航空电子系统网络安全防护探讨

宁亚锋　陈　健
陕西飞机工业有限责任公司　陕西　汉中　723000

摘　要：本文分析综合化航空电子系统网络拓扑结构，梳理外部攻击、内部隐患、运维风险三类安全威胁，划分协议、硬件、软件三层系统漏洞。从技术、架构、管理、适航管控维度剖析现有防护短板，剖析先天设计、机载环境、行业标准滞后核心成因。结合航电时延、体积功耗及适航约束，提出架构优化、轻量化安全技术、全周期管控、行业配套完善四项防护策略，兼顾飞行运行确定性与安全性，为航电网络安全防护提供参考。

关键词：航空电子系统；网络安全；防护策略

引言：现代航空电子系统依托机载总线与空地无线链路实现一体化组网，系统综合化、互联化程度不断提升，但网络安全风险同步加剧。传统航电研发侧重飞行功能安全，未兼顾网络攻防需求，老旧协议、嵌入式固件、运维管理均存在安全缺陷，加之适航审定壁垒、攻击技术快速迭代，各类链路劫持、固件篡改、内网渗透攻击频发。为此立足航电系统安全痛点，剖析风险与防护缺陷，制定适配机载场景的防护方案，具备极强工程应用价值。

1 航空电子系统网络架构及安全风险分析

1.1 主流航空电子系统网络拓扑结构

（1）分布式综合航电网络架构以AFDX（航空全双工交换式以太网）为骨干，采用星型或混合型拓扑，集成飞行管理、导航、通信、显示等子系统，通过端系统交换机实现数据确定性交换。（2）机载总线包括ARINC429（低速单向）、ARINC659（背板总线）、CAN及1553B等，用于传感器与执行器互联；无线通信链路涵盖VHF/HF数据链、卫星通信及ADS-B，与地面站、其他飞机形成空地一体化组网。（3）机载设备通过标准化接口（如RDC远程数据集中器）接入网络，运维网络经专用维护端口与航电系统隔离，但故障诊断、软件加载等操作需逻辑贯通，通常依赖时间触发以太网（TTE）实现关键/非关键数据混合传输。

1.2 航空电子系统典型网络安全威胁

（1）外部网络攻击：攻击者通过无线链路劫持空地通信（如ACARS欺骗）、向机载维护口注入恶意固件，或利用供应链环节实施跨域渗透，从娱乐系统跳转至飞行关键网络。（2）内部安全隐患：机载嵌入式系统（如FMS）存在未修补固件漏洞，老旧ARINC429协议缺乏加密与认证机制，且多层级用户权限划分粗放，易导致越权访问关键航参数据[1]。（3）运维衍生风险：地面调试时维护端口默认口令未修改，或通过USB加载更新包引入病毒；运维人员误操作（如误删路由表、配置错误分区）可诱发逻辑链路中断。

1.3 航电系统网络安全漏洞分类

（1）通信协议层漏洞：AFDX虚链路调度机制可能遭受流量注入与带宽耗尽攻击，ARINC429无源消息易被嗅探、重放，且协议栈缺乏完整性校验与源认证，存在固有设计缺陷。（2）硬件嵌入式设备底层安全漏洞：FPGA/ASIC设计可能存在未公开后门，芯片侧信道泄漏（如功耗、电磁辐射），存储芯片未受物理防篡改保护，攻击者可利用JTAG或SWD调试接口绕过安全启动机制，直接读取固件。（3）机载操作系统与应用程序漏洞：基于VxWorks653、INTEGRITY等RTOS的驱动模块存在缓冲区溢出、越界读写风险；飞行计划加载、导航数据库更新、气象雷达数据处理等应用软件缺乏数字签名强制校验，易被恶意篡改。

2 航空电子系统现有网络安全防护短板与成因分析

2.1 现有技术层面防护缺陷

（1）传统防火墙基于地面网络设计，采用深度包检测与状态跟踪机制，其规则库与连接表占用内存过大，难以裁剪至机载嵌入式环境（通常仅有百兆级RAM）；轻量化改造后，对AFDX虚链路调度、时间触发流量的过滤精度严重退化，无法识别恶意帧间隔扰动，且自身计算时延易破坏航电系统确定性时延要求。（2）机载无线通信仍广泛采用AES-128以下强度的加密算法，部分老旧机型使用WEP级保护，密钥预置且多年不变；ADS-B报文完全明文广播，攻击者可伪造虚假飞机坐标；卫星数据链加密仅覆盖链路层，端到端身份认证缺失，中间人攻击可截获并篡改飞行计划上传指令。（3）当前入侵检测多依赖地面服务器周期性下载机载日志进行离线分析，缺乏机载实时流量基线建模能力；无法对微秒级异

常帧注入、合法指令重放等隐蔽攻击进行快速溯源，异常告警延迟通常超过500毫秒，远高于飞行控制闭环的50毫秒容忍上限，导致响应窗口丧失。

2.2 系统架构层面安全短板

（1）航电安全域划分仅按功能模块（如飞控、导航、娱乐）粗粒度隔离，域间访问控制依赖静态虚链路ID映射，缺乏动态双向认证与加密隧道；攻击者可通过娱乐系统Wi-Fi入口渗透，利用域间网关的ACL策略遗漏，横向移动至飞行关键域，而域内敏感数据（如惯导原始值）未区分安全等级。（2）机载软硬件采用深度绑定开发模式，安全增强模块（如可信平台芯片、安全启动固件）需改动底层板级支持包和操作系统内核，涉及DO-178CDALA级重新认证，改造周期长达2~4年且成本超千万；多数现役机型被迫放弃底层加固，仅靠应用层补丁应付，安全能力碎片化[2]。（3）双余度或三余度飞行控制计算机虽提供功能冗余，但主备通道间的同步数据流未经独立安全校验；若主通道被污染，备机通过交叉传输链路直接复制恶意状态，导致切换后攻击载荷延续，冗余架构反而成为攻击扩散的加速器，且备机缺乏独立的异常检测传感器。

2.3 管理与适航管控层面问题

（1）多数运营单位未建立航电网络安全配置基线库，漏洞修复、补丁测试、配置变更等环节缺乏闭环管理流程；应急响应预案模糊，发生疑似攻击时无法快速隔离受染设备，且机载日志存储容量有限，事后调查难以复现攻击链。（2）新型安全设备（如嵌入式IDS、硬件加密协处理器）需通过RTCADO-326A/DO-356适航安全审定，涉及威胁分析、验证用例、符合性证明等大量文档工作，平均取证周期超3年；而攻击技术迭代速率已达每季度出现新漏洞，导致安全方案落地即面临过时风险，适航门槛成为技术更新的实质阻碍。（3）飞行员、机务及签派员的网络安全培训多以理论宣贯为主，缺少实操演练；常见问题包括使用默认维护口令、跳过安全启动引导加载第三方软件、未识别钓鱼式固件更新包，人为操作失误占航电安全事件的40%以上，凸显安全文化薄弱。

2.4 安全防护问题核心成因

（1）早期航电系统需求规范聚焦功能安全（Safety），未将网络威胁纳入设计约束，协议栈、总线仲裁、任务调度均未考虑恶意输入场景，导致“天生缺乏攻击面消减”的架构缺陷，后期修补成本呈指数增长。（2）机载设备SWaP（重量、功耗、体积）约束严苛，加之高温振动环境限制，无法部署高性能加密引擎或AI异常检测模块，安全防护只能选用极简算法，在性能与安全之间被迫让位于飞行功能，形成长期技术欠账。（3）航空电子国际标准（如DO-178C、ARINC653）修订周期平均5~7年，且安全附录（如DO-326A）仍处于指导性阶段，缺乏强制性技术指标；而网络攻击手法在暗网中月级迭代，标准制定流程难以同步，防护基线始终滞后于真实威胁演进。

3 航空电子系统网络安全优化防护策略

3.1 分层分级网络架构优化防护方案

（1）划分飞行控制域、运维数据域、机载娱乐域三级安全隔离域，各域间部署轻量级安全网关，实施严格的单向数据流策略：飞控域仅接收来自导航、气象等信任源的校验数据，娱乐域严禁向飞控域发起主动通信；运维域需经多因素身份认证后方可临时接入，并在维护任务完成后自动切断链路，实现最小权限暴露。（2）优化AFDX总线逻辑隔离与物理边界防护设计，在端系统交换机中增加虚链路（VL）标签加密校验机制，禁止未授权VLID的数据帧进入核心交换区；同时在物理层增加光耦隔离或电磁屏蔽分区，防止侧信道耦合攻击从非关键区域传导至飞行关键总线。（3）搭建机载网络动态权限访问控制体系，基于时间触发调度表及任务阶段（滑行、起飞、巡航、着陆）动态调整设备访问权限——巡航阶段禁止地面调试端口激活，着陆后自动触发日志上传与会话密钥轮换，并结合信任链证书实现设备入网逐跳认证，杜绝非法终端伪装接入。

3.2 轻量化专用网络安全技术落地策略

（1）适配机载环境的轻量化加密算法迭代应用，选用ChaCha20-Poly1305或SM4国密轻量版替代老旧DES/AES-128，优化算法轮次与S盒规模使其运行于百兆级嵌入式处理器时额外时延控制在50微秒以内；采用物理不可克隆函数（PUF）实现密钥动态派生，避免密钥固化存储于EEPROM中的泄露风险，同时支持无线链路按会话周期实时更换密钥，提升抗重放攻击能力。（2）机载嵌入式入侵检测与异常流量溯源系统部署，设计基于白名单行为基线的轻量级IDS——离线训练各航电子系统典型通信模式（帧间隔、数据长度、源目地址特征），在FPGA中固化匹配引擎，实现微秒级异常帧检测；同时增设数据帧染色标记溯源机制，恶意帧一经识别即打标并记录注入端口、时间戳与链路跳数，支撑快速攻击路径还原[3]。（3）机载固件可信启动与漏洞静默修复技术应用，采用硬件信任根（RoT）逐级哈希校验引导加载程序、操作系统内核及关键应用程序，任何固件篡改将触发自动回滚至备份安全版本；同时引入差分静默更新机

制，在飞行巡航阶段利用空闲计算资源后台下载补丁增量包，着陆后校验激活，无需中断航电任务即可完成高危漏洞修复，缩短漏洞暴露窗口。

3.3 全生命周期安全管理体系构建

（1）航电设备研发、出厂、运维全流程安全管控，在需求阶段嵌入STRIDE威胁建模分析，设计阶段完成攻击面评审，出厂前强制通过模糊测试与渗透测试联调验证；运维阶段建立唯一设备指纹台账，每台机载设备的软件版本、补丁状态、配置基线均需在航空公司安全运营中心统一登记，确保全生命周期可追溯。（2）机载网络安全风险定期评估与漏洞闭环整改机制，每季度执行一次航电系统风险评估（涵盖CVSS评分、可利用性分析、业务影响评估），漏洞整改采用PDCA闭环流程——发现→验证→优先级排序→方案制定→测试验证→部署上线→复查确认；对无法立即修复的缺陷，部署虚拟补丁或流量过滤规则进行临时缓解，最长缓解周期不超过90天[4]。（3）人员专项安全培训与岗位权责划分制度，实行分层次培训体系：飞行员重点学习识别钓鱼式固件更新、异常驾驶舱告警研判；机务人员考核安全引导操作、调试端口管控规程；管理员接受攻防实战演练，每年至少组织一次红蓝对抗。严格划分权限矩阵——飞控参数修改仅授权试飞工程师，运维人员无权访问飞行敏感数据，实现职责与安全密级精准匹配。

3.4 行业标准与应急保障配套完善措施

（1）贴合民航、军机适航要求优化安全防护标准，推动RTCADO-326A/DO-356修订增设强制性安全能力指标（如加密算法最低强度、补丁响应时限、域间隔离强度），并纳入机载设备型号合格审定的必须条款；同步建立安全标准动态维护机制，每18个月发布技术修订通告，跟进最新攻击手法库更新，缩短标准迭代周期至2年以内。（2）搭建机载网络突发攻击应急响应处置流程，制定四级响应等级（一般告警、轻度影响、业务中断、飞行安全威胁），分别对应标准操作程序：一级由机载自动响应（切断可疑链路并切换冗余通道），二级需地面支持远程研判，三级启动航班备降预案，四级联合空管与安全专家现场处置；全流程要求从检测到决策通信延迟不超过100毫秒，并配备机载应急隔离按键供飞行员一键物理断除非关键网络[5]。（3）军民航电网络安全防护技术协同共享优化，建立军民航安全情报互通机制，共享恶意IP/域名特征、固件哈希黑名单、新型攻击手法TTP（战术、技术、流程），避免军民航各自孤立防御；定期举办跨领域联合安全演习，模拟针对空地链路协同渗透、虚假TCAS诱导等复杂攻击场景，从情报维度提升航空电子系统整体防御韧性。

结束语

本文完成航电系统网络安全风险、防护短板及成因系统性分析，贴合机载硬件、飞行工况、适航合规多重限制，落地分层架构、轻量化安全技术、管理制度、行业标准多维优化方案，破解现有防护矛盾。航电网络安全属于动态化防御工程，后续需跟进新型攻击技术迭代方案，打通军民航安全情报共享渠道，优化适航安全审定流程，补齐人员管理短板，持续提升航空电子系统网络防御能力与运行韧性。

参考文献

[1]赵启明,吴亚锋.网络化航空电子系统跨域安全隔离与防护技术[J].计算机工程与应用,2023,59(18):236-242.

[2]王布宏,罗鹏.航空机载网络安全威胁建模与防护技术综述[J].电子与信息学报,2025,47(5):161-165.

[3]孙文轩.民用飞机航空电子系统网络安全合规设计与防护优化[J].民用飞机设计与研究,2024,17(1):87-92.

[4]高健,田甜.异构航空电子网络入侵检测与主动防护方法[J].火力与指挥控制,2022,47(11):156-161.

[5]刘泽宇.新形势下军用航空电子系统网络安全管理与防护对策[J].舰船电子工程,2024,44(8):78-81.