民用飞机ACARS数据链适航审定方法研究

李嘉年,沈金清
(上海飞机设计研究院,上海 201210)

摘 要: 飞机通信寻址和报告系统(ACARS,aircraft communications addressing and reporting system)是影响民航飞行安全与运行效率的关键数据链系统,确保其适航性是型号合格审定的基本前提。为应对传统审定方法难以覆盖机载系统网络化带来的网络安全风险,本文通过系统解析民用航空规章及相关行业标准,构建了一套ACARS数据链适航审定框架。该框架提供了一个整合的符合性矩阵,将涉及基础功能、冗余设计、系统安全与持续适航等方面的适航条款具体映射至设计审查、分析及试验等验证活动,此外,还明确了以专用条件形式引入网络安全验证的审定路径。本文所构建的适航审定框架为ACARS数据链的符合性验证提供了结构化思路与规范化流程,旨在提升适航审定工作的系统性与完整性。

关键词: 飞机通信寻址和报告系统(ACARS)数据链;适航审定;符合性验证;空地通信
中图分类号: V243.1;TN915 **文献标志码:** A **文章编号:** 1674-5590(2026)02-0006-07

Research on airworthiness certification methodology for civil aircraft ACARS data link

LI Jianian, SHEN Jinqing
(*Shanghai Aircraft Design and Research Institute, Shanghai* 201210, *China*)

Abstract: The aircraft communications addressing and reporting system (ACARS) is a key data link system affecting flight safety and operational efficiency of civil aviation. Ensuring its airworthiness is a fundamental prerequisite for type certification. To address cybersecurity risks posed by the networking of airborne systems, which traditional certification methods cannot fully cover, this paper systematically analyzes civil aviation regulations and relevant industry standards, and establishes an airworthiness framework for the ACARS data link. This framework provides an integrated compliance matrix, which maps specific airworthiness clauses involving basic functions, redundancy design, system safety and continued airworthiness to verification activities such as design review, analysis and testing. In addition, it clarifies the certification path for introducing cybersecurity verification in the form of special conditions. The framework constructed in this paper provides a structured idea and standardized process for the compliance verification of the ACARS data link, aiming to improve the systematicity and integrity of the certification work.

Key words: aircraft communications addressing and reporting system (ACARS) data link; airworthiness certification; compliance verification; air-ground communication

飞机通信寻址和报告系统(ACARS,aircraft communications addressing and reporting system)数据链作为国际民用航空组织推荐的空地数据链架构,支持飞机机载应用系统通过甚高频(VHF,very high frequency)、高频(HF,high frequency)及卫星通信(SATCOM,satellite communication)等信道,实现空地数据链消息的实时交互传输。ACARS数据链作为中国民航主用的空地数据链网络架构,已深度集成至航空器运行的全生命周期,其业务范围涵盖合同式自动相关监视、航空气象情报、航空公司运行监控等关键场景的标准化报文传输[1]。

传统ACARS数据链的适航审定方法主要基于功能失效模型进行验证,其审查重点聚焦于系统硬件和软件在功能失效状态下产生的具体影响。传统适航审定方法严格遵循中国民用航空规章(CCAR,Civil Aviation Regulations of China)及其配套咨询通告,针对单

收稿日期:2025-06-13; **修回日期:**2025-09-17
作者简介:李嘉年(1996—),男,上海人,工程师,硕士,研究方向为数据通信设计.

点故障、冗余设计和电磁兼容性等具体条款展开合规性验证，其审查手段主要依赖于系统可靠性分析、功能危险性评估与功能失效树分析等定量方法。这些方法的根本目的是评估由内部组件随机失效或软件错误引发的功能中断的影响，并确保灾难性失效的发生概率满足规章要求的极低水平。这一套基于概率论和功能验证的框架，在保障系统应对内源性故障及确保基础功能可靠性方面已形成成熟的适航审定体系。

然而，随着机载系统网络化程度不断加深，来自外部的恶意电子行为（如网络攻击、数据劫持等）带来了新型风险，而这类风险在传统适航审定框架中未能得到充分覆盖。这些威胁并非内部组件的随机失效事件，无法简单套用概率模型进行评估，这显示出了传统适航审定方法的局限性。因此，需研究并提出一套覆盖功能、安全与网络的系统化 ACARS 数据链适航审定思路。本文首先梳理了相关的适航条款并构建了符合性验证矩阵，随后对具体的符合性验证思路、网络安全验证方法及其他系统支持工作进行了详细阐述，以应对当前型号合格审定工作的实际挑战。

1　ACARS 数据链功能要求

1.1　ACARS 数据链功能特性

ACARS 数据链作为航空无线电公司（ARINC，Aeronautical Radio，Inc.）618[2]标准定义的空地数据链通信架构，构建了航空器与地面服务提供商之间的数字报文交换平台。其核心功能在于通过 VHF（118~137 MHz）、HF（2~30 MHz）及 SATCOM（L-band）等多模态信道，实现飞行运行全周期（涵盖推出、滑行、起飞、爬升、巡航、下降、着陆及停机阶段）的报文数据交互。尽管存在信道带宽限制导致其仅支持 ASCII 文本传输，无法承载多媒体数据流，但其基于前向纠错与循环冗余校验的双重保障机制，保障了报文传输的完整性。

ACARS 数据链实现的各类基础功能包括：

（1）管制服务，如基于自动终端信息服务的气象更新、航路变更指令传输；

（2）运行监控，如推出—起飞—着陆—滑入事件检测、燃油消耗率监测；

（3）维护管理，如发动机振动监控、辅助动力系统监控；

（4）记录打印，如舱单打印、上下行数据链报文发送至飞行数据记录器（EAFR，event activated flight recorder）记录。

在空域资源管理中，ACARS 数据链的应用实现了管制指令的数字化传输，优化了传统的陆空通话模式。ACARS 数据链通过数据链传递放行许可、流量管理信息及提供自动终端信息服务，减轻管制员和飞行员的语音通信负荷，提升信息传递的准确性和整体运行效率，从而有效缓解繁忙空域的通信信道拥塞问题。

ACARS 数据链的扩展功能模块已突破传统空中交通服务范畴，深度整合至航空运营控制体系：通过标准化的数据采集接口，实时获取飞机状态参数，包括但不限于燃油消耗率、襟翼位置状态、发动机性能指数等。在此基础上，ACARS 数据链自动生成包含关键时间节点（推出—起飞—着陆—滑入事件时间戳）、货载配置验证、预计到达时间等的消息报文。航空公司运行控制中心可通过地面网络在接收报文后完成数据解析与可视化，为航班运行品质分析提供数据支撑。

1.2　ACARS 数据链整体系统架构

ACARS 数据链由飞机机载系统、多模态传输网络与地面处理系统构成，如图 1 所示。

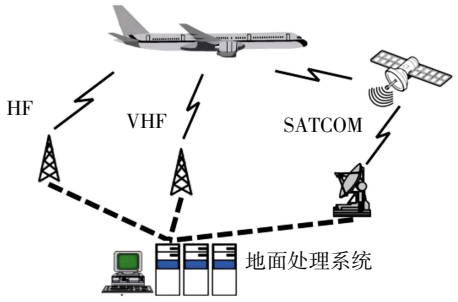

图 1　空地数据链通信拓扑结构示意图

Fig.1　Schematic diagram of air-ground data link communication topology structure

1.2.1　飞机机载系统

典型的 ACARS 数据链通信飞机机载系统采用分层架构设计，如图 2 所示。

飞机机载系统的核心是作为应用程序运行在综合模块化航电平台上的数据链软件，其一般包含航空公司运行控制模块、空中管制模块及航务通信模块。在下行报文的生成过程中，该平台首先整合来自飞行控制系统、导航系统、燃油系统、舱门系统等多个机载系统的实时数据，这些数据在图 2 中被定义为运行数据。机组人员通过作为人机交互界面的多功能控制与显示组件（MCDU，multipurpose control and display unit）对这些数据进行监控、确认或手动输入更改。该接口的功能和人机交互特性需遵循 ARINC 739A-1[3]等行业规范，以实现报文编辑、链路监控及多信道自动切换。

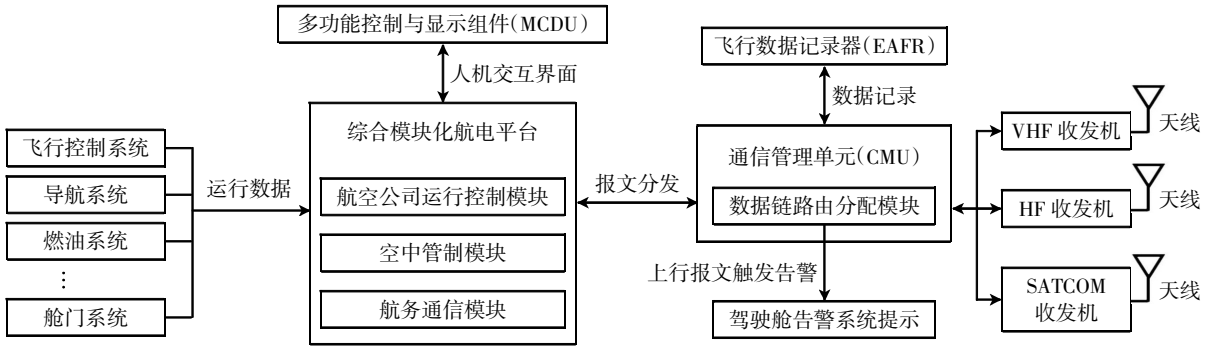

图 2　ACARS 数据链通信飞机机载系统架构

Fig.2　Airborne architecture of the ACARS data link communication system

经机组确认的报文信息在下发至地面后,平台内的数据链软件将对应的结构化数据按 ARINC 618[2]规范封装为可发送的数据链报文。随后,平台通过报文分发流程,将原始报文数据传送至通信管理单元(CMU,communication management unit)进行封装和转发。CMU 作为严格遵循 ARINC 758[4]标准的核心路由设备,其内部的数据链路由分配模块负责报文的最终处理,并依据报文头部标识和当前链路状况,决策选择 VHF、HF 或 SATCOM 信道进行空地传输。为确保飞行数据的可追溯性,CMU 在发送报文的同时,会将报文副本通过数据记录接口发送至 EAFR,实现飞行数据存档。

在上行报文的接收流程中,当地面发送的报文被飞机接收时,信号首先到达 CMU;CMU 解析报文后,通过上行报文触发告警机制,联动驾驶舱告警系统在显示界面生成报文接收提示通告,同时由扬声器广播提示音,确保机组能及时获知新信息;机组可在 MCDU 的操作指引下查看报文。此外,为保障系统安全,该系统的安全架构通常通过应用层准入白名单机制来限制非授权应用的服务请求。

1.2.2　多模态传输网络

ACARS 数据链支持 3 类通信子网:HF 数据链、VHF 数据链及 SATCOM 数据链。

(1)HF 数据链作为极区及跨洋飞行的关键通信保障,其系统架构遵循 ARINC 753-3[5]技术规范。机上通过集成 HF 数据单元与自适应阻抗匹配天线耦合器,支持 300~1800 bps 动态速率调整;依托全球 12 个 HF 数据链地面站构建广域通信网络。HF 数据链通过复用现有 HF 话音信道实现双模通信,尽管其具备超视距传输优势,但受限于天线尺寸与信道多径效应,其误码率较 VHF 数据链高 1~2 个数量级。

(2)作为 VHF 频段上发展的新型数据链技术,VHF 数据链(VDL,very high frequency data link)模式 2 采用基于航空无线电技术委员会(RTCA,Radio Technical Commission for Aeronautics)DO-224[6]标准的差分调制技术。该模式支持的数据传输速率可达 31.5 kbps。VDL 系统以地面基站为中心构建蜂窝网络,其信号传播严格受限于视距,因此需密集部署地面站以支撑航路覆盖,但无法独立保障跨洋与极区通信。

(3)SATCOM 数据链架构包含地球同步轨道或低轨卫星、机上多频段卫星通信终端与地面段的网络运营中心。虽然 SATCOM 数据链提供全球无缝覆盖,但其端到端延迟与运维成本制约了其大规模应用。

现行ACARS 数据链采用智能切换策略:优先使用 VHF 数据链,当接收信号强度降低时,自动切换至 SATCOM 数据链或 HF 数据链。

1.2.3　地面处理系统

地面处理系统在收到下行报文后,通过报文解析将数据定向传输至空中交通管制服务基站、航空公司运行中心和机务系统等终端位置,同样,地面终端也可经由地面处理系统向飞机端系统发送上行报文指令,实现数据链报文端到端的交互。

地面处理系统为保障传输安全需部署专用网络加密传输通道,并在网络边界配置入侵检测系统及防火墙,以实现流量审计与访问控制。通过实时监测与全链路日志管理,确保地面处理系统全流程安全可控。

2　ACARS 数据链适航审定

2.1　审定基础的一般原则

中国民用航空局(简称民航局)针对运输类飞机的适航审定需依据现行有效的《运输类飞机适航标准》(CCAR-25-R4)[7]开展合规性验证。为满足实际运行需求,ACARS 数据链还需同步符合《大型飞机公共航空运输承运人运行合格审定规则》(CCAR-121-R7)[8]与《一般运行和飞行规则》(CCAR-91-R4)[9]中关

于数据链服务的强制性条款。鉴于不同机型 ACARS 数据链在架构设计与功能实现上的差异性，其审定基础文件需与民航局进行专项技术协调后最终确定。

依据 CCAR–121.97 条通信设施的规定，航空器须在全航段具备陆空双向通信能力，确保飞机与空中交通管制单位间的实时可靠通信。ACARS 数据链通过集成 VHF、HF 及 SATCOM 3 套独立子系统实现冗余设计。当任一子系统失效时，系统可切换至其他通信模式，以保障数据传输的连续性。又根据 CCAR–121.346(a)条空地双向数据通信系统的规定，旅客座位数超过 99 座的航空器须配备符合适航标准的空地数据链系统。

在数据记录规范方面，根据 CCAR–91.209(c)条记录设备与 CCAR–25.1457(a)(6)条驾驶舱录音机的要求，数据链通信内容需完整记录于 EAFR 中。每条记录均应包含报文类型、校验信息及通信时间戳，并确保该时间戳与驾驶舱语音记录的时间基准精确对应。在飞机追踪要求上，根据 CCAR–121.533(b)条飞机追踪的规定，最大起飞重量超过 27 000 kg 的航空器在境外运行时，需每 15 min 自动报告飞机位置。该条款要求 ACARS 数据链通过集成惯性导航系统与全球定位系统获取坐标。

在满足 ACARS 数据链传统功能安全要求的基础上，需将航空电子系统的网络安全防护能力提升至同等重要的高度。当前基于功能失效模型的适航审定方法对网络攻击、数据劫持等新型威胁的覆盖存在局限。现代民用飞机已普遍采用系统性防护架构应对此类风险，例如 A350 客机通过构建逻辑与物理隔离相结合的多层级防护体系，划分不同的安全域，并借助安全网关实施严格的访问控制。因此，在中国 CCAR–25 规范尚待完善的背景下，参照成熟的国际标准与实践来构建网络安全验证框架，是确保 ACARS 数据链满足现代适航安全目标的必要原则。通过将网络安全防护要求融入适航审定流程，可实现功能安全与网络防护的协同审定，保证数据链功能在网络安全威胁下仍能保持完整性与可信性。

2.2　ACARS 数据链审定和运行符合性适用条款

在型号合格证申请过程中，ACARS 数据链的适航符合性验证需分层实施。

(1)基础功能验证：依据 CCAR–121.97(通信设备配置)、CCAR–121.346(a)(数据链服务可用性)、CCAR–25.1301(a)(1)(设备安装合理性)及 CCAR–25.1301(a)(4)(功能完整性)进行系统级测试。

(2)冗余性设计验证：按 CCAR–25.1307(d)(系统冗余度)要求评估故障容限能力。

(3)电子系统安全性验证：覆盖 CCAR–25.1309(d)(软硬件开发保证等级)、CCAR–25.1353(a)(电气设备兼容性)和 CCAR–25.1431(c)(电磁防护特性)等条款。

(4)持续适航与操作程序验证：按照 CCAR–121.533(b)(机组操作程序)、CCAR–25.1529(持续适航文件)、CCAR–25.1581(a)和(b)(飞行手册条款)、CCAR–25.1585(a)(维修手册要求)、CCAR–25.1309(a)和(b)(失效状态影响分析)及 CCAR–25.1322(告警装置有效性)进行验证。

(5)交联系统补充验证：增加 CCAR–25.1457(a)(6)(驾驶舱语音记录器接口)与 CCAR–91.209(c)(数据记录完整性)等关联条款。

(6)网络安全验证：鉴于当前 CCAR–25 规范中尚无明确的网络安全审定标准，申请人可参照欧盟航空安全局(EASA，European Union Aviation Safety Agency)的 CS 25.1319[10]等条款中的防护理念。必须明确，此类参考仅为满足审定要求的过渡性方法，不构成最终符合性依据。实际审定以针对具体机型发布的专用条件为核心依据，建议在型号合格证申请初期与民航局协商确定威胁场景及防护层级要求。为系统证明 ACARS 数据链对网络安全相关条款的符合性，申请人须开展全面的网络安全风险评估，其具体方法可参照相关指导材料。

为了简化验证，ACARS 数据链传输路径中涉及的射频设备(如天线、收发机)功能验证，可纳入 VHF/HF/SATCOM 通信系统的独立审定流程，不在数据链专项审查中重复开展。

3　ACARS 数据链符合性验证

表 1 构建了 ACARS 数据链的符合性验证技术框架，明确了各审定条款与符合性验证方法的对应关系。该表将各项适航条款逐条分解，并为每一条款列出了对应的具体验证手段，涵盖了设计审查、分析及试验等类别。但其所列的方法名称本身并不能完全揭示适航审定工作的复杂性与深度。例如，对于 CCAR–25.1309(a)和(b)这类涉及极低概率定量安全目标的条款，仅通过试验无法完成验证，必须采用系统安全性评估等分析手段，这体现了验证方法的选择需基于具体的规章要求与工程可行性。因此，本节将对表 1 中

的验证方法展开系统性论述，从符合性验证的整体思路与行业实践入手，深入分析网络安全这一特殊领域的验证要求，并最终扩展至系统集成层面，探讨其与其他机载系统的协同验证分工。

表 1　ACARS 数据链审定条款的适航要求与符合性验证方法

Tab.1　Airworthiness requirements and compliance verification methods for ACARS data link certification provisions

序号	条款号	适航要求	符合性验证方法
1	CCAR–25.1301(a)(1)	证明 ACARS 数据链的功能设计能够满足其预期的运行功能要求	1.设计审查：审查系统功能描述、接口控制文件等，确认设计满足运行需求 2.分析：通过软件结构覆盖率等分析，证明软件设计的完整性
2	CCAR–25.1301(a)(4)	证明 ACARS 数据链在集成安装至飞机后，其功能和性能依然完整、正常	1.实验室试验：验证核心功能及多信道切换性能 2.机上地面试验：确认机上集成后，系统与飞机其他交联系统的数据交互正常 3.飞行试验：在典型运行场景下，验证端到端的空地通信功能
3	CCAR–25.1307(d)	证明 ACARS 数据链的冗余设计有效，单一传输路径的失效不会导致整个空地通信功能丧失	1.安全性评估：通过失效模式与影响分析，识别并分析单一路径的失效状态 2.试验：通过故障注入试验，验证主备链路的切换逻辑和成功率
4	CCAR–25.1309(d)	证明 ACARS 数据链已全面考虑系统的失效组合，并确保机组能够及时、准确地识别故障	1.安全性评估：提交系统安全性评估文件，证明故障的可探测性和告警设计符合要求 2.分析：通过故障覆盖率分析，证明诊断逻辑的有效性
5	CCAR–25.1353(a)	证明 ACARS 数据链设备工作时，其电磁辐射不会对其他关键航电系统造成有害干扰	1.试验：依据 RTCA DO–160 标准，对设备进行电磁兼容性测试 2.机上地面试验：在全机通电状态下，验证系统协同工作时的电磁兼容性
6	CCAR–25.1431(c)	证明 ACARS 数据链设备能够承受外部电磁环境（如高强度辐射场、雷击）的影响并保持功能	1.试验：依据 RTCA DO–160 关于高强度辐射场和雷电防护的相关章节进行合格性试验 2.分析：通过电磁分析，证明设备安装和线路防护设计的合理性
7	CCAR–25.1457(a)(6)	证明所有收发的数据链报文都被驾驶舱记录器完整、准确地记录，且时间戳同步	1.设计审查：审查记录系统的接口设计，确认报文记录的逻辑和数据格式 2.机上地面试验：模拟报文收发，检查记录器内容，验证记录的完整性与时间戳同步精度
8	CCAR–25.1529	证明申请人已提供了完整的持续适航文件，包含 ACARS 数据链所有必要的维护程序	文件审查：对持续适航说明中的维修章节进行审查，确认其包含 ACARS 数据链的维护要求和流程
9	CCAR–25.1581(a)和(b)	证明飞机飞行手册中包含了操作 ACARS 数据链所需的所有限制、程序及性能信息	1.文件审查：对飞机飞行手册草案的相关章节进行评估，确认信息的准确性、完整性和清晰度 2.分析：对人机交互界面进行人因工程评估，或结合模拟器试验验证操作程序的合理性
10	CCAR–25.1585(a)	证明维修手册等文件中包含了 ACARS 数据链设备的标准操作、故障隔离和维修程序	文件审查：对维修手册和故障隔离手册草案进行审查，确认相关程序的准确性和可操作性
11	CCAR–25.1309(a)和(b)	通过定量分析证明 ACARS 数据链的失效状态满足规章所定义的灾难性（$<1\times10^{-9}$/fh）等概率要求	安全性评估：提交 ACARS 数据链安全性评估报告，其中应包含功能危险性评估、故障树分析和共因分析，以定量证明安全目标的满足性
12	CCAR–25.1322	证明 ACARS 数据链相关的告警信息在驾驶舱的显示和音响提示能够清晰、及时地提醒机组	1.设计审查：审查告警逻辑和显示方案设计，确认其符合告警等级划分原则 2.机上地面试验/飞行试验：通过模拟故障，触发并验证告警的显示、音响和延迟时间
13	CCAR–91.209(c)	证明数据链通信记录功能在飞行的所有阶段都能持续、可靠地工作	1.分析：提交对记录设备的可靠性分析报告 2.试验：通过耐久性或飞行试验数据，证明记录功能的持续运行能力
14	CCAR–121.97	证明飞机在航路飞行的所有阶段均具备可靠的双向空地数据通信能力	1.分析：提交航路通信覆盖性分析报告 2.飞行试验：在典型航路上模拟长航时连续通信负载，验证双向通信的可用性
15	CCAR–121.346(a)	证明飞机已按规章要求安装 ACARS 数据链，并具备双向通信性能	1.检查：对飞机进行物理检查，确认 ACARS 数据链设备已按批准的构型安装 2.试验：通过机上地面试验或飞行试验，验证其端到端的双向通信性能
16	CCAR–121.533(b)	证明 ACARS 数据链具备按规章要求（≤15 min）自动报告飞机位置的功能	1.设计审查：审查自动位置报告功能的触发逻辑和报文格式 2.飞行试验：在正常运行条件下，验证飞机位置报告的自动发送功能、间隔时间和数据准确性
17	CS 25.1319	证明 ACARS 数据链已设计并实施了充分的网络安全防护措施，以抵御恶意电子交互对飞行安全造成的风险	1.分析：提交网络安全风险评估报告，包括威胁建模、风险等级划分及防护方案 2.试验：通过实验室渗透测试，验证异常数据拦截、访问控制等防护措施的有效性 3.检查：对软硬件构型及运行维护程序进行检查，确认网络安全措施已正确实施

国际主流的适航审定体系，如 EASA 与美国联邦航空局，均要求申请人采用一套标准化的符合性验证方法来证明产品符合所有适航条款。该框架将验证手段系统地划分为 10 个类别，涵盖了从设计审查、数值模拟、安全评估到实验室测试、机上地面测试及飞行试验等多元化手段。具体实施流程参照《航空器型

号合格审定程序》[11]的技术框架执行。

3.1 系统安全性与功能符合性验证

ACARS 数据链的符合性验证需遵循系统工程原则。在系统顶层设计阶段，需依据汽车工程师学会（SAE，Society of Automotive Engineers）的《民用机载系统和设备安全性评估过程指南》（ARP4761）[12]要求，自上而下地开展功能危险性评估以确定失效影响等级。这直接关联到 CCAR–25.1309（a）和（b）条款的符合性验证路径：为证明灾难性失效发生的平均概率小于 1×10^{-9}/fh，必须通过故障树分析等定量评估方法对系统架构进行数学证明，并形成系统安全性评估报告作为核心证据。

在此基础上，通过实施失效模式影响分析等活动，形成完整的技术文档体系。随后的系统集成与试验阶段，则需通过构建功能干扰矩阵、模拟通信链路异常等方法，验证 ACARS 数据链在非正常工况下不会引发飞行关键系统的功能降级。这一系列活动旨在确保系统满足 CCAR–25.1301 的功能与性能要求。具体到 CCAR–25.1307（d）所要求的冗余性，试验中会通过故障注入等方式，模拟 VHF、HF 或 SATCOM 单路径失效场景，验证 CMU 的链路自动切换逻辑的正确性。同时，机上地面试验也是验证 CCAR–121.346（a）条款符合性的关键，通过检查设备的物理安装、接口连接与软件版本，确认其与经批准的构型完全一致。

在设备层面，获得技术标准规定（TSO，technical standard order）批准是证明其满足最低性能标准的有效证据，例如 ACARS 数据链中的 VDL 收发机可获得《甚高频数字链模式 2 通信设备》（TSO–C160a）[13]批准。但这不能替代在具体机型上的集成验证，申请人仍需验证其安装适用性与接口兼容性。此外，设备的环境适应性需严格遵循 RTCA《机载设备环境试验程序》（DO–160G）[14]要求，完成包括电磁兼容性、高强度辐射场防护等在内的严酷环境试验。

3.2 文件审查与程序验证

除了工程验证，符合性验证还包含对文件的严格审查。对于 CCAR–25.1529、CCAR–25.1581 和CCAR–25.1585 等条款，审定人员需审查申请人提交的持续适航文件、飞行手册及维修手册草案。审查要点在于确认其中包含 ACARS 数据链的全部操作限制、正常与非正常程序、性能信息及故障隔离和维修步骤，且所有描述必须准确、清晰、易于理解，确保运营人和维修人员能够正确地使用和维护该系统。

3.3 网络安全符合性验证

适航安全符合性验证工作需基于 RTCA《适航安全流程规范》（DO–326A）[15]所定义的适航安全流程来系统性地建立。该流程的第一步是安全范围定义，要求清晰界定 ACARS 数据链的安全边界与关键数字资产，例如 CMU 的路由表、飞行计划数据等。在此基础上，进入安全风险评估阶段，采用结构化的威胁分析方法，系统性地识别潜在攻击路径与脆弱性。例如，不仅要考虑通过 SATCOM 接口注入恶意指令的外部威胁，还应评估通过维护接口加载被篡改软件的内部风险，并依据其对飞行安全的影响进行量化分级。

在完成风险评估后，进入安全开发与安全有效性保证阶段。首先，需设计并实施具体的安全防护措施，并将这些措施明确追溯至已识别的风险。随后，必须通过一系列验证与确认活动来证明这些措施的有效性。例如，针对 ARINC 429 总线接口的脆弱性，需在集成试验中验证其协议过滤规则对异常数据包的拦截能力；针对伪造管制报文的威胁，则需通过注入攻击用例，评估系统入侵检测与防护机制的响应延迟和拦截成功率等关键性能指标，以客观数据验证其防护能力满足适航安全目标。

为确保防护措施在飞机全生命周期内持续有效，还需制定相应的运行与维护指南。其内容应包含密钥管理体系、安全日志审计机制及应急响应程序，通过文件体系明确日常维护与突发状况下的处置指引。最终形成的威胁分析报告、测试用例集与运维规程等共同构成符合性证据链，其完整性与防护等级的判定应与 RTCA DO–326A 的风险评估矩阵保持一致。

3.4 关联系统协同验证

ACARS 数据链的功能与安全依赖于多个机载系统的协同工作，因此符合性验证必须覆盖这些关联接口。

（1）显示与机组告警系统：需配合验证 CCAR–25.1322 条款，在故障注入试验中，确认 ACARS 数据链相关的告警信息能够以正确的等级和形式及时呈现，确保机组对 CCAR–25.1309（d）所要求的可探测故障有清晰的感知。

（2）飞行管理系统：需通过提供精确的飞机位置与航路数据，支持对 CCAR–121.533（b）自动位置报告功能的验证，在飞行试验中需确认报告间隔与数据精度满足规章要求。同时，为验证 CCAR–121.97 的全航段通信能力，飞行试验需要在规划的典型航路（特别是边远地区）上进行，以检验 ACARS 数据链在不同通信模式间的切换性能与数据传输的连续可靠性。

(3)驾驶舱记录系统:需在飞行试验中同步采集 VHF 话音信道与 ACARS 数据链的时序标记,验证驾驶舱语音记录与通信报文的时间同步精度,以满足 CCAR-25.1457(a)(6)等条款的要求。

(4)机载维护系统:需通过地面试验或飞行试验,验证 ACARS 数据链向其传输故障诊断数据接口的完整性。

(5)机载娱乐系统:需通过地面试验验证乘客终端与 ACARS 数据链的物理或逻辑隔离性,确保旅客服务数据流不会干扰关键通信。

4 结语

本文针对 ACARS 数据链的适航符合性问题,构建了系统的审定方案。该方案以符合性矩阵为基础,其验证思路体现在方法与范围两个层面。在验证方法上,将独立于功能安全的网络安全审查作为新维度,并将其验证活动与基于故障树分析等定量手段的传统安全性评估整合。在验证范围上,需从系统自身扩展至持续适航文件及所有关联的系统接口,以确保系统集成的有效性。该方案与验证思路可为当前型号审定工作提供技术参考,同时也可为后续开展国内网络安全适航标准制定和端到端数据链认证研究提供参考方向。

参考文献:

[1] 中国民用航空局. 民航数据链技术发展路线图(2022—2035)[R]. 北京: 中国民用航空局, 2022.

[2] ARINC. Air/ground character-oriented protocol specification: ARINC 618[S]. Annapolis: ARINC, 2018.

[3] ARINC. Multi-purpose control and display unit: ARINC 739A-1[S]. Annapolis: ARINC, 1998.

[4] ARINC. Communications management unit (CMU) mark 2: ARINC 758[S]. Annapolis: ARINC, 2007.

[5] ARINC. HF data link systems: ARINC 753-3[S]. Annapolis: ARINC, 2016.

[6] RTCA. VDL mode 2 operational requirements: DO-224[S]. Washington DC: RTCA, 2003.

[7] 中国民用航空局. 运输类飞机适航标准: CCAR-25-R4[S]. 北京: 中国民用航空局, 2011.

[8] 中国民用航空局. 大型飞机公共航空运输承运人运行合格审定规则: CCAR-121-R7[S]. 北京: 中国民用航空局, 2021.

[9] 中国民用航空局. 一般运行和飞行规则: CCAR-91-R4[S]. 北京: 中国民用航空局, 2022.

[10] EASA. Certification specifications for large aeroplanes: equipment, systems and network cyber security protection: CS 25.1319[S]. Cologne: EASA, 2020.

[11] 中国民用航空局航空器适航审定司. 航空器型号合格审定程序: AP-21-AA-2011-03-R4[S]. 北京: 中国民用航空局, 2011.

[12] SAE INTERNATIONAL. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment: ARP4761[S]. Warrendale: SAE International, 1996.

[13] FAA. VHF digital link (VDL) mode 2 communications equipment: TSO-C160a[S]. Washington DC: FAA, 2011.

[14] RTCA. Environmental conditions and test procedures for airborne equipment: DO-160G[S]. Washington DC: RTCA, 2010.

[15] RTCA. Airworthiness security process specification: DO-326A[S]. Washington DC: RTCA, 2014.

(责任编辑:明 月)

(上接第 5 页)

Processing Systems, December 4-9, 2017, Long Beach, California, USA. ACM, 2017: 4768-4777.

[5] 陈 琨, 李鹏飞, 解 江, 等. 基于可解释机器学习的翼身融合民机乘员撤离出口决策研究[C]//第七届中国航空科学技术大会论文集, 成都, 2024: 760-767.

[6] RATHSAM J, LOUBEAU A, KLOS J. A study in a new test facility on indoor annoyance caused by sonic booms[R]. Hampton, VA: NASA Langley Research Center, 2012: 217332.

[7] KLOS J, LOUBEAU A, RATHSAM J. Overview of an indoor sonic boom simulator at NASA Langley Research Center[J]. The Journal of the Acoustical Society of America, 2011, 129(S4): 2379.

[8] LOUBEAU A, RATHSAM J, KLOS J. Evaluation of new indoor sonic boom subjective test facility at NASA Langley Research Center[J]. The Journal of the Acoustical Society of America, 2011, 129(S4): 2379.

[9] LOUBEAU A, NAKA Y, COOK B G, et al. A new evaluation of noise metrics for sonic booms using existing data[J]. AIP Conference Proceedings, 2015: 090015.

[10] YADAV M, CABRERA D, LOVE J, et al. Workplace noise assessments by open-plan office occupants: relationship with ISO 3382-3 metrics, and psychoacoustic parameters[J]. The Journal of the Acoustical Society of America, 2018, 144(3_Supplement): 1928.

[11] ZWICKER E, FASTL H. Psychoacoustics: facts and models[M]. 2nd Updated ed. Berlin: Springer, 1999.

[12] RIBEIRO M T, SINGH S, GUESTRIN C. "Why should I trust you?": explaining the predictions of any classifier[C]//22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco California USA. ACM, 2016: 1135-1144.

[13] WANG S, PENG H, HU Q, et al. Analysis of runoff generation driving factors based on hydrological model and interpretable machine learning method[J]. Journal of Hydrology: Regional Studies, 2022, 42: 101139.

(责任编辑:明 月)