European Union Aviation Safety Agency

Explanatory Note to Decision 2020/006/R

Aircraft cybersecurity

CS-25 Amendment 25 — CS-27 Amendment 7 — CS-29 Amendment 8 CS-APU Amendment 1 — CS-E Amendment 6 — CS-ETSO Amendment 15 CS-P Amendment 2— AMC-20 Amendment 18 — AMC and/GM to CS-23 AMC/GM to Part 21

RELATED NPA/CRD: 2019-01 — RMT.0648

EXECUTIVE SUMMARY

The objective of this Decision is to mitigate the potential effects of cybersecurity threats on safety. Such threats could be the consequences of intentional unauthorised acts of interaction with the aircraft on-board electronic networks and systems.

This Decision issues amendments to CS-25, CS-27, CS-29, CS-APU, CS-E, CS-ETSO, CS-P, and to the related acceptable means of compliance (AMC) and/or guidance material (GM), together with AMC-20, AMC/GM to CS-23 and AMC/GM to Part 21. The aim of the amendments is to introduce cybersecurity provisions into the relevant certification specifications (CSs), taking into account:

— the existing special conditions (SCs), and

— the recommendations of the Aircraft Systems Information Security/Protection (ASISP) Working Group of the Aviation Rulemaking Advisory Committee (ARAC)

by following a proportional approach.

The amendments are expected to contribute to the update of the European Union Aviation Safety Agency (EASA) CSs and AMC and GM to reflect the state of the art of the protection of products and equipment against cybersecurity threats. They are also expected to improve harmonisation with the Federal Aviation Administration (FAA) regulations. Overall, they would improve safety, would have neither social nor environmental impact, and would have a negative-to-neutral economic impact.

Action area:	Impact of security on safety		
Related rules:	CS-25, CS-27, CS-29, CS-APU, CS-E, CS-ETSO, CS-P, AMC-20, AMC/GM to CS-23 and AMC/GM to Part 21		
Affected stakeholders:	Applicants for type certificates (TCs)/supplemental type certificates (STCs) for large aeroplanes or large rotorcraft or for European Technical Standard Orders (ETSOs)		
Driver:	Safety	**Rulemaking group:**	No
Impact assessment:	Yes	**Rulemaking Procedure:**	Standard

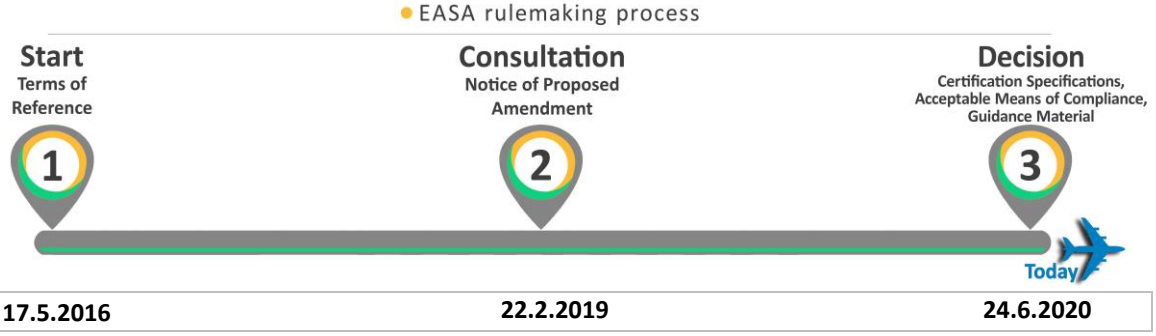

Table of contents

1. About this Decision

EASA developed ED Decision 2020/006/R in line with Regulation (EU) 2018/1139[1] ('Basic Regulation') and the Rulemaking Procedure[2].

This rulemaking activity is included in the European Plan for Aviation Safety (EPAS) for 2020–2024[3] under rulemaking task RMT.0648. The scope and timescales of the task were defined in the related Terms of Reference[4].

The *draft* text of this Decision has been developed by EASA, considering existing special conditions (SCs), and has been also based on the ARAC ASISP Working Group recommendations. All interested parties were consulted through Notice of Proposed Amendment (NPA) 2019-01 'Aircraft cybersecurity'[5,6].

287 comments were received from all interested parties, including industry and national aviation authorities (NAAs).

EASA reviewed the comments received during the public consultation. The comments received and EASA's responses to them are presented in Comment-Response Document (CRD) 2019-01[7].

The *final* text of this Decision with the CSs, AMC and/or GM has been developed by EASA.

The major milestones of this rulemaking activity are presented on the title page.

1 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1535612134845&uri=CELEX:32018R1139).

2 EASA is bound to follow a structured rulemaking process as required by Article 115(1) of Regulation (EU) 2018/1139. Such a process has been adopted by the EASA Management Board (MB) and is referred to as the 'Rulemaking Procedure'. See MB Decision No 18-2015 of 15 December 2015 replacing Decision 01/2012 concerning the procedure to be applied by EASA for the issuing of opinions, certification specifications and guidance material (http://www.easa.europa.eu/the-agency/management-board/decisions/easa-mb-decision-18-2015-rulemaking-procedure).

3 https://www.easa.europa.eu/document-library/general-publications?publication_type%5B%5D=2467

4 https://www.easa.europa.eu/document-library/terms-of-reference-and-group-compositions/tor-rmt0648

5 In accordance with Article 115 of Regulation (EU) 2018/1139, and Articles 6(3) and 7 of the Rulemaking Procedure.

6 https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-01

7 https://www.easa.europa.eu/document-library/comment-response-documents

2. In summary — why and what

2.1. Why we need to change the CSs, AMC and GM

In the context of aircraft certification, cybersecurity is commonly understood as the protection of aviation information systems against intentional unauthorised electronic interactions (IUEI), and the means to mitigate their consequences on safety.

Aircraft systems and parts are increasingly interconnected, and those interconnections are susceptible to security threats. These threats have the potential to affect the airworthiness of an aircraft due to unauthorised access, use, disclosure, denial, disruption, modification or destruction of electronic information or electronic aircraft system interfaces. The threats mentioned do not include physical attacks.

Currently, cybersecurity is addressed as part of the certification activities for new large aeroplane type designs and supplemental type certificates (STCs). In the absence of dedicated provisions in CS-25, this is currently done in accordance with point 21.B.75 of Annex I (Part 21) to Regulation (EU) No 748/2012[8] through an SC called 'Information Security Protection of Aircraft Systems and Networks'.

That SC requires aircraft systems and networks to be assessed against the potential effects that information security threats could have on safety.

The threats identified for large aeroplanes could also be applied to other aircraft types, engines, propellers or ETSO articles that make use of interconnected technologies.

In November 2016, the FAA tasked ARAC to address the issue of Aircraft Systems Information Security/Protection (ASISP). The ARAC provided recommendations regarding ASISP rulemaking, policy, and guidance on best practices, including initial and continued airworthiness. EASA participated in the ASISP Working Group whose assigned subtasks included considering the EASA requirements and guidance material for regulatory harmonisation purposes.

The ARAC report contains recommendations that affect large aeroplanes, general aviation (GA), rotorcraft, engines, propellers, portable electronic devices (PEDs), field-loadable software, commercial off-the-shelf (COTS) equipment, and communication, navigation and surveillance/ air traffic management.

Since aircraft systems are increasingly interconnected, and thus potentially vulnerable to security threats, EASA needs to consider the state-of-the-art means of protection against these threats when certifying new products or parts. EASA has, therefore, decided to transpose the above-mentioned SC into certain CSs and AMC and/or GM, while also considering the recommendations of the ASISP Working Group report.

2.2. What we want to achieve — objectives

The overall objectives of the EASA system are defined in Article 1 of the Basic Regulation. This Decision will contribute to the achievement of the overall objectives by addressing the issues outlined in Section 2.1.

[8] Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations (OJ L 224, 21.8.2012, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1579001172632&uri=CELEX:32012R0748).

The specific objective of this Decision is to take into account the interdependencies between aviation safety and security in order to mitigate the safety effects caused by potential cybersecurity threats.

2.3. How we want to achieve it — overview of the amendments

It is proposed to introduce cybersecurity provisions into certain CSs, considering the SC mentioned above and the recommendations of the ASISP Working Group. These provisions would require the applicant to show during certification that the possible security risks have been identified, assessed, and mitigated as necessary. They would be included in:

— CS-25 'Large Aeroplanes',

— CS-27 'Small Rotorcraft',

— CS-29 'Large Rotorcraft',

— CS-APU 'Auxiliary Power Units',

— CS-E 'Engines',

— CS-ETSO 'European Technical Standard Orders',

— CS-P 'Propellers', and in their related AMC and/or GM,

as well as in:

— AMC-20 'General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances',

— AMC/GM to CS-23 'Normal, Utility, Aerobatic and Commuter Aeroplanes', and

— AMC/GM to Part 21.

2.4. What are the stakeholders' views

The commentators are in general supportive of the proposed amendments to the CSs and the creation of a new AMC-20 to address cybersecurity. They also appreciate the regulatory harmonisation effort with the FAA.

2.5. What are the benefits and drawbacks

The availability of CSs and AMC/GM that reflect the state of the art in terms of means of protection against cybersecurity threats will ensure that applicants take the necessary actions in this regard during the design of their products or parts, and that the CSs are consistently applied in all certification projects. It is expected that this will reduce the vulnerability of aircraft systems, and ultimately improve safety, by reducing the risk of cybersecurity incidents or accidents.

The new CS requirements would have an economic impact on the applicants that will have to demonstrate compliance with the requirements, but such cost would be balanced by the resilience of the aircraft design to cybersecurity incidents and accidents.

3. How do we monitor and evaluate the rules

EASA shall monitor and evaluate the effectiveness of the proposed amendments to the CSs and the AMC/GM once they become applicable. Due to the evolving nature of cybersecurity threats and vulnerabilities, the monitoring indicators cannot be specified exhaustively. However, access to the number of attempts of intentional unauthorised electronic interactions (IUEIs) with the aircraft systems would be required, as well as a review of the results of regular proactive testing of the effectiveness of the cybersecurity protection means. It should be noted that EASA can access the cybersecurity occurrences related to aircraft design and production through the European Coordination Centre for Accident and Incident Reporting Systems (ECCAIRS) Portal and report on them.

4. References

4.1. Related regulations

n/a

4.2. Related decisions

— Decision No. 2003/12/RM of the Executive Director of the Agency of 5 November 2003 on general acceptable means of compliance for airworthiness of products, parts and appliance (« AMC-20 »), as amended

— Executive Director Decision 2003/14/RM of 14 November 2003, issuing Certification Specifications for normal, utility, aerobatic and commuter category aeroplanes (« CS-23 »), as amended

— Executive Director Decision 2017/025/R of 20 December 2017 issuing Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Certification Specifications for Normal-Category Aeroplanes (CS-23) ('AMC/GM to CS-23 — Issue 1'), as amended

— 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 »), as amended

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

— Decision No. 2003/005/RM of the Executive Director of the Agency of 17 October 2003 on certification specifications for auxiliary power units (« CS-APU »)

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

— 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 »), as amended

— Decision No. 2003/10/RM of the Executive Director of the Agency of 24 October 2003 on certification specifications, including airworthiness codes and acceptable means of compliance, for European Technical Standards Orders (« CS-ETSO »), as amended

— 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 »), as amended

— Decision N° 2012/020/R of the Executive Director of the Agency of 30 October 2012 on Acceptable Means of Compliance and Guidance Material for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations ('AMC and GM to Part 21'), as amended

4.3. Other reference documents

Report from the Aviation Rulemaking Advisory Committee (ARAC) Aircraft System Information Security/Protection (ASISP) Working Group, submitted to the Federal Aviation Administration on 22 August 2016