



## 大会 — 第 42 届会议

### 执行委员会

#### 议程项目 13：航空安保 — 政策

#### 先进空中出行及其对航空安保的风险

（由沙特阿拉伯提交）

#### 执行摘要

先进空中出行（AAM）以及无人驾驶航空器系统（UAS）、城市空中出行（UAM）和先进飞行器等新兴技术彻底改变了航空业。但是，包括未经授权的访问、网络攻击以及恐怖分子可能滥用等威胁在内的这些发展情况，对航空安保构成了重大挑战。本文件审查了与先进空中出行相关的风险，评估了现行的航空安保框架，并强调了国际民航组织提供指导材料以协助缔约国保障航空安保并制定国家要求的必要性。

**行动：请大会：**

- a) 注意到本文件提供的信息。
- b) 鼓励缔约国与秘书处分享任何信息或经验，以建立一个协助航空安保专家组制定监管框架的参考数据库，并通过积极主动的做法向缔约国提供指导，以应对风险并确保将 AAM 安全融入现有航空系统。（该工作文件包括先进空中出行安保业务的拟议指南和最佳做法）。
- c) 鼓励缔约国与当地利害关系方协作，实施定制的安保措施，并促进对先进无人机交通管理解决方案、保护互联系统的网络安全工具以及与其他国家共享威胁信息等技术的投资。

|       |                                              |
|-------|----------------------------------------------|
| 战略目标： | 本工作文件涉及战略目标：每次飞行都安全和安保。                      |
| 财务影响： |                                              |
| 参考文件： | 附件17 — 《航空安保》<br>国际民航组织《航空安保手册》（Doc 8973号文件） |

<sup>1</sup> 阿拉伯文版本和英文版本由沙特阿拉伯提供。

## 1. 引言

1.1 先进空中出行（AAM）的概念正在技术进步的驱动下迅猛扩展。在提供增长机遇的同时，也带来了新的安保风险和潜在的漏洞，并正在改变民用航空网络的威胁格局。这些风险要求国际民航组织等国际监管机构采取积极主动的做法，以确保全球航空的安全和安保。本文件探讨了 AAM 对航空安保的影响，查明了正在出现的风险，并为应对这些挑战提出了国际民航组织及其缔约国可以采取的行动。

1.2 先进空中出行是指通过各种空中运输手段，包括通过无人驾驶航空器系统（UAS）、城市空中出行平台（UAM）和电动垂直起降（eVTOL）飞行器运送旅客和货物。

## 2. 讨论

2.1 先进空中出行代表了航空业的重大进步，但也带来了新的安保挑战。因此，至关重要的是制定综合安保做法，其中虑及潜在风险并确保保护航空生态系统免遭这一技术演进带来的威胁。这些风险包括：

a) 未经授权的访问和内部威胁：

1. UAS 和 UAM 运行的增加导致机场限制区和飞行航道出现漏洞。
2. 先进空中出行系统可能被利用进行非法干扰。

b) 网络安全威胁

1. UAM 数字系统与自动化的集成增加了遭受网络攻击的风险。
2. 恐怖分子可能破坏导航系统、通信网络或运行数据。

c) AAM 系统滥用

1. AAM 系统可能被用于监视、走私或运输爆炸物。
2. 涉及机场附近先进空中出行系统的征候事件可能扰乱空中交通并构成碰撞风险。

### 2.2 航空安保的现行法律框架：

2.2.1 附件 17 概述了保护民航免遭非法干扰行为的国际标准。但是，AAM 的快速发展需要更新以应对无人驾驶飞行器、自主飞行器与低空空域业务的一体化。

2.2.2 一些国家已经制定了使用无人机和 UAS 的单独法律框架。但是，这些政策往往与国际标准缺乏协调，并导致不一致的情况。

### 2.3 缔约国之间的国际合作：

2.3.1 数据共享：促进各国之间及时交换安保信息。

2.3.2 联合讲习班：举办协调一致的演习和培训课程，以应对先进空中出行的风险。

2.3.3 标准化努力：在国际上对先进空中出行运行的规章实行协调一致。

### 2.4 AAM 安保运行指南和最佳实践：

2.4.1 本文件附件为缔约国提供了指南，旨在根据附件 17 和国际民航组织 Doc 8973 号文件的要求，确保包括城市空中出行（UAM）、无人机配送和货运服务（RPAS）以及自主航空器（UAS）在内的新兴 AAM 运行的安保。

—————



## APPENDIX

### GUIDANCE AND BEST PRACTICES FOR AAM SECURITY

#### 1. Purpose and Scope

This document provides guidance for Contracting States on securing AAM operations, including UAM such as air taxis, RPAS cargo and delivery services, and UAS, in accordance with Annex 17 and operational considerations in Doc 8973.

#### 2. Scope of Application

- Civil Aviation Authorities.
- Airport Operators and Air Navigation Service Providers.
- AAM Operators and Service Providers.
- Relevant National Security Agencies.

#### 3. Objectives

- Prevent acts of unlawful interference via AAM systems.
- Protect civil aviation infrastructure from physical and cyber threats related to AAM.
- Ensure safe integration of AAM into national airspace systems.

#### 4. Best Practices for States

##### 4.1 National Civil Aviation Security Regulatory Framework

- Integrate AAM into National Civil Aviation Security Programs (NCASPs).
- Require all AAM operators to establish written security programs/procedures.
- Require registration and licensing of all AAM operations.

##### 4.1.1 Operator Licensing and Security Programs

- All AAM operators (UAM, UAS) must undergo security audits and be licensed by the Civil Aviation Authority.
- Operators must submit and maintain a security program aligned with the NCASP, including:
  - Roles and responsibilities of all personnel.
  - SOPs for normal and emergency conditions.
  - Coordination with local law enforcement, CAA, and ANSPs.

- Security programs should include regular training, recordkeeping, and quality control mechanisms.

#### 4.2 Security Risk Assessments

- Conduct targeted threat and risk assessments for:
  - Low-altitude operations near critical infrastructure.
  - Launch/recovery sites and vertiports.
  - Communication and navigation systems.
- Update risk assessments periodically and post-incident.

#### 4.3 Access Control and Perimeter Security

- Establish security zones around AAM facilities.
- Secure ground control stations and command centers.
- Integrate AAM vertiports into civil airport perimeter control policies.

#### 4.4 Personnel Security

- Conduct regular background checks on remote pilots, engineers, and ground personnel.
- Ensure training on insider threats and cybersecurity awareness.

### 5. Operational Security Measures

#### 5.1 Secure Launch/Recovery Sites / Vertiports

- Designated launch/recovery sites and vertiports must:
  - Fenced and access-controlled with human or video surveillance and lighting.
  - Equipped with personnel ID verification systems.
  - Integrated with airport security infrastructure, where applicable.
- Clear operational security responsibilities must be assigned.
- Emergency response procedures (e.g., hijacking, cyber breach) must be established and tested regularly.

## 5.2 Pre-Flight Screening

- Implement screening controls for cargo or passengers aboard AAM vehicles.
- Verify pre-departure data exchange with competent authorities.
- Advanced Air Mobility operations must follow appropriate pre-flight security procedures.
- When used for commercial passenger/cargo transport:
  - Apply security screening consistent with Annex 17.
  - Verify the identity of all passengers and cargo handlers.
- The possibility of implementing a smart verification mechanism as an alternative to manual verification, such as:
  - Developing an electronic platform for digital user identity verification.
  - Benefiting from national information centers or security databases.
  - Two-factor authentication with biometric verification (e.g., facial recognition).

## 5.3 Security Monitoring and Oversight

- Deploy counter-UAS (C-UAS) near airports.
- Manage AAM and UAS flights to:
  - Ensure real-time tracking and identification.
  - Detect and respond to operational interference.

## 5.4 Real-Time Communication and Command

- Operators of Advanced Air Mobility (AAM) systems, such as Urban Air Mobility (UAM) vehicle operators and unmanned aircraft (drone) operators, are required to:
  - Use encrypted communication between aircraft and control stations.
  - Establish a direct communication line with airspace authorities to redirect the aircraft or return it to the ground in emergency situations.

## 5.5 Cybersecurity Protocols

- Assess cybersecurity vulnerabilities in:

- Autonomous flight software.
- Remote control stations.
- Communication networks.
- Ensure alignment with ICAO's Cybersecurity Strategy.

## 6. Incident Response and Coordination

### 6.1 Reporting and Notification

- Integrate AAM systems into national aviation security incident reporting systems.
- Establish a point of contact for coordination with:
  - Air traffic services.
  - Intelligence and law enforcement agencies.

### 6.2 Response to Unlawful Interference

- Develop emergency response plans for unauthorized interference scenarios.
- Train aviation security staff in response procedures.

## 7. International and Regional Cooperation

- Data Sharing: Facilitate timely exchange of threat intelligence among States.
- Joint Exercises: Conduct coordinated training and simulation exercises.
- Standardization: Harmonize standards for AAM operations.

## 8. Capacity Building and Training

- Develop specialized aviation security training modules for:
  - Operators.
  - Security screening personnel.
  - Cybersecurity and risk managers.
- Promote use of ICAO Aviation Security Training Centers (ASTCs) for AAM simulations.

## 9. Continuous Monitoring and Quality Assurance

- Include AAM systems in national quality control programs.
- Ensure internal compliance monitoring aligns with national and ICAO standards.