民航空管系统网络安全协同防护体系研究

——基于动态韧性防御视角

郑晓兰
民航贵州空管分局　贵州贵阳　550012

摘　要：本研究聚焦民航空管系统网络安全协同防护体系，从动态韧性防御视角展开。首先阐述民航强国战略下智慧空管的网络安全需求及保障国家关键基础设施安全的紧迫性。接着分析空管网络安全威胁，包括攻击向量与系统脆弱点。然后介绍技术防护体系设计和管理韧性机制构建，前者基于特定架构及关键技术，后者涵盖制度、人员和应急响应方面。通过某空管局实例和仿真测试进行效能评估，最后总结“技术－管理－人员”三位一体防御模式，并提出6G时代空天地一体化网络安全挑战。

关键词：民航空管系统；网络安全；协同防护体系；动态韧性防御视角

在民航业迈向强国战略的进程中，智慧空管成为发展的关键方向，其高度依赖网络系统。然而，民航空管系统面临诸多网络安全挑战，这不仅影响民航业的安全高效发展，更关系到国家关键基础设施安全。本研究旨在从动态韧性防御视角出发，构建民航空管系统网络安全协同防护体系，通过深入分析网络安全威胁，设计有效的防护体系并构建管理韧性机制，最终保障空管系统的网络安全。

一、引言

（一）研究背景

在民航强国战略不断推进的大背景下，智慧空管成为民航业发展的重要方向。智慧空管高度依赖信息技术，从航班调度、空中交通管制到航空通信等各个环节，都离不开复杂的网络系统支持。随着信息技术的深度融合，空管系统面临着前所未有的网络安全挑战。例如，航班信息管理系统需要实时处理海量的航班数据，包括旅客信息、航班动态等，这些数据一旦遭到泄露或篡改，将对航空安全和旅客权益造成严重损害。同时，空中交通管制自动化系统的稳定运行对于保障飞机在空中的安全间隔和有序飞行至关重要，任何网络攻击导致的系统故障都可能引发灾难性后果。此外，航空通信网络需要在不同的空域和地面设施之间准确无误地传递信息，网络安全问题可能导致通信中断或错误指令的传递。因此，满足智慧空管的网络安全需求是确保民航业安全、高效发展的必然要求。

（二）研究意义

民航空管系统作为国家关键基础设施的重要组成部分，其网络安全直接关系到国家的安全和稳定。航空运输业在国民经济和社会发展中扮演着重要角色，它不仅是人员和物资快速运输的重要手段，还在国际交往、应急救援等方面发挥着不可替代的作用。空管系统一旦遭受网络攻击，可能导致大面积航班延误、取消，甚至危及飞行安全，这将对国家的经济、社会秩序和国际形象产生严重的负面影响。例如，在全球化的今天，国际商务往来频繁，航班的正常运行对于跨国企业的运营至关重要。如果空管网络安全出现问题，将影响跨国贸易、外交交往等多方面活动。此外，空管系统的网络安全还涉及到国家安全的战略层面，因为航空领域与国防、情报等领域存在着千丝万缕的联系。因此，保障民航空管系统的网络安全是保障国家关键基础设施安全的紧迫任务。

二、空管网络安全威胁建模

（一）攻击向量分析

民航空管系统网络环境存在多种攻击向量，病毒、APT和内部威胁较常见且危害严重。病毒可多途径传播，进入系统会破坏文件、干扰程序，像感染航班数据处理软件会致航班信息问题。APT隐蔽复杂，由专业攻击者发起，目标是窃取敏感信息，长期潜伏收集信息建立通信渠道，传统防护手段难发现。内部威胁不可小觑，内部人员可能疏忽、恶意或被利用而损害系统，如工作人员误删配置文件，技术人员窃取信息售卖。内部人员熟

作者简介：郑晓兰（1983.01－）女，汉族，浙江浦江人，硕士研究生，高级工程师，主要从事空管系统通信导航监视设备建设及维护管理工作。

悉系统，能利用信任关系攻击，防范内部威胁是空管网络安全的重要挑战。

（二）系统脆弱点评估

民航空管系统的自动化系统、通信协议和移动介质易有脆弱点。自动化系统对提高空管效率至关重要，但存在安全脆弱点。其软件有漏洞可被利用篡改航班数据、干扰管制逻辑，且因复杂性，漏洞难发现与修复，被攻击会使空管运行混乱。通信协议在设计和实现中可能有安全缺陷，缺乏加密和身份验证手段，攻击者可伪装节点插入假指令或获取敏感内容，影响信息传递准确性和安全性。移动介质也是潜在脆弱点，像U盘、移动硬盘用于数据传输，若携带病毒或恶意软件且未严格检测就接入空管设备，会传播病毒引发安全问题。

三、技术防护体系设计

（一）基于“一个中心，三重防护”的架构

基于“一个中心，三重防护”的架构对民航空管系统网络安全意义重大。安全管理中心是防护体系核心，有集中管理、监控与决策功能，能收集、分析与整合计算环境、通信网络和区域边界的安全信息，及时察觉潜在威胁，像监测各类异常情况。计算环境防护关乎空管系统内部设备与软件安全运行，涉及设备安全配置、漏洞修复加固，还要保护数据防止泄露篡改。通信网络防护针对通信链路，采用加密通信技术确保信息传输的保密性与完整性，如用VPN技术建安全通道，且要监控流量、检测入侵。区域边界防护构建外部安全防线，在区域边界设置防火墙、入侵检测系统等过滤检测进出流量，仅合法的可进出，防止外部攻击入侵。

（二）关键技术实现

网络接口数据自动获取技术在民航空管系统网络安全防护中具有重要意义。空管系统涉及众多的网络设备和接口，这些接口产生大量的数据，如网络流量数据、设备状态数据等。通过网络接口数据自动获取技术，可以实时、准确地收集这些数据，为后续的安全分析提供基础。例如，该技术可以自动采集网络交换机端口的流量数据，包括数据包的数量、来源和目的地等信息。主机加固与漏洞扫描自动化是保障空管系统主机安全的关键技术。主机加固包括对操作系统、应用程序等进行安全配置的优化，如关闭不必要的服务、设置强密码等。通过自动化的主机加固技术，可以提高主机的安全性，减少被攻击的风险。同时，漏洞扫描自动化能够定期对主机进行全面的漏洞扫描，及时发现系统中存在的安全漏洞。

四、管理韧性机制构建

（一）制度层面

在制度层面建立安全合规与量化考核标准是提升民航空管系统网络安全管理韧性的重要举措。安全合规要求空管系统的各个部门和相关人员遵守国家和行业制定的网络安全法规、标准和规范。例如，在数据保护方面，必须遵循相关的数据隐私法规，确保旅客信息和航空运营数据的安全存储和使用。安全合规性检查应定期进行，以确保空管系统始终处于合法、安全的运行状态。量化考核标准则为空管系统的网络安全管理提供了可衡量的依据。通过设定量化的指标，如系统漏洞数量、安全事件响应时间、安全培训参与率等，可以对各部门和人员的网络安全工作进行客观评价。

（二）人员层面

在人员层面，安全文化培育与跨部门协同演练对于民航空管系统的网络安全至关重要。安全文化培育旨在提高全体人员的网络安全意识和责任感。通过开展网络安全培训、宣传活动等方式，让空管系统中的每一位工作人员都认识到网络安全的重要性。这种安全文化的培育可以使工作人员在日常工作中自觉遵守网络安全规定，减少因人为疏忽导致的安全风险。跨部门协同演练则有助于提高空管系统应对网络安全事件的整体能力。空管系统涉及多个部门，如管制部门、通信部门、设备维护部门等，在网络安全事件发生时，需要各部门之间密切协作才能有效应对。通过跨部门协同演练，可以模拟各种网络安全场景，如勒索病毒攻击、通信网络故障等，让各部门熟悉应急响应流程和自己的职责。

（三）应急响应

勒索病毒事件处置流程的设计是民航空管系统应急响应管理的重要内容。当勒索病毒入侵空管系统时，需要迅速启动应急响应流程。首先，要进行事件的检测和确认。通过监测系统的异常行为，如文件加密、系统运行缓慢等现象，结合安全防护设备的报警信息，确定勒索病毒的入侵。一旦确认，应立即隔离受感染的系统或设备，防止病毒进一步传播。随后，对勒索病毒进行分析，确定病毒的类型、传播途径和加密算法等信息。这有助于制定针对性的恢复措施。在分析的同时，要及时向上级部门和相关机构报告事件情况，以便获取更多的技术支持和资源。接下来，根据病毒的分析结果，尝试使用备份数据进行系统恢复。如果备份数据不可用或者无法完全恢复系统，可能需要寻求专业的安全厂商或研究机构的帮助，探索解密方法或者进行系统重建。

五、案例验证与效能评估

（一）实例分析

某空管局的态势感知平台在提升空管系统网络安全效能方面取得了显著成果。该态势感知平台通过整合空管系统中的各种安全信息，包括网络流量数据、设备日志、安全告警等，实现了对空管网络安全态势的全面感知。在实际应用中，该平台成功降低了告警响应时间达40%。这意味着当出现网络安全威胁时，安全管理人员能够更快地接收到告警信息，并及时采取相应的措施。例如，以往在检测到网络攻击时，由于安全信息分散在不同的系统和设备中，安全管理人员需要花费大量时间收集和分析这些信息，才能确定攻击的来源和性质，然后做出响应。而现在，态势感知平台能够实时对这些信息进行关联分析，一旦发现异常，立即发出准确的告警，并提供详细的攻击信息，使得安全管理人员可以迅速做出决策，启动相应的防护或应急响应措施。这不仅提高了空管系统应对网络安全威胁的效率，也有效降低了网络安全事件可能带来的损失。

（二）仿真测试

基于ATT&CK框架的仿真测试为评估民航空管系统的网络安全防护能力提供了有效的手段。在红蓝对抗测试中，红方模拟攻击者，采用各种网络攻击手段对空管系统进行攻击，而蓝方则代表防御方，运用现有的网络安全防护体系进行防御。通过这种模拟实战的测试，可以全面了解空管系统在面对不同类型网络攻击时的防御效果。在某次基于ATT&CK框架的红蓝对抗测试中，红方发动了包括针对空管自动化系统漏洞的利用攻击、通信网络的中间人攻击等多种复杂攻击手段。蓝方则依靠构建的技术防护体系和管理韧性机制进行防御。测试结果显示，蓝方在大部分攻击场景下能够成功检测和抵御攻击，但也暴露出一些薄弱环节，如在应对APT攻击时，对潜伏性攻击的早期发现能力还有待提高。

六、结论与展望

（一）总结“技术–管理–人员”三位一体防御模式

民航空管系统网络安全的有效防护需要“技术–管理–人员”三位一体的防御模式。在技术方面，基于“一个中心，三重防护”的架构以及关键技术的实现，为空管系统构建了坚实的网络安全技术防线。例如，通过安全管理中心对计算环境、通信网络和区域边界的集中管理，以及网络接口数据自动获取技术和主机加固与漏洞扫描自动化等关键技术的应用，能够有效地抵御各种网络攻击。在管理方面，制度层面的安全合规与量化考核标准以及应急响应流程的设计，确保了空管系统网络安全管理的规范性和有效性。在人员方面，安全文化培育与跨部门协同演练提高了全体人员的网络安全意识和团队协作能力。例如，通过安全文化的培育，工作人员能够自觉遵守网络安全规定，减少人为失误，而跨部门协同演练则使各部门在应对网络安全事件时能够密切配合，提高整体应对能力。这种三位一体的防御模式相互补充、相互促进，共同为空管系统的网络安全提供了全面的保障。

（二）提出6G时代空天地一体化网络安全挑战

随着6G时代的即将到来，民航空管系统将面临空天地一体化网络安全的全新挑战。6G技术将实现空天地网络的深度融合，使得航空通信网络的覆盖范围更广、传输速度更快、连接更加智能。然而，这种新的网络架构也带来了更多的安全风险。例如，空天地一体化网络的复杂拓扑结构使得网络攻击的面更广，攻击者可能从不同的接入点发起攻击。同时，6G网络中的大量物联网设备的接入也增加了安全管理的难度。这些物联网设备可能存在安全漏洞，一旦被利用，可能会对整个空管系统的网络安全造成威胁。此外，6G网络的高速数据传输和低延迟要求可能会导致安全防护机制在性能和效率方面面临新的挑战。如何在满足6G时代空天地一体化网络需求的同时，确保民航空管系统的网络安全，将是未来研究的重要方向。

结束语

本研究构建的民航空管系统网络安全协同防护体系在应对当前网络安全挑战方面具有重要意义。通过“技术–管理–人员”三位一体的防御模式，为空管系统网络安全提供了全面保障。然而，随着技术的不断发展，尤其是6G时代的临近，空天地一体化网络安全面临新的挑战。未来需要进一步深入研究，不断优化防护体系，以适应新的发展需求，确保民航空管系统网络安全的持续稳定。

参考文献

[1]刘大伟.民航空管通信网的安全性能分析[J].电子技术，2024，53（12）：116-117.

[2]白宇晨.针对民航空管流量系统的渗透测试及问题分析[J].网络安全技术与应用，2023，（04）：131-134.

[3]吴昊，李上.民航空管场景下的网络攻击手段与防范策略探析[J].电脑知识与技术，2023，19（09）：79-81+84.