IMA 平台分区分析方法研究

郭 庆 孔德岐 赵 茜
(中航工业西安航空计算技术研究所,西安,710065)

摘要:依照综合模块化航空电子系统(Integrated modular avionics ,IMA)平台的健壮性分区特点,IMA 平台必须能够为驻留应用和驻留功能提供健壮分区隔离和其他保护能力,这些措施要允许多个驻留应用共享一个平台及平台上的资源,且自身的资源支持系统级分布功能在容错网络上运行。根据综合模块化航空电子系统开发指南与认证考虑 RTCA DO-297 标准中关于 IMA 平台健壮性分区、安全性以及认可证明数据的要求,本文对 IMA 平台分区分析展开研究,重点对 IMA 平台及其组件通用处理模块(General processing module, GPM)、航空数据网络 ARINC664 交换机和远程数据集中器(Remote data concentrator, RDC)进行分区分析方法的研究。给出每个组件的分区分析策略和目标,明确每个任务需要进行的活动,为 IMA 平台及其组件的健壮性分析、缓解潜在风险、安全性分析和认可提供充足的证据。

关键词:IMA 平台;分区分析;通用处理模块;ARINC664 交换机;远程数据集中器
中图分类号:TN958 **文献标志码**:A **文章编号**:1005-2615(2017)S-0136-04

Study on IMA Platform Partition Analysis Method

GUO Qing, *KONG Deqi*, *ZHAO Qian*
(Xi′an Aeronautics Computing Technique Research Institute, AVIC, Xi′an, 710065, China)

Abstract: According to the integrated modular avionics (IMA) platform characteristics of robust partitioning, the IMA platform should be capable of providing robust partitioning and other protection, for hosted applications and hosted functions, which allows multiple hosted applications to share a platform and its resource and the resource can, support systematic distributed functions running on a fault-tolerant network. According to the requirements of robust partitioning, safety and acceptance data of evidence for IMA platform in integrated modular development guidance and certification consideration RTCA-DO-297 standard, the IMA platform partition analysis is studied in this paper, whose key points include the IMA platform and its general processing module (GPM), ARINC664 switch and remote data concentrator (RDC). The strategy and objective of the partition analysis for each item are provided to confirm the activities required for each task, which can supply sufficient evidence for robust partitioning analysis, potential risks mitigation, safety analysis and the acceptance of the IMA platform and its items.

Key words: IMA platform; partition analysis; general processing module(GPM); ARINC664 switch; remote data concentrator(RDC)

当前先进的大型民用客机均采用综合模块化航空电子系统(Integrated modular arionics, IMA),其系统设计、验证、安全性要求和认证相比传统的联邦式航电系统更为复杂[1]。为提供一个健壮的、安全的 IMA 平台以满足综合更多不同安全等级的 ATA 系统应用,需要对 IMA 平台进行充分的分区分析。确保驻留在 IMA 平台中的通用处理模块(General processing module, GPM

收稿日期:2017-05-15;**修订日期**:2017-06-20
通信作者:郭庆,男,工程师,E-mail:gqing@avic.com。

引用格式:郭庆,孔德岐,赵茜. IMA 平台分区分析方法研究[J]. 南京航空航天大学学报,2017,49(S):. GUO Qing, KONG Deqi, ZHAO Qian. Study on IMA platform partition analysis method[J]. Journal of Nanjing University of Aeronautics & Astronautics,2017,49(S):.

ARINC664 交换机[2]和远程数据集中器(Remote data concentrator, RDC)的基础软件能够安全运行;确保 IMA 平台提供给驻留应用和驻留功能的所有硬件和软件资源足够健壮[3];确保某些驻留应用和驻留功能的故障或者操作不会影响到其他驻留应用和驻留功能[4]。

当前国内外成熟的 IMA 平台和组件供应商均按照公司特定的设计架构及局方和飞机制造商的要求进行详细的分区分析工作[5],以降低 IMA 平台和组件在 IMA 系统和飞机运行时的潜在非预期风险,提高 IMA 平台及其系统的安全性、可靠性和健壮性,为审查人员提供强有力的证据来显示 IMA 平台及组件的预期工作能力[6]。同时飞机制造商通过 IMA 系统的安全性分析证明材料(包括 IMA 平台的分区分析)、飞机级信号验证、多故障分析、飞机制造商的铁鸟实验和机上的确认活动来验证 IMA 平台满足飞机制造商对安全性的要求。

本文通过对使用 AE653 核心操作系统[7]的 IMA 平台及其组件的分区方法的研究,旨在为国内现有使用 IMA 平台的大型客机提供安全性技术需求和认证需求的参考。重点围绕 IMA 平台中的 3 个核心组件,即 GPM、ARINC664 交换机和 RDC,详细阐述了分区分析的目标和方法,以指导 IMA 平台及组件研发单位能够开发出获得飞机制造商和局方认可的产品。在 IMA 平台支持的驻留应用和驻留功能中,通常会涉及到 3 个主要环节,即 GPM 的数据运算或处理、ARINC664 的航空数据传输及 RDC 的驻留功能数据采集与控制。因此,要想在 IMA 系统中实现不同 ATA 系统之间的驻留应用或/和驻留功能隔离,同样需要从 IMA 平台及各组件的分区任务中考虑驻留应用和驻留功能的处理、数据传输和控制操作环节的分区隔离,以确保 IMA 平台提供给不同安全等级 ATA 系统的计算、通信和 I/O 等资源具备高隔离分区和容错能力。

1　IMA 平台分区

IMA 平台的分区分析主要是为 IMA 平台的安全性分析提供充足的证据,主要通过对 IMA 平台各功能块之间分区机制的分析来验证是否满足健壮性和分区要求。

IMA 平台的分区分析需要证明分区中的任何应用或子功能都不会对其他任何分区的某个应用或子功能产生不利影响。分区之间信息的所有传播路径都应当得到识别,每个路径所带来的影响都应当记录在系统文件中。分区分析应当作为输入提供给 IMA 平台的故障分析活动,以及 IMA 平台和 IMA 系统的失效模式分析中所涉及的分区冲突失效模式[8]。同样在 DO-297 标准中,IMA 平台开发过程中要求提交分区分析数据和失效分析与安全性分析报告,且这两份数据均要满足 CC1 控制。

IMA 平台基础服务软件包的一个主要功能就是为 IMA 平台中的系统驻留软件提供一个预先定义好的分区计算环境。这些分区计算资源的划分是在驻留应用软件开发前分配的,作为核心操作系统运行时间的一部分进行统一计算。那么此时对于分区完整性的要求就特别重要。对 IMA 平台进行系统的分区分析,可确保在 IMA 平台分区中发现的所有问题得到解决。

IMA 平台的分区分析主要满足 DO-178C 目标(A4-13 软件分区完整性[9])以及 DO-297 里所定义的分区和验证目标,并保证充足的分区活动满足 DO-178C 中 A 级软件对于健壮性分区的要求。

1.1　IMA 平台分区服务

针对 IMA 平台中的组件需要开发独立的分区分析机制,这些机制涉及到 IMA 平台中的各个组件(GPM、ARINC664 交换机和 RDC 等组件)以及这些组件中加载的驻留应用和配置文件等软件。对这些组件进行分区分析的目的主要是为了预防一些非预期交互事件的发生。IMA 平台的主要分区服务工作包括:

(1) GPM 通用处理模块中的分区计算、分区隔离和各类调度等核心处理服务[9];

(2) ARINC664 交换机中的故障隔离和消息传输服务;

(3) RDC 远程数据集中器中的故障隔离、应用资源和网关服务。

根据 IMA 平台的特点,对这 3 个组件进行完整的分区服务分析,就可以满足整个 IMA 平台中这 3 个组件整体的分区服务。

1.2　IMA 平台分区分析要求

IMA 平台中的模块级故障控制,主要用来控制和保护模块级故障,每个 GPM、ARINC664 交换机、RDC 以及这些组件中的端系统都包含一个故障控制区域。为防止故障扩散到其他模块或在本模块中进行蔓延,需要对 IMA 平台中的潜在弱点进行分析。

IMA 平台的基础架构软件主要为应用软件提供一个健壮的分区环境。该分区计算环境必须确保在一个或多个 GPM 中的应用之间没有非预期的交互关系,为每一个应用这就需要在分区环境中确定一个固定的计算资源,并为存在交互关系的应用需要设置一个共享的资源环境,以确保分区间的

正常通信。为了确保IMA平台分区的正确性和完整性,需要对IMA平台潜在的弱点进行分析并提出详细的缓解措施,然后对IMA平台中的问题区域进行分析,并针对这些潜在问题研究缓解这种非预期交互的策略。

1.3 IMA平台分区分析策略

IMA平台分区需要进行两个方面的活动,其一是IMA平台需求规范中涉及到的分区和保护需求验证;其二是针对IMA平台的分区分析验证活动,结合安全性和安全性关联的需求验证。

分区分析的机制是明确IMA平台的能力及可能存在的所有潜在风险,通过关联需求分析进行分区分析,并降低IMA平台潜在弱点的风险。在IMA平台开发过程中应当进行潜在弱点的辨别和相应缓解需求的开发。IMA平台需求规范中的分区和保护需求按照正常的验证流程和方法执行。

1.4 IMA平台的健壮性分区

针对IMA平台中潜在的弱点,需要对以下特点健壮性分区分析:

(1) 提供健壮性资源保护硬件,需要唯一匹配到某软件指定的分区区域,而不能对其他软件分区或其他硬件资源产生不利影响[11];

(2) 提供健壮性的时间保护,需要确保某软件分区在自身的执行周期中可以正常使用处理器资源,同时不会对其他分区的处理器资源造成抢占;

(3)提供健壮性资源保护的时间和空间资源为驻留软件分区的I/O资源应当是固定设置的(这些资源分配需要在配置文件中提前规定好),且不能妨碍到任何其他分区的工作;

(4) 缓解或者降低健壮性资源保护的分区污染,某软件分区在故障或禁止时不能污染另一个分区的代码执行、I/O通信、数据存储区域、核心软件运行及数据计算。

1.5 IMA平台分区目标

IMA平台分区分析的目标为:

(1) IMA平台的分区分析要求源于飞机系统安全评估的要求;

(2) 确保在一个分区内没有功能存在不可接受的影响;

(3) 确保在一个分区内没有应用存在不可接受的影响;

(4) 确保在一个分区内没有功能可以有不可接受的影响发生在另一个分区中应用或者功能的操作;

(5) 确保分区之间的所有传播路径正确和完整;

(6) 定义每个传播路径可能的不利影响;

(7) 对所有分区之间存在的不可接受的交互作用要有明确的缓解措施或者策略;

(8) IMA平台中所有通用处理模块之间的硬件计算资源不会相互影响;

(9) IMA平台中所有模块间通信母版的通信互不影响;

(10) IMA平台中其他功能模块之间不能产生不利影响。

(11) 分析假设的组合性故障和它们之间可能互相影响的概率;

(12) 更新验证和确认分区保护需求的计划和验证程序。

2 通用处理模块分区方法

IMA平台的通用处理模块主要是为一个或多个应用软件提供一个驻留的运行环境,在同一级别中提供一个功能性隔离,及给应用软件提供一个预期的执行环境[12]。通用处理模块由核心软件和计算硬件提供一个主要的分区服务,通过两级故障控制环境来满足功能性隔离要求。核心软件在GPM提供的ARINC653分区操作系统的计算分区故障控制区域中运行,主要用来保护每个驻留应用以防止故障扩散到其他驻留应用[13]。

实际上模块级的故障控制区域并不直接涉及到分区。每个模块的故障控制区域都应当具有相关联的需求符合硬件故障控制。通过对通用处理模块的研究,合理分配通用处理模块的计算时间、计算资源,可降低在资源分配中存在的技术风险。主要的分析工作包括:

(1) GPM中基础软件的分区分析;

(2) GPM中ARINC653操作系统的环境分析[14];

(3) GPM的分析,包括专用集成电路(Application specific integrated circuit, ASIC)、现场可编程门阵列(Field-programmable gate array,FPGA)和ARINC664端系统的分析。

3 ARINC664交换机分区方法

ARINC664交换机主要在IMA平台中为驻留功能提供数据传输和I/O服务。ARINC664交换机将传输信号的带宽和延迟定义在虚拟链路(Virtual link, VL)中,每个虚拟链路的路径则写在ARINC664交换机的配置文件中,需要对这些配置文件进行分析来确保所有的VL满足带宽和延迟条件约束。那么VL就对驻留功能的数据提供了一种逻辑隔离的健壮分区方式。ARINC664交换机分区服务管理的逻辑隔离主要包括:(1) VL带宽

管理;(2) VL 数据源鉴定;(3) VL 边界延迟管理。

ARINC664 交换机分区服务主要用来缓解和减轻 ARINC664 交换机自身的潜在风险,以及在 IMA 平台中的潜在风险。对 ARINC664 交换机分析的主要技术点包括:开关转换过滤;虚拟链路源端;虚拟链路目的端;虚拟链路自身的损坏情况;数据传输的网络带宽;数据传输的网络延迟;数据完整性;顺序完整性;数据冗余性;位完整性;消息顺序;时间完整性;消息传输的路径;消息源鉴定;交换机存储器;交换机配置文件信息。

4　RDC 分区方法

RDC 在 IMA 平台中主要提供一个数字网关、模拟量和数字量的输入/输出,起到数据计算和转移的功能,且根据不同的架构需要可以驻留应用和增加嵌入式功能,所以必须要保证远程数据集中器正常运行,确保没有非预期的耦合事件发生,因此远程数据集中器包含多个独立的故障隔离区域。对 RDC 进行分区分析的主要目的是为了缓解或减轻 RDC 在 IMA 平台运行中对自身或系统的非预期影响,主要的分析包括:模拟信号的独立故障区域;数字信号的独立故障区域;离散信号的独立故障区域;操作系统使用环境影响分析;RDC 基础服务软件分析;双路径网关;存储器数据、标志、控制耦合;存储器外部、外部耦合;时间控制;嵌入式功能耦合分析;共享的通用资源;RDC 配置表分析。

通常 RDC 设计要保证高度集成网关架构的健壮性,确保和预防 RDC 内部没有检测到系统的错误或者影响驻留功能信号。因此在进行 RDC 的分区分析时,同样需要对各类信号的独立故障区域进行分析。

5　结束语

通过对 IMA 平台及其组件分区的研究,明确了 IMA 平台及其组件的分析策略和方法,并给出了分区分析需要完成的详细技术点。帮助 IMA 平台开发人员对阐述的这些定义的分区分析点进行详细分析,避免 IMA 平台及其组件中潜在风险的出现,缓解或者降低这些潜在的技术漏洞,增加 IMA 平台及其组件的健壮性和安全性。完成本文所述各组件的分区分析任务,提交 IMA 平台及其组件的分区分析数据、失效分析与安全性分析报告,并形成系统的分区分析报告,将对 IMA 平台及其组件认可增加置信度,为 IMA 平台和 IMA 系统的安全性分析提供详细的证据,对 DO-297 和 DO-178C 标准中要求的分区和健壮性活动进行覆盖和实现,帮助审查人员明细 IMA 平台及其组件的分区内容。

参考文献:

[1] MOIR I, SEABRIDGE A, JUKES M. Civil avionics systems[M]. 2nd edition, Aerospace Consultant, UK:Wiley, 2013:79-213.

[2] Airlines Electronic Engineering Committee (AEEC), [s]. ARINC 664 Part7-1. [s. l.]: Aeronautical Radio Inc, 2009.

[3] LEWIS J, RIERSON L. Certification concerns with integrated modular avionics (IMA) projects[C]// Digital Avionics Systems Conference[S. l]: IEEE, 2003,1(10):1. A. 3-1. 1-9.

[4] RUSHB J. Partitioning in avionics architectures: Requirements, mechanisms, and assurance [R]. NASA/CR-1999-209347,2000.

[5] BARTLEY G, LINGBERG B. Certification concerns of integrated modular avionics (IMA) systems[C]// Digital Avionics systems conference. [S. l.]:IEEE, 2008: 1. E. 1-1-1. E. 1-12.

[6] CHEVREL C. Integrated modular avionics certification process in Europe[C]//International IMA Conference. Moscou: THALES Avionics, 2012.

[7] PRISAZNUK P. ARINC 653 role in integrated modular avionics (IMA) [C]//27th Digital Avionics Systems Conference. Piscataway, USA: IEEE, 2008:1. E. 5-1-1. E. 5-10.

[8] U. S. Department of Transportation, Federal Aviation Administration. Integrated modular avionics (IMA) development guidance and certification consideration[S]. EUROCAE ED 124. Washington, DC: FAA,AC,2005.

[9] RTCA. Software considerations in airborne systems and equipment certification, DO-178C. [S]. [S. l.]: RTCA,2012

[10] KRODEL J, ROMANSKI G. Real-time operating systems and component integration considerations in integrated modular avionics systems report [R]. DOT/FAA/AR-07/39,2007.

[11] FAA. AC20-170-Integrated modular avionics development, verification, integration and approval using RTCA/DO-297 and technical standard order C-153 [S],[S. l.]:FAA.

[12] ARINC. Avionics application software standard interface ARINC 653. [S]. [S. l.]: Aeronautical Radio Inc, 1997.

[13] KRODEL J, ROMASKI G. Handbook for real-time operating systems integration and component integration considerations in integrated modular avionics systems[R]. 2008.

[14] CONMY P, MCDERMID J . High level failure analysis for integrated modular avionics[C]//Australian Workshop on Safety Critical Systems and Software. Australian:[S. n.]2007:13-22.