ICAO

SAFE SKIES.
SUSTAINABLE FUTURE.

Workshop on Unmanned Aircraft System Integration in National and High Seas Airspace (AVSEC Session)

Ross Lockie, Regional Officer AVSEC & FAL

4-6 November 2025

ICAO

AVSECP/36

- Forty-four (44) working papers
- Nine (9) information papers

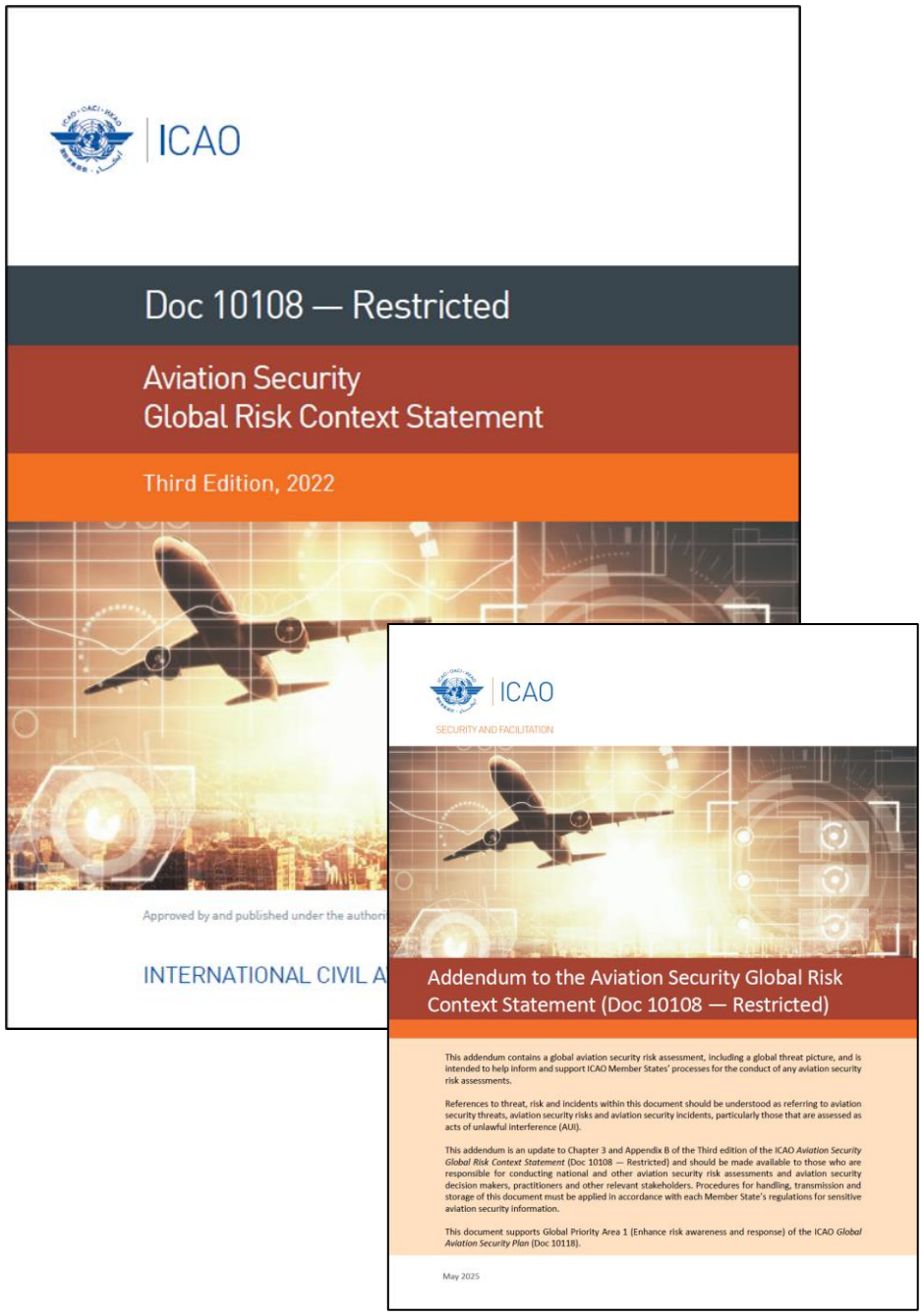
- Meeting held from **7 to 11 April 2025** (hybrid meeting)
- 32 Panel Members
- 219 participants from:
  - 66 Member States
  - 13 International Organizations
  - 45 ICAO staff, all Regional Offices represented
- **Chairperson**
  - Mr. Hamad S. Al Muhairi, Nominated by the United Arab Emirates
- **Vice-Chairperson**
  - Mr. Ricardo Fernandes, Nominated by Portugal

Update on UAS/AAM during AVSECP36

Evolving and emerging threats and vulnerabilities

Regulatory framework for UAS / AAM operations including security requirements

Need for additional information AND guidance from States and Industry



Risks identified:

- Attacks using cargo and mail consignments
- Attacks at a distance, especially in conflict zones
- **Attacks using unmanned aircraft systems (UAS)**
- Threat posed by insiders
- Violent extremism, which may include politically motivated acts
- Cyber-attacks
- Acts attributed to unrest and attacks in, or near, conflict zones
- Attacks at airport landside areas
- Communication of false information

Risks under in-depth assessment:

- Liquids, Aerosols and Gels (LAGs)
- Cargo and Mail
- Artificial Intelligence (AI)

UAS Security Risk Assessment

Likelihood

- Smaller UA are easily obtained and widely used. Their purchase and use would not attract suspicion
- Attack planning on civilian targets has been reported in a number of States
- Examples of disruption caused by the use of small UAS around airports has revealed the ease with which incursions can occur
- The capability and ease of use of small and medium-size drones have also increased rapidly over recent years
- There is increasing terrorist interest in using biological and chemical agents

Consequence

- The larger the aircraft, the greater the potential for structural damage caused by explosion, or collision

Vulnerability

- The inherent difficulty in preventing the acquisition
- Malicious use of UAS devices
- The increasing range and payload of UAS
- The limited ability to track and prevent use near airports

ICAO

Risk assessment by the WGTR

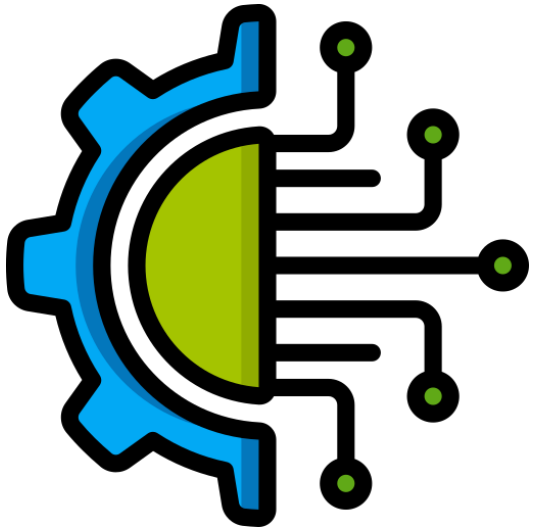
ATTACKS USING UNMANNED AIRCRAFT SYSTEMS

Attacks using smaller UAS on aviation targets are relatively limited in their destructive power because of the short range and small payload of such devices, and larger and military-grade UAS are more difficult to acquire. However, due to developments in technology, there is a growing market for medium-sized UAS, which could put systems with a range of hundreds of kilometers and capable of transporting payloads of a few kilogrammes within reach of perpetrators.

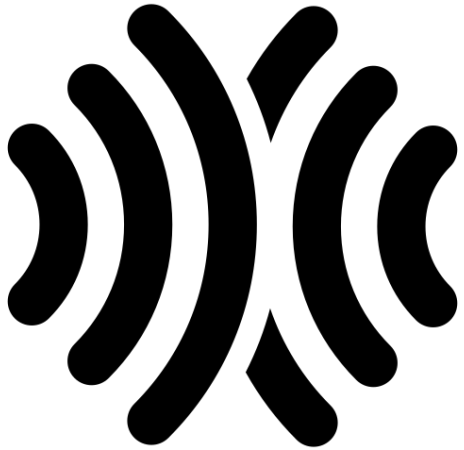
Likelihood	Consequence	Residual Vulnerability	Residual Risk	Trend
MEDIUM-HIGH	**HIGH**	**MEDIUM-HIGH**	**MEDIUM-HIGH**	▬

Mitigation: Measures include surveillance of areas around airports that may serve as launch sites, response and resilience plans, regulatory systems (for example, licensing and registration), technical solutions, awareness of all actors operating at the airport.

Counter UAS technologies



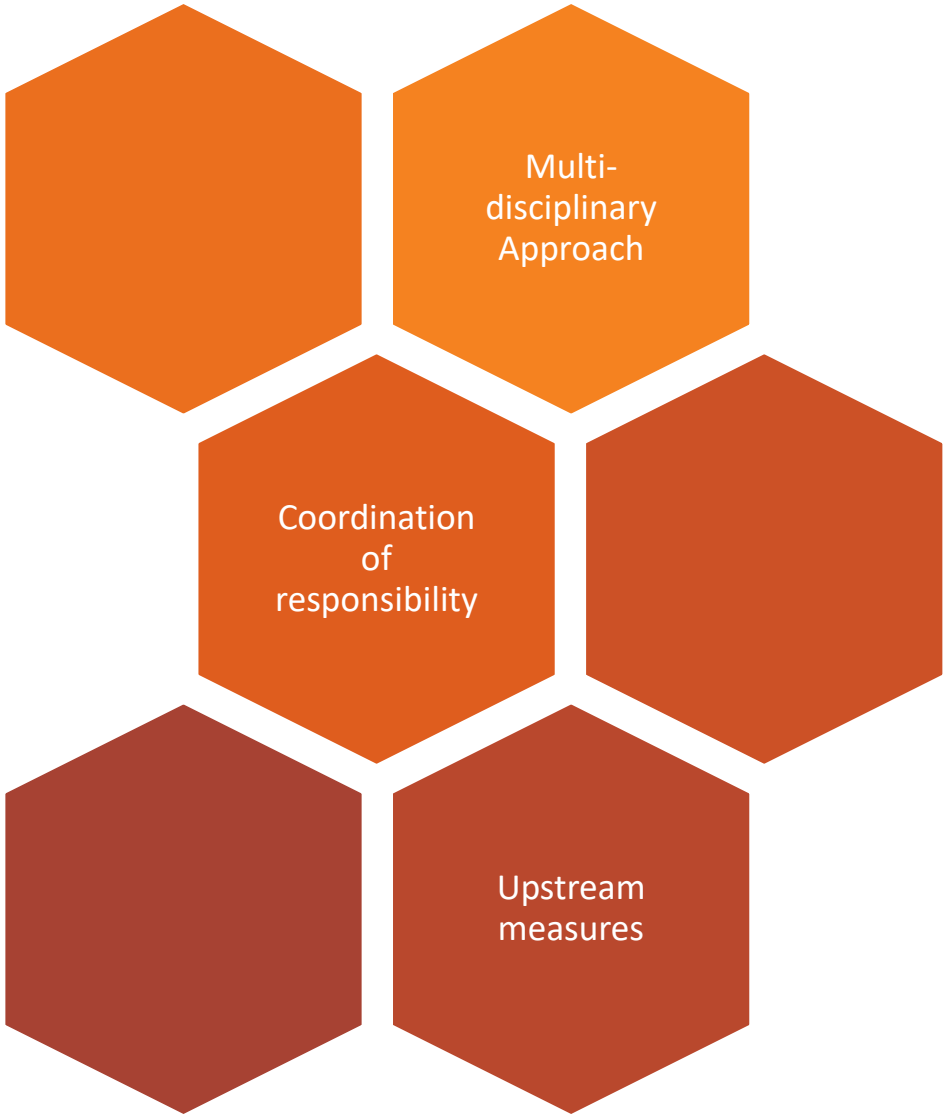
Technologies

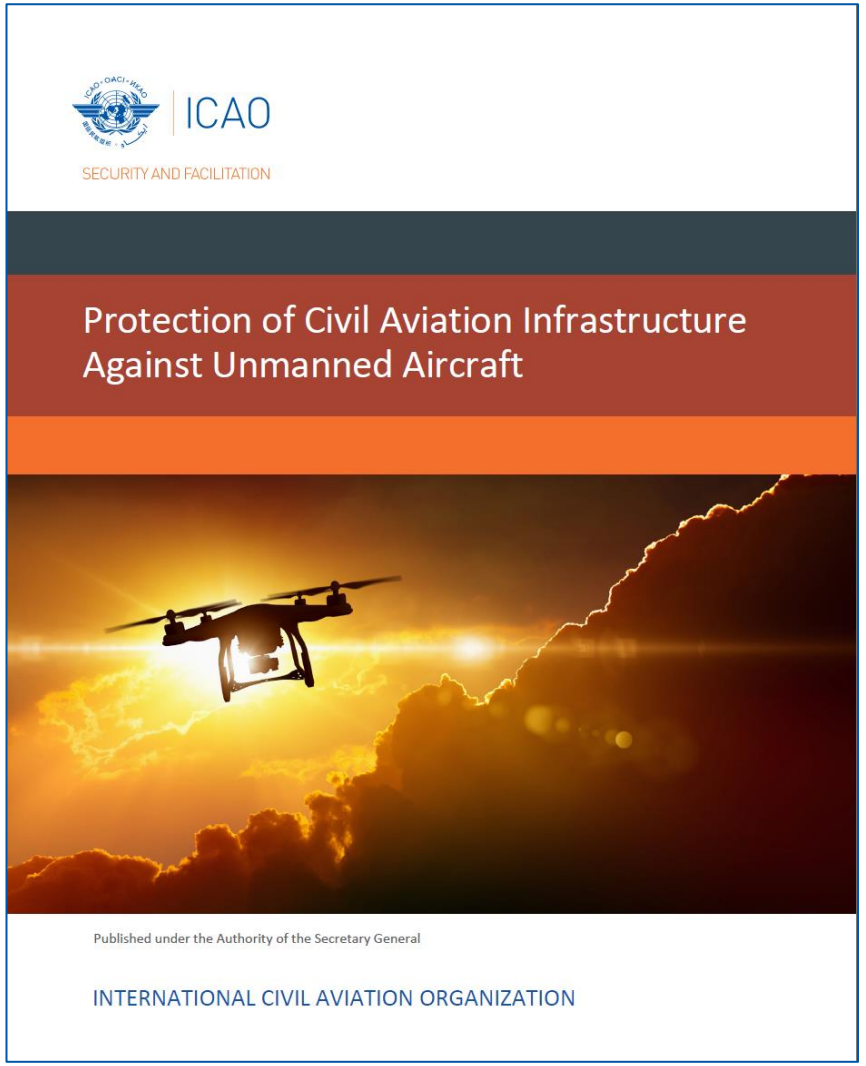


Impacts and interferences

Legal compliance

Preparedness and incident response





Protection of aviation infrastructure

- Multidisciplinary approach
- Coordination of responsibilities
- Prevention thru regulatory systems i.e. licensing and registration
- Application of technical solutions to disrupt UAS in flight
- Raising of public awareness
- Conducting the surveillance of areas surrounding airports that may serve as potential launch sites
- Development of response plans to mitigate risk by controlled evacuation
- Development of resilience plans to enable services to be restored in the event of disruption
- No universal effective technical counter-UAS technology

Preparedness and incident response

AAM Symposium - AAM Security Session

Key outcomes

- A wide range of challenges to cover
- Role of Infrastructure
- Coordination with all relevant authorities, especially international operations
- Same methodologies but different tools and results

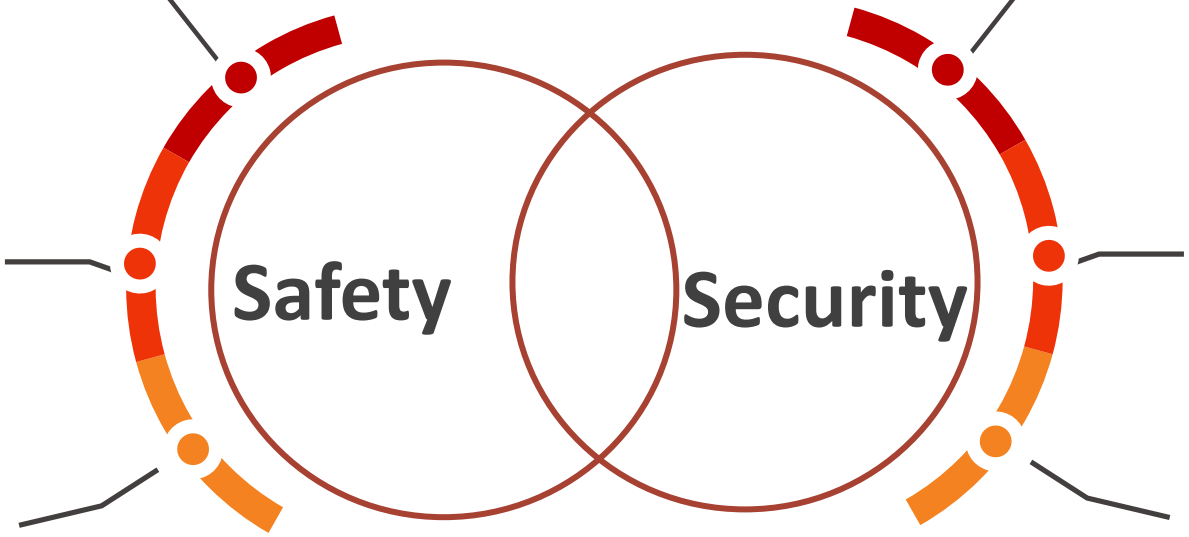
Summary of UAS frameworks
Focus on Security

ICAO Annexes

ICAO Model UAS Regulations

Advisory Circulars

UAS Toolkit



Aviation Security Global Risk Context Statement (Doc 10108, Restricted)

The ICAO Aviation Security Manual(Doc 8973 – Restricted)

Protection of Civil Aviation Infrastructure Against Unmanned Aircraft

UNSCR 2341 (2017), 2370 (2017), 2396 (2017), 2617 (2021)

Abu Dhabi Guiding Principles

Aviation Security Provisions and Guidance Bundle

The ICAO initiative to bring updated security guidance to the people who need it, when they need it.

Why?

To establishing a one stop shop for security publications (cybersecurity included) in ICAO while ensuring protection of sensitive information.

Because ICAO-NET and Secure Portals are not widely available

What documents?

- Annex 17, GASEP, Doc 8973, 10108, 10184, 10207, standalone guidance, public and restricted.
- In French, English and Spanish

Who has access?

- Everyone with a need to know
- Free of charge for “States”
- 1350 USD per year for all security documents in 3 languages

Aviation Security Provisions and Guidance Bundle

How often is it updated ?

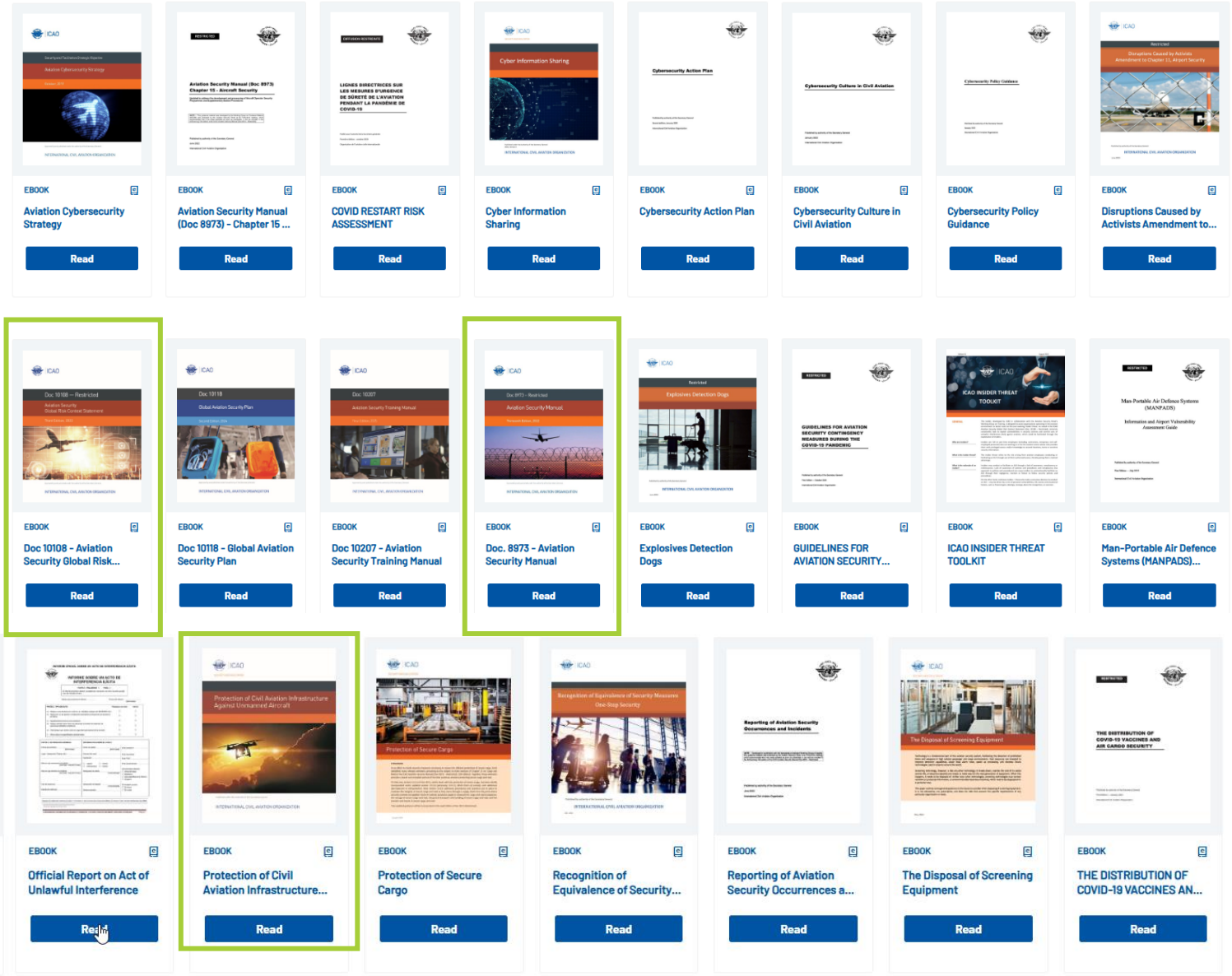
As soon as a guidance is published, it is available in the Bundle

Subscriptions :

https://store.icao.int/en/aviation-security-provisions-guidance

Questions ?

asp@icao.int



Thank You

ICAO80