International Civil Aviation Organization

WORKING PAPER

HLCAS/2-WP/27
9/11/18
English only

SECOND HIGH-LEVEL CONFERENCE ON AVIATION SECURITY (HLCAS/2)

Montréal, 29 to 30 November 2018

Agenda Item 2: Future Approaches to Managing Aviation Security Risks

AIRCRAFT DIGITAL PROTECTION – AN INTEGRATED APPROACH

(Presented by the International Air Transport Association)

SUMMARY

The paper presents the International Air Transport Association (IATA) views on the need for the Integrated Risk Management approach to Cyber threats and Risks for aircraft systems.

Action by the High-level Conference on Aviation Security is in paragraph 3.

1. INTRODUCTION

1.1 Public and industry concern around vulnerabilities and risks associated with aviation cyber security continue to escalate. Additionally, state and non-state cyber actors are increasingly demonstrating their interest in targeting civil aviation systems, with intents ranging from proving antagonistic capabilities, stealing data and to disrupt continuity of operations. Their interests also include civil aircraft as noted by paragraph 2.5 of HLCAS/2-WP/6 "Update on Aviation Security Threat and Risk". However, currently, aircraft systems are believed to remain highly resilient against attempted electronic interference. But, potential vulnerabilies are regularly highlighted and regulators and industry must increasingly develop a pro-active, resilient and continuously evolving aviation cyber security posture as aircraft data optimization and connectivity efforts increase.

1.2 IATA has established an aircraft cyber security task force (ACSTF) reporting to the Security Group (SEG), tasked to develop high-level risk-based guidance and best practices for the digital protection of complex aircraft systems. Additionally, the ACSTF leverages existing guidance available to industry, such those published by the European Organization for Civil Aviation Equipment (EUROCAE) Working Group 72 (EU) and Radio Technical Commission for Aeronautics (RTCA) Special Committee (US), to make recommendations for an industry-led approach when addressing cyber-risks associated with the safe operation of aircraft critical systems.

1.3 In connection to the ICAO Annex 17 standard 4.9.1 there are several risk assessment methodologies available for States and Industry to consider and IATA would strongly support the development of an ICAO led cyber security strategy for the aviation industry. However, traditional approaches to Information Technology (IT) vulnerabilities follow a cycle of discovery-exploit-disclosure-patching and as noted by Cooper (2017), *"…corporate IT approaches to cybersecurity tend to have*

higher rates of failure than critical aviation systems would support and may be otherwise ill fit for an aviation environment"[1]. Thus IATA recommends any State or supranational aviation cyber security strategy establish the principals required to manage the interdependent and complex risk vectors that cyber represents. For these principles to have longevity, it is also recommended that they not be tied to technology. Moreover, to be effective in such a globally interconnected industry, any such strategy must also acknowledge and accommodate differing maturity levels in terms of cyber posture as well as regional nuances.

2. DISCUSSION

2.1 The current high-security reliability of aircraft systems has so far been successfully served by security-by-design principals as promulgated by the Aeronautical Radio, Incorporated (ARINC) organization. Aircraft safety critical networks are required to be isolated in order to avoid forms of avionic domain data corruption. Coupled with robust airworthiness security standards during the aircraft design and development cycle, and continued airworthiness outside of design and development[2], today's safety-critical airborne systems are comparatively secure from intentional unauthorized electronic interaction.

2.2 Increasing demand for enhanced connectivity is changing the way in which aircraft are serviced and operated. Real-time aircraft IP connectivity continues to increase and evolve and as a result, the connected aircraft now forms part of the Internet of Things (IoT) attack surface. A critical challenge is that with on-board systems having comparatively long lifecycles and slow software update cycles, keeping ahead of new attack techniques and patching vulnerabilities industry wide regardless of region will be as difficult as it is essential. Additionally, due to the interconnectedness and complexity of aircraft systems, an immediate loss of certified aircraft airworthiness is highly likely in the event of an intentional or unintentional compromise of aircraft safety critical systems.

2.3 Going forward, efforts to be able to quickly assure the integrity and security of aircraft systems will have multiple operational and safety benefits. This all reinforces the requirement for aviation systems to be demonstrably resilient, so that in the event of an unforeseen attack, for example, compromising system segregation, it does not cause a critical failure or loss of consumer confidence. Other safety critical sectors facing complex cyber security challenges have already experienced significant disruption and it is a reasonable assumption that with increased air-to-air, air-to-ground and air-to-space connectivity, that civil aviation may as well.

2.4 Safety systems have previously not had to consider the risk of intentional interference the way in which security systems do. Moving forwards, an integrated risk management approach to safety and security, which incorporates a pro-active assessment of hazards, vulnerabilities and threats is required to ensure information security risks are managed within acceptable levels. States need not impose a new requirement for an Aircraft Information Security Plan on aircraft operators. But rather permit aircraft operators to evolve continued airworthiness controls based on Integrated Risk Management (IRM) models. This will best be done by takings advantage of existing authorised methodologies in Security Management Systems (SeMS), Safety Management Systems (SMS) and the Information Security Management Systems (ISMS).

2.5 With the multiple cyber security challenges faced by the industry, there are two focus areas that IATA consider critical to supporting safe and secure growth for industry. Firstly, in order to

[1] Cooper, P. (2017). Aviation Cybersecurity. Atlantic Council.
[2] EUROCAE ED-203A and EUROCAE ED-204

best minimize systemic cyber risk quickly, responsible disclosure of vulnerabilities, cyber threats and risks and information sharing must be encouraged and supported internationally. Secondly, a vision for a cyber secure aviation industry needs to be agreed at the highest international levels in order to drive coherent, industry-wide improvement, management of cyber risk and resilient trust and systems.

3. ACTION BY THE HIGH-LEVEL CONFERENCE

3.1 The High-level Conference on Aviation Security is invited to:

a) support the establishment of an ICAO Cyber Security Panel, with the responsibility to develop an ICAO cyber security vision and strategy recognizing that security measures to mitigate information security risks include physical and organizational perspectives;

b) promote the development of an Integrated Risk Management (IRM) approach, made up of SeMS and SMS elements, to manage cyber risk to aircraft systems;

c) encourage States and Industry stakeholders to fully comply with the new ICAO Annex 17, Amendment 16 provisions on information sharing, risk assessments, and incident reporting when it comes to cyber security affecting critical aircraft systems; and

d) encourage responsible disclosure and information sharing with National Computer Emergency Response Terms (CERTs) and other relevant organizations, such as the Aviation – Information Sharing Analysis Centre (A-ISAC), for aviation cyber threats, vulnerabilities and risks.

— END —