European Aviation Safety Agency

Terms of Reference

for a rulemaking task

Aircraft cybersecurity

RMT.0648— ISSUE 1 — 17.5.2016

Applicability		Process map	
Affected regulations and decisions:	ED Decision 2003/014RM (CS-23) ED Decision 2003/002/RM (CS-25) ED Decision 2003/015/RM (CS-27) ED Decision 2003/016/RM (CS-29) ED Decision 2003/009/RM (CS-E) ED Decision 2003/007/RM (CS-P)	Concept Paper:	No
		Rulemaking group:	No
		RIA type:	Full
		Technical consultation during NPA drafting:	TBD
		Publication date of the NPA:	2016/Q4
Affected stakeholders:	Appplicants for TC/STC for aircraft, engine, or propeller	Duration of NPA consultation:	2 months
		Review group:	No
		Focussed consultation:	TBD
Driver/origin:	Safety	Publication date of the Opinion:	N/A
Reference:	N/A	Publication date of the Decision:	2017/Q2

1. Issue and reasoning for regulatory change

Aircraft systems designs are evolving from simple, proprietary and isolated architecture communicating via unidirectional point-to-point databuses to more complex ones using standardised protocols and common platforms whose technical documentation is easily accessible. Communication between systems is widely using switched Ethernet technology. Gateways also connect these avionics critical assets with passenger information and entertainment systems. These systems may also be connected to the ground worldwide internet through satellite communication (SATCOM). Aircraft maintenance functions are also connected to the operator's servers for long-distance data loading or maintenance operations.

These interconnections are susceptible to new threats, which may potentially have catastrophic effects on the safety of air transport. Those threats are caused by unauthorised electronic interaction that can be triggered by human action either intentionally or unintentionally. Such threats have the potential to affect the airworthiness of the aircraft due to unauthorised access, use, disclosure, denial, disruption, modification or destruction of electronic information or electronic aircraft system interfaces. The threats include the effects of malware on infected devices, but do not include physical attacks or electromagnetic jamming.

All recently designed large aeroplanes are known to be potentially sensitive to those airworthiness-related security threats due to the interconnectivity features of some of their avionics systems. Moreover, some recent avionics modifications may also render legacy aeroplanes sensitive to this risk.

In the context of aircraft certification, cybersecurity is commonly defined as the protection of electronic systems from malicious electronic attack and the means of dealing with the consequences of such attacks on safety. It comprises managerial, operational and technical activities, and relates to the electronic systems themselves and to the information held and processed by such systems.

Today, cybersecurity is addressed as part of the certification activities of new large aeroplane type designs and supplemental type certificates. In the absence of dedicated specifications in CS-25, this is done in accordance with Part 21A.16B through the special condition called 'Security Assurance Process to isolate or protect the Aircraft Systems and Networks from internal and external Security Threats'.

The special condition requires that aircraft systems and networks be assessed against potential failure caused by information security threats in order to evaluate their vulnerabilities to these threats.

The treat identified on large aeroplanes can potentially be applicable to other aircraft types making use of the connected technologies presented above. Engines and propellers also need to be considered.

The FAA assigned in February 2015 a new task to the Aviation Rulemaking Advisory Committee (ARAC) to provide recommendations regarding Aircraft Systems Information Security/Protection (ASISP) rulemaking, policy, and guidance on best practices for airplanes and rotorcraft, including both certification and continued airworthiness. The Agency is participating in the ASISP working group. One of the assigned subtasks is to consider EASA requirements and guidance material for regulatory harmonisation.

2. Objectives

The specific objective of this task is to mitigate the safety effects stemming from cybersecurity risks due to acts of unlawful interference with the aircraft on-board electronic networks and systems. To achieve this objective, it is proposed to introduce in CS-25 new cybersecurity provisions taking into account the

special condition mentioned above and the recommendations of the AISP ARAC group. The need to include similar provisions such as CS-29, CS-27, CS-23, CS-E, CS-ETSO, and CS-P will also be considered.

3. Activities

— To review the special condition 'Security Assurance Process to isolate or protect the Aircraft Systems and Networks from internal and external Security Threats'.

— To take into account the recommendations of the ASISP working group.

— To propose new certifications specifications (and/or acceptable means of compliance/guidance material) for CS-25 based on analysis of impact (assessment of safe and cost-efficient requirements to prevent the risk). This analysis will also consider other certification specifications such as CS-23, CS-29, CS-27, CS-E, CS-P.

4. Deliverables

— Notice of proposed amendment (NPA) with an amendment to CS-25 (and possibly to CS-23, CS-29, CS-27, CS-E, CS-P), including a regulatory impact assessment (RIA);

— Comment-response document (CRD) providing responses to the comments received on the NPA;

— Executive Director decision(s) amending CS-25 (and possibly CS-23, CS-29, CS-27, CS-E, CS-P).

5. Interface issues

The recommendations from the ARAC ASISP working group need to be considered during the development of this rulemaking task.

6. Annex I: Reference documents

Affected regulations

N/A

Affected decisions

— Decision No. 2003/14/RM of the Executive Director of the Agency of 14 November 2003 on certification specifications, including airworthiness codes and acceptable means of compliance for normal, utility, aerobatic and commuter category aeroplanes (CS-23)

— Decision No. 2003/2/RM of the Executive Director of the Agency of 17 October 2003 on certification specifications, including airworthiness codes and acceptable means of compliance, for large aeroplanes (CS-25)

— Decision No. 2003/15/RM of the Executive Director of the Agency of 14 November 2003 on certification specifications for small rotorcraft (CS-27)

— Decision No. 2003/16/RM of the Executive Director of the Agency of 14 November 2003 on certification specifications for large rotorcraft (CS-29)

— Decision No. 2003/9/RM of the Executive Director of the Agency of 24 October 2003 on certification specifications, including airworthiness codes and acceptable means of compliance, for engines (CS-E)

— Decision No. 2003/7/RM of the Executive Director of the Agency of 24 October 2003 on certification specifications, including airworthiness codes and acceptable means of compliance, for propellers (CS-P)

Reference documents

N/A