国 际 民 用 航 空 组 织

工 作 文 件

A41-WP/241
EX/108
2/8/22

大会 — 第 41 届会议

执行委员会

议程项目 14：航空安保 — 政策

通过零信任方法确保航空安保

（由南非提交）

执行摘要

航空业有时依赖于跨越不同行业的扩展供应链，从而使航空威胁形势增生。采用基于互联网协议（IP）的系统来提高效率，使得应用必要的主动方法来防卫当前和老旧系统势在必行。

国际民航组织网络安保行动计划概述了有必要集中资源和行动，以实现管理航空网络安保的系统方法；目标是开发系统方法，使航空能够及时适应并抵御新的威胁。

本工作文件旨在介绍零信任的概念，各国和其他航空参与者可将其作为一项缓解原则加以采用。结合零信任方法具有潜力，可通过强制执行端到端系统保护来增强当前的网络安保保护能力。它摆脱传统的周界安保，在边缘或在更靠近最终用户交通管制设施和远程站点（供应雷达）地面导航辅助数据处实施安保资源。

行动：请大会：

a) 认识到实施敏捷和具适应性的连续适应风险和信任评估（CARTA）方法在保障航空运行方面的益处；
b) 要求国际民航组织通过网络安保专家组制定技术指导材料，以支持各国将零信任框架纳入信息安保管理系统（ISMS）；和
c) 敦促各国考虑将零信任原则纳入其信息安保管理系统。

战略目标：	本工作文件涉及安保和简化手续战略目标。
财务影响：	没有额外的预算影响，因为这将在国际民航组织分配的预算范围内进行。
参考文件：	网络安保行动计划 Doc 8973 号文件：《国际民航组织航空安保手册》

1. 引言

1.1 近年来，航空业经历了技术采用而驱动的转型，因此增加了需要关注的网络风险。由于在技术采用方面出现前所未有的巨大飞跃，这使得持续采用连续适应风险和信任评估（CARTA）方法与模型势在必行。

1.2 过去一直对航空业孤立看待。然而，航空生态系统中信息技术（IT）/运行技术（OT）的相互依赖和融合引入了不受航空合规机制约束的各种利害攸关方。这增加了可能的网络攻击面，并需要修改某些传统概念。

1.3 以前，航空硬件和软件的管理和维护可以通过安保可信的远程访问虚拟专用网络（VPN）来实现，在当今世界，这种连接已导致系统安保遭到破坏的经验。

1.4 如勒索软件、数据盗窃和网络钓鱼攻击等网络威胁在航空界已盛为猖獗，影响了信息技术（企业资源规划系统（ERP）访问、协作服务、电子邮件服务）和运行技术环境（监督管制及数据获得（SCADA）、可编程逻辑控制器（PLC））并针对机场内及周边的管制区域和数据中心作为目标。

2. 讨论

2.1 航空扩展供应链有可能引入网络威胁，因此提高了对创新和新方法的需求，以据此应对这些威胁。这是因为航空业依赖多个利害攸关方，这些利害攸关方拥有不同的系统、应用程序和技术，需要相互整合。

2.2 还需要注意的关键是，这些运行的启用可能需要来自国家边界内外资源的远程支持，这进一步使航空运输价值链面临网络威胁。

2.3 以前用于处理所需安保的基于周界网络安保传统方法已证明无效。航空网络事件的增加验证了这点。一旦攻击者突破周界，就能进一步横向移动无阻。

2.4 如零信任等概念有潜力应对下一代威胁和目前猖獗的先进威胁。这允许每项资源请求在经过周密考虑和有效的安保管制下，启用态势评估、态势验证和授予资源访问权限的流程。

2.5 零信任为工作流、系统设计和运行提供了一套指导原则，可用于改善关键和敏感活动的安保态势。目的是防止数据泄露并限制内部横向移动。

2.6 零信任方法的假设是，无论是组织内部还是外部，谁都不能信任。这种方法旨在基于以下关键想法将攻击面最小化：

a) 不存在周界。通过淘汰出于某人已进入公司网络而信任其人的这种假设来实现；

b) 确保在授予访问权限之前验证用户并在连接到网络之前验证装置的完整性；

c) 淘汰用户会正确行事的这种假设。相反地，对每项服务请求都要求经验证的访问权限；和

d) 与其跟踪不良行为者，不如设置障碍以降低绩效。

2.7 结合零信任具有潜力，可通过强制执行端到端系统保护来增强当前的网络安保保护能力。它摆脱传统的周界安保，在边缘或在更靠近最终用户交通管制设施和远程站点（供应雷达）地面导航辅助数据处实施安保资源。

2.8 零信任的实施由不同底层技术加以支持，这些技术在各个方面提供保护：

a) 微分段零信任的最早概念，其主要目的是防止横向移动，以尽量减少违规的影响。多起攻击事件的核心要素均是以横向移动从数据中心关键资产中捕获信息。这种方法旨在通过最大限度地减少违规的影响来限制工作负载之间未经批准的通信（如果没有有效的理由这样做）。与防火墙提供的典型南北保护不同，微分段着眼于工作负载的东西向安保；

b) 零信任网络访问为应用程序访问创建了一个基于上下文的逻辑边界。目标是最大限度地减少用户和设备上下文驱动的应用程序访问的访问和滥用。它挑战了根据实体所在位置（例如在网络内部）即被自动授予信任的假设；

c) 它隐藏网络上的所有应用程序，并允许基于用户身份、装置、地理位置和安保态势等属性进行访问。这意味着，用户可以访问所需的应用程序，但他们在网络上什么也看不到；和

d) 远程浏览器隔离的运作原则是最终用户代表任何组织中最薄弱的环节，互联网访问是导致违规行为的最大攻击面之一。因此，最大限度地减少端点/最终用户导致破坏的最有效方法之一，就是隔离网络访问以消弭浏览器漏洞和威胁，例如勒索软件、嵌入式恶意软件和网络钓鱼。

3. 结论

3.1 零信任原则可用于通过采用“内置安保”方法确保民用航空自我加强。“通过设计”确保关键要素和流程的安保，将安保模式从被动（固栓）转变为主动，并促进发展自强的民航系统，从而使其能够演变并能以自动化更高的方式情况下加强复原力，这些已证明是有效的。

— 完 —