（奥）罗兰·沃尔夫格（Roland Wolfig） 著
牛文生 等 译

综合化模块化航空电子系统的分布式平台

——对未来航空电子系统及其认证需求的见解

A DISTRIBUTED PLATFORM FOR INTEGRATED MODULAR AVIONICS

INSIGHTS ON FUTURE AVIONICS SYSTEMS AND THEIR CERTIFICATION REQUIREMENTS

航空工业出版社

综合化模块化航空电子系统的分布式平台

——对未来航空电子系统及其认证需求的见解

（奥）罗兰·沃尔夫格（Roland Wolfig） 著
牛文生 等 译

航空工业出版社
北京

内 容 提 要

本书描述了综合化模块化航空电子（IMA），特别是分布式综合化模块化航空电子（DIMA）系统的平台和模块化认证。本书共计8章，第1章为引言部分，介绍（分布式）综合化模块化航空电子系统和模块化认证的概念，第2章讲述航空电子系统架构，第3章为通信系统，第4章是关于系统架构的内容，第5章为模块化认证，第6章介绍分布式综合化平台的解决方案，第7章对DIMA的发展进行展望，第8章是对本书的总结。

本书适合航空电子相关领域技术人员使用，也可以作为高等院校相关专业学生的参考用书。

图书在版编目（CIP）数据

综合化模块化航空电子系统的分布式平台：对未来航空电子系统及其认证需求的见解／（奥）沃尔夫格（Wolfig，R.）著；牛文生等译. --北京：航空工业出版社，2015.3

书名原文：A distributed platform for integrated modular avionics - insights on future avionics systems and their certification requirements

ISBN 978-7-5165-0664-6

Ⅰ.①综… Ⅱ.①沃…②牛… Ⅲ.①航空电气设备—电子系统 Ⅳ.①V242

中国版本图书馆CIP数据核字（2015）第026279号

北京市版权局著作权合同登记

图字：01-2014-7710

Publication of this translation in consultation with OmniScriptum.

综合化模块化航空电子系统的分布式平台

——对未来航空电子系统及其认证需求的见解

Zonghehua Mokuaihua Hangkong Dianzi Xitong de Fenbushi Pingtai

——Dui Weilai Hangkong Dianzi Xitong Jiqi Renzheng Xuqiu de Jianjie

航空工业出版社出版发行

（北京市朝阳区北苑2号院 100012）

发行部电话：010-84936597 010-84936343

三河市华骏印务包装有限公司印刷 全国各地新华书店经售

2015年3月第1版 2015年3月第1次印刷

开本：710×1000 1/16 印张：8.25 字数：139千字

印数：1—3000 定价：60.00元

译 者 序

在多年从事综合化模块化航空电子（Integrated Module Avionics，IMA）平台的研究过程中，一直感到国内缺乏系统、完整的理论基础。尽管国内的研究者从国内外公开发表的文献中获得了不少信息，也开展了工程项目研制，但是知识点非常零散，没有形成完整的知识体系。缺乏完整的理论基础使我们对 IMA 的许多基础问题认识不足，对很多问题知其然不知其所以然，特别是对下一代 IMA 的发展趋势缺乏足够的预测能力，自主创新能力不足。近年来，中航工业西安航空计算技术研究所的下一代综合化模块化航空电子系统平台先期研究项目组在研究过程中，感到始终有两个问题一直没有得到明确的结论：IMA 究竟是什么？除了目前我们能够看到的诸如波音 787/777、空客 A380 等先进民用客机的航空电子系统，以及 F－22、F－35 等第四代军用飞机的航电结构外，下一代的 IMA 结构形式可能是什么呢？

通过一次偶然的机会发现国外出版的本书英文版，读后感到该书对近年来 IMA 的一些新技术做了较为系统的总结，于是就推荐作为本研究所内研究生学习 IMA 技术的辅助教材。在对译稿进行多次校对的基础上，最终将本书中文版在航空工业出版社正式出版，希望能够帮助国内更多的飞机系统设计师、教师和学生全面了解 IMA 的进展情况。

本书中既系统总结了 DIMA 的优点，也指出了目前技术上存在的困难和可能的解决方案，以及带来的技术难度更大的模块化

认证问题（实质上是系统安全性设计和验证问题）。从中我们可以得出结论：DIMA 2.0 目前尚处于研究阶段，距离工程实现还有许多问题需要解决，需要国内外学者继续深入地研究。

本书由牛文生组织翻译，牛文生、李亚晖、郭鹏、孙东亚、刘洋、胡国、李明娟、刘小剑、段宇博、白林亭、蒋挺宇、韩伟等完成了翻译的初稿；牛文生对全书进行了统稿；周耀荣、谢克嘉和刘英华进行了校对。限于译者水平，难免有错误和疏漏之处，恳请读者不吝指正。

摘　要

综合化模块化航空电子（IMA），尤其是分布式综合化模块化航空电子（DIMA）以及模块化认证，是目前航空航天界广泛讨论的方法。IMA 采用模块化架构方法，利用硬件资源共享并将多个飞机功能综合于一个硬件单元的思想，旨在减小重量、体积、机上布线、功耗和成本。

与已研制出的 IMA 系统不同，DIMA 架构为所使用的硬件提供了更大的灵活性。也就是说，并不一定要将所有硬件都放在一个箱体里，硬件可以分解为多个较小的硬件单元，这些硬件单元将由一个安全关键的通信系统连接，并广泛地分布在整个飞机上。

模块化认证利用 IMA/ DIMA 系统提供的模块化特点，将认证工作分割成几个部分。通过与基于优化的流程的高效认证方法相结合，减少了开发时间和研制工作量。

基于上述前提，我们引入了分布式综合化平台解决方案（DIPS）的概念。这一概念以 DIMA 架构为基础，定义了灵活的平台所必需的约束和服务。该平台与驻留的应用软件组合在一起，通过提供模块之间的数据交换和不同模块封装技术，就能够承担飞机中所有安全关键功能的处理任务。

本书描述了这样一个平台，讨论了它的属性和认证要求，识别了它的需求和约束，并考虑了它的商业机会和未来应用。

术　语

本书使用了下列术语，这些术语也是统一理解本书内容的基础。

- 飞机功能——一组硬件和软件模块。它们共同提供了所需要的航空电子功能（如飞行控制系统、自动驾驶仪、电力分配等）。
- 应用软件——具有一组确定接口的软件，可以执行某一功能。
- 架构——提供平台的理论环境。它主要研究服务、接口、拓扑、需求、约束，以及综合和实现细节。
- 组件——自包含的硬件部件、软件部件、数据库，或它们的组合。组件本身不提供飞机的功能。
- 核心通信系统——一个分布式平台的核心组件。它是一种节点间的安全关键的、高速的连接，并必须提供一些基本的平台服务。
- 核心软件——操作系统和支持软件。它们管理资源以提供一个应用软件执行的环境。核心软件是一个平台的必备组件，一般都包括一个或多个模块。
- 主机（处理器/ CPU）——是执行核心软件和应用软件的处理单元。在与一个通信接口进行连接的时候，它是系统的一个节点。
- （D）IMA 系统——包括一个平台和一组确定的驻留应用软件。
- 模块——一个组件或一组组件的集合。它可以是软件、硬件，或硬件、软件的组合，向驻留应用软件提供资源。模块可以在飞机上分布地存在，也可以共同位于同一位置。
- 节点——一个节点由宿主机 CPU 和通信接口组成。
- 分区化——一种架构技术。向功能或应用软件提供必要的隔离性和独立性，以确保只产生应有的耦合。
- 平台——一个或一组模块。包括负责管理资源，以支持至少一个应用的核心软件、硬件和通信。平台本身并不提供任何飞机功能。平台是一种

架构的实现，它建立计算环境、支持服务以及平台相关功能，如健康监控和故障管理等。平台可以从驻留应用软件中独立出来单独进行认证。

- 可重用——先前已认可的模块和应用软件的设计保证数据，不太需要重新设计和额外验收，就可以在后续的飞机系统设计中使用。
- 子系统通信系统——除了核心通信系统，还需要提供一些平台服务的低成本的子系统通信。

目　录

第1章　引言 ……（1）

1.1　动机和目的 ……（1）

1.1.1　（分布式）综合化模块化航空电子系统 ……（1）

1.1.2　模块化认证 ……（2）

1.1.3　小结 ……（2）

1.2　相关工作 ……（3）

1.3　本书的结构 ……（3）

第2章　航空电子系统架构 ……（5）

2.1　简介 ……（5）

2.2　联合式航空电子 ……（6）

2.3　综合化模块化航空电子系统 ……（7）

2.4　分布式综合化模块化航空电子系统 ……（10）

2.5　通信系统 ……（11）

2.6　从联合式到综合化 ……（12）

2.7　联合式与综合化的比较 ……（13）

2.7.1　联合式系统的优点 ……（13）

2.7.2　综合化系统的优点 ……（13）

2.8　总结 ……（14）

第3章　通信系统 ……（15）

3.1　简介 ……（15）

3.2　通信系统分类 ……（15）

3.2.1　简介 ……（15）

3.2.2　核心通信系统 ……（16）

3.2.3　子系统通信系统 ……（16）

3.3　时间触发协议（TTP） ……（16）

3.3.1 简介 …… (16)
3.3.2 概念属性 …… (16)
3.3.3 实现属性 …… (20)
3.3.4 应用属性 …… (21)
3.3.5 小结 …… (21)
3.4 FlexRay …… (21)
3.4.1 简介 …… (21)
3.4.2 概念属性 …… (22)
3.4.3 实现属性 …… (22)
3.4.4 应用属性 …… (23)
3.4.5 小结 …… (23)
3.5 分层的 TTP 和分层的 FlexRay …… (24)
3.5.1 简介 …… (24)
3.5.2 概念属性 …… (24)
3.5.3 应用属性 …… (25)
3.5.4 小结 …… (26)
3.6 航空电子全双工交换式以太网（AFDX） …… (26)
3.6.1 简介 …… (26)
3.6.2 概念属性 …… (26)
3.6.3 实现属性 …… (28)
3.6.4 应用属性 …… (28)
3.6.5 小结 …… (29)
3.7 时间触发以太网（TT - Ethernet） …… (29)
3.7.1 简介 …… (29)
3.7.2 概念属性 …… (30)
3.7.3 实现属性 …… (30)
3.7.4 应用属性 …… (30)
3.7.5 小结 …… (31)
3.8 SPIDER - ROBUS …… (31)
3.8.1 简介 …… (31)

3.8.2 概念属性 …… (31)
3.8.3 实现属性 …… (33)
3.8.4 应用属性 …… (33)
3.8.5 小结 …… (34)
3.9 比较 …… (34)
3.10 总结 …… (35)
第4章 系统架构 …… (36)
4.1 简介 …… (36)
4.2 设计 …… (36)
4.2.1 简介 …… (36)
4.2.2 可组合性 …… (36)
4.2.3 可伸缩性 …… (37)
4.2.4 可扩展性 …… (38)
4.2.5 复杂性 …… (38)
4.2.6 可信性 …… (38)
4.2.7 分区化 …… (39)
4.2.8 分层 …… (41)
4.2.9 时间 …… (41)
4.2.10 小结 …… (42)
4.3 实现 …… (42)
4.3.1 简介 …… (42)
4.3.2 容错 …… (42)
4.3.3 冗余 …… (44)
4.3.4 诊断 …… (44)
4.3.5 认证 …… (44)
4.3.6 小结 …… (45)
4.4 硬件考虑 …… (45)
4.4.1 简介 …… (45)
4.4.2 硬件的类型 …… (45)
4.4.3 节点设计 …… (45)

4.4.4 接口和外围设备 …… (46)
4.4.5 商用货架产品 …… (46)
4.4.6 通信集成 …… (47)
4.4.7 小结 …… (47)
4.5 操作系统 …… (47)
4.5.1 简介 …… (47)
4.5.2 设计考虑 …… (47)
4.5.3 ARINC 653 规范 …… (49)
4.5.4 范例 …… (51)
4.5.5 小结 …… (52)
4.6 开发环境 …… (53)
4.6.1 简介 …… (53)
4.6.2 设计方法 …… (53)
4.6.3 通信系统 …… (54)
4.6.4 操作系统 …… (55)
4.6.5 下载 …… (55)
4.6.6 诊断和调试 …… (56)
4.6.7 小结 …… (56)
4.7 范例 …… (57)
4.7.1 时间触发架构（TTA） …… (57)
4.7.2 可拓展可靠性的可扩展处理器独立设计（SPIDER） …… (60)
4.7.3 可信的嵌入式组件和系统（DECOS） …… (62)
4.8 总结 …… (66)
第5章 模块化认证 …… (67)
5.1 简介 …… (67)
5.2 航空航天领域内的软件认证 …… (67)
5.2.1 简介 …… (67)
5.2.2 DO-178B …… (68)
5.2.3 DO-178C …… (71)
5.2.4 小结 …… (71)

5.3 DO-297《综合化模块化航空电子开发指南和认证考虑》 …… (72)
5.3.1 简介 …… (72)
5.3.2 综述 …… (72)
5.3.3 架构上的考虑 …… (72)
5.3.4 整体流程 …… (73)
5.3.5 小结 …… (74)
5.4 有效认证的一些数据 …… (75)
5.4.1 简介 …… (75)
5.4.2 工作量与节约 …… (75)
5.4.3 需求、设计和可追溯性 …… (76)
5.4.4 验证和确认 …… (77)
5.4.5 优化的流程和流程的不断改进 …… (78)
5.4.6 小结 …… (79)
5.5 调查假设和实际结果的比较 …… (80)
5.5.1 需求 …… (80)
5.5.2 验证和确认 …… (80)
5.5.3 流程 …… (81)
5.5.4 小结 …… (81)
5.6 总结 …… (82)
第6章 分布式综合化平台的解决方案 …… (83)
6.1 简介 …… (83)
6.2 需求和建议 …… (83)
6.2.1 系统架构的变化 …… (83)
6.2.2 传统系统的重用 …… (84)
6.2.3 初期工作量和长期优势 …… (85)
6.2.4 通信基础设施 …… (85)
6.2.5 小结 …… (86)
6.3 平台属性 …… (86)
6.3.1 综合化与分布式 …… (86)
6.3.2 飞机功能开发 …… (86)

6.3.3 平台通信 …… (87)
6.3.4 模块化设计 …… (87)
6.3.5 开发控制和知识产权 …… (87)
6.3.6 可重用性和可组合性 …… (87)
6.3.7 COTS …… (88)
6.3.8 认证 …… (88)
6.3.9 小结 …… (88)
6.4 综合化平台方案的优点 …… (88)
6.4.1 降低复杂性 …… (89)
6.4.2 减少空间、重量和功耗 …… (89)
6.4.3 独立开发 …… (89)
6.4.4 简化认证 …… (89)
6.4.5 增加灵活性 …… (90)
6.4.6 增加可维护性 …… (90)
6.4.7 小结 …… (90)
6.5 总结 …… (90)
第7章 展望 …… (92)
7.1 简介 …… (92)
7.2 架构的演变 …… (92)
7.3 航空航天领域 …… (93)
7.3.1 “猎户座”飞船（Orion – CEV） …… (93)
7.3.2 商用飞机 …… (94)
7.3.3 小型飞机 …… (94)
7.4 汽车领域 …… (95)
7.4.1 汽车开放系统架构联盟 …… (95)
7.4.2 通信系统 …… (95)
7.5 经济影响 …… (96)
7.5.1 可重用性 …… (96)
7.5.2 更快的开发速度 …… (96)
7.5.3 更快的产品更新 …… (96)

7.5.4 更廉价的开发和生产 …… (97)
7.6 未来发展趋势 …… (97)
7.6.1 开发和综合 …… (97)
7.6.2 诊断和维护 …… (97)
7.6.3 重量和成本 …… (97)
7.7 总结 …… (97)
第8章 结论 …… (99)
致谢 …… (101)
附录A 缩略语 …… (102)
参考文献 …… (106)

第1章 引 言

1.1 动机和目的

成本、重量[①]和安全性可能是航空航天产品开发中最重要的关键特性。人们花费很大精力希望在保持甚至提高安全水平的前提下来降低成本和重量。此外，电子器件的数量及其功能越来越多，系统的复杂性也日益增加，从而造成了许多由于过度复杂的设计导致的开发问题。

现有的飞机中，有多种不同系统，如多媒体、动力或控制系统。其中一些系统对安全起关键作用，另外有许多系统需要与其他系统共享数据。这样一方面能够缓解系统的复杂性，确保高效开发系统，另一方面使得人的智力能够应对系统的复杂性，所以在开发中就需要某种形式的抽象。因此，这些系统需要分解成多个子系统，以降低整体复杂性。

目前正热议的一些新概念，可以改变航空航天领域电子系统的开发。其中一个就是（分布式）综合化模块化航空电子系统（D）IMA，它试图通过减少硬件来提高效率；另一个就是模块化认证，它试图通过减少认证工作量来降低开发成本。这两个概念都采用了将大系统分割成小的子系统的方法。

1.1.1 （分布式）综合化模块化航空电子系统

综合化模块化航空电子系统[105]的概念涉及独立开发和认证的软件组件和硬件组件的模块化架构。与 IMA 不同的是，DIMA 模块广泛地分布在整个飞机中，并通过通信系统连接。

这些分布式模块的组合，创建了可以在各功能之间进行交互操作的航空

① 本书中重量为质量的概念，单位为克（g），千克（kg）等。——译者注

电子功能。这种方法为系统设计者提供了更大的灵活性，降低了产品成本和维护费用，并且允许重用已有的模块。但是，这种方法在航空航天应用的设计方面也产生了一些新难题。

最大的难题之一是，如何确保不同的飞机功能之间互不干扰。为了保证这一点，我们就需要一个基础的分布式平台，它可以提供飞机所需要的服务，同时又能够处理不同应用软件之间的数据交换。

另一个难题就是，如何通过对先前认证过的模块（可以来自不同的源，也可以有不同的关键性级别）进行综合，形成一个可以根据适航要求进行认证的系统。（美国）航空无线电技术委员会（RTCA）和欧洲民用航空设备组织（EUROCAE）与SC－200/WG60 工作组一起来解决这种需求。这个工作组为 IMA/DIMA 系统的使用研发了一套新的指南——DO－297《综合化模块化航空电子开发指南和认证考虑》[98]。

1.1.2 模块化认证

依据 DO－178B[95]，认证软件项目的成本是一般软件项目[54]的认证成本的两倍。模块化认证的概念试图通过将认证过程分解成多个部分的方法来解决这个问题。

与只认证整个系统的现有方法不同，模块化认证验证单个部件的开发是否正确，其次要验证这些模块的部件是否被正确综合到整个系统中。这形成了一种基于模块的认证方法。使用这种方法要把系统分解成多个需要分别认证的模块。这种方法的优点在于，一方面，模块的开发者只需要专注于他所开发的单个模块及接口，而不需要关心整个系统及其认证；另一方面，经过认证的模块及其认证证据可以被重用。

使用上面所述的 IMA 的概念，模块化认证允许组成平台的软、硬件组件的独立开发和认证。只有模块的综合是需要额外认证的，系统中的模块可以直接被替换而不必对整个系统进行完整的再次认证。在第二次使用这些模块的时候，认证成本将大大降低。

1.1.3 小结

本书的目的在于讨论分布式综合化模块化航空电子系统和模块化认证的