



大会 — 第 42 届会议

技术委员会

议程项目 25：由技术委员会审议的其他问题

航空安全培训现代化：将人工智能与网络安全
纳入国际民航组织（ICAO）航空电信技术员（ATSEP）能力标准

（由国际航空交通安全电子协会联合会（IFATSEA）提交）

执行摘要

随着人工智能、自动化和数字化等技术的迅猛发展，航空业日益复杂化。这些技术正在快速地重塑和重新定义技术操作的执行方式。鉴于航空业高度依赖高标准的安全水平，确保处于技术操作核心的专业人员能够熟练掌握和管理这些已融入民航运营的技术，对整个行业具有重要意义。本文件建议对《航空交通安全电子人员能力本位培训与评估手册》（Doc 10057 号文件）进行更新，明确将人工智能（AI）和网络安全列为独立且重要的培训领域纳入其中。这些快速发展的技术为航空业带来了挑战，也带来了变革性的机遇。在 ICAO 培训指导中，并肩《航空导航服务培训程序》（Doc 9868 号文件）中的条例，纳入这些内容，对于确保各成员国的准备度、安全性和韧性至关重要。

行动：请大会：

- a) 批准将人工智能和网络安全领域纳入 ICAO Doc 10057 号文件；
- b) 要求国际民航组织秘书处启动起草工作并征求相关专家意见；和
- c) 鼓励成员国试点新培训模块并分享成果。

战略目标：	本工作文件涉及战略目标每一次飞行都安全可靠，航空业实现环境可持续性，航空为所有人提供无缝、可达和可靠的出行和不让任何国家掉队。
财务影响：	待定
参考文件：	Doc 10057 号文件，《航空交通安全电子人员能力本位培训与评估手册》 Doc 9868 号文件，《航空导航服务培训程序》

¹ 中文，阿拉伯文，英文，法文，俄文和西班牙文版本由国际航空交通安全电子协会联合会提供。

1. 引言

1.1 民航业正在经历一场技术革命。自动化、预测分析和数字安全正在重新定义民航运营的管理、操作和保护方式。人工智能已应用于民航运营控制系统、机组调度、安全分析和乘客服务等领域。日益增长的网络安全威胁要求航空系统配备强大的专业网络安全队伍。为跟上这一发展趋势，需更新《航空交通安全电子人员能力本位培训与评估手册》（Doc 10057 号文件），纳入关于人工智能和网络安全培训项目的结构化指南。

1.2 国际民航组织 10057 号文件中增加人工智能和网络安全培训领域，将使各地区航空电信技术员（ATSEP）具备统一技能，提升其在空中交通管理、数据共享和网络安全响应方面的能力。

1.3 ATSEP 在人工智能和网络安全方面的专业能力可增强系统韧性，培养主动预防、缓解和恢复数字威胁的文化。

1.4 为使国际民航组织能力框架与技术发展同步，应更新 10057 号文件，提供关于人工智能和网络安全的结构化指南，作为《航空导航服务程序 — 培训》（PANS-TRG, Doc 9868 号文件）基础培训原则的补充。

2. 讨论

2.1 人工智能和网络安全威胁正通过数字化、自动化、数据集中化和互操作性深刻改变民航业和全球空管系统（ATM）。这些发展对确保空管系统安全和性能的核心岗位 ATSEP 专业人员将产生重大影响。

2.2 ATSEP 专业人员将越来越多地接触以下新兴技术：

- a) 人工智能驱动的自动化系统；
- b) 数字化信息共享平台；
- c) 模块化和虚拟化基础设施；和
- d) 实时系统性能工具。

2.3 ATSEP 的工作范围正从传统系统的维护操作，逐步扩展到管理集成化、数字化和动态化的基础设施。

2.4 鉴于民航系统正向系统集成和网络安全转型，ATSEP 将在以下方面发挥关键作用：

- a) 设计、实施和保护互联系统；
- b) 确保高度网络化空管环境中的网络韧性；
- c) 支持“人在环内”和“人在环上”系统；

- d) 开发维护供管制员与系统协同管理空域操作的工具；和
- e) 确保系统设计直观、可追溯并能响应实时操作需求。

3. 结论

3.1. 在 10057 号文件中纳入人工智能和网络安全培训领域，国际民航组织将通过以下方式推动建设更具韧性、统一性和前瞻性的全球航空社区：

协作课程开发

- a) 鼓励成员国、航空院校和行业伙伴联合开展课程建设。
- b) 帮助资源欠发达国家利用全球专业知识，本土化尖端培训项目。

集体创新

- a) 共享培训促进国家与运营商之间的思想交流，助力开发更智能、更安全的技术。
- b) 培育协作文化，使人工智能解决方案和网络安全框架能吸纳多元视角和联合研究成果。

3.2. 在文件 10057 中增加该培训领域，可为新兴经济体参与航空创新提供培训路径，通过普及关键的人工智能和网络安全教育缩小数字鸿沟。

3.3. 国际民航组织主导的协调工作将确保课程设置与 Doc 9868 号文件框架下的人工智能和网络安全模块保持一致。

3.4. 具备网络安全意识的专业人员能更有效防御勒索软件和系统入侵等日益增长的威胁。

3.5. 请大会审议摘要部分提出的行动建议。