http://myfj.cnjournals.com myfj_sadri@163.com (021)20866796

DOI: 10.19416/j.cnki.1674-9804.2024.01.023

机载软件网络安保管理策略研究

姜嘉锐* 李翰泽 吕昌翰

(北京飞机维修工程有限公司,北京 100621)

摘 要: 随着信息化和网络技术在民航领域的不断深化应用,民用飞机机载软件的数量和重要性都大幅增加,机载软件的传输方式也由实物运输方式转变为通过网络进行传输和存储。这些变化在带来便利和效率提升的同时也引入了网络安保风险,给飞机持续适航管理中的机载软件管理提出了新的要求。总结了机载软件网络安保相关的审定政策和技术标准,分析了飞机持续适航管理中机载软件网络安保管理的要求,并提供了运营人机载软件网络安保管理实施政策的制定思路和体系建设的建议方法。

关键词: 机载软件;持续适航;网络安保

中图分类号: TP393 **文献标识码**: A **OSID**:

0 引言

随着技术的发展,航电系统数字化、集成化和模块化成为了新一代民航客机(如波音 787、A350 机型等)最显著的特征之一[1]。其中,机载软件在飞机系统中扮演了关键的角色,飞机上许多关键系统的功能和控制逻辑都通过机载软件实现。同时,大量信息和网络技术被引入新一代民机和民航系统中,如 4G、5G、WiFi、卫星地空宽带等,TCP/IP 通讯技术逐步替代了传统的机载软件实物运输方式,为运营人提供了极大的便利并降低了相关成本。

新技术的使用也使包括机载软件在内的飞机机载网络系统面临着潜在的网络安保威胁[2]。例如波音 787 客机上安装了核心网络系统(core network),其利用网络技术可以存储飞机的部分数据和应用程序并连接外部网络。2019 年 IOActive 研究团队宣称通过对高度网络化的波音 787 飞机部件进行逆向工程,成功发现了波音 787 飞机核心网络中存在的多个安全漏洞,这些漏洞可能会允许攻击者远程访问飞机上的敏感航空电子网络[3]。与地面网络系统需要应对种类繁多的黑客攻击、病毒感染、信息篡改等安保威胁一样,如何应对机载软件的网络安保威胁成为了民用飞机持续适航管理中必须要考虑的问题。

为此,各国局方和行业技术组织颁布了相关政策和技术标准文件指导民用飞机和机载软件的网络安保工作[4]。各飞机制造商在符合相关初始适航要求的同时,近年来也发布了操作指导文件指导运营人符合飞机和机载软件的持续适航网络安保要求。运营人需要针对机载软件的网络安保管理建立一套适用的管理策略以满足要求。

1 机载软件网络安保管理政策和技术标准分析

1.1 美国联邦航空局(FAA)政策分析

FAA 在适用机型的审定基础中加入了网络安保相关的专用条件。以波音 787 飞机为例,FAA 发布的专用条件(special conditions, 简称 SC)[5] 25-356-SC 和 25-357-SC 分别对飞机设计和飞机运行提出了网络安保要求。

当某飞机审定基础中包括网络安保要求的 SC 时,运营人也需要符合相关 SC 的要求。为了向运营

* 通信作者. E-mail: Jiangjiarui@ameco.com.cn

引用格式: 姜嘉锐,李翰泽,吕昌翰. 机载软件网络安保管理策略研究[J]. 民用飞机设计与研究,2024(1):145-150. JIANG J R,LI H Z,LYU C H. Research on cyber security management strategy of field loadable software[J]. Civil Aircraft Design and Research,2024(1):145-150(in Chinese).

人提供一种可接受的符合性方法,FAA 发布了咨询通告 AC 119-1“Airworthiness and Operational Approval of Aircraft Network Security Program(ANSP)”[6],其中明确了飞机网络安保计划的管理目标,飞机制造商和飞机运营人各自的职责以及飞机网络安保管理的符合性方法。此咨询通告主要依据技术标准 RTCA/DO-355 编写,适用于运营人,为其提供飞机运行阶段的工作指导。

FAA 发布的咨询通告 AC 43-216“Software Management During Aircraft Maintenance”[7]为飞机维修活动期间制定机载软件管理程序提供了指导,以确保符合相关的持续适航法规。值得注意的是,AC 43-216 中明确对于审定基础中包含网络安保要求 SC 的飞机,即使其运行不受 ANSP 的约束,机载软件的管理也需要符合网络安保 SC 条款的要求。FAA 已计划对此 AC 进行改版,发布了 AC 43-216A 草案并进行意见征询。AC 43-216A 加入了更多机载软件网络安保要求,并认可技术标准 RTCA/DO-355 可以作为该 AC 范围以外的可接受网络安保管理程序来源。

1.2 欧洲航空安全局(EASA)政策分析

EASA 于 2022 年颁布实施规则 EU 2023/203,搭建了航空业内信息安保的监管法规框架。EU 2023/203 附件 Part-IS(information security)规定了对可能影响民航系统内的信息和通信数据安全的风险进行识别和管理的要求。Part-IS 也包括对于飞机初始适航、持续适航和运营人等的信息安保管理要求。

对于民用大型客机,EASA 发布的审定规范(certification specifications,简称 CS)CS 25.1319“Equipment, System and Network Information Security Protection”[8]对飞机的设计和运行中的网络安保管理提出了总体要求。具体到各机型,EASA 也发布了 SC,对相关飞机型号的网络安保提出要求。例如:EASA 针对 A350 机型发布了 F-38 SC:“Security Assurance Process to Isolate or Protect the Aircraft System and Networks from Internal and External Security Threats”。

为了提供飞机适航网络安保要求的符合性方法,EASA 发布了可接受的符合方法 AMC 20-42“Airworthiness Information Security Risk Assessment”[9]。AMC 20-42 明确了遵循技术标准 RTCA/DO-326A、DO-355 和 DO-356A 的要求可作为符合飞机网络安保要求的方法。

1.3 中国民用航空局(CAAC)政策分析

我国局方对于民用飞机机载网络和机载软件的网络安保管理尚处于起步阶段,CAAC 对 C919 颁发了专用条件 SC-25-031《机载网络安保》。SC-25-031 对 C919 飞机机载网络安保威胁和风险的消除措施和机载网络安保的设计提出了要求。但针对飞机持续适航管理中的机载网络或机载软件的网络安保管理,CAAC 还未颁布 AC,对飞机制造厂家和运营人无法提供明确的指导。

1.4 技术标准分析

1.4.1 飞机网络安保技术标准

DO-355A/ED-204[10]是用于飞机持续适航网络安保管理的技术标准,其内容涵盖了对飞机机载软件、飞机部件、飞机网络接近、地面设备、地面信息系统等,为应对飞机运行和维护中的网络安保威胁提供信息技术、管理体系建设和安保事件管理等安全措施的要求。

DO-326A/ED-202A[11]是用于适航当局和航空工业在研发或改装飞机系统进行适航认证过程中,当涉及可能造成安全影响的未授权的电子交互威胁时,进行适航认证的支持性文件。其中定义了在适航认证过程中处理可能未授权的电子交互导致飞机安全风险的符合性目标和方法。

DO-356A/ED-203A[12]是在 DO-355A/ED-204 和 DO-326A/ED-202A 基础上对飞机网络安保适航认证过程的补充指导文件,对飞机网络安保的安全性评估和有效性保证提供具体的风险分析准则、方法和工具。

以上三个技术标准中,DO-355A/ED-204 是运营人在飞机持续适航管理中应主要遵循的技术标准。DO-355A/ED-204 中第 2 章规定了机载软件使用中各项工作应满足的网络安保管理要求,其中大量引用了 ARINC 和其他技术标准的内容作为依据。

1.4.2 机载软件网络安保技术标准

ARINC 667-2[13]是对飞机运行阶段使用中的机载软件管理的指导文件。其对机载软件的分类进行了定义,并明确了使用过程中机载软件的各项工作活动的要求。其在机载软件安保管理部分中明确要求运营人应符合 DO-355A 和 ANSP 的要求,对与机载软件有关的环节和过程,地面网络和系统进

行网络安全性评估和管理。2022 年发布的 ARINC 667-3 增加了 7.5 节“Process Control for Software Security”,详细说明了机载软件在存储、分发和装载等环节中应符合的各项网络安保要求。

ARINC 645-1[14] 为运营人、飞机制造商、飞机设备供应商等提供了机载软件分发和装载过程中的技术标准。文档的第 5 节详细说明了飞机数据装载过程中的安保标准和适用的安保类别。

ARINC 835-1[15] 是为运营人提供应对机载软件的网络安保威胁措施的指导文件,提供了机载软件网络安保现有管理方法的背景和详细技术信息。该文件分别说明了波音飞机和空客飞机的机载软件网络安保管理过程和要求,并对验证机载软件所使用的数字身份验证技术规范进行了说明。

ATA SPEC42[16] 提供了符合法规和行业技术标准要求的、不同级别安全需求的数字身份认证应用的标准化方法,并且给出了用于航空运输行业的数字凭据保证的安全强度建议。

2　机载软件网络安保实施要求

随着关于飞机和机载软件网络安保的局方政策法规和行业技术标准的不断完善,行业内也明确了机载软件网络安保管理要求。飞机制造商和运营人都应承担各自的机载软件网络安保管理责任。为了支持和指导运营人应对机载软件网络安保威胁,飞机制造商应提供飞机网络安保管理指导文件,其中的强制性措施应明确将持续性适航要求加入持续适航文件(ICA)中。例如波音公司已发布服务信函(SL)告知运营人,波音公司将更改相关 ICA,加入机载软件的网络安保要求。

目前飞机制造商已经发布的典型的飞机网络安保指导文件有空客公司的“Security Handbook”和波音公司的“Airplane Network Security Operator Guidance(ANSOG)”等,指导手册中包含机载软件的网络安保要求和符合性方法。

运营人进行机载软件网络安保管理工作时应遵循飞机制造商的网络安保指导手册和其他持续适航文件的要求,并参考相关政策性文件和技术标准。本文通过对局方政策法规、航空工业技术标准和飞机制造商的指导手册和持续适航文件进行了梳理和分析,总结得出机载软件网络安保管理实施策略应主要包括以下几个方面内容。

2.1　公钥基础设施(PKI)

机载软件的传输和装载过程中需要利用 PKI 进行身份验证识别,以保障机载软件来源的可靠性和完整性。在 ARINC835-1 和 ATA Spec42 中要求用于机载软件的身份验证保证的 PKI 应满足最高级即第 4 级的要求,并且存放 PKI 密钥的数字凭据还应满足中级硬件保证(medium hardware assurance)的要求。中等硬件保证级别要求使用者的 PKI 密钥存储设备应使用加密令牌(如智能卡、U 盘、PCMCIA 卡等),这种设备被认为是安全签名创建设备(SecSCDev)。

2.2　机载软件装载设备

机载软件装载设备,如便携式装载机、通用维护设备等是用于存储和向机载系统装载软件的便携式装载工具。机载软件装载工具应满足 ARINC 645-1 标准中的安保要求,包括机载软件数字签名验证、接近控制、防病毒等。需要特别注意的是,由于此类工具为公用设备,故实施有效的接近管控手段、对使用人员进行有效控制、防止未经授权的人员使用装载设备获取和装载软件是非常必要的。

2.3　机载软件存储服务器

机载软件存储服务器相当于机载软件的“电子库房”,用于存储和电子化分发机载软件,某些存储服务器还具备与飞机直接传输数据的能力。因此,除了应满足服务器本身的网络信息安保要求以外,运营人还需要采取必要的措施防止未授权人员登录或操作机载软件存储服务器,以防止未经授权的软件上传、下载或分发。

2.4　机载软件媒体介质

对于通过传统方式传输的机载软件,软件存储在媒体介质中,如软盘、U 盘、CD 和 PC 卡等。软件存储介质应按照航材管理的要求,在获取后进行验收并妥善储存。运营人应建立相应的管理制度或实施技术手段,防止未授权人员获取或篡改软件存储介质。同时,为了防止使用非法的机载软件存储介质装载软件,在使用软件存储介质的各环节应加入数字身份验证要求。

3　运营人机载软件网络安保实施策略

飞机持续适航管理中,机载软件网络安保管理的目的是确保将来源可靠、未被篡改过的机载软件正确地装载到飞机上。同时,为了防止通过对机载软件逆向工程而攻破机载网络的安保系统,也要防

止未经授权的人员获取机载软件。为达到以上目的,机载软件网络安保管理可以从来源合法性验证和接近控制这两个方面着手。

3.1 加强机载软件数字身份验证管理

目前,公钥基础设施(PKI)技术已经应用于部分新型号飞机的机载软件管理流程中,但对于在役机队中还占多数的传统机型,运营人应尽快部署和应用公钥基础设施(PKI)技术,在机载软件的接收、传输和装载等各个环节要求进行机载软件身份验证和完整性检查。同时,为满足中级硬件保证对 PKI 密钥存储设备的要求,运营人可以选用硬件安全模块(HSMs)或智能卡作为 PKI 密钥存储设备。硬件安全模块是一种专门具有嵌入式处理执行加密操作的硬件,已经广泛地应用于各类身份验证和加密等使用场景,如网上银行和电子商务等[17]。智能卡是一种内嵌有微芯片的塑料卡,广泛应用于支付、门禁和身份验证等场景,具备高可靠性和高安全性的特征[18]。

3.2 加强与机载软件有关的设备、应用软件的接近控制

涉及与机载软件有关的设备,应用软件包括各类移动装载设备、机载软件分发服务器、机载软件制作工具、机载软件存储服务器等。针对这些设备,运营人除了应做好病毒防护、漏洞修复等网络安全防护措施外,还必须采取必要的接近控制措施,防止未授权人员接近或访问,而接近控制又可细分为电子接近(登录访问)控制和物理接近两方面。

电子接近控制等级由高到低可以分为三级,如表 1 所示。

表 1 电子接近控制等级

控制等级	控制措施
高等级	多因子认证接近控制(如密码、生物识别、人脸识别等)
中等级	符合工业标准的高强度密码登录控制
低等级	共享高强度密码登录或个人使用低强度密码登录控制

物理接近控制是指对多人共用移动设备或存储媒介的人员接近控制,对各不同区域的控制级别举例说明如表 2 所示。

表 2 物理接近控制等级

控制范围	高等级控制措施	低等级控制措施
设备存储区域限制	有访问控制措施的专用存储区域	普通存放
设备发放时间限制	只限于完成授权维护、操作任务或工作所需的时间内发放	一段时间内
人员接近控制程序	定期对设备领用过程和程序进行审核	发生差错或意外情况后发起审核
设备发放对象	仅对具有特定授权或资质的人员发放	广泛发放
发放原因	专用器材,发放目的明确	多种使用原因或发放原因未跟踪
使用登记	从发放到还回进行跟踪	只跟踪领用记录
库存清点	每日	定期清点或意外发生时
操作系统账户	启用并审计	未启用或未审计
设备丢失或损坏的处置	有专门处理此类事件的部门	由使用者/使用部门处理

运营人可以采取物理和电子接近混合控制的策略以满足机载软件接近安保控制要求。表 3 给出了几种可以接受的接近控制策略组合。

表 3 可接受的接近控制策略组合

电子接近控制	物理接近控制	数据加密
高等级	高等级	加密/未加密
高等级	高/低等级	未加密
中等级	高等级	未加密
中等级	低等级	加密
低等级	高等级	加密

运营人可根据自身实际情况,在既保证管控措施有效,又不至于过渡管控,同时避免造成资源和人力浪费的前提下,选择合适的管控策略。

3.3 升级软件装载设备,应用新的网络安保管控技术

对于波音 737NG、A320CEO 等传统机型,以及部分用于向飞机机载系统装载软件的便携式机载软件装载设备,由于这些机型和设备设计时间较早,在软件的传输和装载过程中不能验证机载软件的完整性和来源的合法性,并且不能对机载软件进

行有效的接近控制,所以不能满足最新的机载软件网络安保要求。例如波音公司已通知运营人,未来将从其飞机维护手册中删除不符合 ARINC 645-1 标准要求的机载软件装载方法[19]。因此,运营人应与飞机制造商和部件、设备供应商主动沟通,讨论制定符合持续适航管理要求的改装、设备升级方案和软件装载管控流程。

4　机载软件网络安保管理体系建设

运营人除了应用新技术、采用接近控制等实施策略加强机载软件网络安保管理外,还应该建立机载软件的网络安保管理体系。

4.1　制度建设

运营人应制定机载软件网络安保管理的规章制度,此管理制度是运营人对机载软件网络安保管理的依据。制度内容应满足局方法规、行业标准、飞机制造商指导文件的相关要求,主要内容可包含但不限于管理规定、风险管理、组织管理、人员培训、手册管理等。运营人应参考 ANSP 的要求,制定飞机网络安保管理手册,手册内容应包含机载软件网络安保的相关内容。

4.2　组织管理和培训

清晰的组织管理体系是机载软件网络安保管理的关键一环。运营人应明确承担机载软件网络安保管理责任部门或工作岗位,并对关键人员进行培训和工作资质认证,使相关人员认识到其面对的网络安保潜在威胁,并掌握必要的政策知识、工作流程和技术技能。

4.3　风险管理

运营人应将机载软件网络安保风险纳入自身风险管控范围,制定流程持续识别涉及机载软件的工作中所面临的网络安保威胁,并进行安全风险评估。对于已识别的风险,应按照其评估结果制定风险应对措施。

4.4　事件管理

为了能够对机载软件网络安保进行有效地管理,运营人应建立网络安保事件管理和上报机制。运营人应保证与机载软件相关的网络安保事件能够被及时发现并采取纠正和预防措施。当网络安保事件对飞机持续适航或飞机安全具有潜在影响时,运营人应按照航空安全事件上报的法规要求进行处理。另外,运营人也应建立机制将网络安保事件提交给飞机制造商进行协助调查,以发现对飞机安全可能造成的潜在影响。

4.5　加强与局方沟通

前文已经提到,我国对于机载软件网络安保的管理法规政策制定还处于起步阶段。因此,运营人应加强与局方的沟通,积极参与局方法规政策的制定,协助局方建立符合我国民机和机载软件网络安保管理要求的法规政策体系,并结合运营人的实践经验将行业内已经成熟的技术标准纳入我国的管理要求,从而为飞机持续适航管理中的机载网络和机载软件网络安保管理提供依据,更好地保障飞机的飞行和运行安全。

5　结论

随着航电技术的发展和信息技术在飞机系统中的广泛应用,机载软件在飞机系统中扮演更加重要角色的同时,也面临着愈加严重的网络安保威胁。机载软件的网络安保管理已成为了飞机持续适航管理中至关重要的一环。本文通过对机载软件网络安保管理的政策和技术标准进行分析,总结了机载软件网络安保管理的要求,并为运营人制定机载软件网络安保实施策略及建设网络安保体系提出了合理的建议。

参考文献:

[1] 李军生, 李京生. 民机综合模块化航空电子系统及其发展[J]. 航空制造技术, 2013(19): 42-45.

[2] 曹全新, 杨融, 孙志强, 等. 民用飞机网络安全问题与策略探究[J]. 网络安全技术与应用, 2016(12): 150-151,153.

[3] SANTAMARTA R. Arm IDA and cross check: reversing the 787's core network [EB/OL]. (2019-08)[2023-06-11]. https://i. blackhat. com/USA-19/Wednesday/us-19-Santamarta-Arm-IDA-And-Cross-Check-Reversing-The-787-Core-Network. pdf.

[4] 赵庆贺, 廖健, 何娣, 等. 民机机载系统网络安保适航政策分析[J]. 民用飞机设计与研究, 2020(2): 103-107.

[5] FAA. B787 type certification data sheets(TCDS):FAA T00021SE[S]. U. S. :Federal Aviation Administration, 2021.

[6] FAA. Airworthiness and operational approval of aircraft network security program (ANSP): FAA AC 119-1[S]. U. S. : Federal Aviation Administration, 2015.

[7] FAA. Software management during aircraft maintenance:

FAA AC 43-216[S]. U. S.: Federal Aviation Administration, 2017.
[8] EASA. Certification specification and acceptable means of compliance for large aeroplanes: EASA CS-25 Amendment 27[S]. Brussels: The European Aviation Safety Agency, 2021.
[9] EASA. Airworthiness information security risk assessment: EASA AMC 20-42[S]. Brussels: The European Aviation Safety Agency, 2020.
[10] RTCA. Information security guidance for continuing airworthiness: DO-355A/ED-204[S]. U. S.: Radio Technical Commission for Aeronautics, 2020.
[11] RTCA. Airworthiness security process specification: DO-326A/ED-202[S]. U. S.: Radio Technical Commission for Aeronautics, 2014.
[12] RTCA. Airworthiness security methods and considerations: DO-356A/ED-203[S]. U. S.: Radio Technical Commission for Aeronautics, 2018.
[13] ARINC. Guidance for the management of field loadable software: ARINC 667-3[S]. U. S.: ARINC Industry Activities, 2022.
[14] ARINC. Common terminology and functions for software distribution and loading: ARINC 645-1[S]. U. S.: ARINC Industry Activities, 2021.
[15] ARINC. Guidance for security of loadable software parts using digital signatures: ARINC 835-1[S]. U. S.: ARINC Industry Activities, 2014.
[16] ATA. Aviation industry standards for digital information security: ATA Spec42[S]. U. S.: Air Transport Association Of America, Inc, 2018.
[17] 胡嘉航. 硬件安全模块的设计及应用[D]. 杭州:杭州电子科技大学, 2017.
[18] 张平,贾亦巧,王杰昌, 等. 基于智能卡的匿名认证与密钥协商协议[J]. 计算机应用与软件, 2023, 40(4): 282-288.
[19] Boeing. Enhanced airplane software security-ARINC 641-1 compliant PDL and digitally signed software parts [Z]. U. S.: Boeing, 2023.

作者简介

姜嘉锐 男,本科,工程师。主要研究方向:飞机电子化运行。E-mail:Jiangjiarui@ameco.com.cn

李翰泽 男,本科,工程师。主要研究方向:飞机电子化运行。E-mail:lihanze@ameco.com.cn

吕昌翰 男,本科,助理工程师。主要研究方向:飞机电子化运行。E-mail:vchanghan@ameco.com.cn

Research on cyber security management strategy of field loadable software

JIANG Jiarui * LI Hanze LYU Changhan

(Aircraft Maintenance and Engineering Corporation, Beijing 100621, China)

Abstract: With the deepening application of information technology and network technology in the field of civil aviation, the quantity and importance of field loadable software on civil aircraft have increased greatly, and the transmission mode of field loadable software has changed from physical transportation to transmission and storage through the network. While these changes bring convenience and efficiency, they also introduce cyber security risks, placing new requirements on the field loadable software management for aircraft continuous airworthiness management. This paper summarizes the certification policies and technical standards related to filed loadable software network security, analyzes the requirements of field loadable software network security management for aircraft continuing airworthiness, and provides ideas for operators to implement filed loadable software network security management policies and build system of software protection.

Keywords: field loadable software; continuing airworthiness; cyber security

* Corresponding author. E-mail: Jiangjiarui@ameco.com.cn