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

DOI: 10.19416/j.cnki.1674-9804.2020.02.019

民机机载系统网络安保适航政策分析

赵庆贺[1] 廖 健[1] 何 娣[1] 赵长啸[2]*

(1. 中电科航空电子有限公司,成都 611731; 2. 中国民航大学 适航学院,天津 300300)

摘 要:

随着信息化、网络化技术的不断发展,机上互连接口的数量和种类越来越多,在带来性能提升的同时也引入了安保风险,给民机安全性带来了挑战。梳理了新一代民机内部网络域、外部网络域的接口类型,总结了国际民航组织、美国联邦航空局、欧洲航空安全局等各机构针对网络安保问题的审定政策,分析机载网络安保相关的工业标准及审定要求,给出了在实际审定中的审定要素和要求。本研究可为我国民机机载系统网络的适航审定提供理论支撑。

关键词: 机载系统;网络安保;适航审定;安全性

中图分类号: V243; V221.91 **文献标识码:** A **OSID:**

0 引言

随着技术的发展,机载系统向着综合化、智能化、网络化发展[1],网络安保问题成为民机机载系统面临的新的安全性问题[2]。民机客舱网络的发展,大幅提升了民航的服务水平,同时也带来了许多潜在的网络安全威胁和隐私风险。2016 年 9 月,美国国土安全部(United States Department of Homeland Security, 简称 DHS)的专家在大西洋城的机场通过无线电通信系统远程侵入了一架波音 757 飞机的通讯系统[3]。民航作为一个特殊的行业,飞机的安全飞行是行业发展的第一要素,如何保证机载网络在与地面系统通信,尤其是途经公共网络的通信时不受各种网络威胁的影响,是推动现代飞机逐步信息化的安全保障。民机网络安保的实质就是在被保护的资产和威胁源之间的威胁途径上建立一道防护屏障屏蔽或隔离外部威胁,过滤出安全的数据保证正常的数据通信[4]。

为此,各国局方发布了相关的政策文件来指导新研飞机、已有飞机加改装网络安保设备等工作,而我国局方目前尚未针对网络安保问题发布审定指导文件,网络安保的审定问题将是中国局方目前面临的一个重大技术难题。

本文通过梳理网络安保相关的标准、政策、文件,为我国各类民机及相关设备、系统的适航审定提供理论支撑分析。

1 机载信息系统网络安全边界

对于机载网络安保策略和方案的制定,首先要确定机载网络的安全边界,即飞机或系统内部安全环境和外部安全环境之间的边界,主要指飞机级的外部接口和系统级之间的接口,它标志了安保控制的变化。在飞机级,安全边界和安全环境主要强调机外人员、外部系统和交互,它能够将其所包含的资产与外部世界分开,并能够被那些与外部世界相连接的逻辑接口和物理接口、可能的交互以及与外部世界的信息交换所跨越,所有用于系统操作和控制的关联接口,不管它们是例行使用还是在特殊环境下使用,都应被考虑为飞机安全边界的一部分。在安全边界以外,飞机或系统就会被暴露在人为的或

基金项目: 国家自然科学基金(U1933106);航空科学基金(20185167017)

* **通信作者.** E-mail: cxzhao@cauc.edu.cn

引用格式: 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.
ZHAO Q H, LIAO J, HE D, et al. Airworthiness policy analysis of network security for civil aircraft airborne system[J]. Civil Aircraft Design and Research,2020(2):103-107(in Chinese).

系统的攻击下，任何跨越安全边界的交互行为或信息交换都可能会面临潜在攻击，应该被考虑。

根据 DO-326A / ED-202A[5]，安全边界将飞机或系统与外部系统或人群接触的部分进行分类，特别值得注意的是功能接口，未安装的飞机部件（包括复杂的硬件和软件）、配置管理、数据加载和部分安装流程以及用于操作或管理系统的任何流程。

新一代民机内部网络域与外部网络域之间可能采用的机载网络通信接口类型和通信方式如图 1 所示，机上网络域与机外网络域的主要连接主要包括：专用接口、甚高频通信（Very high frequency，简称 VHF）、高频通信（High frequency，简称 HF）、全球定位系统（Global Positioning System，简称 GPS）、甚高频全向无线电信标（Very High Frequency Omni-directional Radio Range，简称 VOR）、测距仪（Distance Mesurement Equipment，简称 DME）、空中防撞系统（Traffic Collision Avoidance System，简称 TCAS）、空中交通管制（Air Traffic Control，简称 ATC）专用无线数据通信接口、以太网、USB 维护接口、卫星通信链路、公共无线接口等几大类型。这些接口涉及到了飞机控制域、信息授信域、信息开放域、客舱网络域四个机上网络域与飞机外部的地面授信域、公共网络域之间的连接，因此，这些网络接口也被确定为本项目所重点考虑的飞机级机载网络安保边界[6]。

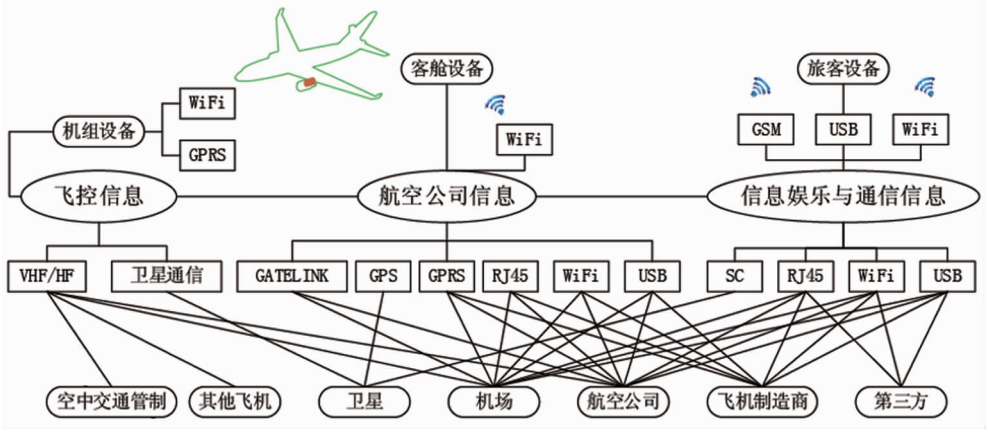

图 1　民机机载网络通信接口类型和通信方式

2　典型机型的机载信息系统域划分

通过不同的域划分，实现不同程度/级别的安保风险控制是计算机信息领域常用的做法，机载信息亦不例外，以空客 A380 为例，其机载系统分为两个部分：航电世界和开放世界，航电世界包括飞机飞行所需的所有航电系统。开放世界由机载信息系统（Onboard Information System，简称 OIS）及其依存的硬件平台——网络服务器系统（Network Server System，简称 NSS）组成。OIS 是一套应用程序、电子文档和数据库。航电世界和开放世界之间通过防火墙通信。机载网络通过 VHF、HF 或卫星通信（SATCOM）连接到地面的空中交通管制中心和航空公司运行控制中心。所有与地面网络的通信都经过防火墙[7]。

机载信息系统 OIS 划分为三个域：航电域、飞行运行域、通信与客舱域。航电域包含与飞机航电系统交换数据的应用，其中包括：支持维护操作的电子记录本、中央维护系统（Central Maintenance System，简称 CMS）；飞行机组和维护机组使用的最低设备清单（Minimum Equipment List，简称 MEL）、构型偏离清单（Configuration Defect List，简称 CDL）、客舱机组操作手册（Cabin Crew Operating Manual，简称 CCOM）等电子文档；加油作业服务工具；管理飞机和操作员运行中心通信的航空公司运行控制（Airline Operational Control，简称 AOC）应用。飞行运行域包含支持地面和空中飞行机组的应用，是电子飞行包（Electronic Flight Bag，简称 EFB）的部分功能，其中包括：起飞、空中和降落的性能计算工具；载重平衡计算工具；飞行机组操作手册（Flight Crew Operating Manual，简称 FCOM）、飞机飞行手册（Aircraft Flight Manual，简称 AFM）、构型偏离清单（Configuration Defect List，简称 CDL）、最低设备清单（Minimum Equipment List，简称 MEL）、飞行机组培训手册

(Flight Crew Training Manua,简称 FCTM)等电子文档;联络管理工具;导航和气象图;电子飞行文件夹(Electronic Flight Folde,简称 EFF)和飞行跟踪(Flight tracking Unit,简称 FFU)工具。通信与客舱域包含客舱运行与维护、旅客服务工具,其中包括:用于旅客服务的互联网电子邮件、信用卡银行业务;客舱和通信域系统维护支持工具;无线局域网管理器应用。

3　机载系统网络安保政策分析

3.1 国际民航组织(ICAO)

国际民航组织针对网络安保(Aircraft Cyber Security)给出了风险矩阵,矩阵中将飞机的功能划分为三个大的区域或域[8],这些区域或域应当在物理上或逻辑上分开,或者有适当的措施来保证其安全:

1)飞行控制-安全关键系统,包括驾驶舱环境中支持飞行的飞机系统,此系统中断或拒绝会直接影响安全性,因此被认为是一个封闭的网络;

2)客舱(操作),用于操作和维护飞机的系统,包括乘客通讯等,此系统中断或拒绝主要影响业务关键操作和可能的维护,因此被认为是一个私有网络;

3)客舱(乘客),那些乘客直接与之交互的系统/接口(个人机上娱乐、他们自己的设备、机内 Wi-Fi 等等),干扰或拒绝具有最小的影响,因此被认为是具有不可信设备的公共区域。

同时将对网络目标的访问分为 5 种不同的方法:

1)远程访问:在没有对系统或本地网络的物理访问的情况下远程获得对目标的访问;

2)本地接入:通过具有或不具有对目标本身的物理接入的"本地"网络获得对目标的接入;

3)近距离访问:获得对目标的直接物理访问,例如恶意插入网络有效载荷的内部人员;

4)直接能量武器和无线电频率:主要通过使用包括射频波的电磁频谱影响目标;

5)供应链:通过供应链将硬件、固件和软件操作或替换为系统。

3.2 美国联邦航空局(FAA)

FAA 于 2015 年发布了资讯通告 AC 119-1《Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP)》[9]规定当某飞机的审定基础中包括与安保相关的专用条件时,此 AC 提供了一种可接受的符合性方法,明确了 FAA 授权的飞机网络安全计划(ANSP)的范围:

1)确保数据安全保护足以防止飞机外部未经授权的设备或人员访问;

2)确保针对证书持有者操作的安全威胁被识别和评估,并且实施风险减轻策略以确保飞机的持续适航性;

3)防止对飞机网络的无意或恶意更改,包括可能由维护活动引起的更改;

4)防止来自飞机上的来源未经授权的访问。

FAA 还针对 A350、波音 787-8、波音 747、Embraer EMB-550、Embraer ERJ-190、Gulfstream G280 等机型颁布了《Electronic System-Security Protection From Unauthorized External Access》、《Isolation or Airplane Electronic System Security Protection from Unauthorized Internal Access》等专用条件。

3.3 欧洲航空安全局(EASA)

2016 年,EASA 针对 A350 发布专用条件"F-38 SC: Security Assurance Process to isolate or protect the aircraft Systems and Networks from Internal and External Security Threats"(2017 年 11 月 21 日获得 TC);2016 年 5 月 17 日,EASA 配合 FAA 的 ASISP 工作组工作,协调 FAA 与 EASA 政策一致性问题,发布纪要 RMT. 0648— ISSUE 1;2017 年 2 月,与欧盟计算机应急组织(CERT-EU)联合成立 European Centre for Cyber Security in Aviation (ECCSA),预计近期将发布 Cyber security 路线图。

4　网络安保相关标准分析

目前,国际上针对网络安保问题的标准主要有 RTCA-DO 326A、DO-355 和 DO-356A。

4.1 DO-326A/ ED-202

DO-326A/ ED-202 为适航当局和航空工业在研发或改装飞机系统时进行适航认证的支持文件。当涉及到未授权的电子交互威胁时,它为相关项目的适航进程提供支持。与通常的组织飞机研发和认证活动一样,它添加了处理由各种未认证交互为飞机安全性所带来威胁的数据要求和合规性目标,处理未授权交互带来的飞机安全威胁。该文档提供的网

络安保适航指南涉及从项目启动到飞机型号认证这一产品生命周期,还包括后续的 STCs 和 TCs 的发行。另外,该文件还包括为确保持续适航中涉及未授权交互的型号设计的信息移交。

4.2 DO-355/ ED-204[10]

DO-355/ ED-204 是针对持续适航的网络安保适航审定的,为以下生命周期阶段提供指导:操作、支持、维护、管理和解构。DO-355/ED-204 仅涉及信息安全风险。减轻这些风险的安全措施并不仅限于信息技术,可能是物理方法或组织管理上的问题。除了与飞机零件和系统直接相关的持续适航经典说明外,该文件还提供了与飞机信息系统和数据网络的安全性相关的地面支持设备和地面支持信息系统的安全指南。

4.3 DO-356 /ED-203[11]

DO-356 /ED-203 是在 DO-326A/ED-202A 和 DO-355/ED-204 的基础上撰写的,是针对进行网络安保适航过程的申请人的补充指导文件。具体地讲,该文档主要涉及以下两个方面:(1)为 DO-326A 中提到的安全性风险评估和有效性保证的实施提供指导;(2)为安全风险分析和网络安全域提供具体的准则、方法和工具。

2018 年 6 月 19 日,SC-216 和 WG-72 联合发布了 RTCA-DO356A,其变化主要体现在以下方面:

1)体量上,DO-356 从 80 页扩展到了 370 页,补充了大量的内容;

2)内容上,其与 RTCA DO-326A 的关系更加紧密,在 356A 中多处对 DO-326A 的内容进行了引用,如在 2.4 节引用了 DO-326A 提出的符合性展示文件,在附录 C 中更是直接给出了“links DO-326A / ED-202A process activities to the sections of this document”;

3)结构上,增加了第 2 章“Regulatory Considerations”、第 5 章“Development Of Security Architecture And Measures”,以及附录对 DO-356 的一些小节进行扩充,并使其独立成章,如将 DO-356 中的第 2.4 节扩充后独立成为第 6 章“Security Event Logging”,第 2.6 节补充内容后独立成为 DO-356A 中的第 4 章“Security Assurance”。第 3.1.1 小结进行了扩充,使之成为附录 F 的 F.2“Threat Trees for Risk Assessment”。此外,给出了新的安保评估方法,如已在其他领域应用的 STPA 方法进行了裁剪定制,形成了 STPA-Sec,作为附录 G 放在了 DO-356A 中。

5 结论

随着技术的发展,智能化、综合化、网络化的机载系统将进一步发展,机载网络安保和风险将变得越来越严峻,相应的针对机载系统网络安保风险的技术、措施、设备等的开发、研制问题亟需解决。本文梳理了各国适航局方针对网络安保问题的政策及相关标准分析,希望可以为后续的设备研制和适航取证提供一定的支持。

采用标准化的网络架构,将网络安保问题纳入到整机的系统安全性分析过程,将网络安保风险作为特种风险或是独立专业进行考虑,是解决机载网络安保问题的一种可行思路。

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.

[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] CLULEY G. A Boeing 757 was hacked remotely while it sat on the runway[EB/OL]. (2017-11-6)[2019-12-6]. https://www. tripwire. com/state-of-security/featured/boeing-757-hacked/.

[4] 李国, 李静雯, 王静, 等. 基于威胁状态的新型机载网络安全风险评估改进模型[J]. 现代电子技术, 2019(2):41-45.

[5] Radio Technical Commission for Aeronautic. Airworthiness Security Process Specification: DO-326A / ED-202A [S]. [S. l.]: Radio Technical Commission for Aeronautic, 2014.

[6] 牛文生. 基于天地一体化信息网络的智能航空客运系统[J]. 航空学报,2019,40(1):236-249.

[7] WANG L, CHENG T, LI Y. Preliminary Research of Secure Integrated Computing in Future Avionics[C]. [S. l.]: International Conference on Computational Intelligence & Security, IEEE, 2017.

[8] ZIEGLER J, KIESLING T, NIEDERL J, et al. A Model-Based Approach for Aviation Cyber Security Risk Assessment[C]. [S. l.]: International Conference on Availability, 2016.

[9] FAA. Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP) Document In-

formation: FAA AC 119-1[S]. U. S.: Federal Aviation Administration, 2015.

[10] Radio Technical Commission for Aeronautic. Information Security Guidance for Continuing Airworthiness: DO-355/ ED-204[S]. [S. l.]: Radio Technical Commission for Aeronautic, 2014.

[11] Radio Technical Commission for Aeronautic. Airworthiness Security Methods and Considerations: DO-356 A/ ED-203[S]. [S. l.]: Radio Technical Commission for Aeronautic, 2018.

作者简介

赵庆贺　女,硕士研究生,工程师。主要研究方向:民用飞机通信导航系统、客舱与信息系统。E-mail:zhaoqh@ cetca. net. cn

廖　健　男,学士,工程师。主要研究方向:民用飞机通信导航系统、客舱与信息系统。E-mail: liaojian@ cetca. net. cn

何　娣　男,硕士研究生,助理工程师。主要研究方向:民用飞机客舱与信息系统。E-mail:hed@ cetca. net. cn

赵长啸　男,博士,讲师,博士生导师。主要研究方向:综合化航电系统适航审定、机载网络安保适航审定。E-mail: cxzhao@ cauc. edu. cn

Airworthiness policy analysis of network security for civil aircraft airborne system

ZHAO Qinghe[1]　LIAO Jian[2]　HE Di[1]　ZHAO Changxiao[2]*

(1. CETC AVIONICS Co., LTD, Chengdu 611731, China;
2. College of Airworthiness, Civil Aviation University of China, Tianjin 300300, China)

Abstract: With the continuous development of information technology and network technology, the number and types of on-board interconnection interfaces are increasing, which brings performance improvement and security risks, and brings challenges to the safety of civil aircraft. The interface types of the internal network and external network of the new generation of civil aircraft were summarized. The policies of ICAO, the Federal Aviation Administration of the United States, the European Aviation Safety Agency for the network security were given. This paper analyses the verification requirements of civil aircraft airborne system network, and gives the verification elements and requirements in the actual verification. This study can provide theoretical support for the airworthiness certification of civil aircraft airborne system network in China.

Keywords: airborne system; network security; airworthiness certification; safety

* Corresponding author. E-mail: cxzhao@ cauc. edu. cn