International Civil Aviation Organization

WORKING PAPER

A42-WP/200[1]
EX/92
31/7/25

ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security – Policy

ADVANCED AIR MOBILITY AND ITS RISKS TO AVIATION SECURITY

(Presented by Saudi Arabia)

EXECUTIVE SUMMARY

Advanced Air Mobility (AAM) and emerging technologies such as unmanned aircraft systems (UAS), urban air mobility (UAM), and advanced aerial vehicles have revolutionized the aviation industry. However, these developments pose significant challenges to aviation security, including threats arising from unauthorized access, cyberattacks, and potential misuse by terrorists. This paper reviews the risks associated with advanced air mobility, assesses the current aviation security framework, and highlights the need for ICAO to provide guidance materials to assist Contracting States in securing aviation and establishing national requirements.

Action: The Assembly is invited to:

a) Take note of the information presented in this paper.

b) Encourage Contracting States to share any information or experiences with the Secretariat to establish a reference database that will assist the Aviation Security Panel in developing a regulatory framework and providing guidance to Contracting States through a proactive approach to addressing risks, ensuring the safe integration of AAM into existing aviation systems. (The working paper includes a propose guidelines and best practices for Advanced Air Mobility security operations).

c) Encourage Contracting States to collaborate with local stakeholders to implement tailored security measures and promote investment in technologies such as advanced drone traffic management solutions, cybersecurity tools to protect interconnected systems, and threat information sharing with other States.

Strategic Goals:	This working paper relates to Strategic Goal of *Every Flight is Safe and Secure*.
Financial implications:	
References:	Annex 17 — *Aviation Security* ICAO *Aviation Security Manual* (Doc 8973)

[1] English and Arabic versions provided by Saudi Arabia.

1. INTRODUCTION

1.1 The concept of Advanced Air Mobility (AAM) is rapidly expanding, driven by technological advancements. While it provides opportunities for growth, it also imposes new security risks and potential vulnerabilities, shifting the threat landscape within the civil aviation network. These risks require a proactive approach from international regulatory bodies such as ICAO to ensure the safety and security of global aviation. This paper discusses the implications of AAM for aviation security, identifies emerging risks, and proposes actions that ICAO and its Contracting States can undertake to address these challenges.

1.2 Advanced Air Mobility refers to the movement of passengers and cargo via various aerial transportation means, including unmanned aircraft systems (UAS), urban air mobility platforms (UAM), and electric vertical take-off and landing (eVTOL) vehicles.

2. DISCUSSION

2.1 While AAM represents a major advancement in aviation, it also introduces new security challenges. Therefore, it is essential to develop an integrated security approach that considers potential risks and ensures the protection of the aviation ecosystem against threats emerging from this technological evolution. These risks include:

a) Unauthorized Access and Insider Threats:
    1. The increase in UAS and UAM operations creates vulnerabilities in airport-restricted areas and flight paths.
    2. Advanced air mobility systems could be exploited for unlawful interference.

b) Cybersecurity Threats
    1. The integration of digital systems and automation in UAM increases exposure to cyberattacks.
    2. Terrorists could compromise navigation systems, communication networks, or operational data.

c) Misuse of AAM Systems
    1. AAM systems may be used for surveillance, smuggling, or transporting explosives.
    2. Incidents involving advanced air mobility systems near airports could disrupt air traffic and pose collision risks.

2.2 CURRENT LEGAL FRAMEWORK FOR AVIATION SECURITY:

2.2.1 Annex 17 outlines international standards for protecting civil aviation from acts of unlawful interference. However, the rapid development of AAM requires updates to address integration of unmanned and autonomous vehicles and low-altitude air operations.

2.2.2 Some states have developed individual legal frameworks for using drones and UAS. However, these policies often lack harmonization with international standards, leading to inconsistencies.

2.3 **INTERNATIONAL COOPERATION AMONG CONTRACTING STATES**:

2.3.1 Data Sharing: Facilitating timely security information exchange between states.

2.3.2 Joint Workshops: Conducting coordinated exercises and training sessions to address advanced air mobility risks.

2.3.3 Standardization Efforts: Harmonizing regulations for advanced air mobility operations internationally.

2.4 **GUIDANCE AND BEST PRACTICES FOR AAM SECURITY OPERATIONS**:

2.4.1 This document provides an annex of guidance to Contracting States for securing emerging AAM operations, including urban air mobility (UAM), drone-based delivery and cargo services (RPAS), and autonomous aircraft (UAS), in line with Annex 17 and ICAO Doc 8973.

— — — — — — — —

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.

— END —