民用飞机综合模块化航电系统分区和资源分配的研究

Research on IMA System Partition and Resource Allocation for Civil Aircraft

周烨斐　刘艳涛 / Zhou Yefei　Liu Yantao
（上海飞机设计研究院，上海 201210）
（Shanghai Aircraft Design and Research Institute, Shanghai 201210, China）

摘　要：
对比航电传统系统架构，分析了综合模块化航电系统（Integrated Modular Avionics，简称 IMA）架构的优点；针对 IMA 系统功能的高集成度带来的资源分配难度和安全性要求，提出了 IMA 系统分区和资源分配策略，并给出了具体方法，对民用飞机 IMA 系统设计具有一定的指导意义和实用价值。

关键词： IMA；分区；资源分配
中图分类号： V243　　**文献标识码：** A

[**Abstract**] This paper compares the general avionics system architecture with integrated modular avionics (IMA) architecture, and the advantages of IMA architecture is analyzed. For the complexity of resource allocation and many safety requirements led by the high-integration of IMA , the processes of IMA system partition and resource allocation are proposed. The proposed method has the practical significance to guide the design of the IMA system.

[**Key words**] Integrated Modular Avionics (IMA); Partition; Resource Allocation

0　引言

随着 IMA 系统在民用飞机上的广泛使用，IMA 系统的集成度越来越高。A380 的 IMA 系统集成了 20 余项功能，A350XWB 的 IMA 则管理多达 40 项功能。虽然 IMA 系统功能的高集成度极大地减轻了飞机的重量，但随着集成度的增加，IMA 系统驻留应用的分配也更为复杂，对安全性的需求也变得更加难以满足。针对 IMA 高集成度所带来的问题，本文对民用飞机 IMA 系统分区和资源分配做了一定的研究。

1　背景

传统航电系统架构中，各航电子系统都包含有自己的处理器、内存、输入输出接口以及内部的通信网络。随着 IMA 系统的出现，航电系统出现了高度综合化的趋势，多个航电子系统可以在一种“虚拟系统”的环境中工作，共享 IMA 的系统资源。而这个“虚拟系统”就是通过 IMA 的分区机制实现的，分区也是 IMA 平台开发中一个重要的环节。IMA 平台可以同时为多个系统提供其所需要的处理器、内存等资源。传统架构和 IMA 架构的比较如图 1 所示。

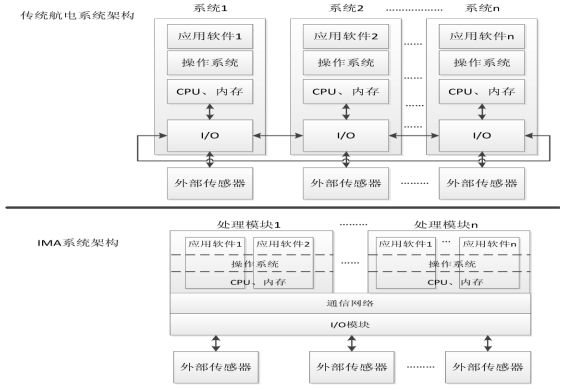

图 1　传统航电系统架构和 IMA 系统架构比较图

IMA 架构相比传统航电系统架构具有如下优势：

首先,IMA 架构的出现使得航电系统的综合更加方便,实现了从多物理设备间的综合到虚拟系统间的综合。在传统的系统架构中,需要定义各系统所采用的设备、不同设备之间的物理接口及不同接口之间的通信协议、线束规格等。而在 IMA 系统结构中,不同的系统都驻留在同一个设备中,它们之前的逻辑接口和通信协议都由 IMA 平台统一定义,并且不需要任何物理线束,通过 IMA 机柜内部的通信网络实现不同系统之间的数据交换。

其次,系统的更改或扩展更加便捷,任何系统功能的变化,不需要更换设备,不需要重新设计物理接口,也不需要重新布置线束,只需要通过更改该系统的应用软件,并采用某些专用的 IMA 构型工具来重新进行资源分配,逻辑接口的更新就可以迅速完成。在这个过程中,由于 IMA 的硬件和 IMA 的平台软件都没有做任何更改,因此 IMA 设备级的安全性分析,电磁、环境的分析以及飞机安装要求也保持不变。

此外,IMA 系统还可以在很大程度上减轻航电系统设备的总重。

由以上三点可知,IMA 系统的应用可以简化系统综合方案,使系统设计具有扩展性和更改性,同时减少设备重量。而 IMA 系统的分区和资源分配机制则直接决定了 IMA 系统所集成的功能深度和广度。

目前,IMA 系统已经在 A380 和波音 787 上得到了成熟的应用,而国内民机 IMA 系统的设计和研发才刚刚起步。

2 IMA 分区的方法研究

DO-178B 对分区的定义是:分区就是一种隔离机制,它能够隔离功能上互相独立的软件组件和故障,减少软件验证工作。

ARINC653 则规定了分区的要求,为了实现在共享资源环境中的分区,硬件必须提供操作系统具有如下的能力:限制每一个分区的内存空间,处理时间,对 I/O 的访问权限。共享资源可以包括:CPU(中央处理单元),FPU(浮点运算单元),MMU(内存管理单元),物理内存,I/O 通道,文件存储设备。

基于以上定义和要求,可知在共享资源的环境下,分区需要提供 2 个主要功能:

(1)保证软件组件和软件运行过程的独立性;

(2)保证一个分区环境中的错误或者故障不会扩散到别的分区中。

据此功能要求,在设计分区时,需要考虑满足开发过程中一系列目标,如下:

(1)支持不同软件过程,软件组件和不同等级的软件功能在同一个处理器上的实施;

(2)在软件分区不变的前提下,应用软件的更新或者修改不需要重新进行分区的验证工作;

(3)确保分区中用户不可更改的软件组件不受用户可更改软件组件的影响;

(4)确保分区中已经得到批准的软件组件不受还未批准的软件组件的影响;

(5)潜在减少后续新增或者更改的应用软件的适航审定工作。

操作系统可以通过一些分区的主要属性来控制和维护分区的运行。

(1)标识:为每一个分区定义一个唯一的标识,用于进行分区激活,消息路由等操作。

(2)名字:定义分区的名字。

(3)存储需求:定义分区的存储边界。

(4)分区运行间隔时间(Period):定义每个分区必须被激活的时间间隔。

(5)分区运行时间(Duration):在每个分区运行间隔时间内,分区需要运行的时间。

(6)分区间通信需求:定义不同分区间通信的端口。

(7)分区健康监视器控制表:定义健康监视器探测分区失效的动作。

(8)分区初始化进入点:定义分区开始或者重启的地址。

(9)系统分区:表明该分区是一个系统分区,主要用于故障管理。

基于以上属性,可将 IMA 的分区分为空间分区和时间分区。空间分区就是给每个分区分配确定的存储边界,指定每个分区可以使用的存储地址的范围,一个分区不能使用不属于它自己的存储空间,通过这种方式来形成空间上的隔离机制。

时间分区就在主时间帧(Major Time Frame)上给每个分区分配运行的时序,主要通过定义每个分区的分区运行间隔时间(Period)、分区运行持续时间(Duration)和分区运行时间偏移(Offset)来确定每个分区的时序。其中偏移指的是从主时间帧开始到分区激活之间的时间。图 2 中展示了 2 个分区的时序的确定方法。

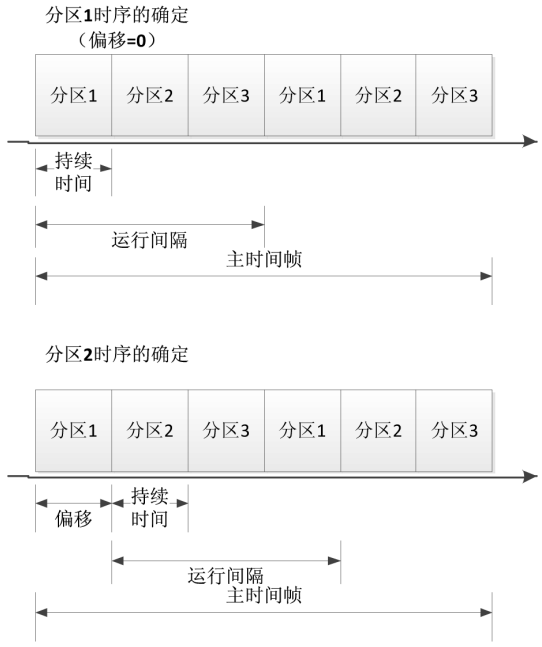

图 2　时间分区的时序

3　应用软件驻留规则及资源分配的方法

在分区建立完毕之后，就需要考虑如何将 IMA 的应用软件驻留到各个分区中，并给各分区分配相应的资源。

在设计 IMA 应用软件驻留架构时，应全面考虑系统安全性需求、系统需求和平台资源的限制等。

在考虑安全性需求的时候，需要同时考虑功能的可用性和完整性。所谓可用性，即功能不失效，可以使用；完整性即表示功能正常，数据完整不出错，功能不产生误指令和误指示。其中，完整性需要考虑软件故障，例如单粒子翻转产生的错误数据；硬件故障，例如数据总线传输了不完整的数据；软硬件设计错误导致的一些不可探测到的数据损坏。因为完整性通常会导致较高级别的故障，故可以首先考虑完整性，然后考虑可用性；必要时需要增加 IMA 公共资源。在同时考虑可用性和完整性的基础上，确定一系列和安全性相关的驻留原则，例如某些应用为了达到可用性的要求，需要采用冗余的方式驻留于 IMA 系统之中，某些应用为了达到完整性的要求，需要采用增加特定应用监视器的方式驻留。

每个驻留的应用都会消耗 IMA 系统的公共资源（包括处理器、内存、接口等），过多的应用驻留在同一个模块上会导致某一处理模块负载过重。在考虑 IMA 平台资源时，需要使得 IMA 中处理模块的资源使用均衡，根据驻留应用供应商提供的每个驻留应用需要消耗的资源进行相关的计算和仿真，同时对其进行资源消耗的最坏情况分析，留有足够的资源余量，以此来确定这些应用可以驻留的模块。

此外，还需要考虑 ARINC 653 中对时间分区和空间分区的要求，比如设计保证等级不同的应用软件不允许驻留在一个虚拟分区中，但是可以驻留在同一个处理器上。

基于上述考虑，图 3 展示了 6 个应用系统软件驻留到一个 IMA 平台上的过程。

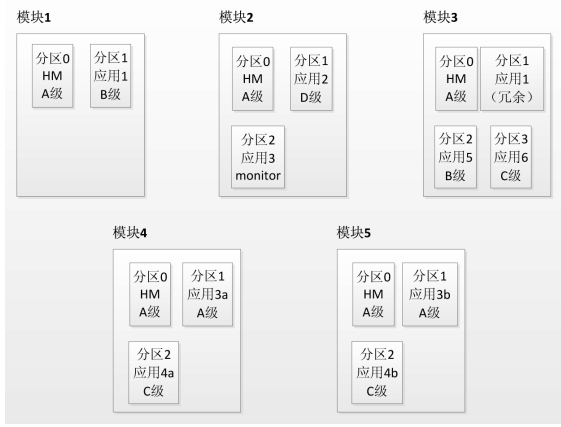

图 3　IMA 系统驻留过程

（1）在每个处理模块上设置一个系统分区，该分区具有最高权限，驻留健康监视器软件（HM），通过 HM 可以记录模块上所有分区的错误，并重启故障分区。所有的模块都设置分区 0 作为系统分区。

（2）不同等级的应用软件不能驻留在同一个分区中。所有的应用软件（A，B，C 级）都驻留在不同的分区中。

（3）基于安全性需求的分析，应用（1）需要采用冗余设计来保证可用性，冗余的应用软件必须要物理隔离，也就是要驻留在不同的模块上。所以应用（1）分别驻留在模块 1 的分区 1 中和模块 3 的分区 1 中。

（4）为了满足安全性需求，应用（3）需要设置监视器功能来保证完整性。应用软件和对应的监视器应用软件必须物理隔离。也就是要驻留在不同的模块上。故应用（3）驻留在模块 4 和模块 5 中，监视器驻留在模块 2 中。

（5）应用（3）和应用（4）需要使用 2 套输出进行比较后表决输出，则这 2 套也必须驻留在不同的模块上，故在模块 4 和模块 5 中分别驻留 1 套软件。

(6)在所有的应用软件驻留分配过程中,还必须考虑到平台资源的可用性,包括处理器的能力、延时和系统物理内存的分配等。模块中的分区数量和驻留应用的数量没有特定限制,需根据具体资源的消耗来决定。

4 IMA 分区和资源分配的工作和步骤

基于上述规则,即可开始具体的资源分配工作,具体工作按图 4 所示步骤展开。

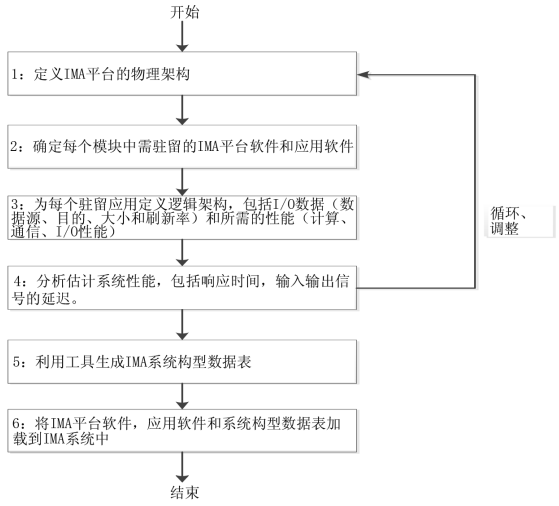

图 4 IMA 资源分配工作步骤

其中需要说明的是:

(1)步骤 1 至步骤 4 为一个循环进行的过程,步骤 4 中分析得出的系统性能如果不能达到系统的要求,则需要返回步骤 1 重新考虑设计。在此循环过程中,需要全面考虑所有驻留 IMA 的飞机系统功能应用所需的资源与IMA实际资源的差异,驻留应用所需的资源必须要考虑最坏运行情况下所消耗的资源,且需要保证资源的余量不小于 30%,如果所有驻留应用所需的某项资源超过了 IMA 的实际资源,或者不能保证资源余量的要求,则必须调整 IMA 平台的物理架构,增加相应的 IMA 资源(例如增加处理模块等)。(2)步骤 5 中的 IMA 系统构型数据表应该包括设备构型数据表、网络构型数据表、输入输出路由表和分区资源构型数据表。

设备构型数据表主要是存储航电系统的设备构型,用于在软件加载后,确认软件与设备匹配;网络构型数据表用于 IMA 系统内部的网络数据传输;输入输出路由表用于 IMA 系统和外部系统的数据传输;分区资源构型数据表用于配置每个分区能够使用的 CPU 和内存资源等。

通过以上 6 个步骤,即可以有效地开展 IMA 系统分区和资源分配的工作。

5 结论

本文研究了 IMA 系统分区、驻留规则及资源分配的方法,并通过实例详细描述了应用软件驻留到 IMA 平台上的过程,建立了一套行之有效的 IMA 资源分配工作步骤,为当前民用飞机 IMA 系统的分区和资源分配提供了指导,并成功应用于某型民用飞机研发工作中。

参考文献:

[1]DO-178B, Software Considerations in Airborne Systems and Equipment Certification, 1992.
[2] Arinc Specification 653P1-3, Avionics Application Softwarewandard Interfacepart 1 - Required Services, 2010.
[3] Arinc Specification 653P2-3, Avionics Application Softwarewandard Interfacepart 2 -Eztended Services, 2008.

(上接第 20 页)

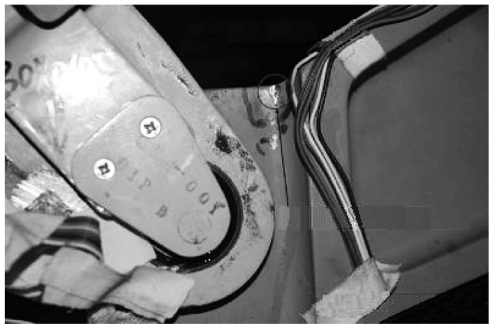

图 11 某型机出现的运动特征故障

自研的疲劳试验用活动面驱动系统具有精度高(活动面控制精度能达到±0.5°)、成本低、速率可调等优点,经连续试验表明,系统具有很高的可靠性。

采用该技术的某型民机前缘缝翼和襟翼及其悬挂结构疲劳试验已完成 50 000 次起落,实践证明,该试验技术是可行的。

参考文献:

[1] 李清蓉,喻溅鉴,史斯佃,等. 直升机主桨毂支臂疲劳试验技术研究[J]. 直升机技术,2012, 1:56-62.
[2] 史坚忠. 飞机全尺寸悬空疲劳试验技术的研究[J]. 测控技术,1994,13(6):40-42.
[3] 潘庆荣. TWIST 编谱方法中阵风载荷谱形状相似准则的实现[J]. 民用飞机设计与研究. 2005,3:8-21.
[4] 郑牧,赵春兰,薛伟松. 一种复杂襟翼试验精确随动加载系统[J]. 测控技术. 2011,30:173-175.