doi:10.3969/j.issn.1671-637X.2015.07.014

机载网络服务系统航电接口应用软件的研究与设计

刘 绚, 李 莉, 张 双, 张军才, 张拓智
(中航工业西安航空计算技术研究所,西安 710068)

摘 要: 分析ARINC763标准以及ARINC834标准,针对当前民用机载网络安全互联过程中的灵活性和扩展性需求,设计了机载网络服务系统航电接口应用软件。定义航电接口数据通信协议,对ARINC834中的协议模型进行集成及扩展,增加了应用认证和应用监控能力;采用应用认证授权和数据操作控制结合的方法,实现动态应用访问控制,减少系统复杂度,增加系统灵活性。该软件已经在某民机项目中安装使用,可以实现航电核心域网络与网络服务系统内部网络之间安全的数据通信。

关键词: 机载网络; 服务系统; 数据服务; 航电接口; 数据通信; 动态访问控制
中图分类号: V243 **文献标志码**: A **文章编号**: 1671-637X(2015)07-0070-05

Design and Implementation of an Avionics Interface Application Software for Onboard Network Service System

LIU Xuan, LI Li, ZHANG Shuang, ZHANG Jun-cai, ZHANG Tuo-zhi
(Aeronautical Computing Technique Research Institute, Xi'an 710068, China)

Abstract: Based on the analysis to ARINC763 Standard and ARINC834 Standard, and considering the flexibility and expansibility requirements to safe connectivity of current civil airborne network, we designed an Avionics Interface Application(AIA) software for the airborne network service system. The key points of the design include: 1) the definition of Avionics Interface Data Communication Protocol, which integrates and expands the protocol models defined in ARINC834 by adding application registration and monitoring capability; and 2) the combination of application access control and data authentication, which refines the architecture defined in ARINC763 and reduces the system complexity. The software has already been applied in a civil aircraft development project, which can realize secure data communication between core avionic network and network service system.

Key words: onboard network; service system; data service; avionics interface; data communication; dynamic access control

0 引言

美国航空运输协会(Air Transport Association of America, ATA)在《ATA需求100——制造商技术数据需求》ATA 46章节对机载信息系统进行了定义[1]。该系统从航电核心系统中获取数据,通过网络传输给系统内部的设备,最后传递给地面运营中心、服务供应商、客舱系统等。空客A380和A350、波音787飞机都实现了机载信息系统,用以提高航空公司的运营效率,降低维护成本,减轻飞行机组和乘务机组的工作负担,增强乘客愉快飞行的体验,减少航班延误和提高飞机签派率,最终提高民用客机的经济性。我国自行研制的C919飞机为了提升飞机的经济性、增强竞争力,也设计了机载信息系统。

在机载信息系统中,机载网络服务系统(Onboard Network Server System, NSS)负责提供机载信息系统的核心功能,是机载信息系统的关键设备。为了统一NSS的概念和功能定义,ARINC先后发布了ARINC763系列标准[2-3]以及ARINC821[4],以定义NSS系统的物理构成与功能。在NSS的功能中,航电接口应用实现了NSS和航电核心系统之间的数据通信和数据分发的功能,为NSS系统内部其他应用服务(如参数服务、机

收稿日期:2015-01-21 修回日期:2015-02-03
基金项目:航空科学基金(20141931001)
作者简介:刘 绚(1982—),女,陕西西安人,硕士,工程师,研究方向为航空电子设备与系统。

载维护服务、打印服务等)提供飞机数据。

但是由于飞机中的信息分发需要跨越不同的安全域,因此如何保证信息在分发过程中的信息安全已经成为机载信息系统面临的新问题。国外已经开始了这方面的研究,针对未来飞机的连通性,提出了一个适应性的信息安全架构[5],而国内对机载信息安全的开发才刚刚起步。

针对此应用需求,本文将对与 NSS 相关的标准及其实现情况进行分析,描述了一个符合 NSS 航电接口服务需求的集成度较高的 NSS 航电接口应用(Avionics Interface Application,AIA)的设计与实现。该设计定义航电接口数据通信协议(Avionics Interface Data Communication Protocol,AIDCP)及采用动态的访问认证模型,实现了不同机载安全域中的信息通信。

1　工业标准分析

1.1　相关标准简介

从 1999 年发布 ARINC763 到 2008 年发布的最新的 ARINC763A[3] 以及 ARINC REPORT821[4],其目的都是规定可安装于各种飞机机型的典型网络服务系统的物理形态和适应维度,电气接口定义以及典型系统功能。通过 NSS 架构的使用,可在民用飞机中采用通用商业货架组件,包括无线传输设备进行多种数据链路间的通信,从而为多种机上机下应用提供实时在线的通用计算和数据传输服务,实现实时支持机组人员、维修人员、飞机运营以及管理人员进行飞机运行状态监控,故障定位和维修以及飞机运营管理等多种行为。NSS 连通性关系如图 1 所示[2]。

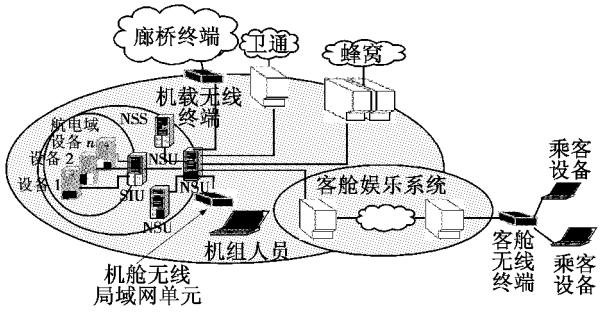

图 1　NSS 连通性示意图

Fig. 1　The connectivity of NSS

ARINC763 定义应用驻留在航电网络服务单元(Network Sever Unit,NSU)上,主要提供通用航电数据/文件存储,开放式处理以及与通过飞机局域网连接的设备间的网络通信服务。NSS 接口服务管理(NISM)组件驻留在服务接口单元(SIU)上,负责使能,监控以及控制航电网络和所有非航电网络组件之间的数据流,它是航电数据的集中器和发布器,也是应用的授权机构。它要向驻留在 NSU 的应用提供以下服务:1)连接服务;2)应用驻留平台 NSU 的身份认证,应用注册以及控制服务;3)航电数据服务;4)应用监控服务;5)配置服务。

ARINC REPORT821[4] 描述了适合在各种机型上安装的飞机网络服务以及网络服务系统功能,在其第 6 章中指出,符合其标准的飞机网络应提供 ARINC834 定义的飞机数据接口功能。

ARINC834-1 Aircraft Data Interface Function(ADIF)则是为了提供不同安全级别的网络域之间的连通性而发布的,它对 ARINC763 系列设定的飞机接口定义进行了加强,并采用了更多的工业界的方法,能够提供更多的功能[6]。它定义了包括 GAPS(Generic Aircraft Parameter Service),STAP(Simple Text Avionics Protocol)以及 ADBP(Avionics Data Broadcast Protocol)在内的一组协议,使得基于商用货架网络组件构建的应用能够通过访问专用航电网络和总线接口来获得航电数据。ARINC834-1 架构如图 2 所示。

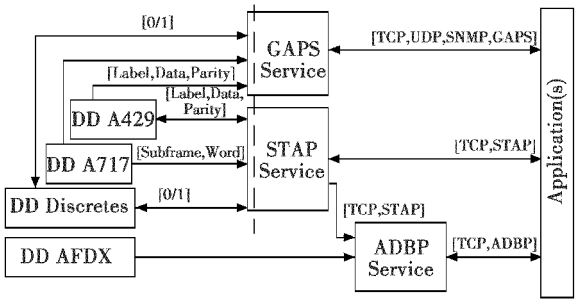

图 2　ARINC834-1 架构

Fig. 2　Role and accessibility of GAPS,STAP and ADBP services ARINC834-1

1.2　实现分析

ARINC763-3 中建议但不限定 NISM 采用 CORBA(Common Object Request Broker Architecture)架构实现,但是 CORBA 架构复杂、庞大的特性,使其在机载环境下的应用受到限制。机载环境下,需要一个更为通用的、适用于嵌入式环境下的架构。

ARINC834-3 没有提供统一的应用管理策略,因此要实现其协议,必须预先对应用的安全级别进行划分,然后根据静态应用的安全级别选取不同的传输协议:对 A429 总线,离散量等具备只读数据权限的应用选取 GAPS 协议;对 A429 总线,离散量数据具备操作权限的应用采用 STAP 协议;而不具备离散量控制、原始数据传输权限,却具有 AFDX(Avionics Full Duplex Switched Ethernet)总线读操作权限的应用采用 ADBP 协议进行传输。这种实现方法的缺点是灵活性和扩展性差,特别是在系统实现后,如果应用的访问权限发生变更,则系统的更改比较困难。

基于以上分析,本文给出了航电接口应用(AIA)软件的设计方法,它通过定义和实现与应用间通信的AIDCP协议以及动态访问控制模型,提供了一种通用、灵活、扩展性强的解决方法。

2 航电接口应用设计

2.1 航电接口应用架构

航电接口应用AIA向应用提供统一的运行在TCP/IP协议之上的访问接口,该接口符合AIDCP协议。AIA软件逻辑架构如图3所示。

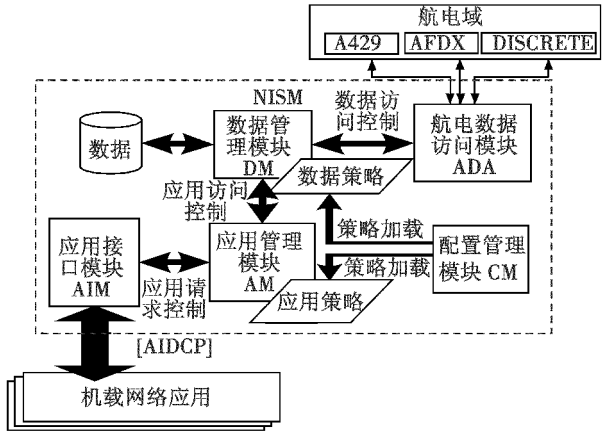

图3 软件逻辑架构图

Fig. 3 Logical architecture of AIA

AIA和应用之间允许通过两个通道进行传输:同步通道和异步通道。同步通道通过"应用请求-AIA响应"的机制进行通信。异步通道采用"AIA发送-应用接收"的单向过程进行数据传输。在AIA内部,依据应用提供的参数动态地对应用的访问权限进行限制。同时,AIA对不同协议的航电总线的访问接口进行封装,对内部提供统一的航电访问接口。在AIA内部,根据数据的参数对数据的可访问性进行限制。AIA内部的模块通过数据进行耦合,功能相互独立。

2.2 航电接口应用构成

2.2.1 应用接口模块

应用接口模块(Application Interface Module,AIM)使用不同的任务并发管理同步连接和异步连接。AIM接收来自TCP/IP连接上的应用请求,解析请求中的有效内容,将该内容传递给应用管理模块(Application Mangement Module,AM)。同时,AIM从AM中获取请求响应的有效数据,对其进行TCP/IP消息封装,并发送给对应的应用。AIM根据AM的数据,向应用申请建立异步通信的连接。同步通信的连接和异步通信的连接占用的资源相互独立,一方的故障不对另一方造成影响。

此外,AIM对应用和AIA之间的TCP连接进行监控和管理。AIM可以建立和断开AIA和应用之间的连接,并对无效连接进行清理。

2.2.2 应用管理模块

应用管理模块(AM)管理基于静态策略,在运行时动态地对应用的访问权限进行管理,包括权限授予,权限验证,权限回收以及按照对应的应用权限给出相应的请求处理和响应。同时,还包括对通过心跳信息传入的应用运行状态的监控功能。

2.2.3 数据管理模块

数据管理模块(Data Management Module,DM)管理基于静态策略,对数据的存储性及可访问性进行管理。存储性指是否允许数据在本地存储区进行存储;可访问性指对数据的读、更新、向应用公开和写入航电总线等权限。DM通过对数据存储对象的操作接口,完成数据的存储、删除、查询和更新功能。

2.2.4 航电访问模块

航电访问模块(Avionic Data Access Module,ADA)完成航电总线访问功能,它屏蔽不同航电总线协议(A429,离散量,AFDX,A717等)的读、写、访问使能以及访问禁止等操作的实现细节,对AIA软件提供统一的访问接口,它按照数据的操作控制权限对航电总线上的数据执行操作,并在发生异常时,执行对应的总线禁止操作,中断和航电的连通关系,实现故障隔离。

2.2.5 配置管理模块

配置管理模块(Configuration Management Module,CM)负责在运行时动态地向AM以及DM模块加载策略文件。

3 关键技术

AIA设计的关键技术有两个:一是定义和应用的通信协议AIDCP协议;二是定义应用的访问控制模型。

3.1 通信协议

AIDCP协议对ARINC834中定义的ADBP协议进行扩展,增加了应用注册和心跳操作,并在数据请求操作的消息中加入CRC验证信息。通过应用注册操作,软件获取应用的运行平台及其自身的身份信息,用于实现注册功能,并对应用的身份认证和授权功能提供支持。通过心跳操作,软件可以实现对应用的运行状态进行监控的功能。通过增加CRC验证信息,可以加强对数据的完整性校验。

AIDCP协议规定了4类操作类型,这些操作定义如下所述。

1)注册操作:由应用提出注册请求,服务器端给出注册请求的响应。消息中包含了应用的身份认证信息,可供应用实现平台NSU的身份认证以及应用注册功能。

2）注销操作：和注册操作相对应。由应用提出注销请求，服务器端给出注销请求的响应。用于应用撤出网络服务系统时使用。

3）心跳监控操作：由应用给出心跳消息，服务器端给出心跳消息的响应。用于监视应用的运行状态，避免“死亡”应用长期占用资源，以及由此而造成的安全隐患，如内存溢出，多次连接形成的网络攻击等。

4）数据操作：数据操作可分为请求数据操作、写入数据操作。请求数据操作又分为只针对当前请求进行响应的获取数据操作，当前及周期性响应的连续型数据操作，当前及在事件触发时进行响应的事件型数据操作以及取消订阅操作。连续型数据操作以及事件型数据操作统称为订阅数据操作。应用请求数据时均采用同步方式交互，而订阅条件满足时使用异步方式交互。取消订阅操作应在订阅数据操作成功后执行。数据操作消息过程中，在原始数据信息中添加了 CRC 属性，用于存储对数据值进行 CRC 计算的结果，以增加数据的完整性。

AIDCP 协议定义了符合 XML V1.0 标准的同步消息和异步消息。消息格式定义见图 4，其中，Method 元素是请求消息和异步消息的根元素，Response 元素是响应消息的根元素。

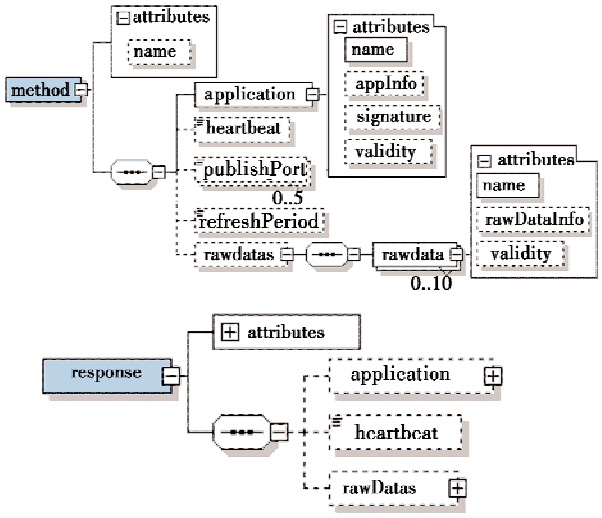

图 4　AIDCP 消息定义

Fig. 4　Message scheme of AIDCP

3.2　访问控制模型

应用的访问控制模型包括数据操作控制和应用访问控制两部分，用于实现对应用的数据访问权限进行动态控制。

3.2.1　数据操作控制

数据特征值（Di）定义为：Di = {DNi, DSi, DOi}。其中：DNi 为数据项的唯一标识；DSi 为数据的源信息，从中可以识别数据的类型和来源；DOi 表示该总线数据可允许的操作。数据操作控制要求 Di ∈ DS，DS 为数据策略库。

3.2.2　应用访问控制

应用的访问控制包含对应用的身份认证 -> 应用的密钥授权 -> 应用操作控制这个过程实现。

应用注册消息中提供应用特征值。应用特征值（Ai）定义为：Ai = {ANi, APKi, APi, AAi}。其中：ANi 指应用的唯一标识；APKi 指系统预先分配给应用的密钥；APi 指应用驻留平台的唯一标识，包含应用的实例号信息；AAi 指应用的网络地址。应用身份认证要求 Ai ∈ AS，AS 为应用策略库。

身份认证通过后，AIA 的 AM 生成应用密钥。应用密钥（Aki）由应用特征值和时间生成，即 Aki = f(Ai, Time)。最后，在 AM 的访问信息库 IM 中保存应用信息 < ANi, Aki >。

当应用提出数据访问请求时，通过请求消息中的三元组 < ANi, Aki, Di > 进行应用的访问控制，< ANi, Aki > ∈ IM&&Di ∈ DS。

应用的数据访问过程序列见图 5。

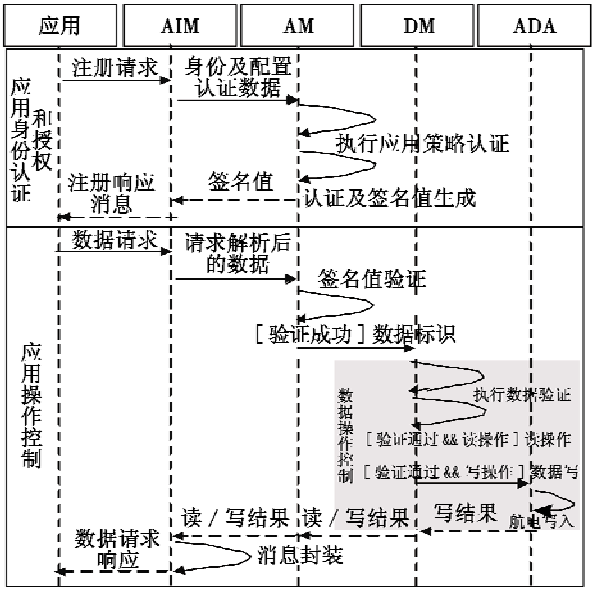

图 5　应用数据访问过程序列图

Fig. 5　Sequence of data access operation

4　应用结果验证

AIA 软件现已驻留在嵌入式操作系统 Vxworks 中运行。其驻留的硬件模块采用 PC7447 芯片，以 600 MHz 的频率运行。动态存储器为 256 MByte，访问带宽理论可达 1600 MByte/s。其实现的外部接口包括：与应用连接的 2 路 100 MByte/s 速率的 A664P3 接口，与航电核心网连接的 8 路 A429 接口和 4 路 A664P7 网络接口。

现有的实验数据表明，AIA 软件可以同时与包括

飞机参数在内的超过4个应用建立同步连接,接收应用注册,对应用实现监控。同时可以对应用的请求进行同步响应以及异步响应,实现预期功能目标。实现环境中对软件的响应要求小于5 ms,本软件的实际响应时间为1 ms,达到了预期的性能要求。

在测试过程中,进行故障注入,使不同的功能出现故障,其他功能的运行不会受到影响,恶意的网络攻击会导致应用接口模块的瘫痪,但是该故障不会蔓延到航电数据访问模块;应用之间访问不同的数据,实现不同的数据操作,AIA能够识别出不合法的应用以及错误的访问。

5 结语

本软件的设计,通过定义和实现AIDCP协议以及动态访问控制模型,实现了机载网络环境下航电数据的安全分发功能,并且达到了增加系统的灵活性和扩展性,减少系统的复杂度,提高系统的集成化的目的。AIDCP协议采用XML语言描述,不需要专门的客户端软件,不受应用端驻留平台及编程语言的限制,实现了对分布式异构平台环境的支持,保证了系统的开放性,节省了系统资源。本应用已在某大型民机项目的原理样机上实现,完成了系统功能的集成,达到了功能和性能要求。

参考文献

[1] Air Transport Association. ATA specification 100 specification for manufacturers'technical data [S]. [S.l.]: ATA, 1999.

[2] SAE. ARINC 763 Network server system (NSS)[S]. [S.l.]: ARINC, 2004.

[3] SAE. ARINC763A Network server system (NSS) form and fit definition[S][S.l.]: ARINC, 2008.

[4] SAE. ARINC 821 Aircraft network server system(NSS) functional definition[S]. [S.l.]: ARINC, 2008.

[5] MAHNOUD M S B, LARRIEU N, PIROVANO A, et al. An adaptive security architecture for future aircraft communications [C]//29th Digital Avionics Systems Conference, IEEE, 2010:3. E. 2-1-3. E. 2-16.

[6] SAE. ARINC 834-1 Aircraft data interface function (ADIF) [S]. [S.l.]: ARINC, 2009.

(上接第51页)

[3] 周淑华,徐贵民,张博,等."动中通"中TCP连接"阴影"恢复时间的研究[J]. 计算机工程与应用,2009,45(8):123-124. (ZHOU S H, XU G M, ZHANG B, et al. Study on TCP connection recovery time from link blockage in SOTM[J]. Computer Engineering and Applications, 2009, 45(8):123-124.)

[4] 林智慧,李磊民. 星通信的技术发展及应用[J]. 现代电子技术,2007(3):38-39. (LIN Z H, LI L M. Technology development and applications of satellite communications [J]. Modern Electronics Technique, 2007(3): 38-39.)

[5] SCALISE S, ERNST H, HARLES G. Measurement and modeling of the land mobile satellite channel at Ku-band[J]. IEEE Transactions on Vehicular Technology, 2008, 57(2):693-703.

(上接第60页)

[3] 范志良,刘光斌. GLONASS卫星信号仿真器设计与实现[J]. 无线电工程,2009,39(3):33-36. (FAN Z L, LIU G B. Design and implementation of GLONASS signal simulator[J]. Radio Engineering, 2009, 39(3):33-36.)

[4] 侯博,谢杰,范志良,等. 多模卫星信号模拟器设计与实现[J]. 计算机测量与控制,2012,20(1):170-172,176. (HOU B, XIE J, FAN Z L, et al. Design and realization of a GNSS signal simulation[J]. Computer Measurement & Control, 2012, 20(1):170-172, 176.)

[5] 罗益鸿. 导航卫星信号模拟器软件设计与实现[D]. 长沙:国防科学技术大学,2008. (LUO Y H. The software design and implementation of navigation satellite signa simlator[D]. Changsha: National University of Defense Technology, 2008.)

[6] 刘旭东,赵军祥. 旋转载体多天线对GPS卫星可见性分析[J]. 全球定位系统,2009(5):11-14. (LIU X D, ZHAO J X. Analysis of the GPS satellite visibility based on rotating carrier[J]. GNSS World of China, 2009(5):11-14.)

[7] 刘丽丽,王可东. 卫星信号模拟器研究现状及其发展趋势[J]. 全球定位系统,2010(3):58-61. (LIU L L, WANG K D. Research status and development tendency of the satellite signal simulator[J]. GNSS World of China, 2010(3):58-61.)

[8] KRAUS J D, MARHEFKA R J. 天线[M]. 3版. 章文勋,译. 北京:电子工业出版社,2004. (KRAUS J D, MARHEFKA R J. Antennas: for all applications[M]. 3rd ed. Translated by ZHANG W X. Beijing: Publishing House of Electronics Industry, 2004.)

[9] 刘旭东,赵军祥. 载体旋转条件下GPS中频信号生成方法[J]. 飞行器测控学报,2009(28):91-94. (LIU X D, ZHAO J X. A generation method of GPS if signal under carrier rotating conditions[J]. Journal Spacecraft TT&C Technology, 2009(28):91-94.)