

doi:10.3969/j.issn.1001-893x.2013.11.002

综合模块化航电系统失效模型分析*

王 鹏^{1,2,**}, 赵长啸², 马 赞²

(1. 民用飞机模拟飞行国家重点实验室, 上海 201210;

2. 中国民航大学 天津市民用航空器适航与维修重点实验室, 天津 300300)

摘 要:通过分析对比联合式航电系统和综合模块化航电系统(IMA)的体系结构特征,针对系统的资源紧耦合特性建立了 IMA 系统功能层次化失效模型。按照失效模型分析的资源解耦需求,对 IMA 系统的功能和服务进行了划分,分析总结了 IMA 平台的 5 类功能模型以及 11 种系统服务模型。按照失效机理对失效模型进行了分类。采用提出的失效模型分析方法对通信功能进行了失效分析并给出了失效应对策略,表明了本方法针对 IMA 系统失效分析的有效性。

关键词:综合模块化航电系统;可靠性;失效模型;体系结构

中图分类号:V243 **文献标志码:**A **文章编号:**1001-893X(2013)11-1406-06

Failure Model Analysis of Integrated Modular Avionics System

WANG Peng^{1,2}, ZHAO Chang-xiao², MA Zan²

(1. State Key Laboratory of Civil Aircraft Flight Simulation, Shanghai 201210, China; 2. Tianjin Key Laboratory of Civil Aircraft Airworthiness and Maintenance, Civil Aviation University of China, Tianjin 300300, China)

Abstract: Through analysis and comparison of federated systems and integrated modular avionics (IMA) architecture features, a hierarchical IMA system failure model is established. According to the need of resource decoupling for the failure model analysis, five functional models and eleven service models of the IMA platform are analyzed and summarized. Also, the failure models of the system are classified. Finally the failure model analysis method is applied to the communication function and the failures coping strategies are given, which shows the effectiveness of the proposed method for the failure model analysis of IMA.

Key words: IMA; reliability; failure model; architecture

1 引 言

综合模块化航空电子系统(Integrated Modular Avionics, IMA)的出现解决了由于功能需求增加而导致的系统尺寸、重量、能耗以及通信复杂度增加等问题,克服了联合式体系结构的固有缺陷^[1]。IMA 构架简化了航电软件与硬件的开发和验证,增强了系统的处理能力与可靠性,并被广泛应用于波音 787、空客 A380、F-22 等新一代民用与军用飞机的系统设计^[2]。IMA 最大限度地推进系统综合,通过在硬件核心处理平台上加加载相应的功能软件来满足不同的应用需求。这种系统综合减少了系统专用模块的种类,带来了维修、认证的便利,但同时各应用资源的紧耦合给系统

分析和失效机理分析带来了挑战^[3]。

系统的可靠性保障一方面依靠系统的可靠性设计,另一方面,良好故障恢复策略也是保证系统安全运行的重要措施^[4]。失效状态确认、失效模式判别是进行健康管理与故障预测的前提。联邦式航电系统中各子系统拥有独立的硬件平台,这种物理隔离的方式具有天然的失效隔离特性。在 IMA 结构中,各应用共享通用的计算平台,采用逻辑分区的手段隔离各功能模块,各功能分区间资源紧密耦合,如何检测系统故障、确认失效模型以及定位故障变得十分困难。

国内外学者对 IMA 系统进行了广泛的研究,在

* 收稿日期:2013-07-01;修回日期:2013-09-25 Received date:2013-07-01; Revised date:2013-09-25

基金项目:航空科学基金项目(20128067003);中央高校基金项目(3122013p004)

Foundation Item: Aeronautical Science Foundation of China(No. 20128067003); The Fundamental Research Funds for the Central Universities (3122013p004)

** 通讯作者:pwang_cauc@163.com Corresponding author: pwang_cauc@163.com

系统体系结构^[5]、健壮分区设计^[6]、处理器关键任务调度^[7]、网络实时性分析^[8]等方面有较多的研究成果,针对 IMA 系统失效模型及分析的研究较少。文献[9]研究了航空电子装备保障中的失效分析,介绍了失效模式影响分析(Failure Mode and Effects Analysis, FMEA)在航电领域的应用;文献[10]研究了航电故障诊断中的参数融合问题;文献[11]从验证角度研究了 IMA 系统需要关注的几类系统失效问题;文献[12]从适航的角度研究了 IMA 系统的安全性问题。这些研究从多方面讨论了 IMA 系统的故障确认、安全分析等问题,但是没有给出通用的 IMA 系统失效模型。本文从分析 IMA 系统的层次结构入手,通过建立系统的功能分层模型,建立了 IMA 系统的层次化失效模型,对各失效模式进行了分类,并给出了失效模型分析实例以及应对策略。

2 IMA 体系结构

IMA 通过在一系列标准化通用功能模块上加载与硬件无关的软件,完成航空电子系统各种功能。在 IMA 中,各子系统功能都是建立在通用功能模块之上的,而通用功能模块在机载资源基础上,通过加载不同的软件完成具体的功能。与传统的联邦式航电相比,各子系统不再拥有独立的计算、I/O 和通信等资源,IMA 实际上是由统一的总线网络连接通用的模块构成硬件基础,并由系统软件提供任务功能的信息交换和处理的实体。采用有限种类的通用模块、标准的设备结构和互连接口是开放式模块化系统的特征^[13],联合式航电系统与 IMA 系统的结构对比如图 1 所示。

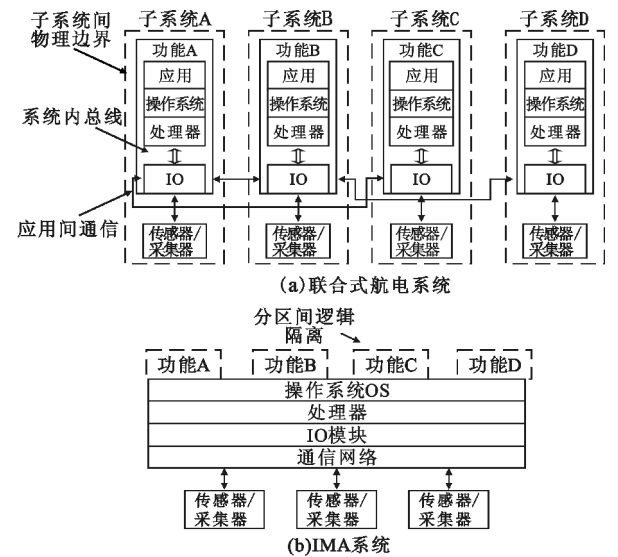


图 1 联合式航电与 IMA 结构对比

Fig. 1 Comparison between IMA and federate avionics

可以看出,传统的联邦式航电,各功能模块独立,不存在功能内部的数据交换和资源共享,其一般是通过总线技术将各功能模块联系起来,如 ARINC 429 等。这为各功能模块提供了物理隔离,而这样设计的缺点也是显而易见的,需要为各功能模块设计专用的软件和硬件,部件重用和升级较为困难。对于 IMA 架构,多个航电子系统通过一个“虚拟系统”共享航电资源,各子系统间通过“分区”来进行隔离,各系统的资源耦合更紧密,可被重用,硬件模块可在不同的飞机上使用,系统容易升级和重配置,仅需少量备用资源。对于 IMA 系统,系统的各功能紧密耦合,难以像联合式航电一样,通过具体的子系统区分各模块。本文通过功能层次来划分 IMA 系统进行系统失效模型的研究。

3 IMA 失效模型分析

失效模型与失效机理研究是航电系统安全研究的重要组成部分,通过建立失效模型、分析失效机理可以为系统设计者和集成者提供指导,提高整体系统的安全性和可用性。传统的联合式航电系统,各子系统之间具有天然的物理边界,系统的失效模型是针对各子系统的失效进行建模。IMA 系统为众多应用提供通用计算资源,同时通过互连网络在各模块和 I/O 设备间分享数据,其各部分资源紧密耦合,依据各子功能系统划分 IMA 来分析失效模型和机理的方法已不适用,因此本研究从系统的资源解耦入手,建立层次化的功能失效模型,同时对 IMA 系统/服务进行合理类别的划分,以建立全面的系统失效分析模型。

3.1 IMA 失效模型

针对不同的系统特征,系统层次划分有两种方法,如图 2 所示,一种是按照系统的模块组成,将系统分解为子系统、单元模块、元件等,这种系统划分方法适合于联合式航电类的资源松耦合系统。对于 IMA 这种共享资源的综合化系统,各子系统资源紧密耦合,难以进行单元划分,本文采用功能、服务的层次系统划分。按照 ARINC 651-1^[14]、ARINC 653^[15]相关说明,按照分层思想将系统分层,系统顶层为 IMA 功能层,其表征 IMA 功能的完整性,这里我们研究的功能不是各航电子系统完成的具体功能,如导航、飞行控制等,而是 IMA 可以提供的通用功能,如通信功能、数据处理功能等。IMA 功能的完成需借助下层操作系统、软件分区等提供的服务,而

服务的完好性依赖于软件、硬件本身的完整性和正确性。同一个功能可能会需要不同的服务支持,而各服务也可以支持不同的功能。

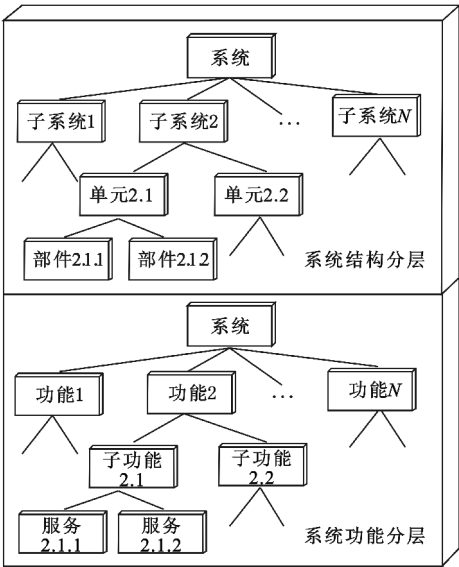


图2 系统结构分层与功能分层

Fig.2 Structure system view and functional system view

针对 IMA 平台通用化的特点,建立层次化的功能-服务-软/硬件失效模型,分析其功能失效模型和服务失效模型。以故障树方式描述 IMA 失效模型,我们将系统的失效按照系统分层,分解为服务失效,进而分析硬件失效、软件失效,软件、硬件本身故障作为失效事件的元事件,我们可以进一步分析引起这些元事件失效的机理。

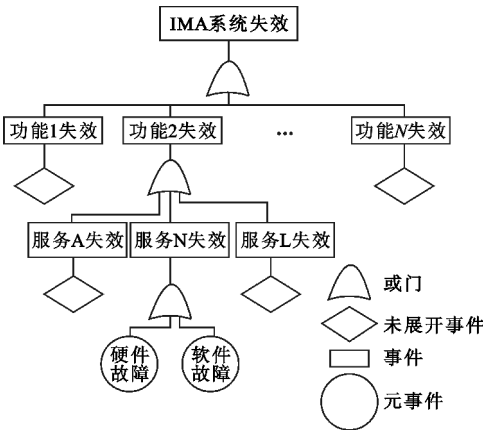


图3 IMA 分层失效模型

Fig.3 The layered failure model of IMA

3.2 IMA 系统功能、服务划分

在 IMA 系统的功能层次化失效模型下,需要对系统的功能/服务进行合理划分,减少各功能资源耦

合,同时使分析能涵盖所有的 IMA 系统功能,根据航电功能所需的通信、处理、存储等需求,以及 IMA 系统执行和架构的生命周期^[16],将 IMA 系统功能分为以下 5 类:安全的数据存储、可靠的计算能力、通信、资源接入控制以及健康监视与故障管理。

首先,系统功能的完成需要处理相应的数据,对于共享资源的 IMA 系统,各功能所需的数据存储空间隔离是通过分区技术实现的,分区的内存存储必须受到保护以防止硬件故障或是其他分区崩溃造成的影响,各分区共享内存资源,那么防止分区间影响就变得格外重要,将此功能归纳为安全的数据存储。

IMA 系统要完成相应的功能必须依靠其计算模块提供的计算能力,多功能共享计算资源时,为各功能分配合理可用的计算资源是 IMA 平台必须考虑的问题。

通信功能也是 IMA 必须提供的功能之一,无论是分区内的数据交换还是分区间的数据交换都需要可靠的通信协议。

IMA 系统内,计算资源、存储资源、通信资源等被多个应用所共享,为保证满足各应用的需求同时充分利用资源,必须限制各应用的资源访问,只有在规定的时间内应用才被赋予访问特定资源的权限,以保证资源的隔离。

健康监视和故障管理是 IMA 平台提供的重要功能,资源的通用性使得 IMA 系统可以在部分功能故障时,采用资源重配置的方式来进行系统重构抵御系统失效,因此监视系统故障,根据故障采取对应的策略以提高系统的安全性。

IMA 系统服务的分类是基于 ARINC653 和 ARINC651-1 标准,服务的完整列表如表 1 所示。

表 1 IMA 系统服务列表
Table 1 The service list of IMA

IMA 服务	服务描述
数据加载	此服务允许在飞机上上载和下载,允许数据加载到分区执行,也允许发生错误后数据重载。
时钟看门狗	看门狗允许处理器处理进程具有时限,并可以检测到失效来避免超时。
分区内通信	此组服务允许驻留在相同分区的处理期间进行数据交换。
分区间通信	此组服务允许不同分区、不同 I/O 设备间进行数据交换。
调度	调度服务允许各任务根据其优先级在其规定时间内访问处理器。
处理	从中央处理单元提供数据/指令处理能力。

续表 1

内置测试和健康 管理	此服务提供健康管理、内置测试 (Built In Test, BIT), 以及当检测到故障时的数据记录。该服务还包括错误检测和恢复。
初始化	系统完全初始化时, 数据根据当前使用的系统配置加载到指定分区。此服务也可以用于错误恢复。
终止	这项服务可以关闭单一的应用程序分区或是单个模块。
分区	此服务描述各分区间的资源分配机制和资源的使用规则。适用于空间分区 (例如接入通信) 和数据分区 (以防止非法访问内存空间)。
配置管理	IMA 系统的配置描述了各应用需求和 IMA 各模块的服务支持, 以确保每个应用程序符合其认证要求。

每一个 IMA 功能由一个或多个较低级别的 IMA 服务所支持, 这些服务还可以支持一个或多个上层的功能, 如图 4 所示。

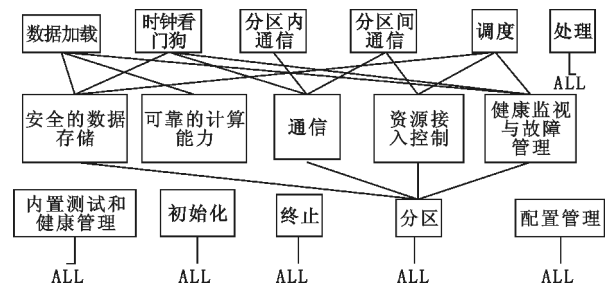


图 4 IMA 功能服务支持结构

Fig. 4 The map between system function and services

3.3 IMA 失效模型分类方法

系统失效模型是多种多样的, 为了得出系统的分析结果, 在研究 IMA 系统功能和服务失效时, 我们对失效模式进行分类, 依据导致系统失效的因素将失效模型分类如下:

- (1) 不作为: 不能提供相应的功能/服务, 如系统断电导致不能提供计算能力;
- (2) 冗余: 提供某种不需要的功能/服务, 如在飞机飞行过程中提供下放起落架服务;
- (3) 超前: 在预期时间之前提供了相应功能/服务;
- (4) 超时: 在预期时间之后提供了相应功能/服务;
- (5) 差值: 提供的功能/服务能力与需求不符合。

4 分析实例

本节应用本文提出的方法来研究 IMA 系统典型的失效模型, 进行失效机理分析和失效应对/恢复

策略的研究。

由图 4 可知, 通信功能的完成需要多种 IMA 服务的支持, 按照层次化失效模式分析方法, 将系统功能的功能失效分解为 IMA 平台服务失效, 依照 3.3 节的失效模型分类方法, 可以将服务失效进行分类, 然后按照各类别的失效特征分析引起系统失效的元事件以及失效应对策略等。图 5 给出了通信功能的层次化失效模型故障树。

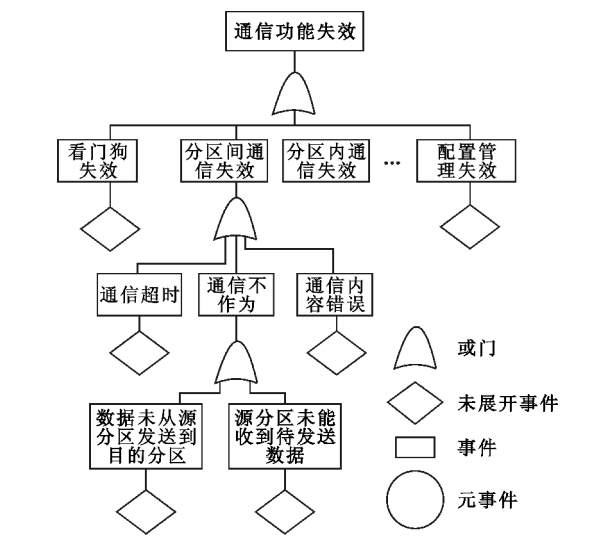


图 5 通信功能失效模型

Fig. 5 The failure model of IMA communication function

根据系统功能确定其失效模式后, 可以进一步分析各服务的失效模式、产生原因, 以及应对方式, 表 2 给出了各服务失效的失效类别, 针对分区间通信失效中通信不作为进行进一步分析, 研究了导致失效的可能原因以及针对失效应对措施, 分析结果如表 3 所示。

表 2 通信功能失效模式列表	
Table 2 The failure modes of communications	
服务类型	失效模式
看门狗	不作为/超时
分区内通信	不作为/ 超时/ 差值
分区间通信	不作为/ 超时/ 差值
调度	不作为/ 超时
处理	不作为/ 超前/ 超时/ 差值
内置测试和健康管理	不作为
初始化	不作为/ 差值
终止	不作为/ 冗余
分区	不作为/ 差值
配置管理	不作为/ 差值

表 3 分区间通信服务不作为分析示例
Table 3 Analytical sample of inter-partition communication service failure

失效模型	失效状态描述	可能的原因	可采取的措施
不 作 为	数据未从源 分区发送到 目的分区	IMA 系统将数据路由到了错误的分区	在数据上加源/目的分区标签,路由过程通过数据上标签与配置表对比来避免此失效。同时发生此失效时,故障管理系统会报告此错误。
		IMA 系统不能将从应用接收到的数据发送到目的分区	目的分区可以通过对于时戳来发现数据丢失,同时故障管理系统会报告此错误。
		网络部件失效	目的分区可以通过对于时戳来发现数据丢失,故障管理系统检测到网络部件失效。
	源分区未能收 到待发送数据	IMA 未能成功初始化源分区	通过检查系统初始化的配置表来避免此种失效。
		由于模块失效导致源分区终止	通过备份系统将该分区配置到其他模块,同时故障管理系统报告此错误。
		分区间干扰导致源分区失效	通过备份系统将该分区配置到其他模块,同时故障管理系统报告此错误。
		IMA 分区未正确调度源分区	看门狗负责检测此错误,备份系统对该源分区进行重配置,同时故障管理系统报告此错误。
		源分区内部错误	清除该分区资源,备份系统对该分区功能进行重新加载。故障管理系统报告此错误。

由此分析可得,本文所提出的 IMA 系统失效模型分析方法可以建立全面的系统失效模型,通过系统层次化功能失效模型分析建立全系统的失效分析框架,通过对服务失效类别的划分可以进一步细化分析结果,为后续分析失效原因及采取失效应对策略提供了很好的理论指导。

5 结论及工作展望

本文首先分析了 IMA 系统的体系结构,根据 IMA 资源紧耦合的特点,提出了一种层次化的功能失效模型,建立了系统故障树模型;根据 ARINC651 和 653 标准定义了 IMA 通用功能和服务模型,细化了失效分析模型;为保证失效模型分析全面及系统化,在分析各系统功能、服务失效模型时,对各类失效进行了分类;最后通过实例详述了失效模型分析方法及失效应对策略。

本文提出的 IMA 系统失效的分析方法可以有效地对 IMA 系统进行失效分析,但 IMA 系统包含的功能、资源庞杂,采用本文方法建立的层次化失效模型规模巨大,在底层资源失效层面各不同功能存在交联情况。今后的研究方向之一是失效树中子树的同构确认,剔除重复的失效子树以减少分析的工作量;另一方面,如何高效地分析大规模失效树模型也是必须考虑的另一个问题。

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 Hua-gang, WANG Zhong-hua. Advanced integrated avionics technology [M]. Beijing: National Defense Industry Press, 2009. (in Chinese)

[2] Itier Jean-Bernard. A380 integrated modular avionics [C]//Proceedings of the ARTIST2 Meeting on Integrated Modular Avionics. [S. l.]:IEEE,2007: 72-75.

[3] 陈世浩. 基于 IMA 的大型客机 CNS 系统集成试验和验证[J]. 电讯技术, 2013, 53(5): 543-547.
CHEN Shi-hao. Integrated Test and Validation for IMA-based Large Civil Aircraft CNS[J]. Telecommunications Engineering, 2013, 53(5): 543-547. (in Chinese)

[4] 孙博,康锐,谢劲松. 故障预测与健康管理系统研究和应用现状综述[J]. 系统工程与电子技术, 2007, 29(10): 1762-1767.
SUN Bo, KANG Rui, XIE Jin-song. Research and application of the prognostic and health management system [J]. Systems Engineering and Electronics, 2007, 29(10): 1762-1767. (in Chinese)

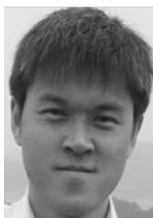
[5] 尤海峰,刘煜. 大型民用飞机 IMA 系统应用分析及发展建议[J]. 电讯技术, 2013, 53(1): 110-116.
YOU Hai-feng, LIU Yu. Application Analysis of and Development Suggestion for IMA System on Large Civil Aircrafts[J]. Telecommunication Engineering, 2013, 53(1): 110-116. (in Chinese)

[6] 郑朝辉,陈新中,张晓先. 综合模块化航空电子系统的可靠性设计[J]. 计算机工程, 2009, 35(23): 272-273.
ZHENG Chao-hui, CHEN Xin-zhong, ZHANG Xiao-

- xian. Reliability Design of Integrated Modular Avionics System[J]. Computer Engineering, 2009, 35(23): 272-273. (in Chinese)
- [7] ZHOU Tian-ran, XIONG Hua-gang. Design of Energy-efficient Hierarchical Scheduling for Integrated Modular Avionics Systems[J]. Chinese Journal of Aeronautics, 2012, 25(1): 109-114.
- [8] 钟杰, 何民, 王怀胜, 等. AFDX 构架及协议分析[J]. 电讯技术, 2010, 50(1): 65-71.
ZHONG Jie, HE Min, WANG Huai-sheng, et al. Avionics Full Duplex Switched Ethernet (AFDX) Frame and Specification Analysis[J]. Telecommunication Engineering, 2010, 50(1): 65-71. (in Chinese)
- [9] 林志博, 王德功, 常硕. 失效分析在航空电子装备保障中的应用[J]. 装备制造技术, 2010(5): 187-188.
LIN Zhi-bo, WANG De-gong, CHANG Shuo. Failure Analysis in the Application of Aviation Electronic Equipment[J]. Equipment Manufacturing Technology, 2010(5): 187-188. (in Chinese)
- [10] Ding C, Xu J, Xu L. ISHM-based intelligent fusion prognostics for space avionics[J]. Aerospace Science and Technology, 2013, 29(1): 12-15.
- [11] Bartley G, Lingberg B. Certification Concerns of Integrated Modular Avionics (IMA) Systems[C]//Proceedings of 2008 IEEE/AIAA 27th Digital Avionics Systems Conference. St. Paul, MN: IEEE, 2008: 1-10.
- [12] CAI Yong, WANG Ze-xin, OU Xu-po, et al. Approach civil Integrated Modular Avionics Airworthiness Certification by Iterative Incremental Certification Process[C]// Proceedings of 2010 2nd International Conference on Information Science and Engineering. Hangzhou: IEEE, 2010: 148-151.
- [13] 褚文奎, 张凤鸣, 樊晓光. 综合模块化航空电子系统软件体系结构综述[J]. 航空学报, 2009, 30(10): 1912-1917.
CHU Wen-kui, ZHANG Feng-ming, FAN Xiao-guang. Overview on Software Architecture of Integrated Modular Avionic Systems[J]. Acta Aeronautica et Astronautica Sinica, 2009, 30(10): 1912-1917. (in Chinese)

- [14] ARINC 651, Design Guidance for Integrated Modular Avionics[S].
- [15] ARINC 653, Avionics application Software Standard Interface[S].
- [16] Watkins C B, Walter R. Transitioning from federated avionics architectures to Integrated Modular Avionics[C]//Proceedings of 2007 IEEE/AIAA 26th Digital Avionics Systems Conference. Dallas, TX: IEEE, 2007: 1-15.

作者简介:



王 鹏(1982—),男,天津人,2005 年毕业于法国国立航空工程大学获硕士学位,现为副研究员,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 1982.

He received the M. S. degree from Institute Supérieur de l'Aéronautique et de l'Espace in 2005. He is currently 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

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 Chang-xiao was born in Shandong Province, in 1989. He received the Ph. D. degree from Beihang University in 2013. He is now an assistant researcher. His research concerns avionics system design and evaluation, avionics integration.

马 赞(1984—),男,天津人,2010 年于北京航空航天大学获硕士学位,现为助理研究员,主要从事民机系统安全性设计与评估、航空电子适航审定技术研究。

MA Zan was born in Tianjin, in 1984. He received the M. S. degree from Beihang University in 2010. He is now an assistant researcher. His research concerns aircraft system design and evaluation of safety, electronic hardware airworthiness.