



ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 13 : Sécurité de l'aviation — Politique

LA MOBILITÉ AÉRIENNE AVANCÉE ET LES RISQUES QU'ELLE FAIT PESER SUR LA SÛRETÉ DE L'AVIATION

(Note présentée par l'Arabie saoudite)

RÉSUMÉ ANALYTIQUE

La mobilité aérienne avancée (AAM) et les technologies nouvelles telles que les systèmes d'aéronef non habité (UAS), les systèmes de mobilité aérienne urbaine (UAM) et les véhicules aériens avancés ont révolutionné le secteur de l'aviation. Cependant, ces innovations posent des défis importants à la sûreté de l'aviation, comme les menaces que présentent un accès non autorisé, les cyberattaques et une utilisation malveillante dans un but terroriste. La présente note passe en revue les risques associés à la mobilité aérienne avancée, évalue le cadre actuel de la sûreté de l'aviation et souligne la nécessité pour l'OACI de fournir des éléments indicatifs pour aider les États contractants à assurer la sûreté de l'aviation et à établir des critères nationaux.

Suite à donner : L'Assemblée est invitée à :

- prendre note de la teneur de la présente note ;
- encourager les États contractants à faire part au Secrétariat de toute information utile ou de leur expérience afin d'établir une base de données de référence qui aidera le Groupe d'experts de la sûreté de l'aviation à élaborer un cadre réglementaire et à fournir des orientations aux États contractants, en les fondant sur une approche proactive de gestion des risques, en vue d'assurer une intégration sûre de l'AAM dans les systèmes d'aviation existants. (La note de travail comprend une proposition de lignes directrices et de meilleures pratiques pour assurer la sûreté des opérations de mobilité aérienne avancée) ;
- encourager les États contractants à collaborer avec les acteurs locaux pour mettre en œuvre des mesures de sûreté adaptées et promouvoir l'investissement dans des technologies telles que les solutions avancées de gestion du trafic de drones, les outils de cybersécurité pour protéger les systèmes interconnectés et la mise en commun avec les autres États d'informations sur les menaces.

<i>Objectifs stratégiques :</i>	La présente note de travail se rapporte à l'objectif stratégique <i>Chaque vol est sûr et sécurisé.</i>
<i>Incidences financières :</i>	
<i>Références :</i>	Annexe 17 – <i>Sûreté de l'aviation</i> Doc 8973 de l'OACI, <i>Manuel de sûreté de l'aviation</i>

¹ Versions anglaise et arabe fournies par l'Arabie saoudite.

1. INTRODUCTION

1.1 Le concept de mobilité aérienne avancée (AAM) se développe rapidement, sous l'impulsion des progrès technologiques. Bien qu'elle offre des possibilités de croissance, l'AAM est aussi source de nouveaux risques de sûreté et de vulnérabilités potentielles, et vient modifier le contexte de la menace du réseau de l'aviation civile. Pour faire face à ces risques, les organismes de réglementation internationaux tels que l'OACI doivent agir en amont pour assurer la sécurité et la sûreté de l'aviation mondiale. La présente note examine les conséquences de l'AAM pour la sûreté de l'aviation, recense les risques émergents et propose des mesures que l'OACI et ses États contractants peuvent prendre pour relever ces défis.

1.2 La mobilité aérienne avancée fait référence au déplacement de passagers et à l'acheminement de marchandises par divers moyens de transport aérien, comme les systèmes d'aéronef non habité (UAS), les plateformes de mobilité aérienne urbaine (UAM) et les véhicules électriques à décollage et atterrissage verticaux (électro-ADAV).

2. ANALYSE

2.1 Si l'AAM représente une avancée majeure dans le domaine de l'aviation, elle pose aussi de nouveaux défis en matière de sûreté. Il est donc essentiel d'élaborer une approche intégrée de la sûreté qui tienne compte des risques et assure la protection de l'écosystème de l'aviation contre les menaces nouvelles émanant de cette évolution technologique. Ces risques sont :

- a) l'accès non autorisé et les menaces internes :
 - 1) la hausse du nombre d'opérations d'UAS et d'UAM expose les zones des aéroports à accès réglementé et les trajectoires de vol à des vulnérabilités ;
 - 2) les systèmes de mobilité aérienne avancée pourraient être exploités à des fins d'intervention illicite ;
- b) les menaces pour la cybersécurité :
 - 1) l'intégration de systèmes numériques et de l'automatisation dans le domaine de l'UAM augmente l'exposition aux risques de cyberattaque ;
 - 2) les terroristes pourraient compromettre les systèmes de navigation, les réseaux de communication ou les données opérationnelles ;
- c) l'utilisation malveillante des systèmes d'AAM :
 - 1) les systèmes d'AAM pourraient être utilisés à des fins de surveillance, de contrebande, ou de transport d'explosifs ;
 - 2) les incidents impliquant des systèmes de mobilité aérienne avancée évoluant à proximité d'un aéroport pourraient perturber le trafic aérien et présenter des risques de collision.

2.2 CADRE JURIDIQUE ACTUEL POUR LA SÛRETÉ DE L'AVIATION

2.2.1 L'Annexe 17 énonce les normes internationales de protection de l'aviation civile contre les actes d'intervention illicite. Cependant, compte tenu de l'évolution rapide de l'AAM, des mises à jour s'imposent pour tenir compte de l'intégration des véhicules non habités et autonomes et des vols effectués à basse altitude.

2.2.2 Certains États ont élaboré des cadres juridiques individuels pour réglementer l'utilisation de drones et d'UAS. Toutefois, il arrive souvent que ces politiques ne soient pas harmonisées avec les normes internationales, ce qui entraîne des incohérences.

2.3 COOPÉRATION INTERNATIONALE ENTRE LES ÉTATS CONTRACTANTS

2.3.1 Mise en commun des données : faciliter l'échange rapide entre les États de renseignements relatifs à la sûreté.

2.3.2 Ateliers conjoints : mener des exercices et des séances de formation coordonnés pour aborder les risques liés à la mobilité aérienne avancée.

2.3.3 Efforts de normalisation : harmoniser les réglementations relatives aux opérations de mobilité aérienne avancée à l'échelle internationale.

2.4 CONSEILS ET BONNES PRATIQUES POUR ASSURER LA SÛRETÉ DES OPÉRATIONS D'AAM

2.4.1 L'appendice à la présente note comporte des conseils à l'intention des États contractants pour assurer la sûreté des opérations d'AAM menées à l'aide de technologies émergentes, comme les systèmes de mobilité aérienne urbaine (UAM), les services de livraison et de transport de fret par drone (les systèmes d'aéronef télépiloté, ou « RPAS »), et les aéronefs autonomes (les systèmes d'aéronef non habité, ou « UAS »), conformément à l'Annexe 17 et au Doc 8973 de l'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.