



ASAMBLEA — 42º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 13: Seguridad de la aviación - Política

MOVILIDAD AÉREA AVANZADA Y SUS RIESGOS PARA LA SEGURIDAD DE LA AVIACIÓN

(Nota presentada por Arabia Saudita)

RESUMEN

La movilidad aérea avanzada (AAM) y las tecnologías emergentes, como los sistemas de aeronaves no tripuladas (UAS), la movilidad aérea urbana (UAM) y los vehículos aéreos avanzados, han revolucionado la industria de la aviación. Sin embargo, estos adelantos plantean importantes dificultades para la seguridad de la aviación, incluidas las amenazas derivadas del acceso no autorizado, los ciberataques y el posible uso indebido por parte de terroristas. La presente nota examina los riesgos asociados con la movilidad aérea avanzada, evalúa el marco actual de seguridad de la aviación y destaca la necesidad de que la OACI proporcione textos de orientación para ayudar a los Estados contratantes a proteger la aviación y establecer requisitos nacionales.

Decisión de la Asamblea: Se invita a la Asamblea a:

- Tomar nota de la información aquí presentada;
- Alentar a los Estados contratantes a compartir con la Secretaría cualquier información o experiencia que pueda servir para establecer una base de datos de referencia que ayude al Grupo Experto en Seguridad de la Aviación a formular un marco reglamentario y proporcionar orientación a los Estados contratantes con un enfoque proactivo para hacer frente a los riesgos que posibilite la integración segura de la AAM en los sistemas de aviación existentes. (En esta nota se incluye una propuesta de orientaciones y mejores prácticas para la seguridad de las operaciones de AAM).
- Alentar a los Estados contratantes a colaborar con las partes interesadas locales para implementar medidas de seguridad a medida y promover la inversión en tecnologías tales como las soluciones avanzadas de gestión del tránsito de drones, las herramientas de ciberseguridad para proteger sistemas interconectados y el intercambio de información sobre amenazas con otros Estados.

<i>Objetivos estratégicos:</i>	Esta nota de estudio está relacionada con el objetivo estratégico: <i>Todos los vuelos son seguros y protegidos.</i>
<i>Repercusiones financieras:</i>	
<i>Referencias:</i>	Anexo 17 — <i>Seguridad de la aviación</i> <i>Manual de seguridad de la aviación</i> (Doc 8973) de la OACI

¹ Versiones en inglés y árabe proporcionadas por Arabia Saudita.

1. INTRODUCCIÓN

1.1 El concepto de Movilidad Aérea Avanzada (AAM) se está expandiendo rápidamente, impulsado por los avances tecnológicos. Si bien brinda oportunidades de crecimiento, también trae consigo nuevos riesgos y posibles vulnerabilidades que reconfiguran el cuadro de amenazas dentro de la red de aviación civil. Estos riesgos requieren un enfoque proactivo de los organismos internacionales de reglamentación como la OACI a fin de salvaguardar la seguridad operacional y la protección de la aviación a escala mundial. En la presente nota se analizan las implicaciones de la AAM para la seguridad de la aviación, se individualizan los riesgos emergentes y se proponen medidas que tanto la OACI como sus Estados contratantes pueden tomar para darles respuesta.

1.2 La movilidad aérea avanzada se refiere al movimiento de público pasajero y carga a través de varios medios de transporte aéreo, incluidos los sistemas de aeronaves no tripuladas (UAS), las plataformas de movilidad aérea urbana (UAM) y los vehículos eléctricos de despegue y aterrizaje vertical (eVTOL).

2. ANÁLISIS

2.1 Si bien la AAM representa un gran avance, también plantea nuevas dificultades en materia de seguridad de la aviación. Por lo tanto, es primordial formular un enfoque de seguridad integrado que considere los riesgos potenciales y proteja el ecosistema de la aviación contra las amenazas que surgen de esta evolución tecnológica. Entre estos riesgos pueden citarse los siguientes:

- a) Acceso no autorizado y amenazas internas:
 - 1. El aumento de las operaciones de UAS y UAM crea vulnerabilidades en las zonas restringidas de los aeropuertos y las trayectorias de vuelo.
 - 2. Los sistemas de movilidad aérea avanzada podrían ser utilizados para interferencias ilícitas.
- b) Amenazas de ciberseguridad:
 - 1. La integración de sistemas digitales y automatización en la UAM aumenta la vulnerabilidad a ciberataques.
 - 2. Los elementos terroristas podrían comprometer los sistemas de navegación, las redes de comunicación o los datos operacionales.
- c) Uso indebido de los sistemas de AAM:
 - 1. Los sistemas de AAM podrían utilizarse para operativos de vigilancia, contrabando o transporte de explosivos.
 - 2. Los incidentes que afecten a sistemas de movilidad aérea avanzada cerca de los aeropuertos podrían interrumpir el tránsito aéreo y crear riesgos de colisión.

2.2 MARCO JURÍDICO ACTUAL PARA LA SEGURIDAD DE LA AVIACIÓN

2.2.1 El Anexo 17 establece las normas internacionales para la protección de la aviación civil contra los actos de interferencia ilícita. Sin embargo, el rápido desarrollo de la AAM exige que se las actualice para dar cuenta de la integración de los vehículos autónomos y no tripulados y las operaciones aéreas a baja altitud.

2.2.2 Algunos Estados han elaborado sus propios marcos jurídicos para el uso de drones y UAS. Sin embargo, estas políticas a menudo carecen de armonización con las normas internacionales, lo que da lugar a incoherencias.

2.3 COOPERACIÓN INTERNACIONAL ENTRE LOS ESTADOS CONTRATANTES

2.3.1 Intercambio de datos: Facilitar el intercambio oportuno de información de seguridad entre los Estados.

2.3.2 Talleres conjuntos: Realización de ejercicios coordinados y sesiones de instrucción para tratar los riesgos de la movilidad aérea avanzada.

2.3.3 Iniciativas de normalización: Armonización internacional de la reglamentación que rige las operaciones de movilidad aérea avanzada.

2.4 ORIENTACIÓN Y MEJORES PRÁCTICAS PARA LA SEGURIDAD DE LAS OPERACIONES DE AAM

2.4.1 Esta nota de estudio incluye un apéndice con orientación para los Estados contratantes con el fin de hacer más seguras las operaciones de la AAM emergente, incluida la movilidad aérea urbana (UAM), los servicios de reparto y transporte de carga con drones y los sistemas de aeronaves no tripuladas (UAS), de conformidad con el Anexo 17 y el Doc 8973 de la OACI.

— — — — —

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.

A42-WP/200
EX/92
Apéndice
En inglés y árabe únicamente

— FIN —