*International Civil Aviation Organization*

**MIDANPIRG/20 and RASG-MID/10 Meetings**

***(Muscat, Oman, 14-17 May 2023)***

**Agenda Item 2.2: Update from States and International Organizations**

# AIRCRAFT NETWORK SYSTEMS CYBER SECURITY

*(Presented by Saudi Arabia)*

## SUMMARY

This paper provides an overview of the transition of aircraft systems and highlights the importance of distinguishing cyber security in aircraft networks from terrestrial IT systems. The paper also identifies several cyber security vulnerabilities that could compromise aircraft safety and discusses current and future aviation authorities' efforts to mitigate cyber security risks.

## REFERENCES

– ICAO Cybersecurity Policy Guidance

– ICAO Aviation Cyber Security Strategy

## 1. INTRODUCTION

1.1 Aircraft manufacturers, avionics/electronics suppliers, and owners/operators are implementing technologies that are convenient to use, cost-effective, and increase connectivity but may also introduce cyber security flaws.

1.2 These flaws can compromise aircraft safety, and while Aircraft Manufacturers and Supplemental Type Certificate (STC) holders develop secure designs and instructions for secure operations, proper implementation of these instructions is essential for achieving aircraft safety.

## 2. DISCUSSION

2.1 The Commercial Aircraft Information Security Concepts of Operation and Process Framework has defined new aircraft systems, which have been separated into three domains by the ARINC 811 standard. The standard is related to Commercial Aircraft Information Security Concepts of Operation and Process Framework which provides a common understanding of information security concepts as they relate to airborne networks, and provides a framework for evaluating the security of airborne networked systems. Aircraft network domains may be directly or indirectly connected to equipment owned by crew or passengers as well as external connections, which could result in vulnerabilities that could be exploited.

2.2 Civil aviation regulatory authorities do not provide sufficient coverage of cybersecurity vulnerabilities due to lack of standards. However, the Federal Aviation Administration (FAA) has established and made public Special Conditions for some systems and aircraft.

2.3 The EASA has amended the rules related to product certification to reduce the potential effects of cybersecurity threats resulting from unauthorized interactions with on-board electronic networks and systems. The EASA Certification Specifications (SC), Acceptable Means of Compliance (AMC), and Guidance Material (GM) are being updated to reflect recent developments in the defense of goods and equipment against cybersecurity threats.

2.4 The ICAO Global Aviation Security Plan (GASeP) recognizes the need for accelerated development of a policy and programming framework for Aviation Security. However, the ICAO Aviation Cybersecurity Strategy and ICAO Annex 17 Standard 4.9.1 and Recommended Practice 4.9.2 do not adequately address aircraft system cyber security.

2.5 In order to meet the expectations of ICAO's Global Aviation Safety Plan (GASP) Aviation Cyber Security be integrated into the Air Carrier's Security Management System (SeMS), and Aviation Cyber threats to all areas of the Air Carrier's Aviation Security, including Aircraft System Security should be also considered. Additionally, it is proposed that aircraft cyber security and aviation security may be integrated and not kept in separate silos.

2.6 In order to ensure the safe and sustainable operation of aircraft, it is necessary to take proactive measures to address potential cyber security threats. One crucial aspect of achieving this goal is to implement a secure Network Design. It is imperative that ICAO Member States comply with the relevant standards and guidelines established by the ICAO regarding Cyber Security Certification. Obtaining information about the certification process and regulations involved in the certification and Initial Airworthiness of new and innovative aviation equipment and vehicles is of paramount importance. This will provide assurance that the highest level of cyber security is maintained and that the aviation industry is adhering to common standards.

2.7 These guidelines should be based on common standards to effectively mitigate the risk level of aircraft safety and security. ICAO to introduce and promote such standards and recommended practices through relevant ICAO documents, including the respective Annexes. By following these standards and guidelines, member states can ensure that aircraft systems are secure and resilient against cyber threats, thereby promoting safe and efficient air travel.

## 3. ACTION BY THE MEETING

3.1 The meeting is invited to note the information in this paper.

- END -