International Civil Aviation Organization
CAR/SAM Regional Planning and Implementation Group (GREPECAS)

WORKING PAPER

ePPRC/03 — WP/11
15/07/21

GREPECAS Programmes and Projects Committee (PPRC) Third Virtual Meeting (ePPRC/03)
Online, 22 – 23 July 2021

Agenda Item 4: Other Business

EMERGENT TECHNOLOGIES ANALYSIS AND AVIATION CHALLENGES

(Presented by the Secretariat)

EXECUTIVE SUMMARY

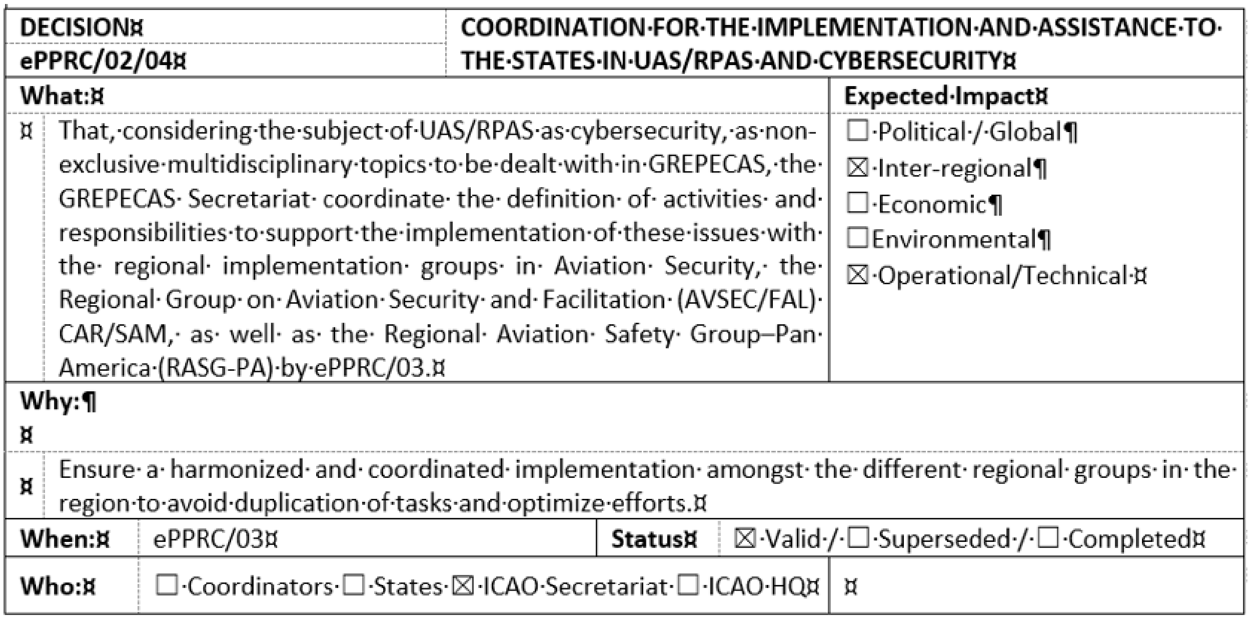
This working paper presents information providing follow-up in Decision eCRPP/02/04 in which the guidelines to assists the States in Unmanned Aircraft Systems (UAS) and cybersecurity matters are requested.

Action:	Suggested actions are presented in Section 4.
Strategic Objectives:	• Air Navigation Capacity and Efficiency • Economic Development of Air Transport • Environmental Protection
References:	• GREPECAS Programmes and Projects Review Committee (PPRC) Second Virtual Meeting (ePPRC/02), October 2020

1. Introduction

1.1 During the GREPECAS Programmes and Projects Review Committee (PPRC) Second Virtual Meeting (ePPRC/02), in October 2020, emergent technologies like operations of Unmanned Aircraft Systems (UAS) and new aviation cybersecurity challenges that States must face in its operations were discussed. The need that States must be prepared to face both challenges in a timely manner was identified.

1.2 In attention to Decision eCRPP/02/04 “coordination for the implementation and assistance to States in UAS/RPAS and cybersecurity”, in the outcome of the analysis of this matter was considered the need to define the activities and responsibilities to support the States in the development of these activities.



DECISION **ePPRC/02/04**	**COORDINATION FOR THE IMPLEMENTATION AND ASSISTANCE TO THE STATES IN UAS/RPAS AND CYBERSECURITY**		
What:			**Expected Impact**
That, considering the subject of UAS/RPAS as cybersecurity, as non-exclusive multidisciplinary topics to be dealt with in GREPECAS, the GREPECAS Secretariat coordinate the definition of activities and responsibilities to support the implementation of these issues with the regional implementation groups in Aviation Security, the Regional Group on Aviation Security and Facilitation (AVSEC/FAL) CAR/SAM, as well as the Regional Aviation Safety Group–Pan America (RASG-PA) by ePPRC/03.			☐ Political / Global ☒ Inter-regional ☐ Economic ☐Environmental ☒ Operational/Technical
Why:			
Ensure a harmonized and coordinated implementation amongst the different regional groups in the region to avoid duplication of tasks and optimize efforts.			
When:	ePPRC/03	**Status**	☒ Valid / ☐ Superseded / ☐ Completed
Who:	☐ Coordinators ☐ States ☒ ICAO Secretariat ☐ ICAO HQ		

1.3 In this regard, an analysis of the impact that the unmanned aircraft operations and the challenges on the traffic control operations regarding cybersecurity and the responsibility of the Working Groups that support the regional implementation tasks.

2. Analysis

Unmanned aircraft systems and Remote piloted aircraft system (UAS/RPAS

2.1 UAS UAS are increasingly used around the world to support emergency and rescue missions, urban fires, wildfires, floods, earthquakes, operations with UAS assist firefighters, police, paramedics/medics, and during pandemic of COVID-19 have seen its applications in many other activities, from socialization, sanitation, shipment of supplies and medicines, etc.

2.2 Operations with unmanned aircrafts and services that they provide are exponentially growing and one fundamental concern is that States are not prepared for these operations and their implications. One of the biggest challenges that the States are facing is the establishment of a regulatory frame for the UAS operations that are integrated in the civil aviation State regulation, specially the establishment between the regulations and the requirements of the RPAS and UAS operations, and the preparation and development of the capacity of national inspectors.

2.3 ICAO has developed a series of documentation to support the States in the development process or their regulations, procedures among other tools, for the integration of these operations in their airspace. This documentation will support the States in the establishment of harmonization in the development of their regulation, the establishment of security for the integration of unmanned aircraft systems operations and, overall, to establish the documentation on how the States must address this issue and, in line with ICAO documentation, integrate the requirements and regulations for its operations.

2.4 ICAO has established the following documentation for unmanned aircraft systems opeations:

1. Categorization

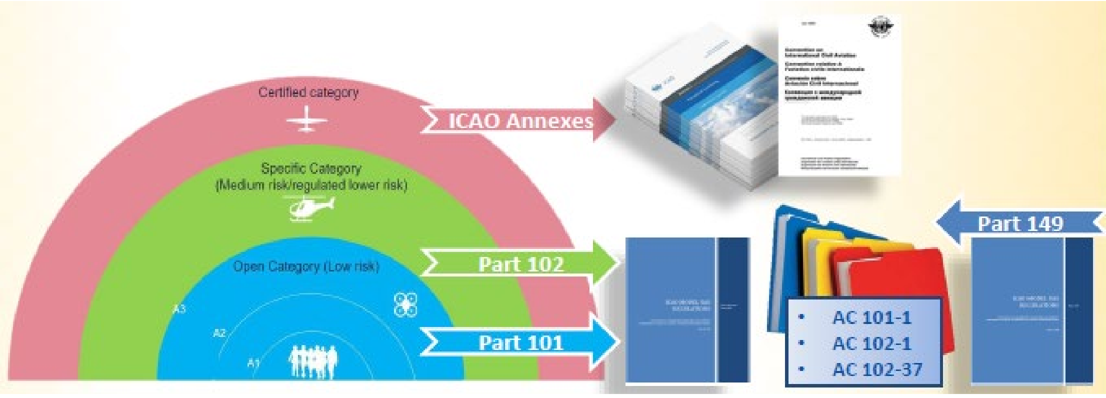
a. Open category and specific categories: ICAO Model for the regulation of UAS Part-1 and Part-2, which is an example for ICAO Member States to establish a regulation for unmanned aircraft operations. Document under the following link: https://www.icao.int/safety/UA/Documents/Final%20Model%20UAS%20Regulations3%20-%20Parts%20101%20and%20102.pdf

b. Certified category: All ICAO annexes apply.

c. Aviation Organization Approval (AAO): For unmanned aircraft operators, example for regulation development: ICAO Model for UAS Part-149 regulation: https://www.icao.int/safety/UA/Documents/Final%20Model%20UAS%20Regulations3%20-%20Part%20149.pdf

d. In addition to information and guides that ICAO has developed to support States in dealing with the operation of unmanned aircraft due to the diversity of applications.

ICAO regulatory model for unmanned aircrafts



2.5 In the case of the certified aircrafts category, the here-under requirements are followed in accordance with the ICAO Annexes.

2.6 **Appendix A** to this working paper presents the requirements to take into consideration for unmanned aircrafts operations. All the ICAO annexes are affected by this operations, that is why at the moment of development of national regulation, procedures and other documents, these requirements must be integrated and its applicability analysed according with the type of operation.

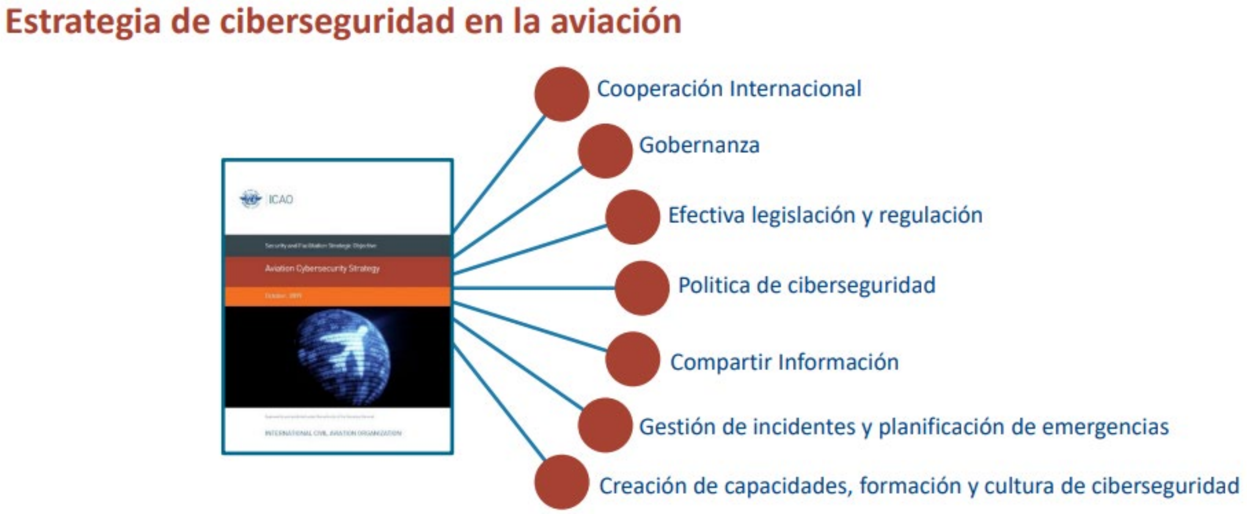
1. Air navigation services: AIM, AGA, ATS, CNS y MET ***(GREPECAS)***
2. Security and facilitation ***(AVSEC/FAL)***
3. Safety ***(RASG-PA)***

Ciberseguridad

2.7 Technology and cyber systems have become essential for modern society, we depend even more on technology, which provide greater efficiency to all activities that are carried out day to day. Along with the benefit of cyber technologies, insecurities arise that affect all systems and infrastructures. Cyber-threat and cyber-attack have a transnational component and effect, as global systems are interconnected. Furthermore, the complexity of the action has implications for various actors at the national, regional and international levels.

2.8 The Aviation Cybersecurity Strategy developed by ICAO indicates that the civil aviation sector is increasingly dependent on the availability of information and communication technology systems, as well as the integrity and confidentiality of data. The threat of potential cyber incidents to civil aviation is constantly evolving, with perpetrators acting maliciously to disrupt operations and steal information for political, financial and other reasons.

2.9 ICAO's cybersecurity strategy establishes seven important pillars for cybersecurity implementation:


Estrategia de ciberseguridad en la aviación
ICAO
Aviation Cybersecurity Strategy
Cooperación Internacional
Gobernanza
Efectiva legislación y regulación
Politica de ciberseguridad
Compartir Información
Gestión de incidentes y planificación de emergencias
Creación de capacidades, formación y cultura de ciberseguridad

2.10 The ICAO Cybersecurity Strategy can be found under the following link: https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.SP.pdf

2.11 Resolution A40-10: Ways to address cybersecurity in civil aviation as a result of ICAO Assembly 40 urges States and Industry to adopt the following measures to counter cyber-threats to civil aviation:

a) implement the cybersecurity strategy;
b) identify the threats and risks of potential cybersecurity incidents in critical civil aviation operations and systems and the serious consequences that may result from such incidents;
c) define the responsibilities of national bodies and industry stakeholders with regard to cybersecurity in civil aviation;
d) promote a common understanding among Member States of cyber threats and risks and the formulation of common criteria to determine which assets and systems are critical and must be protected;
e) promote coordination between government and industry regarding aviation cybersecurity strategies, policies and plans, as well as the exchange of information to help identify critical vulnerabilities that need to be addressed;
f) form and participate in associations and mechanisms between government and industry, nationally and internationally, to systematically share information on cyber threats, incidents, trends and mitigation actions;

g) based on a common understanding of cyber threats and risks, adopt a flexible and risk-based approach to protect critical aviation systems through the implementation of cybersecurity management systems;
h) foster a strong cybersecurity culture in all aspects within national agencies and throughout the aviation sector;
i) promote the development and application of international standards, strategies and best practices to protect critical information and communication technology systems used in civil aviation from interference that may threaten the safety of civil aviation;
j) establish policies and allocate resources where necessary to ensure that critical aviation systems have an architecture designed to be secure; that are resilient; that have secure data transfer methods that guarantee its integrity and confidentiality; that they have methods of surveillance, detection and reporting of incidents and that forensic analysis of incidents are carried out; and
k) collaborate in the development of the ICAO cybersecurity framework adopting a horizontal, inter-sectoral and functional approach that integrates air navigation, communications, surveillance, aircraft operations, airworthiness and other relevant disciplines.

2.12 Air Navigation operations are supported by state-of-the-art technology, both at the level of the equipment on the ground and the avionics on board the aircraft. Facilities such as aeronautical information exchange, automated protocols between control centres, ATFM, A-CDM, among others, require that the data have quality, availability and certification measures, this information is the basis for decision-making in real time.

2.13 Our sector includes airspace users, air navigation providers, airport operators, civil aviation authorities and equipment manufacturers, among others. In this sense, it is necessary to carry out an analysis of the aviation system integrating all the interested parties that are part of the system.

2.14 Cybersecurity requires a holistic approach. The interfaces between aviation security components deserve special attention, such as air traffic management (ATM) security, the security of Communication, Navigation and Surveillance (CNS) components and operations. (ADS-B, GNSS, data Link), and airspace security and airport security. Air traffic management security must be an integral part of the aviation security system. **Appendix B** provides information on the applicability of the documentation available to begin risk analysis and cybersecurity work for air traffic control operations. All areas of aviation can be affected by cyber-attacks.

3. Conclusions

3.1 For unmanned aircraft operations and for cybersecurity challenges, is required a joint work of all areas of the Civil Aviation system, integrating both internal areas and parts of the system, as well as stakeholders external to civil aviation operations.

3.2 The challenges we face as States and as a region cannot wait:

— — — — — — — — — — — —

- Every day we have more unmanned aircraft flying, new services emerging, technology in constant development providing new aircraft and operations that must be regulated to ensure efficient and safe airspace.
- Cyber-attacks have been increasing in recent years, aviation did not think that it could be a target of this type of threats, but the use of cutting-edge technology, regional and global interconnectivity, as well as other interests make our sector vulnerable to this threat.

3.3 Both challenges cannot be worked on in isolation by the aviation sectors, both require a job that includes all the disciplines of aviation and require seeing the system as a whole and not by parts.

4. Suggested actions

4.1 States are invited to:

a) take note of the information presented in this working paper;

b) consider adopting multidisciplinary approaches to work on both challenges;

c) the adoption of tasks according to the regional working groups; and

d) any other activity that applies.

— — — — — — — — — — —

APPENDIX A
Provisions of the ICAO Annexes for the operation of Unmanned Aircraft}

Annexes	Provisions	Area
Annex 1: Personnel licenses	Remote pilot licenses	*Safety (SAF)*
Annex 2: Rules of the Air	General rules and additional documentation under development.	*Air Navigation (ATM)*
Annex 3: Meteorological services for international air navigation	Requirements for operations	*Air Navigation (MET)*
Annex 4: Aeronautical charts	Requirements for operations	*Air Navigation (AIM)*
Annex 5: Units of measurement to be used in air and land operations.	To be determined	*Air Navigation (AIM)*
Annex 6: Aircraft operations	New volume in development	*Safety (SAF)*
Annex 7: Aircraft nationality and registration marks	Unmanned aircraft registration and marking	*Air Navigation (AIM)*
Annex 8: Airworthiness	Requirements according to the type of aircraft	*Safety (SAF)*
Annex 9: Facilitation	Entry and take-off of aircraft and transport operations	*Security and facilitation (AVSEC/FAL)*
Annex 10: Aeronautical Telecommunications	New volume under development for links required for unmanned aircraft operations	*Air Navigation (CNS)*
Annex 11: Air Traffic Services	Provisions for unmanned aircraft operations	*Air Navigation (ATM)*
Annex 12: Search and Rescue	According to the operations and type of aircraft	*Air Navigation (ATM)*
Annex 13: Aviation Accident and Incident Investigation	Requirements for unmanned aircraft operations	*Safety (SAF)*
Annex 14: Aerodromes	Requirements for unmanned aircraft operations	*Air Navigation (AGA)*
Annex 15: Aeronautical Information Services	Requirements for unmanned aircraft operations	*Air Navigation (AIM)*
Annex 16: Environmental protection	Requirements for unmanned aircraft operations	*Air Navigation (MET)*
Annex 17: Security	Cybersecurity and Physical Security Requirements	*Security and facilitation (AVSEC/FAL)*
Annex 18: Safe transport of dangerous goods by air	Transport of dangerous goods in unmanned aircraft	*Safety (SAF)* *Security and facilitation (AVSEC/FAL)*
Annex 19: Safety management	Risk management and analysis for unmanned aircraft operations	*Air Navigation (AIM, AGA, ATM, CNS, MET)* *Safety (SAF)*

In addition, they apply to UAS / RPAS Operations:

1. Chicago Convention: Article 2, 8, 29, 44.
2. Doc 9859: Operational Safety Management Manual
3. ICAO model for the regulation of unmanned aircraft operations (PART 101, 102, 149).
4. Others according to the operation of unmanned aircraft.

— — — — — — — — — — —

APPENDIX B
ICAO documentation available to States on Cybersecurity

Cybersecurity must interact with other disciplines (security, efficiency) in a similar way to what currently occurs with "traditional" aviation security to ensure accurate assessment of exposure to Cybersecurity threats and ensure the development of cybersecurity strategies. -effective and efficient protection based on risk.

Cybersecurity must build bridges between aviation security and protection, since the multidisciplinary nature of Cybersecurity must benefit from security and protection

Why Cybersecurity in Civil Aviation?

The interconnection and interoperability of digital systems among aviation stakeholders broadens the landscape of cyber threats.

Air navigation areas affected:

1. ***Air navigation***
2. ***Security and facilitation***
3. ***Safety***

Available documentation:

1. Resolution A40-10: Addressing Cybersecurity in civil aviation
2. Cybersecurity policy template for air traffic management.
3. Security Management Manual (SMM) (Doc 9859).
4. ICAO Aviation Security Global Risk Context Statement (Doc 10108)
5. Aviation Security Manual (Doc 8973)
6. Annex 17: Security provisions
7. Safety Manual for Air Traffic Management (Doc 9985)
8. Annex 19; Security management.
9. ICAO Aviation Cybersecurity Strategy
10. CANSO Standard of Excellence in Cybersecurity
11. The ISO/IEC 27000 series comprises information security standards
12. ICAO Cybersecurity Action Plan

— END —