

doi:10.3969/j.issn.1001-893x.2016.08.016

引用格式:赵长啸,阎芳,张帆,等.综合模块化航电系统驻留功能适航审定要求分析[J].电讯技术,2016,56(8):923-927.[ZHAO Changxiao, YAN Fang,ZHANG Fan,et al. Airworthiness certification requirements analysis of hosted function of integrated modular avionics system[J]. Telecommunication Engineering,2016,56(8):923-927.]

综合模块化航电系统驻留功能适航审定要求分析^{*}

赵长啸^a, 阎芳^a, 张帆^b, 王鹏^{**a}

(中国民航大学 a. 天津市民用航空器适航与维修重点实验室;b. 安全科学与工程学院,天津 300300)

摘 要:综合模块化航电系统以功能分区的形式在资源共享平台上综合了多种航电功能,系统功能与硬件平台不再具有唯一对应性,给适航审定技术带来了困难。首先分析了综合模块化航电系统的特点和民机产品的适航方式,然后依据局方的相关技术标准文件,给出了综合模块化航电系统驻留功能的适航需求分析,最后总结了审定要素和评审要求分析。相关研究成果有助于解决功能-硬件分离的航电产品的取证问题,是对现有综合模块化航电系统审定体系的有效补充。

关键词:综合模块化航电系统;驻留功能;适航审定

中图分类号:V243 文献标志码:A 文章编号:1001-893X(2016)08-0923-05

Airworthiness Certification Requirements Analysis of
Hosted Function of Integrated Modular Avionics System

ZHAO Changxiao^a, YAN Fang^a, ZHANG Fan^b, WANG Peng^a

(a. Civil Aircraft Airworthiness and Repair Key Laboratory of Tianjin;
b. College of Safety Science & Engineering, Civil Aviation University of China, Tianjin 300300, China)

Abstract: The feature of the integrated modular avionics (IMA) system is that it uses the shared resource and robust partitioning to host multiple functions. The system function and hardware platform no longer have the unique correspondence, which poses a great challenge for the tradition airworthiness certification which aims at the federate avionics. Firstly, the characters of the IMA system and the airworthiness methods of the avionics product are analyzed. Secondly, according to the relevant technical standards document, the certification requirements of the hosted function of IMA system are summarized, . Finally, the review and validation elements for the hosted function of IMA system are concluded. The research in this paper is helpful to solve the airworthiness problem of the avionics products that do not rely on specific hardware, which is an effective complement to the existing IMA airworthiness system.

Key words: integrated modular avionics system; hosted function; airworthiness certification

1 引 言

机载电子系统是民用飞机的“大脑和中枢神

经”^[1]。随着微电子与计算技术的飞速发展,综合模块化航电系统(Integrated Modular Avionics, IMA)

^{*} 收稿日期:2016-01-05;修回日期:2016-04-08 Received date:2016-01-05;Revised date:2016-04-08
基金项目:国家重点基础研究发展计划(973 计划)项目(2014CB744902);国家自然科学基金委员会-中国民航局民航联合研究基金资助项目(U1533105);中央高校基金项目(3122015C028)

Foundation Item: The National Basic Research Program of China(973 Program)(2014CB744902); Joint Fund of the National Natural Science Foundation of China and the Civil Aviation Administration of China(U1533105); The Scientific Research Foundation of Civil Aviation University of China(3122015C028)

^{**} 通信作者:pwang_cauc@163.com Corresponding author:pwang_cauc@163.com

以其资源平台的通用性和强大的资源配置力逐渐开始替代传统的联邦式航电系统。空客 A380、A350，波音 777、787，以及我国商飞自主研发的 C919、C929 都选择了 IMA 系统架构^[2]。系统体系结构的变革在带来系统能力大幅提高的同时，也给系统适航审定工作带来了挑战^[3]。

2005 年 8 月 1 日，马来西亚航空一架从珀斯飞往吉隆坡的波音 B777-200 客机在自动驾驶阶段，飞行显示仪器显示飞机速度过低，之后飞机超速并出现失速，飞机紧急降落在珀斯，该事故未发生人员伤亡。澳大利亚运输安全局 2007 年发布的最终事故报告^[4]显示，事故发生原因是大气数据及惯性基准系统重构时启用了已失效的大气数据惯性基准单元，而“最初系统设计、安全性评估过程中未能覆盖此问题”。美国联邦航空管理局（Federal Aviation Administration, FAA）官员 Kirk Baker^[5]通过引用一个飞机起飞过程中反推力的虚假信号导致襟翼缩回的事故说明了 FAA 对传统适航审查方法对 IMA 系统适用性的担忧。

在 IMA 系统中，不同航电功能共享硬件平台，各驻留功能执行着原联邦式系统中各设备的功能，但并不存在独立的设备，原有的针对各硬件独立设备的适航审定方法难以适用。为了解决这一问题，FAA 提出了功能 TSO（Functional TSO, FTSO）批准的概念，并在 AC 20-170 中列举了部分 IMA 系统中可能涉及的 TSO 功能。

目前，我国局方针对 IMA 系统的审定指导文件 TS0-C153 已进入征求公众意见阶段，同时我国的 C919 大型客机已总装下线，进入技术审查阶段，其 IMA 系统的审定问题是我国局方亟需解决的一项技术难题。本文针对 IMA 系统中驻留应用特点进行分析，同时结合我国现有的民机产品取证方法及适航审定工作经验，给出 FTSO 的审定关注点及适航评审要素，以完善 IMA 系统审定体系，为大飞机的适航审定工作提供技术支持。

2 IMA 系统特性及适航方式

2.1 IMA 系统特性

IMA 是一系列灵活、可重用、协同的软/硬件资源集成在一起形成的服务平台。IMA 系统由其系统架构确定，包括平台和一系列的驻留功能，具体如图 1 所示。

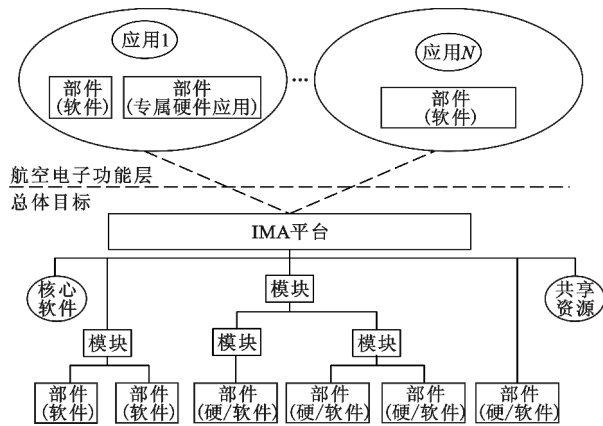


图 1 IMA 系统架构

Fig. 1 The architecture of IMA system

IMA 系统两个主要的组成部分为平台和驻留功能。IMA 平台的特性见表 1。

表 1 IMA 平台特性

Tab. 1 The features of IMA platform

主要 IMA 平台特性	描述
平台资源共享	一个 IMA 平台通过分区和其他保护功能(例如 HIRF/IEL、供电、自检)驻留多个应用
强健分区	确保共享资源可以按需提供给驻留功能,并且避免资源受到任何应用异常行为的影响;确保任何驻留功能或功能不会受到其他应用或功能非预期的影响
确定的交互接口	隔离平台和驻留功能间更改;允许在尽量减少对驻留功能影响情况下,更改 IMA 平台,或反之
资源可配置	可配置 IMA 平台资源,以支持不同驻留功能的资源需求

IMA 驻留功能重要特性见表 2。

表 2 IMA 驻留功能特性

Tab. 2 The features of hosted function

主要特性	描述
设计独立,分别获取累积信任度	驻留功能可以在平台上分别单独进行验证,而无需安装所有应用
应用如果与其他应用不存在非预期交互,则可集成在 IMA 平台中	如果不同的应用互相独立执行并验证,则应将它们作为完整的驻留功能组合,集成在平台中;应该对应用间的交互进行验证
可重用	应用模块化和移植性可以使其在不同的工程和产品中方便使用
可独立更改	每个应用在更改时,不会影响其他应用和平台资源、模块;应确定所有的影响,并与受影响的部件进行协调

2.2 机载设备适航方式

机载设备取得适航批准的方式一般分为 4 类:“技术标准规定项目批准书”(CTSOA)、“零部件制

造人批准书”(PMA)、“随航空器型号合格审定一起批准”(“随机批准”)及局方规定的其他方式。其中 CTSO 取证属于单独批准的方式。目前 CTSOA 件主要有 4 大类: 飞行仪表, 如空速表、自动驾驶仪和飞行指引设备等; 通信设备, 如机载无线电信标接收设备和机载选择通话设备等; 结构组件, 包括机械紧固件、轴承及液压软管组件等; 机内物品, 如航空器座椅、救生衣和安全带等。“技术标准规定”主要规定了该 CTSO 所涉及设备必须符合的最低性能标准。

可见, CTSO 批准不针对具体的机型, 获得 CTSO 批准的设备具有较强的通用性, 使其能覆盖较宽的产品范围(如既能符合 23 部小型飞机的要求, 也能符合 25 部大型飞机的要求)。截止到 2013 年 3 月 15 日, 国内已获颁 CTSOA 的民机产品达 118 项。

3 IMA 驻留功能审定需求

IMA 系统功能与具体的航空器或发动机应用相关, 其可以驻留不同的系统功能, 而这些功能传统上是由功能和物理独立的系统实现的。当各功能以软件形式驻留在 IMA 系统中时, 需考虑耦合资源对各不同应用的影响。尤其当不同安全性需求的系统功能集成到同一 IMA 平台时, 需表明整个 IMA 系统的符合性, 因此驻留功能对可用性、完好性、安全性等问题提出了特别的审定关注。

3.1 平台级 (Platform) 需求

(1) 可用性

功能性能——将驻留的飞机级功能分配给 IMA 系统架构。

资源管理——分配 IMA 平台资源、共享和专用资源的控制和被多个驻留飞机功能或应用所使用的 IMA 平台资源保护。

可靠性和维护性——对主最低设备清单 (Master Minimum Equipment List, MMEL), 飞机派遣能力、修理、更换和完成确保持续适航能力的维护活动的影响。

健康监控——监控系统状态和运营维护相关事件。

(2) 完好性

设计保证, IMA 安全性和防护特征, 故障探测和分区——保护驻留功能和应用的能力, 以确保独立性, 并避免在使用共享资源时出现非预期交互。

(3) 安全性

安全性评估——确保适当的架构、设计保证、失效保护, 考虑共模因素和飞机功能失效组合的影响, 以及适航性。

故障管理、故障报告和恢复特性——探测和确定故障、失效和异常行为, 并提供适当的回应。

(4) 组合性

如果集成过程不会改变任何已集成应用的需求验证结果, 则允许将新应用集成在 IMA 平台中。

在可组合的架构中, 系统需求与分配给 IMA 应用的需求一致。对于具有明确接口范围的 IMA 平台, 可以对其中集成的部分应用进行接受。强健分区是达成该目标的前提。

3.2 软件级需求

许多 IMA 系统的驻留功能使用现场可加载软件 (Field Loading Software, FLS) 作为 TC/STC/ATC/ASTC 安装的组成部分。FLS 是那些可以不需要将设备从航空器安装中移除即可加载到驻留硬件中的软件。FLS 也可以包含在维修站或航材店内加载到航线可更换组件 (Line Replaceable Unit, LRU) 或硬件部件中的软件。FLS 可以是执行码或数据, 例如数据库。当为 FLS 的使用寻求批准的时候, 应该考虑如下内容:

(1) DO-178 要求

FLS 应该满足 RTCA DO-178B/C 的目标和指南, 或申请人和局方审查代表达成共识的其他可接受符合性方法。FLS 应该加载到在 DO-178B/C 目标验证测试阶段软件验证所需的目标计算机和硬件构型中。必须可以通过某种方法确保 FLS 加载到正确的航空器已批准的 IMA 构型中。

如果 IMA 系统的冗余功能是现场可加载的, 则申请人应确保这些功能有相同的软件构型, 除非通过安全性评估过程支持不同软件构型的组合, 并且该组合也获得航空器构型和型号设计的批准。

申请人应该通过一些活动来保证加载的软件已获得批准, 并且没有被破坏——例如, 循环校验或其他数据转换完好性检验。不同的数据完好性算法对数据转换正确的保证等级不同。确保使用的算法满足加载数据的软件等级所要求完好性水平。

(2) 存储媒介要求

如果申请人为加载 FLS 提出了多种媒介, 例如软盘、海量存储设备或光盘等, 则无论采用哪种媒介进行加载都应该符合要求。申请人应该表明机载设备软件部件号可以通过机载设备、便携式设备、自动构型管理机制, 或其他适当的方式来验证。

(3) 保护机制要求

IMA 系统应具备加载保护机制, 禁止在飞行阶段加载 FLS。这些机制的可靠性应与飞行阶段软件意外加载相关失效状态一致。对于执行电子飞行包功能的可加载 IMA 软件部件, FAA AC120-76A“电

子飞行包计算设备的审定、适航和运行批准指南”有详细说明。

(4) 安装文件要求

FLS 安装文件应该详细说明如下内容：

对于需加载软件的冗余系统，航空器和硬件的适用性及交叉混合性容差；

验证程序，以确保软件正确加载到已批准可兼容的目标计算机和存储设备中；

表明符合本 AC 指南所要求的任何加载后验证和/或测试程序；

采取的活动——例如如果存在不成功的加载，则禁止航空器派遣；

索引已批准的加载程序；

要求用来记录和维护构型控制的维护记录接入程序；

索引相关航空器飞行手册 (AFM)，航空器飞行手册补充材料 (AFMS) 或操作人员手册 (如必要)。

3.3 恢复机制需求

由于环境的不可预见性，IMA 驻留功能、IMA 驻留功能集合或一个完整的 IMA 机柜都可能在驻留的 IMA 硬件部件没有发生永久性失效的情况下，意外关闭。IMA 系统必须有能力重启任何持续运行对系统或航空器安全性评估产生影响的驻留功能或功能集合。

IMA 系统中 IMA 驻留功能或系统重启特性应在探测到安全性关键功能丧失时自动启动 (如可行)。

如果自动可恢复特性不可行，并且需要由机组启动，即执行非自动恢复特性，则应该制定保护机制和操作系统，以避免机组错误启动可恢复特性。

系统设计应该仔细考虑在重启已失效 IMA 驻留功能时，需要自动尝试启动的次数。当失效 IMA 驻留功能反复自行关闭时，无限制的尝试重启会增加机组负担，分散注意力。如果多次重启尝试后仍然失效，则不应该再对该失效 IMA 资源进行重启。系统重启机制设计应该考虑可能会引发重启的原因，并确定在断定系统失效前尝试重启的适当次数。影响该架构的因素是与 IMA 功能丧失相关的失效状态，功能或功能组合多次重启对接口系统的影响，以及来自非 IMA 系统的功能裕度。

IMA 设计不应该通过拨动航空器断路器来重启任何 IMA 驻留功能。如果使用由机组人员启动的手工恢复特性，则设计一种除简单拨动断路器以外的方式完成。申请人应该评估所有飞行阶段正常和失效条件下自动和/或手动启动恢复特性的影响。申请人应该评估所有飞行阶段手工或自动启动时功能丧失的影响。

4 IMA 驻留功能审定要素和评审要求

IMA 系统驻留的审定过程涉及对系统驻留功能软件、硬件平台要素、功能综合等各方面，本文以检查单的形式对各部分的审定关注点进行了归纳，如表 3 所列。

表 3 IMA 系统驻留功能适航评审要素及评审要求
Tab.3 Airworthiness review and assessment requirements for the hosted function of IMA system

项目分类	适航审定要素及评审要求
驻留硬件平台	(1) 当与其他硬件单元和功能软件在指定飞机上综合时，每个硬件单元的设计和制造是否可提供不会破坏或降低飞机适航能力的安装方法？
	(2) 除了不会引起火势快速扩散的小部件 (例如旋钮、紧固件、密封件、扣眼和小电子部件)，其他所有使用的材料是否是耐火的？
	(3) 硬件单元及其试验程序的设计都是否使得该程序的应用能导致任何明显危害硬件单元性能和可靠性的情况？
驻留功能应用	(1) 接口定义部分：是否确定所使用的 IMA 平台资源；
	(2) 需量化所需的 IMA 平台资源 (接口定义部分)；
	(3) 将驻留功能安全性评估映射到 IMA 平台安全性评估和能力 (即 PSSA、FHA 和 CCA)；
	(4) 是否为驻留功能定义 HM/FM 需求，并定义与 IMA 平台 HM/FM 功能的接口；
	(5) 是否确定 IMA 平台外的专用资源 (例如应用专属硬件)；
	(6) 是否具体说明专用资源的环境鉴定等级；
	(7) 是否将应用集成在平台上，并执行软件/硬件集成测试；
	(8) 是否评估针对 IMA 平台性能的人为因素需求。
认证部件集成	(1) 具有 CTSO 认证并不能取消或减少申请人的责任——应确保所安装的 IMA 系统 (包括所有 CTSO 认证部件) 满足相关航空器或发动机规章要求；
	(2) 功能 CTSO 一般不涉及与其他航空器功能或硬件/软件在整个 IMA 系统中的集成；每个 CTSO MPS 通常假设功能是独立的，并且没有在航空器中集成的相关要求；在表明整个 IMA 系统的符合性时，除 CTSO 认证外还需要完成其他的一些工作 (详见 RTCA DO-297, 4.4 节)；
	(3) CTSO 认证 IMA 部件的安装说明应该包含申请人和/或 IMA 研制商/系统集成商所需的所有信息，以将 CTSO 认证的 IMA 部件完全集成在 IMA 系统中。

续表 3

项目分类	适航审定要素及评审要求
系统资源分配	(1) IMA 系统的处理吞吐量是否考虑了应用所需的执行时间、报文转换次数、平台开销和所有处理需求; (2) 计算资源和网络带宽的确定考虑与上下文转换、数据调度和其他限制相关的开销; (3) IMA 系统架构是否可以支持飞机功能和驻留功能最高层级的完好性和可用性。
健康监控和故障管理	(1) IMA 平台是否为 IMA 平台模块提供基础的健康监控和故障管理, 具体包括受监控部件和方面的识别、每个应用的健康确定、IMA 系统整体的健康确定、对每类失效或异常行为进行回应、飞行机组通告和信息、维护活动和报告的控制、冗余管理、单粒子翻转; (2) 共享数据库是否符合 RTCA DO-200 的指南。

5 结束语

本文分析了 IMA 系统及相关电子设备的取证需求, 梳理了 IMA 系统驻留功能的适航审定需求, 分析了驻留功能所特有的平台需求、软件需求及恢复特性, 最后给出了典型 IMA 驻留功能的审定要素和评审要求。

下一步的工作将针对 IMA 系统的“增量审定”特性开展研究。与传统的审定任务不同, IMA 系统部分增量审定任务完成时, 全系统的构型尚未确定, 因此其增量批准任务需要特别的批准信函, 明确当前审定任务的认可内容, 并保证审定任务进入下一阶段。

参考文献:

[1] 熊华钢, 王中华. 先进航空电子综合技术[M]. 北京: 国防工业出版社, 2009.
XIONG Huagang, WANG Zhonghua. Advanced integrated avionics technology [M]. Beijing: National Defence Industry Press, 2009. (in Chinese)

[2] 王鹏, 赵长啸, 马赞. 综合模块化航电系统失效模型分析[J]. 电讯技术, 2013, 53(11): 1406-1411.
WANG Peng, ZHAO Changxiao, MA Zan. Failure model analysis of integrated modular avionics system[J]. Telecommunication Engineering, 2013, 53(11): 1406-1411. (in Chinese)

[3] 赵长啸, 阎芳, 王鹏. 综合模块化航电系统适航审定要求分析[J]. 电讯技术, 2015, 55(10): 1134-1140.
ZHAO Changxiao, YAN Fang, WANG Peng. Airworthiness certification requirements analysis for the integrated modular avionics system[J]. Telecommunication Engineering, 2015, 55(10): 1134-1140. (in Chinese)

[4] Australian Transport Safety Bureau. In-flight upset event 240km North-West of Perth, WA, Boeing Company 777-2000, 9M-MRG, 1 August 2005 [R]//Aviation Occurrence Report 200503722. Canberra, Australia: Australian Transport Safety Bureau, 2007: 1-38.

[5] BAKER K. Filling the FAA guidance and policy gap for systems integration and safety assurance[C]//Proceedings of 2011 IEEE/AIAA 30th Digital Avionics Systems Conference (DASC). Seattle, WA: IEEE, 2011: 1-4.

作者简介:



赵长啸(1989—), 男, 山东人, 2013 年于北京航空航天大学获博士学位, 现为中国民航大学适航审定技术与管理中心助理研究员, 主要从事民机航电系统设计与评估、航空电子综合研究;

ZHAO Changxiao was born in Shandong Province, in 1989. He received the Ph. D. degree from Beihang University in 2013. He is now an assistant researcher of Civil Aircraft Airworthiness Certification Technology And Management Research Center, Civil Aviation University of China. His research concerns avionics system design and evaluation.

Email: airworthiness@yeah.net

阎芳(1982—), 女, 山东人, 2005 年于法国国立航空工程大学获硕士学位, 现为中国民航大学适航审定技术与管理中心副研究员, 主要从事民机系统安全性设计与评估、机载电子软件适航技术研究;

YAN Fang was born in Shandong Province, in 1982. She received the M. S. degree from the Institut Supérieur de l'Aéronautique et de l'Espace in 2005. She is now an associate researcher of Civil Aircraft Airworthiness Certification Technology and Management Research Center, Civil Aviation University of China. Her research concerns aircraft system design and evaluation of safety, software airworthiness technology.

Email: fyan@cauc.edu.cn

张帆(1993—), 女, 甘肃人, 现为中国民航大学适航审定技术与管理中心硕士研究生, 主要从事民机系统安全性设计与评估技术研究;

ZHANG Fan was born in Gansu Province, in 1993. She is now a graduate student. Her research concerns system safety design and assessment in civil aircraft.

Email: 105593605@qq.com

王鹏(1982—), 男, 天津人, 副研究员, 2005 年于法国国立航空工程大学获硕士学位, 现任中国民航大学适航审定技术与管理中心副主任, 主要从事民机系统安全性设计与评估、机载电子硬件适航技术研究。

WANG Peng was born in Tianjin, in 1992. He received the M. S. degree from the Institut Supérieur de l'Aéronautique et de l'Espace in 2005. He is now the Deputy Director of Civil Aircraft Airworthiness Certification Technology and Management Research Center, Civil Aviation University of China. His research concerns aircraft system design and evaluation of safety, electronic hardware airworthiness technology.

Email: pwang_cauc@163.com