International Civil Aviation Organization

WORKING PAPER

A39-WP/337
EX/130, TE/145
2/9/16
(Information paper)
English only

ASSEMBLY — 39TH SESSION

EXECUTIVE COMMITTEE AND TECHNICAL COMMISSION

Agenda Item 16: Aviation Security – Policy
Agenda Item 36: Aviation safety and air navigation implementation support

AIRCRAFT CERTIFICATION CYBERSECURITY REGULATORY EFFORTS

(Presented by the United States)

EXECUTIVE SUMMARY

Recent designs for aircraft systems include connectivity to "non-governmental services" such as the internet and use portable electronic devices and commercial-off-the-shelf technologies which are not certified and accredited by a government authority for secure operations. These designs can introduce cybersecurity vulnerabilities beyond the scope of current airworthiness regulations and traditional systems safety assessment methods typically used to show compliance with various airworthiness requirements mandated per Title 14 of the U.S. Code of Federal Regulations. As a result, the Federal Aviation Administration (FAA) applies Special Conditions for airworthiness, which serves as stand-alone rules, for particular aircraft designs to ensure cybersecurity vulnerabilities which could potentially affect critical flight systems and safety are addressed in the safety assessment process, before Type or Supplemental Type Certificates are granted. The FAA-sponsored Aviation Rulemaking and Advisory Committee formed a working group to develop recommendations for Aircraft Systems Information Security Protection (ASISP) rulemaking and/or best practices for aircraft, engines and propellers by August 2016. Using the outputs of this working group, the FAA and the European Aviation Safety Agency (EASA) are working to produce harmonized rule language to address ASISP in place of the current Special Conditions paradigm.

Strategic Objectives:	This information paper relates to the Safety and Security and Facilitation Strategic Objectives.
Financial implications:	This paper has no significant financial implications.
References:	

(4 pages)

1. INTRODUCTION

1.1 Recent designs for aircraft systems include connectivity to non-governmental services on the internet and use portable electronic devices and commercial-off-the-shelf technologies, which are not certified and accredited by a government authority for secure operations. Connecting a non-governmental service to aircraft systems and networks can introduce cybersecurity vulnerabilities beyond the scope of current airworthiness regulations and traditional systems safety assessment methods typically used to show compliance with various airworthiness requirements, as mandated in Title 14 of the U.S. Code of Federal Regulations (CFR). The Federal Aviation Administration (FAA) defines non-governmental services as services not managed by U.S. Federal agencies or their equivalents. The use of these services requires a security risk assessment because the security standards used by these providers vary. Many non-governmental services are public systems using internet protocol (IP) connectivity, and are subject to potential threats from anyone with internet access. Of particular concern is the potential ability to gain unauthorized access to aircraft avionics or networks through IP-connected devices in the flight deck, cabin or during maintenance.

1.2 Without updates to regulations, policy, and guidance to address Aircraft Systems Information Security Protection (ASISP), aircraft vulnerabilities may not be properly identified and mitigated, thus increasing exposure to security threats. Unauthorized access to aircraft systems and networks could result in the malicious use of networks and loss or corruption of data (e.g., software applications, databases, and configuration files) brought about by software worms, viruses, or other malicious entities. In addition, a lack of ASISP-specific regulation, policy, and guidance could result in a lack of standardized and harmonized security related certification criteria between international regulatory authorities.

2. DISCUSSION

2.1 U.S. airworthiness regulations do not specifically define how to address cybersecurity vulnerabilities for any aircraft operating in the U.S. National Airspace System. To address this issue, the FAA issued policy statement, PS-AIR-21.16-02, "*Establishment of Special Conditions for Cyber Security*," which describes when issuance of Special Conditions are required for aircraft systems that directly connect to external/internal services or networks under specific conditions.

2.2 In order to address potential cybersecurity attacks, the FAA publishes Special Conditions addressing this issue as follows: (1) *Isolation or Aircraft Electronic System Security Protection from Unauthorized Internal Access* and, (2) *Aircraft Electronic System Security Protection from Unauthorized External Access*. These Special Conditions address both connectivity to external aircraft access points such as antennas and internal access points such as passenger entertainment systems in order to protect critical systems used for guidance and control of the aircraft.

2.3 The FAA issues Special Conditions when existing airworthiness regulations do not contain adequate safety standards because of novel or unusual design features. Special Conditions are published in the Federal Register as proposed rules for public comment. Since 2005, we have published more than 20 Special Conditions related to cybersecurity on many different transport category airplanes. Examples include several Boeing, Airbus, and Gulfstream model airplanes (e.g., B787, A350, G-VI). The airplane manufacturer, in addition to demonstrating electronic system security design assurance, is also

required to provide instructions for continued airworthiness to the intended operators of the aircraft. These instructions provide information on how to maintain the electronic system security protections throughout the aircraft lifecycle. The operators of these airplanes are required to maintain the continued airworthiness according to the design approval holder's instructions.

2.4 Each Special Condition has a companion issue paper which provides additional information on the means of compliance for ASISP. The Special Conditions and Issue Papers cover regulations, policy, and guidance used to identify and mitigate cybersecurity attacks. The definition of ASISP is broad based and includes any "non-governmental service" electronic interface that could degrade the safety of aircraft operations.

2.5 The AVDEX concept supports community-centric SMS programs. This enables the community to collectively exchange expert knowledge and create a healthier global aviation system, which is especially important for smaller organizations that may not have sufficient data to run a stand-alone SMS program.

2.6 **Committee and Association Support**

2.6.1 Since 2006, the FAA has supported RTCA Inc., Special Committee (SC)-216in coordination with EUROCAE Working Group 72 for Aeronautical Security. This group produced industry documents such as (1) RTCA DO-326A, *Airworthiness Security Process Specification*, which addresses process assurance guidance and requirements for the aircraft design regarding systems information security; (2) RTCA DO-355, *Information Security Guidance for Continuing Airworthiness*, which provides guidance for assuring continued safety of aircraft in service in regard to systems information security; and (3) RTCA DO-356, *Airworthiness Security Methods and Considerations*, which provides analysis and assessment methods for executing the process assurance specified in DO-326A. These documents were created in the context of CFR part 25 regulations for Transport Category Airplanes, which include an approved passenger seating configuration of more than 19 passenger seats.

2.6.2 This guidance was not intended for CFR parts, 23, 27, 29, 33.28, and 35.15 (normal, utility, acrobatic, and commuter category airplanes, normal category rotorcraft, transport category rotorcraft, engines and propellers), or military aircraft without civil type certificates. To address the limitations in the scope of the RTCA documents applicability to certain aircraft types, in 2014 the FAA partnered with the General Aviation Manufacturers Association (GAMA) to create an ad hoc working group. In 2015, the group's activities were moved to the ARAC working sub-group described below.

2.7 **Rulemaking**

2.7.1 In December 2014 the FAA-sponsored Aviation Rulemaking and Advisory Committee (ARAC) established the ASISP working group (WG). The ASISP WG was tasked with providing recommendations on both initial certification and continued airworthiness considerations for ASISP; specifically, recommendations on whether ASISP-related rulemaking, policy, and/or guidance on best practices were needed. The ASISP WG included representation from non-U.S. manufacturers as well participation from EASA, Transport Canada, and the National Civil Aviation Agency of Brazil. The ASISP WG report addressed ASISP from both transport aircraft and general aviation perspectives, and leveraged the membership and work of the GAMA ASISP working group as well as the work of RTCA SC-216 and EUROCAE WG 72. Using the outputs of this working group, the FAA and EASA are working to produce harmonized rule language and recommended best practices to address ASISP.

2.8 **Research and Development**

2.8.1 In addition to the above activities, the FAA initiated a research and development program to evaluate approaches used for ASISP-related cybersecurity vulnerability and risk assessments. Research activities include Aircraft Communication Addressing and Reporting System (ACARS) data-links used for pre-departure clearance, flight planning information and performance calculations. ACARS research will provide recommendations on both electronic security and flight crew procedure mitigations used to address "loss of function" and the use of attack vectors that inject false ACARS messages.

3. **CONCLUSION**

3.1 The FAA applies Special Conditions, which serve as stand-alone rules for certain make and model aircraft, to ensure cybersecurity vulnerabilities which could potentially affect critical flight systems and safety are addressed in the safety and security assessment processes, before Type or Supplemental Type Certificates are granted. The Aviation Rulemaking and Advisory Committee formed a working group in 2015 to develop recommendations for ASISP rulemaking and/or best practices for aircraft, engines. Using the outputs of this working group, the FAA and EASA are working together to produce harmonized rule language and recommended best practices to address ASISP.

— END —