于在飞机下的活动来说，主要目的就是进行能够支持整个飞机认证的那些V&V活动。对于飞机下特殊V&V要得到的认证信任等级应事先与认证机构进行协

调。

任务3和任务4描述的情况随项目的变化程度很大，因此，任务3和任务4的生命周期数据可以混在一起，或者要进行适当地分派。在任务3中不能生成的生命周期数据，就应该在任务4中完成。

4.4.1 IMA系统的认可目标

IMA系统认可过程的目标有：

a. 为了达到飞机级的认证信任，策划IMA平台和系统的活动，这些活动预期是在综合、确认和验证中使用的；

b. 对各应用资源的需求进行合并，以便使用所定义的工具和过程来综合并生成IMA系统的配置；

c. 验证各种应用、模块和平台资源之间正确的交互，包括健壮性测试、正确的资源分配与管理、正确的冗余管理、单个应用的性能不会受到不利影响，以及对安全性、健康监控、故障管理、分区与保护等需求的满足；

d. 证明符合相关的规章、指南和需求；

e. 证明IMA系统的配置是正确的，且是按照批准的过程进行的；

f. 执行IMA系统综合与V&V的活动；

g. 开发IMA系统认可与符合性的数据 ；

h. 评估模块与应用的问题报告，以确定它们对IMA系统的影响，并采取适当的行动。

4.4.2 IMA系统的认可数据

IMA认可过程应该采用结构化的方法，IMA系统的这种认可过程应该纳入IMA系统认证计划(IMASCP)和IMA系统 V&V计划文件中。V&V的结果、系统的约束、限制和所用的工具都应纳入IMA系统的完成总结中(IMASAS)。IMA系统的配置索引应该在IMA系统和飞机级上确定模块与宿主应用之间的兼容性。

认可数据在提交给认证机构之前，应该由认证申请人先进行评审和认可，第4.4.3节到第 4.4.7节描述了需要产生的IMA系统认可数据以及它们的主要内容。

4.4.3 IMA系统的认证计划(IMASCP)

IMASCP至少应该包括：

a. 对IMA系统的功能和操作描述，包括组成IMA系统的模块、资源、平台和宿主应用，这些描述应确定模块、资源、平台、宿主应用和其它外部系统与功能之间的功能、物理以及接口关系等(例如，与非IMA系统功能的接口)。

b. 描述IMASCP与其它相关认证(飞机认证计划)和认可计划的关系。如果要更换标题

或重新组合，则利益相关方应该开发出一套生命周期的映射数据，来证明所有适用的数据都是可以获得。

c. 总结PSSA、可靠性需求、分配给系统、硬件和软件的保证级别以及FHA的假设(飞机的危害性、IMA功能的危害性、失效状态、类别)，另外IMA系统容错、失效-安全设计特性以及恢复能力的描述(例如，资源管理、故障管理、健康监控、失效恢复、降级模式、比较与表决策略、冗余以及功能隔离与独立的能力)。

d. 描述各种新设计的特性，这些特性打算用来满足安全性目标并要符合规章；

e. 人员因素方面问题的高级描述(见第3.10节)；

f. IMA系统认证基础，包括任何特殊条件、解除、偏离或安全性建议的同等级别；

g. 确定现场可加载的软件或硬件、可选软件或硬件的选择，用户可修改的软件，以及对软件的加载、可选项的选择与用户（操作者）的修改进行加载、修改和验证的部分责任；

h. 所提出的IMA系统认可与批准的方法，即系统、硬件和软件的认证方法。对所提出的方法要能证明符合认证基础，包括对所期望的开发保证过程 (安全性评估、开发、确认、验证、配置管理、质量保证和认证联络) 的概述。描述的内容应该包括如何满足本文件中的目标。第5.5.1节和第5.6节详细描述了配置计划和质量保证计划；这些计划可以包括在IMASCP中或可以由IMASCP引用；

i. 综合活动的描述；

j. 任何附加的符合性方法都应该得到描述和证明。如果使用以前开发或认可过的软件或硬件(重用) ，符合性方法还要包括对更改影响的分析、使用范围的分析、模块或应用的重用等；

k. 要提交给认证机构的符合与认可的数据清单，要在配置管理的控制下进行维护，并配有描述或数据形式的样例；

l. 对有相互依赖性的认可、批准和认证事情（活动）要有大致的顺序与计划；

m. 在IMA系统的开发、认可、综合、安装与认证过程中(见第2.4节)，要列出所涉及的所有利益相关方的角色与责任清单；

n. 确定负责认可和认证协调的关键人员或专门组织；

o. 对模块与应用的问题报告如何进行描述，要根据对IMA系统的影响来判断。

4.4.4 IMA系统的确认与验证计划(IMASVVP)

IMASVVP应该包括或引用以下内容：

a. 描述如何把不同的模块、资源、平台和宿主应用综合成IMA系统；

b. 描述用于IMA系统V&V的方法与过程；

c. 描述如何验证和确认容错、失效-安全设计以及（失效）恢复的特性与功能；

d. 在IMA系统V&V活动期间要记录的数据，例如，总结、评审结果、分析、仿真、基准测试结果、综合实验室的测试结果或研究情况；
e. 描述如何确认和验证SSA的假设、系统安全性特性以及系统资源的分配与管理；
f. 对V&V活动的状态如何进行维护或管理，特别是当需求或资源分配有更改时；
g. 描述每一项V&V活动通过/失败的准则；
h. 与V&V活动相关的角色与责任；
i. 关键V&V活动的进度，并描述这些活动的相互依赖性；
j. 描述开发与验证活动的独立程度。

对于综合、确认和验证活动的完整性与协调性应该与所有相关利益关系方进行协调。

4.4.5 IMA系统的配置索引(IMASCI)

IMASCI应该包括以下内容和/或能提供对包含这些内容的其它数据进行引用：
a. 确定IMA系统中的软硬件组件的物理位置；
b. IMA系统中各组件的配置标识；
c. 用于开发、综合与V&V环境的配置索引；
d. IMA系统构成整体所需要的操作或维护的过程与限制；
e. 为了在适用规章下建立IMA系统的安全性，所提供的各种系统设计特性或能力都应该予以确定；
f. IMA平台与宿主应用的相互连接与相互关系；
g. 与飞机其它系统的接口(例如，总线、专用连接，等)；
h. 如果有替换项的话，要有描述允许相互替换和/或相互混合使用的信息；
i. 确定需要鉴定的工具及其相关的工具鉴定数据；
j. 对IMA系统组件配置索引的引用；
k. 对加载、验证和维护IMA系统正确配置的说明，并与IMA系统和飞机型号设计的一致。

4.4.6 IMA系统的完成总结(IMASAS)

IMASAS至少应该包括下列内容：
a. 所包括的内容（信息）与IMASCP(在第4.4.3节)中的内容相同，并对计划的任何偏离都有描述，包括能证实偏离是合理的；
b. 列出所有未关闭的问题报告，简单描述这些问题对IMA系统功能性和/或飞机安全性、操作、维护或限制的影响；
c. 确定IMA系统的组件，包括部件编号和版本；

d. 总结已做过的更改，如果该IMA系统是基于以前批准过的IMA系统基线（开发的话）；
e. 对任何所需限制的说明；
f. 对符合适航规章、本指南以及其它任何适用指南的说明；
g. 列出能够证明符合IMA系统安装批准和飞机认证的数据(包括引用或列出模块、应用和IMA系统的认可和符合性的所有数据)。

4.4.7 IMA系统的其它生命周期数据

a. 所有系统级活动的V&V记录与结果；
b. 配置管理的记录；
c. 质量保证的记录；
d. 安全性评估的分析与报告；
e. 问题报告；
f. IMA系统的需求与设计数据，它们可以是飞机需求的一部分；
g. 在DO-178/ED-12 (参考资料[2]) or DO-254/ED-80 (参考资料[6])中所定义的工具鉴定数据。

4.5 任务4——IMA系统的飞机级综合（包括确认与验证）

最终IMA系统的安装、综合与V&V活动类似于在联合式系统架构下所进行的那些活动，以证明飞机和宿主应用的各项功能都是预期要用的，（同时）支持飞机的安全性目标并能符合适用的规章。然而，在安装活动期间，与飞机功能相关的各宿主应用之间的交互，应该在飞机的地面试验和飞行试验中得到验证和确认。同样，IMA系统与飞机其它系统之间的交互、接口和联接也要得到验证和确认。在任务3中没有涉及到的IMA系统生命周期数据应该在任务4中完成。

更详细的V&V活动在第5.3节和第5.4节中描述。

4.5.1 飞机级综合的目标

IMA飞机级综合的目标有：

a. 策划IMA系统在飞机上进行安装、综合、确认和验证的活动；
b. 利用实验室（测试）、适当的分析、地面和飞行试验，证明符合预期的功能与需求；
c. 验证IMA系统的资源管理、故障容错和管理、健康监控、降级模式和（失效）恢复能力；
d. 证明符合飞机和/或发动机适宜认证基础的规章；
e. 评估特殊异常的反应，例如有多个应用的功能或整个共享资源出错或功能丧失；

f. 进行V&V活动，以解决模块失效模式(模块内部的分析) 对多个宿主应用的影响、模块上的共模故障(模块间的分析)对多个宿主应用的影响以及影响飞机多个系统失效的模式。另外还要解决备份系统和缓解措施的问题；
g. 解决与多项飞机功能失效和异常行为有关的人员因素问题，特别是在异常操作条件和降级模式(见第3.10节)下的人员因素问题；
h. 当要求时，进行高强度辐射场(HIRF)和间接闪电影响(IEL)试验，这些试验会与多项飞机功能的失效和异常行为有关；
i. 在所有的IMA平台之间，验证正确的交互与接口，包括它们的资源与宿主应用，并确保对每个单独的应用、模块或飞机其它系统的性能不会产生任何不利的影响；
j. 在IMA系统的安全性评估中，验证每个IMA模块的失效影响以及作用于一个以上宿主应用的共享资源的失效影响；
k. 为了认证机构的认可，开发飞机级IMA系统的符合性数据；
l. 进行飞机级的安全性评估，这种评估要涉及IMA系统的所有失效影响，包括进行综合及与飞机系统和功能的相互依赖。对于某一单个的应用，只要能证明IMA系统的安全评估充分考虑到了该应用的失效模式，就没有必要只考虑影响该应用的IMA模块的失效影响虑。这些评估应该考虑一般的和级联的失效，包括可能失效的组合；
m. 把IMA系统安装到飞机上。

4.5.2 飞机级IMA系统的符合性数据

飞机上IMA系统的批准应该使用结构化的方法。飞机级的IMASCP计划应该作为一个高级文件开发，以便对飞机上IMA系统的安装提供认证基础和建议的符合性方法，证实与规章的符合性，批准在飞机上的安装和认证。飞机级IMASCP计划可以是飞机认证计划的一部分。在飞机级上IMA系统的综合与V&V过程应该使用在第5.3节和第5.4节中所描述的结构化方法。在飞机级上IMA系统的综合与V&V过程应该纳入飞机级IMASVVP计划的文档中。如果合适的话，V&V和综合计划可以包括在飞机级的IMASCP计划中。IMA系统的配置应该纳入飞机级的IMA系统配置索引文件中。各种结果与符合性数据应该纳入飞机级的IMASAS文件中，下面几节(第4.5.3节到第4.5.7节)描述典型生命周期数据项的内容。

4.5.3 飞机级IMA系统的认证计划(IMASCP)

飞机级的IMASCP计划包括的信息类型应与4.4.3.a到4.4.3.n所列出的项目相同，并应增加下列内容：

a. 开展与IMA系统有关的飞机级安全性评估的计划；
b. 开发与IMA系统有关的持续适航指令的计划。

注意：如果只有一个飞机级的IMASCP计划，以上内容都应该包括在这个计划中。如果在系统级和飞机级都有IMASCP计划，则以上内容可以包括在系统级中或包括在飞机级中，或者根据所策划的活动可在两个级别中都包括。

4.5.4 飞机级IMA系统的确认与验证计划

飞机级的V&V计划包括的信息类型应与4.4.4.a到4.4.4.j所列出的项目相同，并增加下列内容：

a. 考虑单个和多个共模失效，这种失效会影响飞机的持续安全运行；
b. 度量飞机和机组人员对异常操作状态、降级模式和失效模式响应的行动；
c. 对飞机的预期功能进行验证和确认的行动；
d. 对IMA系统不执行非预期功能进行验证和确认的行动。

注意：如果只有一个飞机级的V&V计划，以上所有的内容都应该包括在这个计划中。如果系统级和飞机级都有V&V计划，则以上内容可以包括在系统级中或包括在飞机级中，或者根据所策划的活动可在两个级别中都包括。

综合与V&V的活动应该与涉及到的所有利益相关方协调一致，并在安装批准的过程中理解他们的角色和责任。

4.5.5 飞机级IMA系统的配置索引(IMASCI)

飞机级的IMASCI包括的信息类型应与4.4.5中所列出的项目相同，并增加IMA系统在飞机上进行安装、综合、确认和验证所需要的其它数据。

4.5.6 飞机级IMA系统的完成总结(IMASAS)

飞机级的IMASAS包括的信息类型应与4.4.6中所列出的项目相同，并在飞机级上详细描述。

4.5.7 飞机级的其它数据

a. V&V的记录与结果，包括地面试验与飞行试验的结果，以及人员因素评估；
b. 配置管理的记录；
c. 质量保证的记录；
d. 安全性评估报告。IMA的安全性评估过程应采用由ARP4754/ED-79 (参考资料[7])所定义的系统化的过程，并产生以下的安全性活动：FHA、PSSA、SSA和CCA；
e. 问题报告；

f. 安装说明，包括数据加载的过程；
g. 飞机级的环境试验计划(例如，HIRF和IEL)与结果；
h. 对持续适航的说明；
i. IMA系统的需求和设计数据；
j. 工具鉴定数据，与DO-178/ED-12 (参考资料[2]) or DO-254/ED-80 (参考资料[6])所规定的相同；
k. 如果需要的话，要有MMEL。

4.6 任务5——更改

4.6.1 对IMA系统的模块、资源和应用的更改

对IMA系统的组件更改，很可能发生在IMA系统的整个生命周期中。一次更改可能涉及对资源、模块或宿主应用的修改，包括对IMA系统组件的增加、删除、修理或修改。在有些情况下，为了解决元器件过时和可靠性等问题，在不影响IMA系统功能的前提下可以更改（IMA系统的）组件。更改可以有多种类型，例如，一个新应用可宿主在IMA平台上、对已有的宿主应用进行的修改、新的支持软件和处理硬件、对已有支持软件或硬件进行的修改，或增加新的网络基础。认证机构对更改要求进行重新认可或批准。

4.6.2 更改的目标

IMA系统开发和认可过程的一个主要目标，就是尽量减小由IMA系统组件的更改所带来的对IMA系统和飞机认证的影响。考虑到安装、安全性、操作性、功能和性能的问题，只有被更改的模块和/或应用才可能需要重新认可或重新批准。在IMA系统中更改过程的主要目标就是以某种方式对更改进行限制，使得更改的影响能得以了解，并且更改能得到全面地验证和确认。更改过程的目标有以下几点：

a. 开发一个更改管理过程，并与所有利益相关方一起协调这一过程。该过程应确定各种级别上的开发者、供应商、综合者与认证申请人要如何协调更改和进行更改；
b. 采用已批准过的更改管理过程进行更改；
c. 进行更改影响分析，并编制更改影响分析文档；
d. 把已更改的组件重新综合到IMA系统中，进行所有必要的验证、确认与综合活动(包括回归分析与测试)，以获得对所修改模块或应用的认可，并确保这一更改没有任何不利影响，但不对未更改的模块和应用（进行这些工作）；
e. 维护相关更改的全部生命周期数据的配置控制。

4.6.3 更改的管理过程

更改管理过程应该以文件的形式在所有的级别上(飞机、IMA系统、平台、应用和模块)

作出适当的规定，包括对不同级别之间的相互关系进行识别。对于系统的某些特定级别，如果涉及到多个利益相关方，很可能有多个更改过程，例如，认证申请人、IMA系统的综合者、模块开发者和应用开发者，可能每个都需要定义一个更改管理过程，这一过程要与其它利益相关方的更改过程相协调。该过程至少应该包括以下方面：

a. ***更改建议。*** 更改过程的第一步就是确定所提出的更改和更改的理由。一般来说，同时提出许多更改能够优化更改的效果。这些更改应该采用一种确定的方式(例如，工程更改请求、软件更改请求、问题报告或类似的方式)记入文件中。所建议的更改可能包括修复错误、增加新的特性、修改已有的特性，等；

b. ***进行更改影响的初始分析。***对每个提出的更改都应该进行分析，以确定对组件功能和性能可能产生的影响、对使用要更改组件的其它组件或与要更改组件进行接口的其它组件可能产生的影响，以及对IMA系统和飞机功能、性能与安全性可能产生的影响。第4.6.4节将进一步讨论更改影响的分析过程。一般来说，初始分析是在更改提出过程的早期进行的，但在实施更改后可能需要修改，以确保原来的性能、安全性和资源限制没有受到影响；

c. ***开发一种实现策略。***一旦更改得到批准，就要产生出一种实施策略，并要执行。实施策略应该规定更改过程、要更新的生命周期数据、要实现的活动、要执行的验证活动、要有的资源、要采用的计划，等等。各种开发者、综合者和认证申请人的特定角色与责任应该在实施策略中给出明确的规定。实施策略应该纳入相关的计划文件中，并应在实施更改前与认证机构进行协调；

d. ***按已同意的实施策略进行更改。***实施更改应该按计划文件进行，许多开发者希望同时进行多个更改。如果同时对基线作出更改，则很难确定每个更改的正确性，并难以进行彻底的更改影响分析和回归测试。然而，只要每个更改都能单独地合并到现有的基线中，就可以同时实施更改。为了确保每个更改或组合更改的正确性，这些更改对IMA系统和飞机的影响既要进行单独验证，也要进行联合地验证；

e. ***实施更改控制并进行问题报告。***更改要通过使用某种受控的过程进行，问题报告应该记入文件中，并要能够获取到。

f. ***验证更改。***一旦实施了更改，它们就应该得到验证。验证包括评审、分析和测试；

g. ***综合所更改的项目。***已更改过的项目应该在IMA系统中得到综合和验证。

h. ***完成更改影响分析。*** 在更改过程的早期可能很难完全的评估更改的影响。因此，一旦实施了更改并进行了验证，就应该完成更改影响分析，以确保其影响得到充分地评估和完全地解决(见第4.6.4节)；

i. ***后续过程。***各利益相关方应该按照第5.5节定义来进行配置管理和部件编号。

4.6.4 更改影响分析

当对IMA系统进行了更改时，就应该进行更改影响分析，并要评估该更改对原始的系

统安全性和飞机级安全性的影响。更改影响分析应该确定该更改是否会对系统或产品的安全操作带来不利影响，以及是否会对其它组件产生影响。

以下是一些可能会对安全或操作产生不利影响的例子：

a. 与安全相关的内容受到更改，例如：
   - 以前的危害度，由系统安全性评估所确定的；
   - 失效状态类别，由系统安全性评估所确定的；
   - 软件等级或硬件设计保证等级，特别是，如果新软件或硬件的等级比先前的等级更严酷；
   - 与安全性相关的需求，由系统安全性评估所确定的；
   - 安全性边界范围被缩小；
   - 确认了环境鉴定试验的结果受到影响；
   - V&V的方法或程序有所更改。
b. 飞机的运行或过程特性受到某种方式的更改，这种更改的结果会对飞行安全或操作产生不利的影响，例如：
   - 飞机的运行或适航特性；
   - 飞行机组的操作过程；
   - 增加飞行员的工作负担；
   - 态势感知、告警、提示或提醒；
   - 能（帮助）作出飞行决策的显示信息；
   - 组装和安装的需求；
   - 影响设备互换性和/或与其它设备混用性的更改；
   - 认证的维护需求发生了更改或有所增加。
c. 在现有系统的功能中增加了新功能或特性，这些新增内容可能会对飞机的安全性、功能、性能或操作产生不利影响；
d. 处理器、接口和其它硬件组件或环境发生了更改，这种更改可能会对安全性、功能、性能或操作产生不利影响。见DO-178/ED-12（参考资料[2]，第12.1.3节）和DO-254/ED-80 (参考资料[6] ，第11.1.3节和第11.1.3节)；
e. 生命周期数据（如需求、代码和结构）受到严重更改，这种更改可能会对安全性、功能、性能或操作产生不利影响；
f. 由于共享资源更改引起的性能、综合与开发方面问题，这种更改可能会对安全性、功能、性能或操作产生不利影响。

由于在IMA系统中有各种级别的开发与综合，对已认可的模块、宿主应用、IMA平台、IMA系统的更改以及在飞机级上的更改都要有所处理。

更改要与所有的利益相关方协调，就像上面描述的那样，要消除对飞机的影响。

对任何软件或硬件的更改应该反映在受更改影响的相关生命周期数据上，且要进行验证活动，以确保在更改中不会带来任何不利的影响。

4.6.5 更改数据

对于已更改过的模块或应用，模块开发者、应用开发者、综合者和/或认证申请人应该获得下列数据的批准或认可：

a. 更改影响分析(CIA)，如第4.6.4节描述的那样；
b. 更改管理计划，该计划描述了更改管理的过程(见第4.6.3节)。更改管理计划可以包括在一个已更新过的MAP、PSAC、PHAC和相关的软件或硬件计划中；
c. 能证明相关回归分析和测试的V&V计划、记录和结果；
d. 已修改过的生命周期数据。用来描述模块认可或应用认可的生命周期数据，应该随着所需要的更改进行更新，并要纳入到MCI、软件配置索引(SCI)和/或硬件配置索引(HCI) (即，顶层框图)，也就是说，对生命周期数据的所有更改都应完整，并应纳入到相关的配置索引文档中；
e. 已更新过的模块和应用的完成总结；
f. 维护和更改的历史记录。

4.7 任务6——模块或应用的重用

IMA系统是由模块和应用组成的，这些模块和应用可以在许多不同的配置中使用。重用包括模块和/或应用在后续的安装中使用认证信任(即可以是，全部的、部分的或不使用)。在后续几节中，重点介绍模块认可数据(即，在第4.2.2节到第4.2.12节中的数据)的重用或应用认可数据(即，在第4.3.2节中的数据)的重用。目的就是要重复使用已认可过的数据而不需要重新评估数据本身，但还要评估它的适应性以及在新安装中的综合情况。

4.7.1 重用过程的目标

重用的主要目标就是要能够使用以前已经得到保证和认可过的模块或应用的生命周期数据，只需要由认证机构进行少量的监管。在初始开发过程重用就要纳入计划之中，模块的认可是以能在多个系统中达到重用的目的来进行的，一旦模块或应用得到认可，重用过程的目标就要：

a. 确保模块或应用的生命周期数据不会改变以前认可过的数据；
b. 确保纳入模块或应用验证数据手册中的限制、假设等在后续的安装中得到体现；
c. 通过对使用的领域范围进行分析，来分析模块和应用的重用适应性，以确保要重用的模块和应用与原来预期和认可的方式相同。使用领域范围分析包括在使用领域范围内后续安装特性的V&V；

d. 评估所有未关闭的模块或应用问题报告，以确保这些问题不会对安全性、功能、性能或操作产生不利影响；
e. 将模块或应用综合到后续的安装中，并验证它在IMA系统中功能正常；
f. 向认证机构和用户提交必要的计划和数据。

4.7.2 软件模块或应用的重用

如果要重用的模块只有软件，那么原来的认可应该纳入文件中，说明DO-178/ED-12 (参考资料[2])的目标是完全满足、部分满足，还是不满足(见第4.7.1节、第4.2.3h节、第4.3.2节和AC 20-148 (参考资料[9]))。软件开发商没有满足的目标应该由平台综合者、系统综合者或认证申请人来完成。为了能在后续的安装中重用，应该保证以下项目：

a. 由认证机构以前批准和认可软件的生命周期数据；
b. 要重用的软件生命周期数据，从上次批准后没有改变；
c. 软件应用或模块的软件等级要与初始认可的软件等级相同，或不严酷于初始认可的软件等级；
d. 与应用或模块的接口要维持相同，例如，应用或模块的输入范围与数据类型要在以前认可的范围内或与以前认可的范围相等；
e. 要重用的应用或模块要宿主在同一目标机上，并且要与以前认可时的操作方式相同。如果使用不同的目标机，就要对目标机的相关部分进行重移植和重新验证；
f. 等价的软件/硬件综合测试与系统测试要在以前认可过的目标计算机和系统上进行。如果使用不同的目标机，软件/硬件的综合测试应该在后续的安装中进行；
g. 已经证明软件：(1)对系统的安全性、性能或功能不会产生任何不利影响；(2)对后续的操作能力不会产生任何不利影响；
h. 对所有未关闭的问题报告以及在服务期内与重用软件相关的问题要进行分析，以确保没有任何的安全性和操作性问题；
i. 综合到IMA系统的软件应用和模块要满足DO-178/ED-12 (参考资料[2])中的所有适用的目标。

4.7.3 复杂电子硬件模块或应用的重用

如果要重用的模块是复杂电子硬件(CEH)，这种CEH要求满足DO-254/ED-80 (参考资料[6]) 的目标，则硬件开发者对每个目标都要进行评估，以确定这些目标是完全满足的、部分满足的还是都不满足。硬件开发者没有满足的目标应该由平台综合者、系统综合者或认证申请人来完成。

IMA系统大量地重用CEH。如果要重用CEH，则要确保以下条款：

a. 要重用的CEH生命周期数据，从初始认可起就不能更改；

b. CEH的设计保证级别(DAL)要与初始认可DAL相同，或不严酷于初始认可的级别；
c. 与CEH的接口要保持相同不变(例如，硬件输入的范围与类型要在以前认可的范围内或与以前认可的范围相等)；
d. 要重用的CEH与其它硬件和软件的接口要与以前认可的相同，并且操作方式也要和以前认可时相同。如果接口不同或使用接口的方式不同，就需要对接口和/或相关功能进行环境鉴定试验和重新验证；
e. 等价的综合测试与系统测试要在以前认可的目标环境和目标系统上进行；
f. 已证明CEH：(1)对新系统的安全性、性能或功能不会产生任何不利影响；(2)对新的操作能力不会产生任何不利影响；
g. 所有未关闭的问题报告以及在服务期内与重用CEH有关的问题都要得到分析，以确保没有任何安全性、性能、功能和操作方面的问题；
h. 综合到IMA系统的CEH要满足DO- 254/ED-80 (参考资料[6])中的所有适用的目标。

4.7.4 环境鉴定试验数据的重用

如果要重用的模块是硬件，既可以是复杂的也可以是简单的，则要重用的环境鉴定数据(DO-160/ED-14，参考资料[1])应该进行评估。环境和模块使用的相似性应该得到评估，以确定能否重用或（如果有的话）需要增加那些测试。也就是说，是否以前的EQT结果对当前的安装仍然有效，或者是否需要在某个级别上重复一些测试，当前预期要安装的环境要一致。

当能证明环境鉴定数据适合于新的安装环境或配置时，环境鉴定的数据就可以重用。第5.2.6节所涉及到的环境鉴定试验类型，可以在模块级、平台级、系统级和飞机级上进行。

4.7.5 含有软硬件的模块重用

第4.7.2节到第4.7.4节中的指南应该按照包含有硬件和软件的模块进行。

4.7.6 符合性数据的重用

要重用以前认可过的模块和应用，本节描述的数据就应该可以获得或应该进行开发。

4.7.6.1 初始认可的生命周期数据

下列数据是初始开发和认可应该提供的：

a. 模块和应用初始认可数据的证据，这些数据是在第4.2.2节到第4.2.12节以及第4.3.2节中所描述的那些支持设计保证的数据；
b. 模块和应用的数据手册以及问题报告的汇总；
c. 安装的过程、用户指南、接口规范等。

4.7.6.2 后续认可与综合的数据

当对要重用的模块和应用进行综合时，要认可后续IMA系统的认证申请人、模块/应用开发者或系统综合者应该开发下列数据：

a. 后续认可和综合的生命周期数据（包括要重用的模块和应用）要得到开发，以符合后续安装和本指南所适用的认证需求；

b. V&V的记录应该包括评审、分析和测试(验证和确认)所产生的结果，这些评审、分析和测试是针对重新综合到后续IMA平台、系统和飞机配置中的模块和应用所进行，包括使用领域范围的分析。使用领域范围的分析包括以下内容：

－对于由综合者要进行的后续使用、安装配置和V&V ，由模块或应用的开发者所做出的假设；

－在后续平台、系统和安装配置中，对模块和应用进行重用的影响分析；

－后续系统对模块和应用的影响分析；

－对后续系统综合的接口分析，要与模块或应用的使用领域和接口规范一致。

第5章　综合支持过程

5.1 安全性评估

由于IMA系统固有的高度集成性，建议认证申请人使用ARP 4754/ED-79(参考资料[7])和ARP 4761(参考资料[8])或可接受的替代过程。该过程至少需要考虑以下内容：

a. 能避免低级失效状态严酷度的功能对安全关键功能产生影响的隔离、分离和相互独立措施(例如，分区隔离、资源管理、故障管理与抑制)；

b. 为防止可能同时对多个功能产生不利影响的单点故障和可预见的失效组合而采取的保护措施(如，独立性、冗余、健康监控和故障管理以及安全性监控)；

c. 在飞机级和IMA系统级上（认证申请人）应该进行初步的FHA分析，以评估IMA架构的预期功能、特性和能力；

d. 检查IMA平台的架构设计和与安全性有关的能力，以及对飞机功能分配和宿主应用所施加的限制条件，例如，对应用的独立性、分区隔离、保护、冗余、所需资源、接口通信、性能、网络访问和/或连到飞机传感器和作动器上的专门连接等所要产生的需求。这些检查的结果应该作为IMA的PSSA；

e. 对IMA平台行为方面的检查，包括对由平台提供的诸如健康监控、资源管理和故障管理能力方面的详细描述，以及对可用的失效恢复或抑制的类型的详细描述；

f. IMA平台的性能细节检查，以确保它能满足所宿主应用的性能需求；

尽管单一的利益相关方可能有能力进行上述所有活动，但还是希望将这些活动分配给多个利益相关方来完成。下面几节给出一种典型的责任分配。

5.1.1　认证申请人的职责

认证申请人负责飞机级的系统安全性评估过程，并确保IMA系统、平台、模块和宿主应用满足飞机的安全性、完整性和可靠性需求。认证申请人负责整合IMA系统综合者、平台和模块的开发者以及应用开发者所进行的IMA系统安全性评估的结果，并确保他们的SSA结果符合飞机的安全性评估。

认证申请人应解决以下问题：

a. 在IMA系统和飞机其它系统之间的单一失效与组合失效；

b. 共因和级联失效(参见第5.1.5.4节)；

c. 能证明符合飞机适用规章、操作和持续适航的特定IMA的SSA结果所具有的影响；

d. 网络的信息安全；

e. 其它相关的任何安全性数据。

5.1.2 IMA系统综合者的职责

IMA系统的综合者负责将IMA平台、模块和应用的供应商所做的系统安全性评估结果进行整合，并确保他们的SSA结果与IMA的SSA一致且兼容。作为综合与V&V过程的一部分，IMA系统的综合者应确保IMA系统组件的行为及与安全性相关的属性要与IMA的SSA需求一致。这一过程应包括通过测试平台和系统的资源管理、健康监控、故障管理以及其它保护特性(如，冗余管理、交叉通道比较器、（失效）恢复策略)来验证PSSA/SSA的结果，并应该在多个综合等级上进行。

5.1.3 IMA平台供应商的职责

IMA平台的供应商应进行详细的平台安全性评估。这种评估的结果应该用于第5.1.1节、第5.1.2节和第5.1.4节的整合与综合中。这些分析应该检查IMA平台的特定特性与能力，以支持宿主应用、IMA系统和飞机的安装，这包括由平台提供的健壮分区隔离、资源管理、健康监控、故障管理、输入/输出(网络通信)、性能和架构与保护的其它特性。

IMA平台的供应商负责IMA平台的共模失效分析，这种共模失效分析应该与支持IMA系统级和飞机级安全性分析的应用开发者和IMA系统综合者协同进行。

平台的安全性评估数据、资源管理的保证以及故障管理和健康监控的特性，在其它的利益相关方使用它们进行应用的安全性评估、IMA系统的安全性评估和飞机的安全性评估时，应该是可用的。

为了完成IMA平台的安全性评估任务，平台的供应商可能需要汇集来自多个组件或模块开发者的输入数据。

5.1.4 应用供应商的职责

应用供应商应该对应用进行详细的PSSA，并规定该应用的安全特性、性能和接口需求。作为PSSA的一部分，他们还应该规定这样一些假设：应用是在其要宿主的平台上产生的，以及应用对资源管理、健康监控、故障管理、失效响应等方面的需求。在后续的IMA系统级别和飞机级别的安全性评估中，作为活动的一部分，要验证这些假设和需求。PSSA的结果将用于整合、评估和综合的活动中(见第5.1.2节、第5.1.3节和第5.1.5.3节)。

应用供应商应该确保应用的行为与特性符合特定系统与飞机的安全性需求。

5.1.5 安全性评估活动

下列的安全性评估活动应该在IMA系统开发的多个不同阶段中进行。

5.1.5.1 功能危害性评估 (FHA)

IMA系统的预期功能对飞机安全性的影响应该得到确定和评价。FHA应该在飞机级别

和系统级别上进行，以确定和区分由IMA系统提供的每项功能在功能丧失和故障情况下所产生的相关失效状态与影响。与多个功能（由IMA系统提供的）同时丧失或故障有关的危害也应该得到确定和分类。另外，IMA系统（提供）功能的丧失和故障应该结合与飞机和发动机有关的其它功能丧失和故障进行处理，以确保解决共模失效的问题(见ARP-4754/ED-79的第6.1节, 参考资料[7])。

5.1.5.2 初步系统安全性评估(PSSA)

a. 基于由FHA确定的失效状态分类，对IMA系统组件所提出的设计与架构应该由PSSA进行评估，以确定FHA所确定的系统开发保证等级和安全性需求能够得到实现；

b. PSSA应该确定IMA系统所需要的（余度）数量、隔离和独立特性、软件级别、硬件设计保证等级以及各组件的可靠性，这些组件包括用来保护飞机不受随机硬件失效影响的供电电源、通信接口、显示和控制。为了保护飞机和发动机免受失效和组合失效以及各个组件中软硬件设计错误影响所必须的系统开发保证等级应该得到确定。除非已经提供了保护IMA机箱或机架(或其它放置在一起的模块)不受共因失效(如电气着火)影响的措施，否则由单个IMA机箱或机架(或其它放置在一起的模块)所提供的所有功能，都应视为在出现单点失效时将失效。所有使用单个硬件单元的功能都应视为在出现单点失效或失效组合时将失效。PSSA应确定适用于飞机型号的失效-安全技术和容错需求。当处理失效或其它事件时，因它们引起的或级联的影响也应得到处理；

c. 对于符合FHA需求的所有平台所提供的软件和宿主的软件应用都应确定软件等级；

d. 对于符合FHA需求的所有平台要提供的和专用的硬件设备都应确定硬件设计保证等级；

e. PSSA应对硬件和软件组件确定特定的安全性需求，包括失效抑制、分区隔离、独立性、冗余、健康监控等，并要确定特定的验证策略(见ARP- 4754/ED-79的第6.2节，参考资料[7])

5.1.5.3 系统安全性评估(SSA)

对于要安装到飞机上的IMA系统的宿主应用，应该进行系统的、完整的评估，以证明在PSSA中所确定的相关安全性需求已经得到满足。这种评估可能包括（实验室）基准测试、（机上）地面试验和飞行试验，以确保在PSSA中所作的假设是正确的并能得到确认。当要安装整个系统时，SSA通过综合许多不同分析和测试的结果来验证整个系统的安全性。SSA应该按照ARP 4761 (参考资料[8])中所描述的内容进行。典型的SSA包括：

a. 系统描述，包括功能和接口；

b. 失效状态的列表；

c. 每个失效状态的分类；
d. 每个失效状态的定性分析；
e. 每个失效状态的定量分析，如果需要的话；
f. 共因分析的结果；
g. 确认对能够影响多个系统的任何级联失效和/或单点失效都已得到解决；
h. 在适当时，能够证实飞行机组能识别并响应失效状态的实验室测试、仿真器测试和飞机试验的程序与结果；
i. 对防止较低完整性功能的任何失效模式对较高完整性（更关键）功能造成不利影响的验证；
j. 对所有软件已按照PSSA所确定的适当软件等级完成开发的确认；
k. 对CEH已按照PSSA所确定的硬件设计保证等级完成开发的确认；
l. 对所有安全性相关的软硬件需求已得到正确实现的验证(见ARP-4754/ED-79的第6.3节，参考资料[7])。

5.1.5.4 IMA系统的共因分析

对于IMA系统，在多个飞机级功能和宿主应用之间有资源共享的地方（这些功能和宿主应用在概念（原理）上是独立的），需要在飞机级进行共因分析(CCA)，因为某一单个原因事件就能直接(或间接)地同时引起多种不利影响。另外，级联失效是这种分析的一部分。

CCA的方法不需要改变传统的做法，但要将其使用到飞机系统分层结构的更高级别上。这种方法现在应该用于由IMA系统及其组件实现的一组系统(以及它们要执行的飞机功能)。这就是说，这些分析需要由认证申请人进行，而不是由IMA系统综合者、平台开发者或应用开发者进行。这种分析在IMA系统的配置最后确定时就应该进行，且在初始认证后如果要有新的功能加入到IMA系统，就需要重复进行这种分析。这种分析还包括传统的余度系统分析，这些余度系统可以全部或部分地由IMA系统实现。

CCA要包括下面这三种分析(见ARP-4754/ED-79，参考资料[7]和ARP-4761，参考资料[8])：

a. 共模失效分析；
b. 特殊风险分析；
c. 区域（Zonal）安全性分析。

5.1.5.5 失效模式分析

本节讨论的内容有通用IMA平台组件的分析、有这些分析产生的所期望的数据类型、以及在应用级、平台级、IMA系统综合级以及飞机级上的综合结果。这些综合活动要能够

证明IMA系统的安全性。较高级别的分析应该基于较低级别的分析结果。

5.1.5.5.1 IMA组件的失效模式分析

对IMA组件(模块、平台、资源)的分析能确定组件的失效模式对宿主应用、其它IMA模块、平台、IMA系统与飞机和/或发动机（产生）的影响。为了完成这种分析，就要确定这些组件的失效，并要确定这些失效是如何显现出来的。换句话说，在已知失效状态或原因事件的情况下，组件如何偏离其所需操作或预期功能，以及对其它模块、宿主应用、IMA系统和飞机功能造成什么样的影响。

对于随机失效，通常是通过评估一些元器件失效、确定失效对组件操作的影响来完成分析工作。在有些情况下，这些影响有可能简单地从组件边界观察到，但如果应用或其它组件与该组件有内在的交互关系，则这种影响就应该在这些接口边界上确定。对于那些能给其它多个组件或应用提供共用服务或资源的组件，接口边界是很难隔离的，且很难确定对他们的潜在影响。对于有原因的事件，失效和影响（分析）的重点只需要针对那些对于原因事件比较脆弱的组件。

在有些情况下，在元器件级别的组件上是无法开始进行这种分析的，因为在这个级别上缺乏可见性(如，货架式电源调整模块)。对于这些情况，对组件和它们的失效模式应给出最坏的假设(如，功能丧失、非预期的功能)。

没有在宿主应用或飞机上使用组件的知识，就很难确定失效的影响。为了估计失效的严重程度，对于可能的安装和使用情况要做出假设。在这一级别上所作的假设和确定的失效模式应该作为输入提供给下一级别的分析。

5.1.5.5.2 IMA平台的失效模式分析

在分析IMA平台时，是在没有应用的情况下，把IMA模块和组件结合在一起进行的。此时对单个IMA组件的失效模式与影响分析是在平台架构与接口的范围内进行的，以便确定它们（这些失效模式与影响）在平台边界上是如何显现出来的。由于是与组件一起分析，所以分析的重点是平台如何随组件所给定的行为而变化。

由于大多数宿主应用都要与平台内部的组件进行交互，在内部接口上的这些影响也应得到确认和评估。另外，由共享资源丧失或降级引起的失效也应该在这种分析中得到评估。

5.1.5.5.3 应用的失效模式分析

应用的失效模式分析要考虑每个单独的应用，如果有任何的不属于平台的硬件，但却支持某个宿主应用，则应该使用类似于第5.1.5.5.1节中所描述的方式对该硬件进行分析。差别只是宿主应用通常有一部分飞机FHA与它们有关(至少是那些提供飞机级功能的应用)，且能确定出更好（的方法）分析这些组件失效影响的严酷度。

对每个应用都应该在目标平台和架构范围内且不受其它的宿主应用影响的情况谢进行评估。对应用和平台的失效模式都应该进行分析，以确定它们如何在应用的边界上显现出来的，即，该应用是如何偏离其预期功能和性能的。如果每个应用和其它应用在功能上都是独立的，则只需要对边界上的影响进行分析。

注意：如果这些应用在功能上不是独立的，则就要对它们的相关性和接口进行分析，以确定失效的组合与级联失效。

5.1.5.5.4 IMA系统的失效模式分析

该活动就是将以前的分析作为输入（对组件、模块、平台和应用）来分析IMA系统的失效模式，该分析的结果成为飞机级失效模式分析的输入。

IMA系统失效模式的分析，要考虑宿主应用间的交互关系以及与其它应用和平台共享资源及IMA系统的耦合。应用间的交互应该包括应用与共享资源之间的正常影响和非预期的影响。应检查应用与资源的单个和多个失效，并应确定IMA系统级的失效影响。

如果某个IMA系统是由多个平台组成的，则这些平台之间可能的交互关系也应该得到检查，且失效模式要被确定。

5.1.5.5.5 飞机级的失效模式分析

组件、宿主应用、IMA平台和IMA系统的失效模式分析结果要用于飞机级的失效模式分析。正是这个分析最后来整合所有来自低级分析所预测的失效影响和模式，并要确定这些分析对IMA系统在飞机上的安装与操作是适合的。在飞机级的失效模式分析中，对低级分析中任何错误的假设都应该检测出来并对其更正。另外，应该在飞机级处理IMA系统与飞机其它系统间的交互关系。

5.1.5.6 故障管理、健康监控和余度管理

在第3.6节中谈到的故障管理、健康监控和余度管理应该在设计中实现，并应该在安全性评估过程中考虑。这些功能的失效模式应该在平台和系统的失效模式分析中得到处理，并尽可能地在飞机级的失效模式分析中进行处理。

5.1.5.7 分区隔离分析

分区隔离分析应该作为输入提供给失效分析，以及平台和系统的失效模式分析中所涉及的分区隔离冲突失效模式。第3.5.2节就这一分析提供了特定的指南。

5.1.5.8 网络信息安全

IMA系统中网络信息安全的漏洞会对飞机安全带来不利影响。因此，IMA系统中网络信息安全的失效模式，应该作为飞机级安全评估的一部分进行处理。威胁网络信息安全的实例有：数据内容的完整性(数据值受到更改)、数据源的完整性(假的数据源)以及数据延迟与其它拒绝服务的攻击。本文件可以与其它指南材料结合起来，用于解决网络信息安全的认证问题。

5.2 系统开发的保证

本节描述系统开发保证的关键方面，主要包括有软件指南、硬件设计保证、共享的设计保证、IMA系统的配置管理和环境鉴定。

5.2.1 软件指南

用于IMA系统的软件应该使用DO-178/ED-12 (参考资料[2])指南进行开发，或者遵照与软件等级相适应的其它符合性的方法进行开发。当考虑IMA系统的关键软件认证时，要关注认证的政策与指南，如软件的重用、用户可修改的软件、现场可加载的软件和数据库的完整性。另外，特定的飞机型号项目可以有附加的软件政策或指南，能适用于IMA系统的安装。

5.2.2 电子硬件指南

如果IMA系统包含有CEH器件，其功能不能通过测试和/或分析进行完全地验证，则这种CEH器件就应使用DO-254/ED-80 (参考资料[6])指南进行开发，或遵照与硬件设计保证等级相适应的其它符合性的方法进行开发。当考虑IMA系统的关键硬件认证时，要关注认证的政策与指南，如现场可加载的硬件、环境鉴定试验、硬件模块认可、飞机的个性模块、硬件配置文件等。另外，特定的飞机型号项目可以有附加的硬件政策与指南，能适用于IMA系统的安装。

在IMA系统中可以使用现场可修改的硬件；例如，可编程逻辑器件可以通过外部的方式进行修改。针对这种实现情况，由于DO-254/ED- 80 (参考资料[6])目前还没有给出指南，因此，目前可以使用现场可加载软件的指南(例如，DO-178B/ED- 12B的第2.4节和第2.5节，参考资料[2])。

5.2.3 综合工具鉴定

DO-178/ED-12 (参考资料[2])和DO-254/ED-80 (参考资料[6]) 分别对用于软件和硬件开发的验证工具和开发工具提供了指南，在IMA系统的开发中可以增加用于综合的工具，例如，用于以下方面的工具：

a. 生成和/或验证配置文件与资源分配；

b. 建立和验证分区隔离的保护以及IMA系统的其它安全性和保护特性，如，冗余管理、（失效）恢复、健康监控、故障管理、飞行机组告警，等；

c. 验证IMA系统的配置、平台内部和平台之间数据通信；

d. 验证（IMA系统）与飞机其它系统和传感器接口的正确使用。

对综合工具应该进行评估，以确定它是开发工具（产生IMA系统中某个项目），还是验证工具（验证将在IMA系统实现的某个项目）；如果工具的输出不能完全被验证，就需要对它进行验证。工具鉴定的方法应该基于DO-178/ED-12 (参考资料[2]) 的第12.2节。

5.2.4 共享的设计保证

在IMA系统中，模块的设计保证很可能依赖于另一个组织开发的其它模块的设计保证活动。这种完成设计保证目标的方法将取决于各利益相关方之间的合同关系。各种计划(如，MAP、PSAC、PHAC)应阐述用来证明达到设计保证目标的方法，包括公共的责任。

5.2.5 IMA系统的配置管理

在第3.7节中对IMA系统的配置管理提供了指南，配置管理方法应该得到系统安全性评估过程和适用的生命周期数据的支持 (如，软件需求、设计，等)、并得到验证和确认；配置与变更受到控制。

5.2.6 环境鉴定试验(EQT)

IMA系统的灵活性和可重构特性会导致有大量的软硬件配置需要进行环境鉴定试验。这种配置的灵活性以及能对不含宿主应用的硬件模块进行环境鉴定试验（EQT）的要求，是IMA系统和硬件环境鉴定区别于联合式系统EQT的主要方面。要把EQT扩展到多低的层次上进行主要取决于模块的特定情况以及它们的安装环境。IMA系统模块和硬件的EQT应该在DO-160/ED-14(参考资料[1]，或其它可接受的方法)所定义的适当等级上进行，这种等级由假设或预期的飞机安装和操作环境确定。

以下的指南概括描述了一些要讨论的重点。IMA平台的开发者和/或系统综合者应该编制一个完整的EQT计划，确定如何进行环境鉴定试验，以及通过/失败的准则，该计划应该得到认证申请人的工程批准。

能在模块级别上取得的环境鉴定信任取决于：

－模块所处环境的定义(这种环境应该涉及所期望的模块组合以及它们对环境的影响和对飞机环境的影响)；

－模块可能对其环境产生的影响的定义；

－模块对特殊事件的反应的定义，如HIRF与闪电(使用这些模块的IMA系统应该设计

成可以适当地适应这些已规定的模块反应)。

模块级的环境鉴定不能代替在更高综合级别上进行的更进一步鉴定；然而，在更高综合级别上的环境鉴定应该确认施加在单个模块上的一部分环境需求。如果适用的话，应用供应商应该证明应用在考虑模块反应的环境条件下的行为是可以接受的，这种模块反应既可以在MRS中定义也可以在模块的用户指南中定义。另外，IMA平台(包括在EQT期间的状态)的特殊行为应该是可用的，以允许宿主应用的开发者针对平台的反应进行设计。如果这些反应在MRS中得到了适当的规定，则这些应用就能根据那些性能特征进行设计，而不需要知道能产生这种反应的环境条件。

以下描述的是硬件模块的环境鉴定试验指南：

a. 硬件模块开发者应该规定所假设的或所预期的环境，并规定适用的DO-160/ED-14(参考资料[1])环境试验类别与等级，如果需要的话，要用附加的需求进行补充，这样试验就能代表所期望的状态，这种状态就是模块在实际飞机安装上所要承受的；

b. 针对DO-160/ED-14中每项适用的试验程序，开发者应该规定出模块的性能需求。如果适用的话，开发者可以这样选择：规定一组不同的通过和/或失败准则，和/或环境极限的试验容差。一旦规定了适用的DO-160/ED-14试验条件和类别，硬件模块开发者就应该编写EQT计划，按照此计划进行相关试验。在试验过程中，有必要组合多个模块，以便与实际环境和操作条件更为接近；

c. 如果开发者想要按多种类别的EQT来鉴定某一硬件模块，则对于这些类别，所有适用的试验都应进行；

d. 模块和平台的配置应该包括相应的电气和结构接口的连接器，包含防护套、后附件（back shells）和应力支架（strain relief），预期要用的机箱或机架以及各种模块。设备配置应该包括由DO-160/ED-14中安装程序中所规定的连接导线和电缆；

e. 如果硬件模块能够使用执行飞机功能的软件或宿主的软件应用进行加载，则开发者就应该使用宿主应用软件或专用测试软件来证明硬件模块功能的正确运行。开发者应该验证、确认和控制模块和软件的配置，以确保测试的有效性；

f. 有些开发者可能愿意使用最坏情况下的环境鉴定试验来鉴定有多种安装情况的模块。这样的方式要向认证机构建议。然而，试验结果与各种限制都要用文档完整地记录，这样，当模块使用于所要的安装时，后来的用户和认证机构就能判定试验的有效性；

g. 用于IMA系统的数据总线，可能有特殊的电磁兼容性要求，这种特殊的电磁兼容性取决于数据总线对脉冲的上升时间、总线速率、总线拓扑以及互联方案（等方面）的规范。这些关注点和各种环境影响都可能是共模失效的来源，当适用时，应该在EQT计划中予以描述。

5.3 确认

确认过程应确保IMA系统的需求是正确的和完整的。本节对IMA系统的确认提供了一个框架，并对ARP-4754/ED-79(参考资料[7])提供补充。

确认的目标是：

a. 确保所有级别上IMA系统的需求都正确和完整的，包括模块、宿主应用、平台和IMA系统的需求。在这种分层结构中的各级需求，应该在确认下一低层需求前得到确认；

b. 评估IMA系统的架构和宿主应用的功能分配；

c. 依据处理器能力和使用（情况）、存储器分配、I/O设备与总线以及其它共享资源，确保分区隔离的保护是健壮的。确保冗余、资源管理、健康监控和故障管理的需求对整个IMA系统都是正确的和完整的；

d. 确保每个宿主在IMA系统上的应用符合安全性、完整性和可靠性的需求；

e. 评估模块和应用之间的数据耦合与控制耦合；

f. 确保考虑了正常操作与降级操作的情况、识别了这些操作对飞机安全性的潜在影响。

表5给出不同任务中确认活动的分配情况的示例

表5 典型确认活动概述

任务	确认活动(需要确认的款项)
1－模块和/或平台的确认	－IMA平台的需求对IMA核心软件和模块的分配 －健壮分区隔离需求 －确定性需求
2－应用的确认	－将应用分配到飞机功能上 －对专用硬件（专用资源）和软件的需求功能分配
3－IMA系统级的确认	－将IMA系统的需求分配到IMA平台和平台上的各宿主应用 －将应用分配到IMA处理器上 －IMA资源分配给应用 －I/O需求分配到IMA资源
4－飞机级的确认	－确认从飞机级需求分配给IMA系统的需求

在IMA平台情况下，可能有这样一种情形，IMA平台的需求产生于一组基于对飞机认识的通用需求和假设，然后，将该平台用于特定的飞机上。这时IMA平台的通用需求与假设应该根据实际飞机的需求进行追踪并确认，以完成对IMA系统需求的确认。

5.4 验证

验证过程应该确保对IMA系统特定需求的实现已经得到满足。本节提供了一个IMA系统验证的框架，并对ARP-4754/ED-79(参考资料[7])提供补充。

验证的目标就是确保在所有级别上的需求都正确地、完整地得到实现，以及能保证这点的措施是正确的。验证过程要确保在所有级别上的需求都是完整的、可追踪的、准确的、

可验证的和无歧意的。验证最初可以在一个模拟的、有代表性的目标机和环境上进行(在开发中当平台可用时，通常要确保它会正常工作)；然而，要是没有在目标平台上进行验证，验证活动就不能算是完整的。在应用和平台同时都处于开发的情况下，在获得目标平台之前，（普遍）认为应用起初可以按照DO-178/ED-12 (参考资料[2])所描述的验证过程在某个“宿主宿主”计算机（模拟器）环境上进行。在这种情况下，如果开发者能证实这些验证程序和结果对于目标机和环境是有效的话，可以作为整个验证过程的部分认可信任加以承认。

表6给出在各种任务中分配的验证活动示例。

表6　典型的验证活动概述

任务	验证活动(要验证的项目)
1－模块和/或平台的验证	● 模块的实现符合其物理的要求、安装要求、功能要求、性能要求接口(API)要求以及与安全性有关的要求； ● 模块与核心软件当综合后形成一个平台时，要符合平台的需求； ● 适当时，平台的物理特性； ● 平台的特性，包括服务(API)例如，健壮分区隔离、网络服务、数据通信、资源管理、健康监控、故障管理等； ● 平台为宿主应用提供保护共享资源的能力； ● 平台的配置，以及维护和验证配置的方法。
2－宿主应用的验证	● 在目标模块和平台中，应用满足其所有的需求； ● 应用的配置； ● 应用正确地使用其所分配到的共享资源。
3－IMA系统级的验证	● 在目标平台和系统上，应用都满足它们的需求； ● 模块、平台和宿主应用的配置，以及维护这些配置的方法； ● 模块、平台和宿主应用的共享资源分配； ● 各应用之间、模块资源和应用之间、模块之间以及平台之间的接口与交互关系； ● 当平台综合后形成IMA系统时，平台实现满足IMA系统的需求； ● IMA系统的功能与性能 ● 正常和异常（降级）模式下的IMA系统行为； ● 要综合的应用、模块和他们的平台，以及共享资源的分配，包括功能的交互、内部的通信过程、时间的相互影响，等； ● IMA系统的最终配置，以及维护该配置的方法。
4－飞机级IMA系统的验证	● 在飞机上所安装的IMA系统满足其需求； ● IMA系统的物理特性； ● IMA系统与飞机其它系统的交互与接口； ● 正常和异常（降级）模式下的IMA系统行为； ● (可由地面和飞行试验验证的)飞机的功能、性能和安全性需求。

5.5　配置管理

本节讨论IMA系统生命周期数据和生命周期环境的配置管理(CM)。要安装的IMA系统的CM已在第3.7节和第5.2.5节中讨论过。

IMA系统的生命周期应该管理和维护（以下内容）：

a. 组件、模块、资源、平台、宿主应用和IMA系统的配置；

b. 生命周期数据；以及

c. 用于开发、验证和确认IMA系统的工具和环境。

DO-178/ED-12 (参考资料[2]) 规定了软件(例如，核心服务与宿主应用)的CM指南，并应该用于IMA系统中的软件。DO-254/ED-80 (参考资料[6]) 规定了电子硬件的CM指南，并应该用于IMA系统中的电子硬件。按照ARP-4754/ED-79（的要求）应该实现一种适当的CM过程，用于管理模块、平台、资源和整个IMA系统。

5.5.1 IMA系统的配置管理计划

应该开发IMA系统的配置管理计划(IMASCMP)，并应描述用于IMA系统的配置管理过程、程序和活动，适用于系统所要求的开发保证等级，以证明其符合性。IMASCMP应该定义：处于配置管理之下的通用配置项(例如，模块、资源、平台、接口、宿主应用、数据库、配置文件、数据，等)，如何在受控下更改这些配置项，以及IMA系统的配置纪实方法（这种方法在整个生命周期的特定里程碑节点上，将用于定义IMA系统配置的基线）。CM计划可以编制一个或多个，以管理IMA系统的多种组件（构成）：模块、资源、应用、平台、IMA系统和飞机的安装。 另一种选择就是使用一个联合计划来管理所有的组件。

IMASCMP至少应该包括以下内容：

a. 简要描述要实施CM过程的IMA系统；

b. 简要描述要用于IMA系统和安装的CM过程组织，各个利益相关方的角色与责任、在CM下（管理）的数据、数据的组织、供应商控制以及与其它实体（机构）的接口；

c. 简要描述要使用的CM环境，包括程序、工具、方法、标准、组织责任和接口；

d. 简要描述CM过程的活动，如配置标识、基线、追踪、配置控制、更改管理、状态纪实、配置索引生成、存档和恢复过程，等；

e. CM过程中的转换准则；

f. 简要描述由CM过程产生的数据，包括CM记录、控制类别、IMA的配置索引和IMA生命周期环境的配置索引；

g. 简要描述IMA系统在整个服务生命周期的开发、安装、服务和维护活动中，模块、资源、平台、应用、接口、IMA系统和飞机安装的CM和控制是如何进行维护的；

h. 简要描述健壮的和易于维护的验证方法，这种方法要能验证安装在飞机上的IMA系统配置就是已批准的符合型号设计的配置，特别是对认证后的修改。

5.5.2 配置控制

生命周期数据要确定为两类中的一类：控制类别1(CC1)和控制类别2(CC2)。CC1和CC2

指施加于生命周期数据的配置管理控制。CC2的目标是CC1目标的子集，软件的CC1和CC2定义在DO-178B/ED-12B的第7.3节表7-1中描述。在DO-254/ED-80的第7.3节表7-1中，也有涉及硬件的控制类别1和2 (HC1和HC2)。下面的表7简要说明CC1和CC2的定义。IMA系统的生命周期数据应受到相应的配置管理控制，并应该在IMASCMP中予以描述。在附录A的表中为IMA的生命周期数据提供了通用的CC1/CC2指南。对于有些系统(如，低级别的系统)，如果在IMASCMP中证明是合适的，配置的控制量级可以不太严格。

表7 CC1/CC2 的定义

CM 过程目标	CC1	CC2
配置标识	x	x
基线	x	
追踪性	x	x
问题报告（机制）	x	
更改控制——完整性与标识	x	x
更改控制——追踪	x	
更改评审[3]	x	
配置状态纪实[3]	x	
恢复	x	x
防止未授权的更改	x	x
介质的选择、更新、复制	x	
发布	x	
数据存放保持	x	x

（[3] 这些术语与DO-254/ED-80和DO-178B/ED-12B有微小差异.）

5.6 质量保证(QA)

高度综合与复杂的系统，像IMA系统，对开发错误和不希望或非预期影响的产生创造了很多机会。同时，要为IMA系统开发出有限的测试集，确证没有一点开发错误存在，是不现实的。由于这些错误通常是不可测量的，且也得不到适当的数值方法来刻画这些错误，因此，应该使用其它定性的方法来确定IMA系统能满足规章要求和安全性与功能要求，这种方法对于由设计错误引起不可接受事件发生的可能性应最小。因此，对于高度综合与复杂系统来说，就是依靠开发保证来减少在系统中的错误可能性。

按照ARP-4754/ED-79（的要求），对系统中的模块和IMA系统都应该实施质量保证。QA人员负责监控开发过程，以确保：

a. 已批准的计划、标准、手段和程序要得到遵循；
b. 适当的生命周期数据已产生；以及
c. 最终的IMA系统已使用结构化的、严格的过程（这种过程符合IMA系统的开发保证等级要求）开发完成并得到验证。

DO-178/ED-12 (参考资料[2])确定软件的QA需求，并应该用于IMA系统中的软件。DO-254/ED-80 (参考资料[6]) 确定电子硬件的过程保证需求，并应该用于IMA系统中的电子硬件。QA过程应该确保所执行的开发和验证活动符合已批准的计划、标准和程序。QA过程应该涉及IMA系统开发的所有级别(如，模块、平台、应用、IMA系统和飞机级安装)。

IMA系统质量保证计划(IMASQAP)应该得到开发（编制），并应该描述用于IMA系统的质量和过程保证的方法与活动，这些方法与活动要与系统开发的保证级别相适应，并要证实符合（过程要求）。可以编制一个或多个CM计划以处理多个级别的系统开发，或者使用一个联合的计划来处理IMA系统开发的所有级别。

IMASQAP至少应该包括：

a. QA的环境描述，包括（工作）范围、组织职责与接口、标准、程序、工具和方法；
b. QA权力、责任与独立性说明，包括IMA系统组件的批准权力。应给予QA一定等级的独立性以便于其行使强制执法的权力；
c. 要执行的QA活动，包括QA的方法、QA介入的证据、QA记录的准备、（阶段）转换准则，等；
d. 评估和实施纠正的过程；
e. 由QA过程产生的记录定义。

注意：“质量保证”在DO- 254/ED-80（参考资料[6])和ARP-4754/ED-79 (参考资料[7])中称为“过程保证”

5.7 认证联络

5.7.1 认证联络过程

在IMA系统的整个生命周期中，认证联络过程就是在认证申请人和认证机构之间建立沟通联络与相互了解，以支持认可和认证过程。

本文件自始至终描述生命周期数据的典型内容，但应该注意，生命周期数据可以根据工程项目进行适当的打包并给出标题，但要包括本文件所描述的内容。如果要更换标题或重新打包，则该利益相关方应该开发出一套生命周期的映射数据，它能够证明所有适用的数据都是可以获得。

5.7.2 符合性方法与策划的数据

为了实施认证联络过程，认证申请人要提出一套符合性方法，这种方法要能定义IMA的开发是如何满足认证基础的。IMASCP (见第4.4.3节和第4.5.3节)、模块认可计划(见第4.2.3节)、PSAC和 PHAC都确定了相关IMA系统所建议的符合性方法的部分内容。这些计划也描述系统开发的保证级别、软件级别、硬件级别以及环境鉴定试验的级别，就像系统安全

性评估过程以及计划要安装的环境与飞机所确定下来的一样。认证申请人应该：

a. 当更改影响最小时，也就是说，当更改影响可以控制在项目限制的范围内时，在评审点上要及时地向认证机构提交IMASCP、IMASQAP、PSAC、PHAC、EQT计划和其它所要求的数据；
b. 解决由认证机构所确定的有关所提出（建议）的符合性方法以及IMA认证计划的问题；
c. 获得认证机构对IMASCP、IMASQAP、PSAC、PHAC、EQT计划、飞行试验计划和其它计划的（认同）批准。

图5说明了典型的策划数据。

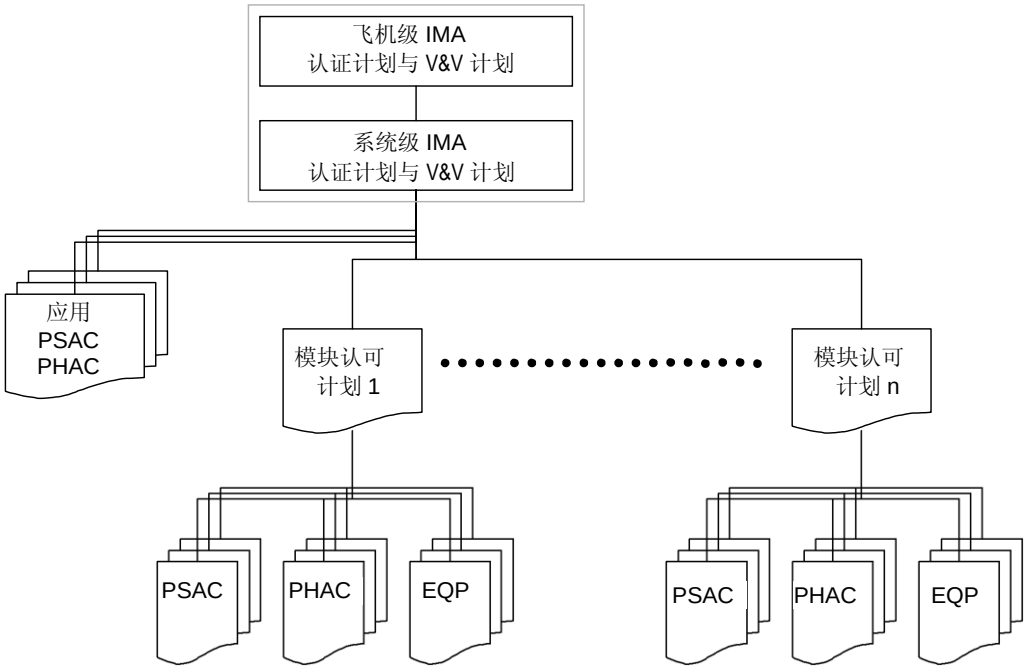


图5　IMA系统的计划数据

5.7.3　开发（过程）的生命周期数据

IMA系统开发以及安装到飞机上的整个生命周期数据都要得到开发。在认证机构需要时，都要能得到这些数据：

a. 模块认可数据(见第4.2.2节到第4.2.12节)，包括所有的MRS、模块的V&V结果、模块的QA记录、模块的CM记录、模块的问题报告和附加的模块认可数据(见第4.2.12节)；
b. 宿主应用的数据(见第4.3.2节)；
c. IMA系统的数据(见第4.4.2节到第4.4.7节)；
d. 飞机级IMA系统综合的数据(见第4.5.2节到第4.5.7节)。

图6 给出了IMA系统生命周期数据的概况，所有数据认证机构都要能够获得。表8说明了要提交给认证机构的生命周期数据。

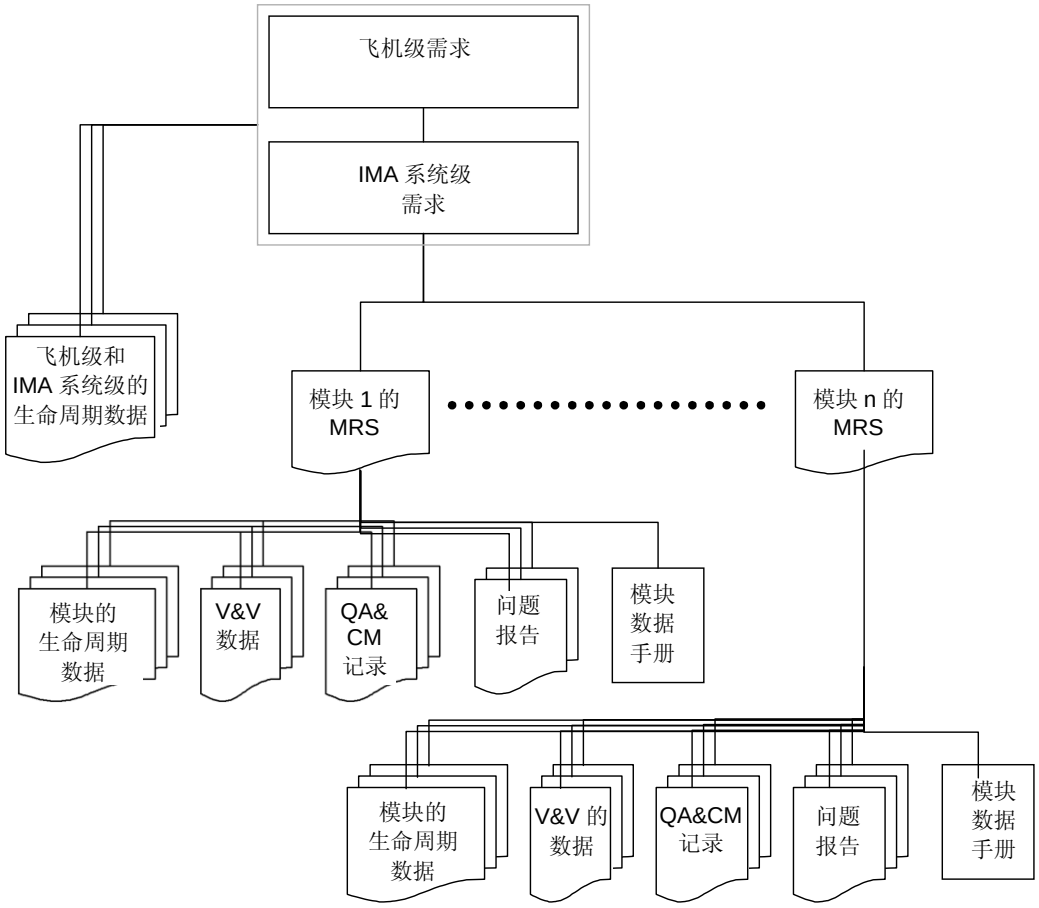


图6 IMA系统的生命周期数据

5.7.4 符合性的证明

认证申请人要提供IMA系统开发过程满足计划的证据，并应证明飞机和所安装的IMA系统符合所有适用的规章。认证机构的评审可以在认证申请人或开发者所在地进行，这些评审可以包括与认证申请人或其开发者之间的讨论。认证申请人安排生命周期过程中的评审活动，且当需要时，要提供IMA系统的生命周期数据。认证申请人应该：

a. 解决认证机构评审提出的问题；

b. 向认证机构提交系统级和/或飞机级IMA系统的完成总结（报告）、MAAS、SAS、HAS、模块的认可数据手册、MCI、SCI、HCI (即顶层图)、EQT报告、飞机安装数据、飞机地面和飞行试验结果以及飞机级和/或系统级IMA系统的配置索引(可以包括在符合性报告中)等。支持模块、平台和宿主应用的数据应该在IMA系统的符合性（情况）中描述；

c. 向认证机构提交或使认证机构可以得到认证机构所需要的其它符合性数据或证据。

图7说明了典型的符合性数据树。

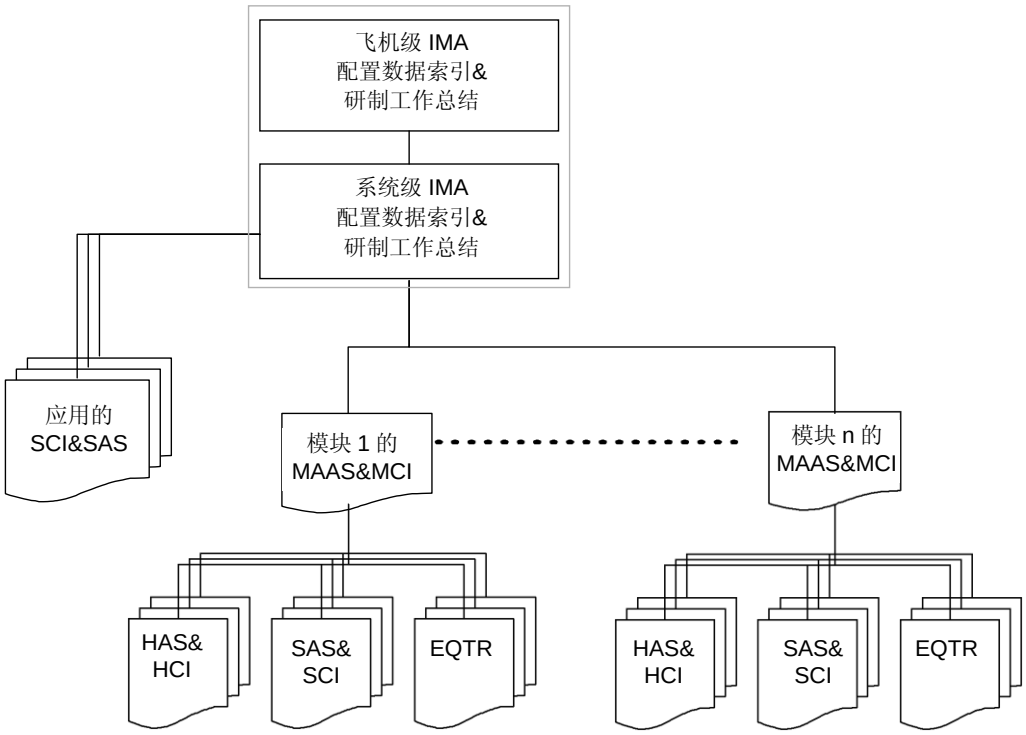


图7　IMA的符合性总结

5.7.5　生命周期数据的提交

表8总结了要提交给认证机构的IMA系统典型生命周期数据。这些数据项，在适当时，可以混合和/或分布在多个文档中，并应在高层的IMA系统认证计划中作出规定。当需要时，认证机构可以要求（提交）附加的数据。

表8　要提交给认证机构的生命周期数据

生命周期数据项目	参考	任务1	任务2	任务3	任务4
模块认可计划(MAP)	4.2.3	X			
模块配置索引 (MCI)	4.2.7	X			
模块认可完成总结（报告）(MAAS)	4.2.9	X			
模块认可数据手册	4.2.10	X			
软件的认证计划(PSAC)	4.2.12.a 4.3.2	X	X		
硬件的认证计划(PHAC)	4.2.12.a 4.3.2	X	X		
软件配置索引(SCI)	4.2.12.a 4.3.2	X	X		

生命周期数据项目	参考	任务1	任务2	任务3	任务4
硬件配置索引(HCI) (即，顶层图)	4.2.12.a 4.3.2	X	X		
软件完成总结（报告）(SAS)	4.2.12.a 4.3.2	X	X		
硬件完成总结（报告）(HAS)	4.2.12.a 4.3.2	X	X		
安全性评估分析/报告	4.2.12.b			X	X
宿主应用的认可数据手册	4.3.2		X		
IMA认证计划(系统与飞机级)	4.4.3 4.5.3			X	X
IMA验证与确认计划(系统与飞机级)	4.4.4 4.5.4			X	X
IMA配置索引(系统与飞机级)	4.4.5 4.5.5			X	X
IMA完成总结（报告）(系统与飞机级)	4.4.6 4.5.6			X	X
环境鉴定试验(EQT)计划	参考资料[1]	X	X	X	X
环境鉴定试验(EQT)报告	参考资料[1]	X	X	X	X

5.7.6 当进行更改时的认证联络过程

当对某个已批准模块或宿主应用提出更改时，应该进行更改影响分析(CIA)，并应按照第4.6.4节所述形成文档。CIA和涉及更改的其它策划文档应及早地提交给认证机构，以获得同意。在获得同意前不能实施更改。所有受更改影响的数据都要进行更新以符合计划要求。在更改完成后，至少应将列入第5.7.5节中那些受到更改影响的数据提交给认证机构。

注意：认证机构可能需要附加的文件来支持更改，如，验证计划。

5.7.7 对于模块重用的认证联络

当提出重用某个模块或宿主应用的认可包时，如第4.7节所描述的那样，在第4.7.6 节中所确定的数据应该提交给认证机构。

第6章　IMA系统的持续适航考虑

本节提出了IMA系统持续适航的指南，涉及到对所安装的IMA系统进行培训、维护和取证后的飞机修改。虽然该指南不是专门针对IMA系统的，但在进行维护和修改过程中，由于综合等级、相互独立性和复杂性的增加有可能会引入新的关注领域。因此对于持续适航，本指南相比在联合式系统架构中变得更为重要，并应该涉及到IMA系统的最初设计以及持续适航的过程。

6.1　培训

为了维持IMA系统的持续适航，维护人员和相关的飞行操作人员要接受对特定IMA系统的培训。

在IMA系统的开发过程中，应该进行人员因素评估，以解决系统在正常配置和降级配置情况下以及在恢复状况下操作的实用性(见3.10节)。培训应该确保飞行操作人员理解降级模式运行、级联故障、多重消息以及听觉告警的作用。

在IMA系统中产生的级联失效有可能会隐藏失效的主要原因，且所要求飞行机组人员采取的行动也不都是明显的。因此，对飞行机组人员的培训需要对失效识别、恢复活动（如果适用的话）以及失效报告有一个定义良好的过程。

由飞行机组人员报告的IMA系统失效或异常行为以及对故障诊断报告 (见3.6.5节)的恢复，对维护都是非常重要的。这些报告应该准确、完整，并应能查到相应的故障代码。

由于集成度、相互依赖性、复杂性的增加，以及可能发生的潜在和级联故障(这些故障是非常难以隔离的，且用传统的方法不能总使其显现确定出来)，因此为了IMA系统的持续适航，对维护人员的培训是非常重要的。提供给维护人员的资料和过程(即，说明书、故障诊断、维修、验证、在维护工作后对IMA配置的确认，等)，应该是策划好的、准确的、完整的和易于理解的。例如，由于失效的级联或延迟，使得难以诊断与识别IMA系统中的故障或失效，而这种失效级联或延迟可能会隐藏失效的主要原因。因此，要求对故障识别与纠正的培训应该是彻底和全面的，比起联合式的系统架构，培训还要更多地围绕IMA系统进行。

6.2　维护

为了持续适航、飞行操作和维护，IMA系统应该能够展现出所加载软件和数据的状态、版本和当前信息。IMA系统的组件配置应该是可以获得的，以便为确定该系统与批准的型号设计一致，实施维修和进行各种测试或检查。

由于软件可以独立于硬件被加载到飞机上，因此操作者应该建立一个维护并记录IMA

系统配置的过程(软硬件组件与模块的标识和版本状态)。这些信息应该是当前（最新的），并应作为飞机记录的一部分进行维护。

当要在现场加载硬件或软件时，应该建立一种严格的过程以确保正确和完整的加载，为了确认所加载的软硬件是批准过的，并验证上载（的内容）没有毁坏(例如，用适当的数据传输完整性检查来进行验证)。这种过程应包括IMA系统加载前和加载后的检查，并对任何加载失败进行报告。操作者还应该能确认软硬件的加载与其它组件的兼容性和相互混用性。

对维护接口和过程的人员因素分析(见3.10节)应包括在IMA系统的设计数据中，在维护手册中对故障识别和诊断过程应该给予清晰无二意性的描述。IMA系统应该提供探测和识别失效的方法，以方便对系统的维护。

6.3 证后修改

在初始认证后对IMA系统的修改应引用认证申请人所建立的设计数据与认证准则。这也适用于那些不是原始认证的申请人。取证后的修改应该包括人员因素评估的评审(包括飞行机组和维护过程两个方面， 见第3.10节)、安全性评估(见第5.1节) 的评审，以及对更改安装认证需求的评审，这种更改对已认证的飞机配置与型号设计会有影响。

由于IMA系统集成度、相互独立性和复杂度的增加，证后修改的进行与实施应该考虑飞机安全性评估、IMA系统安全性评估和飞机认证基础的影响。当提出某项修改时，应该进行更改影响分析(见第4.6.4节)，这种分析应该确定所提出的更改是否会对IMA系统、飞机或发动机的安全操作与持续适航产生不利影响。

IMA系统要特别关注的地方就是，一个失效产生会导致很多失效或显示的告警信息（见3.6节）和/或语音告警同时出现。这些信息应该能清晰地且以某种优先顺序的方式显示出来。语音告警的顺序应该确定出来(例如，状态报告、提示小心、警告、飞行员立即采取行动)。在取证后的修改中，为了符合持续适航并减轻飞行机组的工作负担，应该对这些优先等级进行分析。无论在什么情况下，都期望由飞行机组确定这些消息和提醒优先等级以及对它们进行处理的顺序，因为这些可能会在处理失效时导致不期望的延迟，以及可能引起飞行状态出现不期望的安全问题。

特别委员会 SC-200（模块化航空电子）成员

主席:

RTCA SC-200	Mr. Cary Spitzer	AvioniCon
EUROCAE WG-60	Mr. Rene Eveleens	NLR

秘书:

RTCA SC-200	Mr. John Lewis	Federal Aviation Administration
EUROCAE WG-60	Mr. David Brown	Airbus UK

姓名	公司
Anders Peter	Airbus Deutschland GmbH
Andro Monty	National Aeronautics and Space Administration
Baker Kirk	Federal Aviation Administration
Bauer Brigitte	Thales Avionics
Benich Christopher	Honeywell International, Inc.
Benich Christopher	Honeywell International, Inc.
Berthon Guy	Thales Avionics
Birkedahl Byron	Honeywell International, Inc.
Breunig Jeff	Arthur D. Little
Brodegard William	Ryan International Corporation
Byrum Jim	Cessna Aircraft Company
Canovi Len	Honeywell International, Inc.
Chelini James	VEROCEL, Inc.
Conmy Philippa	University of York
Croker John	DCS Corporation
Cross Joe	Raytheon Aircraft Services
Denzel Paul	The Boeing Company
DeSalvo Richard	Federal Aviation Administration
Devarasetty Krishna	L-3 Communications
DeWalt Michael	Certification Services, Inc.
Doppelbauer Kurt	TT Tech/Computer Technik
Driscoll Kevin	Honeywell International, Inc.
Duff-Cole Chris	UK - Civil Aviation Authority
Ferrell Thomas	Ferrell and Associates Consulting
Ferrell Uma	Ferrell and Associates Consulting
Gallaway Glen	Federal Aviation Administration
Harwood Ray	Tucson Embedded Systems, Inc.
Hayhurst Kelly	National Aeronautics and Space Administration
Hill David	Honeywell International Inc.
Hollinger Kent	MITRE Corporation/CAASD
Holloway C	National Aeronautics & Space Administration
Horton Olly	BAE Systems - CNIR
Hunt Geoffrey	EUROCAE
Jackson Robert	Raytheon Systems Company
Jalalian Myles	Federal Aviation Administration
Jeske Rolf-Jurgen	Airbus Deutschland GmbH
Krodel Jim	Pratt & Whitney ,EB-1

Lambregts Tony	Federal Aviation Administration
Lee Douglas	Transport Canada
LeFebvre Christian	EUROCAE
Livack Gary	Federal Aviation Administration
Mangan Joe	Coanda Aerospace
Mazuk Dan	Rockwell Collins, Inc.
McCormick Frank	Certification Services, Inc.
McGookey Jeff	Smiths Aerospace
Miner Paul	National Aeronautics and Space Administration
Newton Ian	BAE Systems Avionics Group
Nickum Jim	MITRE Corporation/CAASD
Nordsieck Arnold	The Boeing Company
Norris John	Crane Aerospace & Electronics – ELDEC Corporation
Ovens Norman	Rockwell Collins, Inc.
Parker Ted	Honeywell International, Inc.
Parmer Tom	Federal Aviation Administration
Patel D	Department of National Defence
Peri Richard	Aircraft Electronics Association, Inc.
Perry Robin	Smiths Aerospace
Pivetta Enrico	DIEHL Avionik Systeme GmbH
Prisaznuk Paul	ARINC Incorporated
Pruiett Jay	Rockwell Collins, Inc.
Retko Erik	Smiths Aerospace
Rierson Leanna	Digital Safety Consutling
Robinson David	Federal Aviation Administration
Ruana Rudolph	RTCA, Inc.
Rushby John	SRI International
Rybecky Jiri	Airbus Deutschland GmbH
Schieffer Jim	Smiths Aerospace
Schoen David	The Boeing Company
Schroeder Brian	Cessna Aircraft Company
Schwarz Martin	TTTech AG
Severson Mike	Bell Helicopter Textron, Inc.
Shimin Gu	CARERI
Shroyer Gary	Smiths Aerospace
Skaves Peter	Federal Aviation Administration
Smith Bernald	Soaring Society of America
Struck Will	Federal Aviation Administration
Tahir Abdul	Aviso, Inc.
Thedford William	U. S. Air Force
Thompson Ralph	International Air Transport Association
Wade Matthew	Federal Aviation Administration
Walen David	Federal Aviation Administration
Wallington Andrew	Smiths Aerospace
Wilkinson Chris	Smiths Aerospace
Worcester Tom	Honeywell International, Inc.

附录A　目标表

这里的目标是用于策划和保证所安装的IMA系统符合本文件的指南。这些目标应该在飞机认证计划（例如：飞机和/或IMA系统的认证计划、平台的认可计划、模块的认可计划、宿主应用的认可计划）的策划过程中进行描述。在认可和认证工作中，由于通常包括有多个利益相关方，这些计划应该明确地描述每个目标由谁负责来实现。当目标的实现中涉及到一个以上的利益相关方时，计划还应该指明每个利益相关者的角色和职责，且要指出他们如何证实能够符合目标。符合这些目标的证据（全部的、部分的或没有）应该在符合性文档中提供（例如，在飞机级和系统级IMA系统完成总结中，在平台/模块的完成总结中，在宿主应用的完成总结中）。

在“目标”列中给出了本文件的认证目标，这些目标在IMA系统的开发过程中应得到满足。在“文件引用”列中指出了本文件中的章节号，在这些章节中可以得到对目标详细的解释。在“生命周期数据描述”列中指出了满足目标的典型数据。在“生命周期数据的引用”列中指出了章节号，在这些章节中提供更多的解释或数据内容描述。

注意：控制类别(CC) CC1/CC2在这些表中（见5.5.2节）是作为通用指南提供的。对于有些系统、平台、模块或应用，如果在IMA SCMP中证明是合理的（例如较低级的设计保证），配置控制的程度可能不必太严格。

表A-1　IMA 模块/平台的开发过程（任务1）的目标

标识	目标	文件的引用	生命周期数据描述	生命周期数据引用	控制类别
1	模块/平台开发与认可的生命周期以及相关过程的策划与实现，符合DO-160、DO-178、DO-254与本文件中的指南	4.2.1a 3.1.1a	模块/平台的认可计划	4.2.3	CC1
2	模块/平台的需求规范已经得到规定，并可追踪、可验证	4.2.1b 3.1.1b	模块/平台的需求规范	4.2.4	CC1
			追踪性的数据	4.2.5	CC2
3	模块/平台的设计要文档化并且要达到安全性要求。	3.1.1c,d 4.2.1b,c	模块/平台的设计数据	4.2.4	CC1
			模块/平台的失效分析和安全性分析	4.2.12b	CC1
4	当需要时，验证和开发的工具经过评估和鉴定	4.2.1i 3.4 5.2.3	模块/平台的工具鉴定数据	4.2.12c	CC2 或 CC1[4]
5	分区要确保任何宿主应用的行为不会受到任何其它应用或功能的不良影响	3.5 3.1.1c,d 4.2.1c,d 5.1, 5.3, 5.4	分区的分析数据	4.2.4j	CC1
			V&V数据	4.2.5	CC2
			失效分析与安全性分析	4.2.12b	CC1

标识	目标	文件的引用	生命周期数据描述	生命周期数据引用	控制类别
6	模块需求、资源需求等的符合性要得到证实	3.1.1d,e 4.2.1c 4.2.1d 4.2.1e	模块/平台的V&V 数据	4.2.5	CC2
7	确保模块的用户能获得所需的资料，以便进行综合和与模块进行接口	4.2.1g,k,l 3.4	模块/平台的认可数据手册	4.2.10	CC1
			接口规范	4.2.4f	CC1
			模块/平台的用户指南	4.2.12e	CC2
8	平台已完成综合	4.2.1h 3.1.1d 5.3, 5.4	平台的综合、验证和确认的数据	4.2.5	CC2
9	为宿主应用和IMA系统的使用，IMA平台要提供健康监控和故障管理功能并文档化并	4.2.1c 3.6 5.1.5.5 5.1.5.6	平台需求规范	4.2.4f	CC1
10	模块/平台的质量保证、配置管理、综合、确认、验证以及认证联络已实施并且已完成。	4.2.1f,j,k 5.3 to 5.7	模块/平台的QA 记录	4.2.6	CC2
			模块/平台的CM 记录	4.2.8	CC2
			模块/平台的V&V 数据	4.2.5	CC2
			模块/平台认可的完成总结	4.2.9	CC1
			模块/平台的配置索引	4.2.7	CC1
			模块/平台的问题报告	4.2.11	CC2

（4 工具鉴定数据的控制类别在DO-178/ED-12 (参考资料[2])或DO-254/ED-80(参考资料[6])中规定）

表A-2 宿主应用的开发与认可（任务2）目标

标识	目标	文件的引用	生命周期数据描述	生命周期数据引用	控制类别
1	宿主应用的认可计划已完成，要使用的IMA平台资源得到识别，并解决了IMA系统开发和验证生命周期过程的特有问题	3.1.2a,b	宿主应用的PSAC/PHAC	4.3.2[5]	CC1
2	针对相关指南(软件DO-178/ED-12,和硬件DO-254/ED-12)，应用的符合性已得到证实，且相应的生命周期数据已完成开发。	3.1.2g 4.3.1d,e	宿主应用的生命周期数据[4]	4.3.2[5]	[5]
3	宿主应用所需的平台资源已得到规定，应用的安全性、健康监控/故障管理、环境鉴定、平台外的资源以及人员因素等方面的问题也已按要求进行了规定	4.3.1b 3.1.2c,d,e,f,h	宿主应用的生命周期数据[4]	4.3.2[5]	CC1[5]
4	应用已综合到平台上	4.3.1f	宿主应用的生命周期数据[4]	4.3.2[5]	[5]
5	对综合者分配给应用的资源的正确使用要进行验证	4.3.1c	验证与确认的结果	4.3.2	CC2
6	在目标机和环境上，宿主应用的符合性要得到证实	4.3.1a	宿主应用完整的生命周期数据包[4]	4.3.2[5]	[5]

标识	目标	文件的引用	生命周期数据描述	生命周期数据引用	控制类别
7	配置控制得以维护并要确保在开发、综合与验证过程中使用了正确的配置工具、应用和模块	4.3.1g	CM计划、规程和记录[4] 配置索引	4.3.2[5]	[5]
8	如果想得到应用的重用信任，就要在应用的开发过程中解决重用问题	4.3.1h	应用的PHAC, PSAC	4.3.2[5]	[5]

（[5] 保证过程、生命周期数据，以及适当的控制类别要在DO-178/ED- 12 (参考资料[2]) 的软件应用和DO-254/ED-80 (参考资料[6])的硬件应用(HC1或HC2)中进行定义）

表A-3 IMA系统级开发与认可(任务3)的目标

标识	目标	文件的引用	生命周期数据描述	生命周期数据引用	控制类别
1	对于飞机级的认证信任，IMA系统的活动要和预期采用的综合、确认和验证（方法）一起进行策划	3.1.3c 4.4.1a 5.5 5.6	IMA系统的认证计划	4.4.3	CC1
			IMA系统的CM计划	5.5.1	CC1
			IMA系统的QA计划	5.6	CC1
			IMA系统的V&V计划	4.4.4	CC1
2	IMA系统的安全评估与分析要完整	3.1.3b,d 4.4.1c 5.1.5	IMA的安全性分析与报告	4.4.7d	CC1
3	IMA系统架构已得到规定并文档化	3.1.3c	IMA系统的需求与设计数据	4.4.7f	CC1
4	在IMA系统上要进行综合、验证和确认活动	3.2 3.1.3e,f 4.4.1f	IMA系统的V&V 数据	4.4.7a	CC2
5	给平台提供健康监控、失效报告和故障管理的功能，以满足需求	3.6 4.4.1b	IMA系统验证与确认的结果	4.4.7a	CC2
			IMA系统的需求与设计数据	4.4.7f	CC1
6	建立和维护IMA系统的配置管理和质量保证	3.7 4.4.1c, d 5.5 5.6	IMA系统的认证计划	4.4.3h	CC1
			IMA系统的CM计划	5.5.1	CC1
			IMA系统的QA计划	5.6	CC1
			IMA系统的CM记录	4.4.7b	CC2
			IMA系统的配置索引	4.4.5	CC1
			问题报告	4.4.7e	CC2
7	共享资源的分配已经建立并得到验证	3.2 3.5 4.4.1b	IMA系统的需求与设计数据	4.4.7f	CC1
			IMA系统的V&V结果	4.4.7a	CC2
8	设计和配置的工具已完成开发，并确保达到所需要的保证级别，以支持IMA系统	3.4 4.4.1b 5.2.3	工具鉴定的数据	4.4.7g	[6]
9	如果需要，IMA系统的设计要能支持MMEL要求	3.9 5.1.5	IMA的安全性分析与报告	4.4.7d	CC1

标识	目标	文件的引用	生命周期数据描述	生命周期数据引用	控制类别
10	人员因素问题已在IMA系统设计中得到解决	3.10	IMA系统的需求与设计数据	4.4.7f	CC1
11	IMA系统的设计保证活动已完成	3.1.3e,f 4.4.1d,g	IMA系统的配置索引	4.4.5	CC1
			IMA系统的完成总结	4.4.6	CC1
			附加的IMA系统的数据	4.4.7f, g[7]	CC1
			附加的IMA系统的数据	4.5.7a, b,c,d	CC2
12	在系统级上模块和应用的问题报告得到了评估，并且建立了系统级的问题报告系统	4.4.1h	IMA系统的问题报告	4.4.7e	CC2
			IMA系统的认证计划	4.4.3o	CC1

（[6] 控制类别与DO-178/ED-12 (参考资料[2])或DO-254/ED-80 (参考资料[6]) 的定义一样）

（[7] 工具鉴定数据(第4.4.7g节)的控制类别在DO-178/ED-12 (参考资料[2])或DO-254/ED-80 (参考资料[6])中定义））

表A-4 飞机级综合(任务4) 的目标

标识	目标	文件的引用	生命周期数据描述	生命周期数据引用	控制类别
1	飞机级IMA系统的安装、综合、验证和确认活动要得到策划	4.5.1a	飞机级IMA系统的认证计划	4.5.3	CC1
			飞机级IMA系统的V&V计划	4.5.4	CC1
			飞机级IMA系统的CM计划	5.5.1	CC1
			飞机级IMA系统的QA计划	5.6	CC1
2	通过利用实验室试验、地面试验和飞行试验，以及适当的分析，对预期的功能性、性能和安全性需求的符合情况要得到证实	4.5.1b	V&V结果	4.5.7a	CC2
3	IMA系统的资源管理、故障容错与管理、健康监控、降级模式以及（失效）恢复的能力要得到验证	4.5.1c 3.1.3f	V&V结果	4.5.7a	CC2
4	对飞机和/或发动机认证基础符合相关规章的情况要得到证实	4.5.1d	飞机级的IMA完成总结	4.5.6	CC1
			飞机级的IMA配置索引	4.5.5	CC1
5	对特定异常的反应要进行评估，如多个（功能）应用的丧失或故障，或全部共享资源丧失或故障，失效延迟以及失效级联	4.5.1e 5.1.5	安全性分析与报告	4.5.7d	CC1
			V&V结果	4.5.7a	CC2

标识	目标	文件的引用	生命周期数据描述	生命周期数据引用	控制类别
6	执行V&V活动，以解决：影响多个宿主应用的模块失效模式（模块内的分析）；影响多个宿主应用的模块级公共失效模式（模块间的分析）；以及影响多个飞机系统的失效模式。并要采用备份系统与缓解措施。	4.5.1f 3.1.3f 5.1.5	安全性分析与报告	4.5.7d	CC1
			V&V结果	4.5.7a	CC2
7	解决与多项飞机功能失效、飞行员负荷与异常行为，以及正常与紧急操作过程等有关的人员因素问题。	3.10 4.5.1g	飞机级IMA系统的认证计划	4.5.3	CC1
			V&V 结果	4.5.7a	CC2
8	如果需要的话，要进行与多项飞机功能失效和异常行为有关的高强度辐射场(HIRF)和闪电间接影响(IEL)试验。	4.5.1h 5.2.6	飞机级IMA的环境测试计划	4.5.7g	CC1
			飞机级IMA的环境测试结果	4.5.7g	CC2
9	验证IMA系统与其它机载系统之间正常的交互关系	4.5.1i	飞机级IMA系统的认证计划	4.5.3	CC1
			飞机级IMA系统的V&V计划	4.5.4	CC1
			V&V结果	4.5.7a	CC2
10	IMA系统的飞机级认证数据已完成	4.5.1k	飞机级IMA系统的配置索引	4.5.5	CC1
			飞机级IMA系统的完成总结	4.5.6	CC1
			附加的飞机级数据	4.5.7d,f,g8,h,i,j	CC1
			附加的飞机级数据	4.5.7a,b,c,e,g8	CC2
11	解决IMA系统任何失效模式的飞机级安全性评估已经进行	4.5.1j,l 5.1.5	安全性分析与报告	4.5.7d	CC1
			V&V结果	4.5.7a	CC2
12	IMA系统在飞机上的安装与综合已经完成	4.5.1 5.3 5.4	V&V结果	4.5.7a	CC2
			安装说明	4.5.7f	CC1
13	如果需要的话，要编制出能满足飞机级派遣要求的MMEL	3.9	主要的最少设备清单(MMEL)	4.5.7k	CC1
14	IMA系统的持续适航要得到维持	6.1 6.2	飞机级IMA系统的配置索引	4.5.5	CC1
			持续适航说明	4.5.7h	CC1

（[8]工具鉴定数据(第 4.5.7g节) 的控制类别已在DO-178/ED-12 (参考资料[2])或DO-254/ED-80 (参考资料[6])中定义）

表A-5 更改（任务5）的目标

标识	目标	文件的引用	生命周期数据描述	生命周期数据引用	控制类别
1	已开发出更改管理过程，并与所有的利益相关方进行了协调	4.6.2a 4.6.3 6.3	更改管理计划	4.6.5b	CC1
2	已进行了更改影响分析，并实施了更改且记录已形成文档	4.6.2b,c 4.6.4 6.3	更改影响分析	4.6.5a	CC1
3	更改后的模块或应用已重新综合到IMA系统，所有必要的验证、确认与综合活动（回归分析与测试）都已进行。	4.6.2d 6.3	V&V计划	4.6.5c	CC1
			V&V结果	4.6.5c	CC2
			修改的生命周期数据(包括配置索引)	4.6.5d	9
			更新的完成总结	4.6.5e	CC1
			更改历史与维护记录	4.6.5f	CC2
4	与更改有关的所有生命周期数据的配置控制都得到维护	4.6.2e 6.3	修改的生命周期数据(包括配置索引)	4.6.5d	9
			更新的完成总结	4.6.5e	CC1
			更改历史与维护记录	4.6.5f	CC2

（[9]特定生命周期数据的描述、引用和控制类别取决于进行什么修改，并根据每个重用实例都可能有变化）

表A-6: 模块或应用的重用（任务6）目标

标识	目标	文件的引用	生命周期数据描述	生命周期数据引用	控制类别
1	对以前认可过的模块或应用的生命周期数据确保不做任何改变	4.7.1a	提出可重用模块或应用的MAAP、PSAC、PHAC或其它相关计划	4.7.610	10
2	已将限制、假设等纳入到了模块或应用的认可数据手册文档中，并在后续的安装中得到能够找到（查阅到）	4.7.1b	认可数据手册	4.7.610	10
			后续安装的验证结果	4.7.610	CC2
			重用模块或应用的完成总结	4.7.610	CC1
3	对使用范围已进行了分析，以确保模块或应用按照原来预期的（使用）方式得到重用	4.7.1c	V&V结果	4.7.610	10
4	对模块或应用的未关闭问题报告已进行了评估，以确保对安全性、功能、性能或运行不会产生负面影响	4.7.1d	问题报告 分析结果	4.7.610	10
5	先前认可过的可重用模块或应用在新的安装环境中已得到了综合、验证和确认	4.7.1e	综合过程	4.7.610	10
			V&V结果	4.7.610	10
6	向认证机构已提交了必要的数据	4.7.1f	初始认可的生命周期数据	4.7.610	10
			后续认可的生命周期数据	4.7.610	10
			V&V记录	4.7.610	10
			完成总结	4.7.610	10

（[10]特定生命周期数据的描述、引用和控制类别取决于进行什么重用，并根据每个重用实例都可能有变化。模块和应用的重用见第4.7节）

附录B　术语表

认可（Acceptance）：由认证机构对模块、应用或系统满足其规定要求所给出的承认。

不利的（Adverse）：由安全性评估过程所确定的、认为是不能接受或有害的行动、作用（影响）或行为。

飞机功能（Aircraft Function）：由机上的硬件和软件系统提供的一种飞机（功能）能力。

适航（Airworthiness）：项目（飞机、飞机系统或部件）的状况，在这种状况下该项目能以安全的方式完成其预期的功能。

分析（Analysis）：通过分解成为简单要素进行的一种评价。

异常行为（Anomalous behavior）：与规定要求不一致的行为。

适用的要求（Applicable requirements）：对于型号下的飞机、发动机、机载系统或设备、或其中的部件，由认证机构确立的必须遵循的认可（接受）准则。

申请人（Applicant）：寻求认证机构正式批准的个人或组织。

应用（Application）：与平台集成后能执行一种功能的软件和/或有一组规定接口的专用硬件。

应用软件（Application software）：是应用的一部分，通过软件来实现，它可以分配到一个或多个分区中。

专用硬件（Application-specific hardware）：专用于某种应用的硬件。

批准（Approval ）：对遵守（符合）规章给出的正式或官方承认的行为或程序。

组装件（Assembly）：许多部件、分部件或它们的任何组合，结合在一起来完成某种特定功能。

评估（Assessment）：根据某一规定的工程方法进行的一种评价。

假定（Assumptions）：没有证据的陈述（声明）、原则和/或前提。

保证（Assurance）：有计划或系统性的必要活动，为产品或过程满足给定需求提供充分信心和证据。

机构（Authority）：在国家范围内负责有关可适用要求（applicable requirements）的组织和个人。由认证机构处理的、与飞机、发动机或螺旋桨（推进器）型号认证或设备批准有关的事务；由适航机构处理的、与持续适航有关的事务。

可用性（Availability）：在给定的时间点上，某个项目处于工作状态的可能性（或概率）。

基线（Baseline）：已批准、记录过的一个或多个配置项的构型，作为进一步开发的基础，且只能通过更改控制程序才能对其进行更改。

机柜（Cabinet）：包含有一个或多个IMA部件或模块的物理封装，它能对环境影响提供部分的保护（屏蔽），并在物理上不影响机上的其它系统或设备的情况下，能把这些组件或

模块安装到飞机上和从飞机上卸下。

级联失效（Cascading Failure）：不能进行隔离或缓解的（一种）失效的传播。

认证（Certification）：认证机构对产品、服务、组织或个人符合要求的合法认可（承认）。这种认证包括在技术上检查产品、服务、组织或个人的活动，并通过发布国家法律和程序要求的证明、许可证、批准文件或其它文件，正式地认可其符合适用要求（applicable requirements）。具体来说，产品的认证包括：a） 评估产品设计的过程，以确保产品符合该类型产品适用的一组标准，证实安全性等级是可接受的；b）评估单个产品的过程，以保证产品符合所认证型号的设计；c）依照以上两条，颁发国家法律要求的证书，声明具有一致性或符合性。

认证机构（Certification Authority）： 代表制造国家负责对组织或个人授予批准。

认证信任（Certification credit）：认证机构对过程、产品或演示满足认证要求的认可。

更改控制（Change control）：对于配置中某个配置项，在正式建立配置标识后，或在建立基线后，对要批准的更改进行系统性的评估、协调、批准或否决，以及实现。

注意: 这一术语在其它工业标准中可能称为配置控制。

代码（Code）： 特殊数据的实现或符号形式的计算机程序，如源代码、目标代码或机器代码。

商用货架软件（COTS software）：可获得的商品化应用，是由销售商通过公开的产品目录清单销售的。

共因分析（Common Cause Analysis）：通用的术语，包括区域分析、特殊风险分析和共模分析。

共模失效（Common Mode Failure）： 同时影响多个要素的事件，否则认为就是独立的失效。

编译器（Compiler）：能把高级的原代码语句转换成目标码的程序。

复杂性（Complexity）：系统或项目的一种属性，它使得其设计和/或操作难以理解；

符合性（Compliance）：所有强制活动的成功履行；期望或规定的结果与实际结果的一致。

组件（Component）：一个自身含有硬件或软件的部件、数据库，或其组合，且受到配置管理的控制。

计算机（Computer）：执行数据处理的一个或一组设备。

配置控制（Configuration Control）：见更改控制。

配置标识（Configuration identification）：在某个系统中指定配置项目并记录其特性的过程。

配置索引（Configuration index）：经过批准的定义配置项目的文件。

配置项目（Configuration item）：1) 为了配置管理的目的，作为一个单元对待的一个或多个硬件或软件。2) 为了配置管理的目的，作为一个单元对待的软件生命周期数据。

配置管理（Configuration management）：采用技术和行政管理的手段进行指导和监督的一

种纪律，以便：(a)识别和记录某一配置项目的功能和物理特性；(b)控制对这些特性的更改；以及(c)记录和报告更改控制的处理与实现的状态。

配置管理纪实（Configuration status accounting）：为了有效地管理某个配置，必须记录和报告的信息，包括一个已批准过的配置标识清单、对配置提出的更改状态，以及已批准更改的实现状态。

一致性（Conformance）：可表明对一组强制要求的遵守；

抑制（Containment）： IMA系统、模块或组件为了防止错误传播或级联失效的特性。抑制也标识与特殊应用相关的所有边界集合。

控制耦合（Control coupling）：一个软件组件影响另一个软件组件执行的方式和程度。

核心软件（Core Software）：管理平台资源的操作系统和支持软件，以便为应用提供运行环境。

危险度（Criticality）：指示与功能、硬件、软件等有关的危害的等级，涉及到这些单独项目的异常行为，或与外部事件结合（在一起）的异常行为。

数据耦合（Data coupling）： 软件组件对数据的依赖性，这些数据并不完全在该软件组件的控制之下；

未激活码（Deactivated code）—— 由设计给出的可执行的目标代码（或数据），它可以是：a）不希望执行的（代码）或不打算使用的（数据），例如，以前开发的软件的一部分； b）只能在某种目标机环境的配置下才能执行的（代码）或使用的（数据），例如，与硬件插针或软件编程选择有关的代码；

演示（Demonstration）：通过观察来证实性能的一种方法。

可信性（Dependability）：系统的可信性是：系统的一种属性，它允许对使用（服务）中的系统给出正当的信任。

确定性/确定性的（Determinism/deterministic）：一般而言，基于前面进行的操作能产生可预期结果的能力。这种结果发生在规定的时间范围内，具有一定的可重复性。

开发保证（Development assurance） ：所有有计划的和系统性的活动，这些活动以足够的信心证实开发错误已经被识别并得到纠正，从而使系统满足可适用的认证基础和要求；

领域（Domain）：把一些项目分到某些有共同点或特征的区域。

ETSO授权（ETSO Authorization）：认证机构对于系统、设备或部件满足ETSO要求和最低性能规范，并授权生产这种项目，而给出的正式承认。

失效静默（Fail passive）： 系统的一种属性，故障发生后就转移到静默状态，以避免对系统有不利影响。

失效（Failure）：在规定的范围内，系统或系统组件不能执行（完成）所要求的功能。当故障发生时，可能产生失效。

失效条件（Failure condition）：由一个或多个失效引起或造成的对飞机及其乘员直接或间

接的影响。

失效影响（Failure effect ）：一种对项目失效结果的工作描述。

失效模式（Failure mode）： 项目发生失效的方式。

故障诊断（Fault diagnosis）：根据所记录的故障、失效、错误或异常行为事件，正确地识别故障原因的能力。

容错（Fault tolerance）：系统在出现有限数量软硬件故障下，能够持续进行工作的内在能力。

联合系统（Federated System）：主要由现场可更换单元（LRU）组成的一种飞机设备架构，这些LRU能执行特定的功能，并通过专用接口或飞机系统数据总线相互连接在一起。

形式化方法（Formal methods）：描述符号与分析方法，用来构建、开发和推论系统行为的数学模型。

功能（Function）：能执行特定任务的一种指定能力。

功能危害度评估（Function hazard assessment）：根据功能的重要性，通过确定和分类功能的失效条件，对飞机功能所作的系统的全面的检验。

指南（Guidelines）：为了符合规章，给出的推荐过程。

硬件（Hardware）：物理存在的一种项目， 通常指的是现场可更换单元、模块、电路板和电源等这类项目。

硬件/软件综合（Hardware/software integration）：把软件嵌入到目标计算机的过程。

综合模块化航空电子系统（Integrated Modular Avionics）——能够共享的一组可变化的、可重用的、可互操作的硬件和软件资源。这些资源综合在一起能够创建一个平台，而该平台针对所定义的安全和性能要求，能提供已设计和验证的服务，以便管理那些执行飞机功能的应用。

递增式认可（Incremental Acceptance）——通过认可或决定一个IMA模块、应用和/或在机下的IMA系统符合特定要求，来获得批准或认证信任的一种过程。通过为单独任务提供信任，最终实现整个认证的目标。

独立性（Independence）：

第一种解释：职责的分离，这种分离能确保达到客观的评价。

- 对于软件验证过程活动来说，独立性的实现就是，对被验证项目进行验证活动时，由开发者之外的一个或几个人员进行，且工具可以用来完成与人工验证等同的活动；
- 对于软件质量保证过程来说，独立性还包含能确保纠正措施得以落实的权力机构。

第二种解释：一种设计理念，它能确保一个项目的失效不会引起另外一个项目的失效。

初始化（Initialization）：一个活动的序列，这些活动能把系统或其中的组件引导到操作就

绪的状态。

检验（Inspection）：1)按照规定的标准对项目进行的检查；2)对供应品和服务进行的检查和测试，当适宜时，包括原材料、元器件、中间组件和服务，以确定其是否符合规定的需求。

完整性过程（Integral process）：一种能帮助系统、软件或硬件的开发过程以及其它完整过程的过程，而且，在整个生命周期能保持有效。完整性过程包括有验证过程、质量保证过程、配置管理过程和认证联络过程。

综合（Integration）：把若干分离的组件结合在一起，形成一个单独的实现。

完整性（Integrity）：一种保证性的定性测量，这种保证性就是某个系统、硬件或软件能正确地、及时地完成规定要求的功能。通常是通过应用某种指定的、严格的开发过程对项目进行设计、实现和验证，以使项目达到适当的保证级别。

互换性（Interchangeability）：在某个系统中，用一个项目替代另一个项目的能力，并能使系统按照其规范执行。

互操作性（Interoperability）：在一起工作的若干模块能够完成某一特定目标或功能的能力。

混合性（Intermixability）：把不同版本和/或修改标准的软件和/或硬件混合在一起的能力。

库（Library）：可由一个或多个不同应用共用的一组软件功能或资源。

维护性（Maintainability）：有关能方便进行维护活动的可信性属性。如果出现失效，能以某种量化的方式来衡量服务的中断，并且能方便地确定失效和进行正确的修复活动。一种与此测量相关的实用评估单位是MTTR（平均修复时间）。

失灵（Malfunction）：出现操作超出规定的极限的状态。

符合性方法（Means of compliance）：为了满足飞机、发动机和推进器认证基础所述的要求，由认证申请人采用的预期方法。

存储设备（Memory device）：能存储机器可读的计算机程序和相关数据的一种硬件物品。它可以是一块集成电路芯片、一个含有集成电路芯片的电路板、一个磁芯存储器、一个磁盘或一条磁带。

消息（Message）：一个有固定长度的连续数据块，它可由系统进行传输（既可以通过网络，也可以在模块内）。

主要最少设备清单（Master Minimum Equipment List -MMEL）：一种受控的清单，它确定出那些是允许飞机派遣所必需的设备与系统。某个设备单元如果不是必需的，则在MMEL就描述为“GO”；如果是必需的，则描述为“NO GO”。因而，一个设备单元要是失效了且在MMEL中标记为“NO GO”，则在飞机派遣前必须修好或替换掉。

模块（Module）：一个组件或组件的集合，它们可以单独认可或在IMA系统中认可。一个模块也可以包括有其它模块。一个模块可以是软件、硬件或软件和硬件的组合，这些软硬件能为IMA系统运行应用提供资源。

网络（Network）： 用来描述用途相同的一个或多个物理通信链接的术语。

目标码（Object code）：计算机程序的一种低级表示法，通常它不是目标计算机能直接使用的形式，而是包括有在处理器指令中加入重定位信息的形式。

操作系统（Operating system）：1)与执行软件相同； 2)只为低层硬件平台进行服务的软件核；3)指导计算机运行、资源分配与数据管理、控制并调度计算机内宿主应用的执行，并管理内存、存储设备、输入/输出以及通信资源。

可操作性（Operational capability）：一种功能或一组功能，它能对飞行机组或其它人员提供一种可见的飞机能力。

部件号（Part number）：用来标识某个飞机部件或配置项的一组有结构的数字、字母或其它符号。

特殊风险（Particular Risk）：在系统和项目关注范围以外发生的事件或影响所产生相关风险，但他们可能违背失效独立性的主张。

分区（Partition）：一种资源的分配，其属性能得到平台保证和保护，不会受到来自分区外的不利作用或影响。

分区隔离（Partitioning）：一种能为功能或应用提供必要的分离与独立性的架构技术，以确保只发生预期的耦合。

平台（Platform）：一个模块或一组模块，包括以某种方式（至少能为一种应用提供充分支持）来管理资源的核心软件。

可移植性（Portability）：对软件不需要做更改或只需要做很小的更改，就可以从一种计算机、硬件、软件或平台的环境转换到另一种环境上能在后一种环境下正确地运行。软件的这种方便性称为可移植性。

初步系统安全性评估（Preliminary System Safety Assessment - PSSA）：基于功能性危害度评估和失效条件分类，对所提出的系统架构及其实现进行系统的评估，以确定该架构中所有组件的安全性需求。

处理资源（Processing resources）：包括有CPU、存储器和相关接口的物理项目，它能够构成独立的处理单元。

处理器（Processor）：一种用于处理数字数据的设备。

产品服务历史（Product service history）：一个连续的时间周期，在这个时间周期中飞机、产品或部件运行在一个已知的环境中，且发生的失效能被记录。

冗余（Redundancy）：某一功能的多个复制和/或版本，它们使用的规范相同或相异，这些规范使用相同类型的输入并产生相同或相近的输出，能通过比较来获得对输出结果的信任。

余度（Redundant）：为完成一个给定的功能，而结合在一起的多路措施。

a. 在下列余度结构中工作原理之间有所不同：

- 相似余度（具有相同类型的多路措施）；
- 非相似余度（具有不同类型的多路措施）；
- 时间余度（通过进行重复操作来实现余度）。

b. 余度结构的操作有如下分类：

- 主动余度（多路措施执行例行操作，并参与执行任务）；
- 被动余度（只有在故障或失效的情况下，新增的措施才参与执行任务）；
- 热被动余度（新增的措施总是打开的）；
- 冷被动余度（新增的措施只是在故障或失效的情况下才打开）。

可靠性（Reliability）：1)对于连续服务可信性的测量与定量属性。以定量的方式，给出系统或组件在规定环境下能持续生存到时间t的可能性状况，假定系统或组件是从时间0开始运行。与此测量相关的一种评估单位是MTFF（平均首次失效时间）。2)在规定的时间周期内和规定的条件下，一个组件执行某种预期功能（不发生失效）的概率。

需求（Requirement）：一种可识别的规范要素，这种要素可被确认，且对照实现可以进行验证。

资源（Resource）：由处理器、IMA平台、核心软件、或应用所使用的任何对象（处理器、存储器、软件、数据等）或组件。一种资源可以由多个应用共享，也可以只提供给某个专用的应用。资源可以是物理的（硬件设备）也可以是逻辑的（一条信息）。

重用（Reuse）：不受影响地使用以前审批的系统硬件或软件的保证数据。

安全性（Safety ）：没有失效发生或能从失效和其它状况恢复过来的可信性属性，这些失效和状况可能引起飞机、发动机或组件发生不可接受的操作事件。

信息安全性（Security）：能防止遭到破坏或无权对信息进行访问和/或处理的可信性属性。

仿真（Simulation ）：定义功能模型的全部要素（可执行的代码、配置文件、测试集），这种功能模型可由用户处理。

仿真器（Simulator）：一种设备、计算机程序、系统组件或环境，它能接受与目标设备、应用、系统组件或环境一样的输入，并产生与目标设备、应用、系统组件或环境一样的输出。

软件（Software）：计算机程序以及可能适合于计算机操作的相关文件和数据。

软件更改（Software change）：根据以前的基线，对原代码、目标码、可执行目标码或其相关的文件进行的修改。

软件综合（Software integration）：将代码组件结合在一起的过程。

软件生命周期（Software life cycle）：1)为了生产软件产品，由组织确定的一组有序过程的集合。2)一段时间周期，它开始于决定生成或修改软件产品，而结束于产品退出服务。

软件产品（Software product）：计算机的程序集和指定要提交给用户的相关文件与数据。

在本文件中，该术语指的是要用于IMA系统的软件及其相关的软件生命周期数据。

软件工具（Software tool）：一种用于帮助开发、测试、分析、生产或修改另一种程序及其文档和数据的计算机程序。范例有自动设计工具、编译器、测试工具和修改工具。

规范（Specification）：一组需求的集合，这些需求当放在一起时，就构成能定义项目（系统、组件或接口）功能和属性的标准。

标准（Standard）：一种规则或对照基础，对于给定的活动或指定数据项目，它既能提供指南也能进行性能评估。

结构（Structure）：一种特定排列或部件的相互关系，以形成一个整体。

系统（System）：组织在一起能完成一个规定功能或一组功能的软硬件组件的集合。

系统架构（System architecture）：能选择用来实现系统需求的硬件和软件的接口与结构。

系统安全性评估（System Safety Assessment - SSA）：对所实现的系统进行系统的、全面的评估，以证明与安全有关的需求得到满足。

目标计算机（Target computer）：能够在预期目标硬件上执行计算机程序的处理器和资源。

目标计算机环境（Target computer environment）：在实际飞机环境中需要用来行使功能的目标计算机及其所有支持的硬件、软件和系统。

测试[试验]（Test）：一个或一组过程，通过使用带有通过或失败结果的规定目标准则，来证明正确的功能和性能。

测试[试验]程序（Test procedure）：1)对系统或组件进行检验的一套活动，以验证系统或组件能满足规定的需求，并能检测出错误；2)对于建立并执行一套给定的测试[试验]用例进行详细指导，并对评估执行测试[试验]用例的结果进行指导。

工具鉴定（Tool qualification）：在特定的飞机系统中，软件工具获得保证的必要过程。

追踪性（Traceability）：1)项目之间的某种相关证据，如过程输出之间、输出及其初始过程之间、或需求及其实现之间；2)一种特性，通过它，在某个设计的层次上的需求可以对应到另一层次上的需求。

转换准则（Transition criteria）：为了满足进入另一过程的条件，由策划过程确定的最低条件。

技术标准规定授权（Technical Standard Order Authorization）：认证机构对于系统、设备或部件满足TSO要求和最低性能规范，并授权制造这种项目，而给出的正式承认。

非预期的功能（Unintended Function ）：一种功能，它在飞机级上是可见的，并且在PSSA的中它既不是预期的故障条件也不是期望的（或预见的）故障条件。

使用范围（Usage domain ）：一套公开的特性，它们可以证实：

1) 模块符合模块需求规范所规定的功能、性能与安全性要求；
2) 对于所规定的可分配资源和能力，模块能满足所有已声明和保证条款；
3) 模块的性能得到完全描述，包括故障和错误处理、失效模式以及在不利环境影响下

的行为。

确认（Validation）：用来确定需求是正确的且这些需求是完整的过程。系统的开发过程可以在系统确认时使用需求和派生需求。

验证（Verification）：1)为了确定需求已得到满足，对需求的实现情况进行的评估；2)为了确保提供给该过程的输入与标准的正确性和一致性，对过程的结果进行的评估。

区域安全性（Zonal Safety)：安全性的标准，涉及到安装区域、与这些区域相关的潜在危害和环境条件、系统之间的接口或来自外部的接口以及潜在的维护问题。

附录C　缩略语清单

AC	咨询通告　Advisory Circular
AMOC	可接受的符合性方法　Acceptable Means of Compliance
AMJ	联合咨询材料　Advisory Material - Joint
APP	应用　Application
API	应用编程接口　Application Programming Interface
ARINC	航空无线电公司　Aeronautical Radio Incorporated
ARP	宇航推荐实践　Aerospace Recommended Practice
ASTC	修改的补充型号合格证　Amended Supplemental Type Certificate
ATC	修改的型号合格证　Amended Type Certificate
ATM	空中交通管理　Air Traffic Management
BIT(E)	自测试(设备)　Built-In Test (Equipment)
CCA	共因分析　Common Cause Analysis
CEH	复杂电子硬件　Complex Electronic Hardware
CIA	更改影响分析　Change Impact Analysis
CM	配置管理　Configuration Management
CMA	共模分析　Common Mode Analysis
CNS	通信导航与监视　Communication, Navigation and Surveillance
COTS	商用货架(产品)　Commercial Off-The-Shelf
CPU	中央处理单元　Central Processing Unit
CRC	循环冗余检查　Cyclic Redundancy Check
CS	认证规范　Certification Specification
DO	RTCA文件　RTCA Document
EASA	欧洲航空安全局　European Aviation Safety Agency
ED	EUROCAE文件　EUROCAE Document
e.g.	例如　For example
EQTP	环境鉴定试验计划　Environmental Qualification Test Plan
EQT	环境鉴定试验　Environmental Qualification Test
ETSO	欧洲技术标准规定　European Technical Standard Order
FAA	（美国）联邦航空局　Federal Aviation Administration
FAR	（美国）联邦航空规章　Federal Aviation Regulation
FHA	功能危害度评估　Functional Hazard Assessment

FLS	现场可加载软件　Field-Loadable Software
FM	故障管理　Fault Management
HAS	硬件完成总结（报告）　Hardware Accomplishment Summary
HF	高频率　High Frequency
HIRF	高强度辐射场　High Intensity Radiated Field
HM	健康监控　Health Monitor
H/W	硬件　Hardware
ICAO	国际民用航空组织　International Civil Aviation Organization
ICAW	持续适航的指导说明　Instructions for Continued Airworthiness
i.e.	也就是　That is
IEEE	电气电子工程师协会　Institute of Electrical and Electronic Engineers
IEL	间接闪电影响　Indirect Effects of Lightning
IMA	综合模块化航空电子　Integrated Modular Avionics
IMAS	综合模块化航空电子系统　Integrated Modular Avionics System
IMASAS	综合模块化航空电子系统的完成总结（报告）　Integrated Modular Avionics System Accomplishment Summary
IMASCI	综合模块化航空电子系统的配置索引　Integrated Modular Avionics System Configuration Index
IMASCMP	综合模块化航空电子系统的配置管理计划　Integrated Modular Avionics System Configuration Management Plan
IMASCP	综合模块化航空电子系统的认证计划　Integrated Modular Avionics System Certification Plan
IMASQAP	综合模块化航空电子系统质量保证计划　Integrated Modular Avionics System Quality Assurance Plan
I/O	输入和/或输出　Input and/or Output
JAA	联合航空管理机构　Joint Aviation Authority
JAR	联合航空要求　Joint Aviation Requirement
LRU	现场可更换单元　Line Replaceable Unit
MAP	模块认可计划　Module Acceptance Plan
MMEL	主要最少设备清单　Master Minimum Equipment List
MMU	存储器管理单元　Memory Management Unit
MAAS	模块认可完成总结（报告）　Module Acceptance Accomplishment Summary
MADS	模块认可的数据手册　Module Acceptance Data Sheet
MRS	模块需求规范　Module Requirements Specification

MTTR	平均维修时间　Mean Time To Repair
MTFF	平均首次失效时间　Mean Time to First Failure
OS	操作系统　Operating System
PHAC	硬件方面的认证计划　Plan for Hardware Aspects of Certification
PSAC	软件方面的认证计划　Plan for Software Aspects of Certification
PSSA	初步系统安全性评估　Preliminary System Safety Assessment
QA	质量保证　Quality Assurance
RSC	可重用的软件组件　Reusable Software Component
SAE	汽车工程师学会　Society of Automotive Engineers
SATCOM	卫星通信　Satellite Communication
SAS	软件完成总结（报告）　Software Accomplishment Summary
SCI	软件配置索引　Software Configuration Index
SEU	单事件翻转　Single Event Upset
SI	系统综合者　System Integrator
SSA	系统安全性评估　System Safety Assessment
STC	补充的型号认证　Supplemental Type Certification
S/W	软件　Software
TC	型号认证　Type Certification
TSO	技术标准规定　Technical Standard Order
UMS	用户可修改的软件　User-Modifiable Software
V&V	确认与验证　Validation and Verification

附录D　　IMA系统的设计举例

本附录包含了各种系统设计的样例。每个样例对 IMA 的特点如何在典型设计中得以实现都给出了说明。这些样例只是作为信息提供的。

D.1　范例1：单个的LRU平台

D.1.1　本范例的目的

本范例描述了单个LRU中计算和I/O资源的共享，关键的IMA特性包括：

- 宿主多个应用；
- 在LRU中共享处理、存储器和I/O，以及共享网络；
- 平台的配置数据和数据加载；
- 在平台和宿主应用之间定义的API。

一方面，本范例描述了能够提供核心计算资源的单个平台。另一方面，本范例说明了在较大的IMA平台中要使用的某个模块。

D.1.2　平台和模块的定义

本范例的平台是一个能够提供共享计算资源并能宿主多个软件应用的单LRU。这些共享资源包括CPU (中央处理单元) 、MMU (存储器管理单元)、 FPPU (浮点处理单元)、协处理器、支持健壮分区隔离的专用硬件机制、物理的存储器、对飞机网络和I/O通道的访问。配置表决定了一个LRU的特定用途，该LRU是现场可加载的，例如使用ARINC 615A来加载。核心软件提供一套ARINC 653 API，以确保应用的可移植性和健壮分区隔离隔离。

图D-1 给出一个单LRU平台的典型设计，包括：

－硬件：CPU、MMU、网络接口和I/O

－软件: 核心软件与分区的应用软件

－配置表: 分区定义、网络端口分配、I/O映像

D.1.3　在本系统中呈现的IMA关键特性

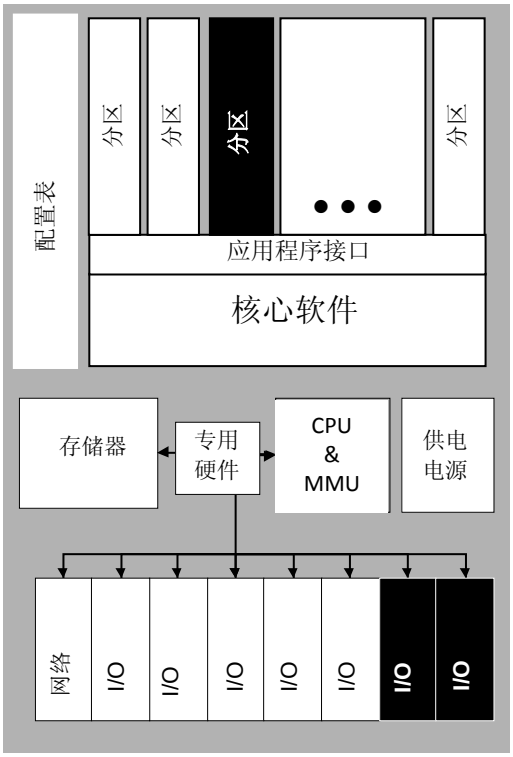
这种LRU可以作为一个能为多个航电功能提供核心计算资源的平台单独认可，也可以作为在较大IMA系统中使用的一个模块来认可。

为了隔离这种平台中的多个分区，平台的专用硬件（MMU、看门狗计时器，等）给核心软件提供管理共享的存储器空间、管理共享的处理时间以及管理共享I/O访问的能力。核心软件管理多个软件分区，并为应用之间提供健壮的分区隔离。

其它要注意的事项就是网络接口的健壮分区隔离，这种网络接口能通过具有确定性框架ARINC 664可将其与其它平台综合在一起来满足带宽的限制，并能通过通道备份来减缓网络的失效。

LRU可以进行适应性调整，以确保满足各个软件应用CPU时间、存储器和I/O的需求。嵌入式的配置表能够提供这种配置能力，它与核心软件一起，可以激活或不激活相应的软件功能，或者给核心软件提供适当的参数。

另一种关键特征就是有高等级的内部故障/失效的检测。



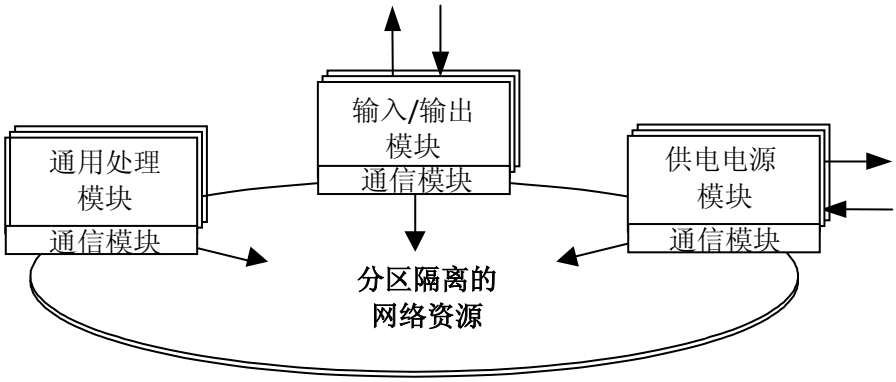
图D-1　已配置的单LRU平台

D.2　范例2：分布式的IMA平台

D.2.1　本范例的目的

这种架构范例说明，如何在基于健壮分区隔离通信网络资源上为实时应用建立容错、分布式的平台。基于一种严格TDMA (时分多模访问)模式，通信平台既能在LRU之间（在分布于整个飞机的子系统总线上）提供健壮分区隔离，也能在LRM之间(在机柜内的背板总线上)提供健壮分区隔离。这种平台要设计成能给宿主应用提供健壮分区的通信服务，即使在任何应用内部或通信网络自身出现软件或硬件单点故障的情况下。

该平台要能允许通过采用分区隔离的容错数字通信网络把一套标准的、可配置的硬件电路板(顶层级别、包括有软硬件模块的平台)的连接在一起，组装成特定应用的容错网络，如图D-2所示。



图D-2　分布式的模块化平台

D.2.2　平台和模块的定义

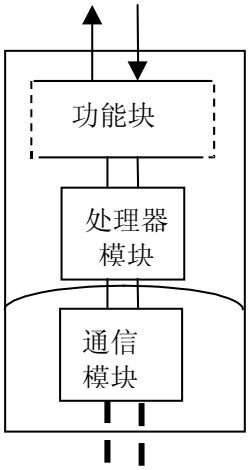
本范例中的平台包括有三个标准的硬件电路板(见图D-2)，当按照模块化系统架构进行组合时，每一个硬件电路板都被设计成能提供一组确定的功能：

－通用处理模块(GPM)

－电源模块(PSM)

－ I/O模块(IOM)

每个电路板都可能是一个在范例1中所讨论的单LRU平台。



图D-3　公共模块结构

在本范例中，所有的电路板都共享一种公共的结构(见图D-3)，包括有：

－处理器模块(可能已按范例1的描述进行了分区)

－通信模块(对通信资源进行健壮分区隔离)

－功能块(对每个硬件电路板都是专用的)

该平台也使用*核心软件组件*，这种组件给应用提供统一的API：

－实时操作系统模块(可能已按范例1的描述进行了分区)
－故障管理
－健康监控组件。

利用这种通用平台，根据需要，通过使用与核心软件有交互关系的多个基本模块的实例，将一个或几个应用综合在一起。这种架构及其模块是高度可组合的：基于这种平台的应用，可以根据分区隔离机制所支持的严格接口定义，各自独立地进行开发。这样在综合上要付出的工作量通常较少。

D.2.3 在本系统中呈现的IMA关键特性

资源的共享，健壮分区隔离:

这种分布式平台的设计要能在通信层次上提供健壮分区隔离。这种平台要基于一种同步、有余度的数据总线来建立这种属性。对通信通道的访问通过专用的通信模块实现，这种通信模块能自主地执行一种静态通信调度。这些模块的正常操作由部署在网络中的独立监护单元（guardian units）进行进一步的监控。这些监护单元只允许一个模块在指定的时间内对共享的通信资源进行访问。使用形式化的正确性证据、验证和确认测试进行的分区隔离分析表明这种架构能够容忍任意节点的失效：分布式平台将能隔离任意一个宿主应用中的单个故障(硬件或软件故障)，并能防止对其它应用所配置(硬实时)的通信活动的任何干扰。

多个应用的宿主，再鉴定的影响:

由于分布式平台的分区隔离需求是按照满足等级A(DO-178/ED-12(参考[2]))进行开发的，不同危害等级的多个应用就能在这种平台上独立地实现并进行综合。针对网络上的各种通信，一种时间触发的通信模块要支持在时间和值域方面有准确定义的接口。这种接口可以在设计的早期中进行冻结，后续单独的应用则可以根据这种接口规范来实现。通过使用与最终系统完全相同的接口规范，与其它应用的交互就能够模拟出来，这样，当其它应用要综合到该平台上时，就不会改变该平台中接口的时序和取值特性。因此，平台上新增应用的综合与修改就不会对以前综合过的应用的验证工作产生任何影响。

平台与应用之间的API接口:

要提供的应用要简单、可配置且有基于状态消息的API，这种API对于平台上的故障管理和健康管理组件，具有定义明确的和可验证的时序与取值的特性。

平台配置数据:

为了使操作系统组件、通信模块、故障管理和健康管理组件都工作起来，就要用配置表来

配置平台。

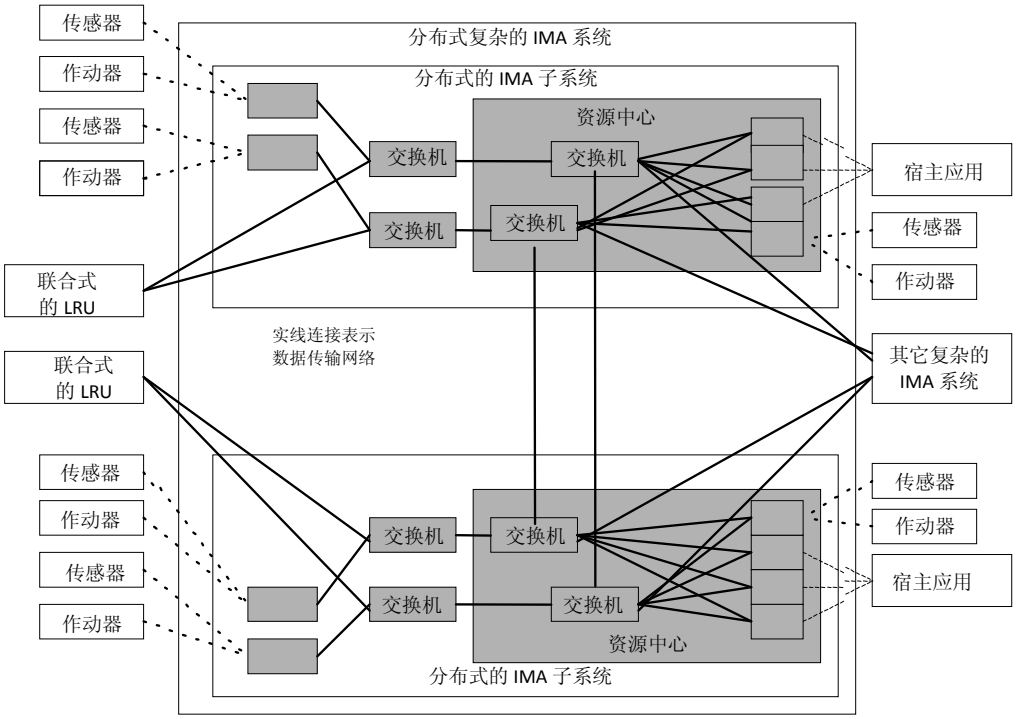
故障管理，监控监控:

只要通信故障通过健壮分区隔离机制进行处理，那么节点失效就可以通过启动冗余模块上的应用复本来屏蔽。平台上的通信模块能提供一种冗余的、确定性消息的传输服务。基于这种基本服务，冗余模块就能综合到这种平台上。通过核心软件组件提供的这种服务，应用就能从故障管理中解脱出来。但它们还要报告出有关硬件模块和在这些硬件模块上宿主的应用组件的健康信息。

D.3 举例3：确定分布式复杂IMA系统的边界

D.3.1 本范例的目的

本范例确定分布式复杂IMA系统的边界范围，并介绍对故障管理和故障报告的考虑。图D-4 提供了一种分布式复杂模块化航空电子系统的范例。



图D-4 分布式的复杂IMA系统

D.3.2 平台和模块的定义

该系统的主要架构元素就是计算资源、数据传输网络和远程I/O单元(RIU)。网络包括位于飞机远处和资源中心的网络交换机、接口的端节点和无形的传输协议。RIU和IOM(I/O模块)是类似的设备，只是一个位于远处，而另一个是在资源中心。每个模块都可以是范例1中所讨论的那种简单LRU平台的实例。有一点很清楚，图D-4没有指定特定功能接口的

实现。飞机系统有很多种方法可以使用这种分布式的复杂IMA系统资源。对于具体的飞机系统或功能，这种使用资源的实际方法将取决于系统或功能的需求。

D.3.3 在本系统中呈现的IMA关键特性

故障管理，健康监控

一个关注的特性就是在分布式复杂IMA系统中出现的失效对飞行座舱造成的影响。这种情况可以分解到一种条件，在这种情况下，成组的级联失效可以由分布式复杂IMA系统、宿主在CPM上的多种应用来报告，也可能由其它分布式的复杂IMA系统或联合式系统来报告。当某人开始观察这样的问题时，必须观察分层内容的情况，这种分层内容情况要报告给飞行座舱和/或记入维护的飞行日志中。

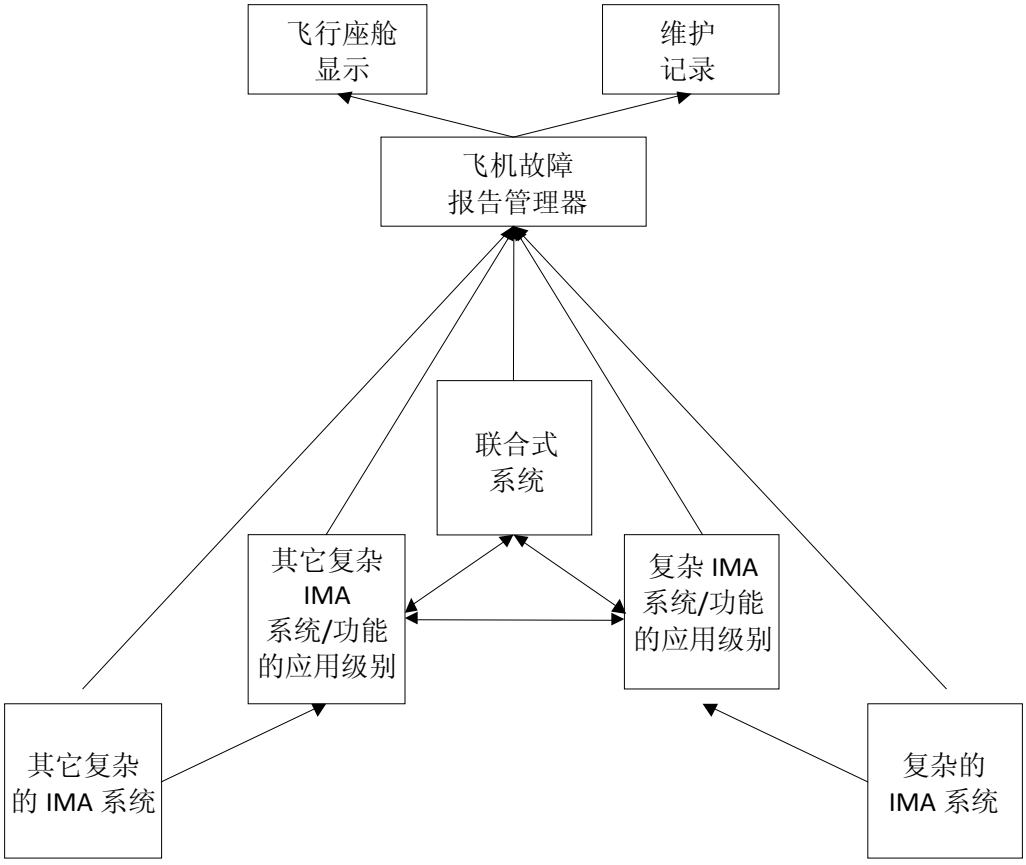


图 D-5 故障报告的层次结构

图D-5给出了故障报告与管理的一种可能的层次结构，其目的是要说明以下内容。

- 在IMA系统、飞机系统功能和IMA宿主应用与联合式系统之间存在有复杂的交互关系，这种交互在发生失效时会导致指示多处失效。剩余未被检查的（失效）指示将会增加飞行机组的工作负担，并会让维护人员混淆（迷惑）；
- 需要提供出这样的功能性，能够正确地确定出要显示到飞行座舱的消息、告警和影响，以及要在维护日志中出现的信息；

一飞机级的故障报告功能不属于特定的复杂IMA系统的内容。

D.4 举例4：软件设计的无线电例子

D.4.1 平台和模块的定义

本范例是一个软件设计的无线电(SDR)平台架构。例如，无线电包括有8.33 kHz和S模式应答机（transponders）。希望不同的公司以不同的时帧格式开发这种平台，并实现这种无线电应用。

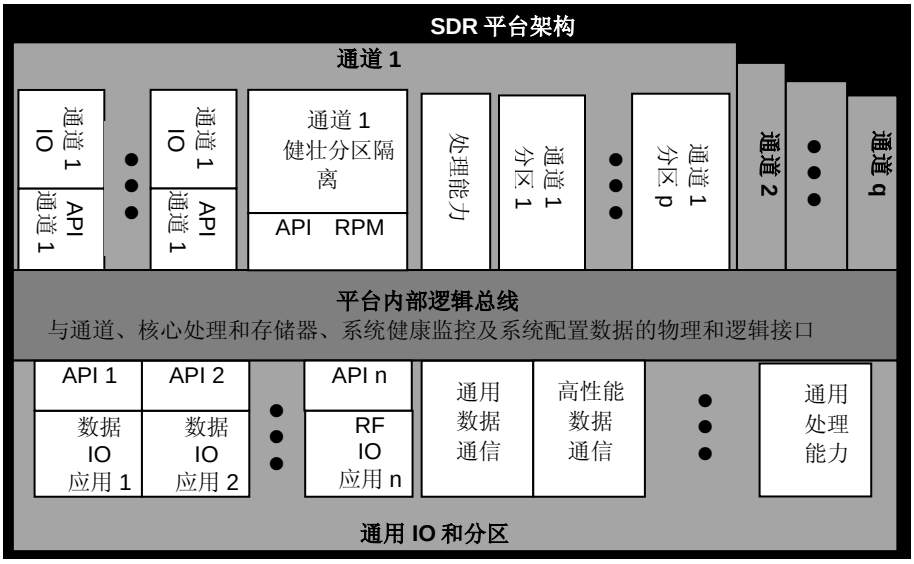
通过收集大量可用的无线电应用，这种SDR平台能在宽阔的频率带范围内同时支持多种不同的无线电。为了满足无线电功能的特殊需求，需要开发一个详细的规范，以适应具有灵活性的应用的重新宿主。

本范例描述了有两个级别的健壮分区隔离；采用存于内存中的应用进行的重构，（一个分区）能满足特定要求接口需求的高性能接口，以及（另一个分区）几乎没有提出需求的结构化兼容接口。

D.4.2 平台和模块的定义

这种架构由平台内部的逻辑总线和若干通道模块组成，如图D-6所示。这种平台内部的逻辑总线包括通道的物理和逻辑接口、核心处理与存储器、系统健康监控器以及系统配置数据。一个通用的数据通信模块能够适应应用的重新宿主[11]。在通用模块（能力）不够的情况下，即需要强实时控制时，应针对这些情况提供高性能的数据通信接口。

（11 公共对象请求代理的架构(CORBA)可以作为一种方法（途径）来使用）



图D-6 SDR IMA平台架构

共用模块和应用（带有相应的API）都包括在基本的平台中，并且可以与平台一起认可。这里包括以太网或ARINC 429、RF信号接口和音频接口。

一个平台有若干个通道模块，这些模块相互间有严格的分区。一个通道模块原则上支持单个无线电功能，但这不是需求。一个通道所包括的模块能提供数据和无线电频率的I/O应用以及API、多个通用处理能力，以及能够监控应用、API和通用处理分区的健壮分区监控器。

D.4.3 在本系统中呈现的IMA关键特性

健壮分区隔离-进入通道

分区隔离到（多个）通道能简化对多个无线电功能的实现。分配到平台上的无线电功能独立于通道的指定，因为每个通道都有相同的资源需求。这种架构能确定通道资源的健壮分区隔离。

在每一种情况中，对通道的操作和控制都要通过平台内部总线进行。没有规范规定在一段时间内一个通道只提供一套无线电，但这已作为通常的原则得到公认。通道有可能共享，且有些无线电可能要求一套以上的通道。

健壮分区隔离-在通道内

一个通道能分成几个分区，在某个通道模块中的隔离分区，允许无线电发送部件或接收部件进行相互完全隔离的处理。例如，军事上可以利用这一特征，对已分类的和未分类的数据进行隔离。多个I/O模块能够支持多个RF和进行接收、发送、数据与控制的数据端口。

利用存储在存储器中的应用重配置

一组可用的无线电应用可以存储于带有通用处理能力的存储器中，通过提供所需要的通道空间、把无线电应用从存储器加载到分区中、更新系统配置并激活无线电，这些存储的无线电应用就可以工作起来。

数据通信-高性能与通用接口

只要可能都要使用通用数据通信接口来提高应用可重新宿主的特性。当通用接口不能满足无线电的性能需求时，就要使用高性能的接口。