European Union Aviation Safety Agency

Notice of Proposed Amendment 2019-01

Aircraft cybersecurity

RMT.0648

EXECUTIVE SUMMARY

The objective of this Notice of Proposed Amendment (NPA) is to mitigate the potential effects of cybersecurity threats on safety. Such threats could be the consequences of intentional unauthorised acts of interference with aircraft on-board electronic networks and systems.

This NPA proposes amendments to CS-23, CS-25, CS-27, CS-29, CS-E, CS-ETSO, CS-P, and, as applicable to their related acceptable means of compliance (AMC)/guidance material (GM), together with AMC-20. The amendments would introduce cybersecurity provisions into the relevant certification specifications (CSs), taking into account the existing special conditions (SCs) and the recommendations of the Aviation Rulemaking Advisory Committee (ARAC) regarding aircraft systems information security/protection (ASISP).

The proposed amendments are expected to contribute to updating the EASA CSs to reflect the state of the art of 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 neutral-to-positive economic impact.

Action area:	Impact of security on safety		
Affected rules:	CS-23, CS-25,CS-27,CS-29, CS-E, CS-ETSO, CS-P and, as applicable their related AMC/GM; AMC-20		
Affected stakeholders:	Applicants for type certificates (TCs)/supplemental type certificates (STCs) or for European Technical Standard Order (ETSO) authorisations		
Driver:	Safety	**Rulemaking group:**	No
Impact assessment:	Light	**Rulemaking Procedure:**	Standard

Table of contents

1. About this NPA

1.1. How this NPA was developed

— The European Union Aviation Safety Agency (EASA) developed this NPA in line with Regulation (EU) 2018/1139[1] ('Basic Regulation') and the Rulemaking Procedure[2]. This rulemaking activity is included in the 2019-2023 European Plan for Aviation Safety (EPAS)[3] under rulemaking task RMT.0648. The text of this NPA has been developed by EASA, considering the existing Special Conditions (SCs), and it is also based on the recommendations of the ARAC regarding ASISP.

— It is hereby submitted to all interested parties[4] for consultation.

1.2. How to comment on this NPA

Please submit your comments using the automated **Comment-Response Tool (CRT)** available at **http://hub.easa.europa.eu/crt/**[5].

The deadline for submission of comments is **22 May 2019.**

1.3. The next steps

— Following the closing of the public commenting period, EASA will review all the comments received.

— Based on the comments received, EASA will develop a decision that amends CS-23, CS-25, CS-27, CS-29, CS-E, CS-ETSO, CS-P, and, as applicable to their related AMC/GM, as well as AMC-20.

— The comments received on this NPA and the EASA responses to them will be reflected in a comment-response document (CRD). The CRD will be appended to the decision.

---

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 52(1) of Regulation (EC) No 216/2008. 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 In accordance with Article 115 of Regulation (EU) 2018/1139, and Articles 6(3) and 7 of the Rulemaking Procedure.

5 In case of technical problems, please contact the CRT webmaster (crt@easa.europa.eu).

2. In summary — why and what

2.1. Why we need to change the rules — issue/rationale

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

Aircraft systems and parts are increasingly connected, 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 of new large aeroplane type designs and STCs. In the absence of dedicated provisions in CS-25, this is currently done in accordance with point 21A.16B of Annex I (Part 21) to Regulation (EC) No 748/2012[6] through a Special Condition (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 ARAC, tasked by the FAA, provided recommendations regarding ASISP rulemaking, policy, and guidance on best practices[7], including for 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, rotorcraft, engines, propellers, portable electronic devices, field loadable software, commercial off-the-shelf (COTS) equipment, and communication, navigation and surveillance/air traffic management.

Since aircraft systems are increasingly connected, 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/or AMC/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 proposal will contribute to the achievement of the overall objectives by addressing the issues outlined in Section 2.1.

---

6 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).

7 https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/ARACasisp-T1-20150203R.pdf

— The specific objective of this proposal 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 proposals

It is proposed to introduce new cybersecurity provisions into certain CSs, considering the SCs mentioned above and the recommendations of the ASISP Working Group. These provisions would require the applicant to show that the possible security risks have been identified, assessed, and mitigated as necessary. They would be included in CS-23, CS-25, CS-27, CS-29, CS-E, CS-ETSO, CS-P, and, as applicable to their related AMC/GM, as well as in AMC-20.

2.4. What are the expected benefits and drawbacks of the proposals

— The availability of CSs that reflect the state of the art in terms of means of protection against cybersecurity threats will ensure that applicants take the necessary actions during the design of their products or parts, and that the CSs are consistently applied through 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.

— No drawbacks or adverse economic impacts are expected.

— For the full ‘light’ impact assessment of the alternative options, please refer to Chapter 4.

3. Proposed amendments and rationale in detail

— The text of the amendment is arranged to show deleted text, new or amended text as shown below:

— deleted text is ~~struck through~~;

— new or amended text is highlighted in blue;

— an ellipsis '[…]' indicates that the rest of the text is unchanged.

— Wherever necessary, a rationale is provided in *blue italics* before or after the proposed amendments.

3.1. Draft certification specifications (Draft EASA decision)

3.1.1. Draft decision amending the AMC and GM to CS-23

In Subpart A, the following GM 23.2500(b) is inserted:

'**GM 23.2500(b)**

Improper functioning of equipment and systems may be caused by intentional unauthorised electronic interaction (IUEI). The applicant may then also consider cybersecurity threats as possible sources of 'improper functioning' of equipment and systems. In showing compliance with CS 23.2500(b) for equipment and systems whose improper functioning could lead to a failure condition more severe than major, the applicant may consider AMC 20-42. This AMC provides acceptable means, guidance and methods to perform security risk assessment and mitigation for aircraft information systems.'

In Subpart F, AMC1 CS-23 is amended as follows:

'CS-23 Amdt 5 **SUBPART F – Systems and Equipment**	**(Ref.: ASTM F44 F3264-17 Standard Specification for Normal Category Aeroplanes Certification)**	**Remarks**
23.2500 *General requirements on systems and equipment function*	9.1 *Systems and Equipment Function and Safety Requirements:* F3061/F3061M-17 Standard Specification for Systems and Equipment in Small Aircraft F3230-17 Standard Practice for Safety Assessment of Systems and Equipment in Small Aircraft F3231/F3231M-17 Standard Specification for Electrical Systems in Small Aircraft F3235-17a Standard Specification for Aircraft Storage Batteries F3232/F3232M-17 Standard Specification for Flight Controls in Small Aircraft F3233/F3233M-17 Standard Specification for Instrumentation in Small Aircraft F3229/F3229M-17 Standard Practice for Static Pressure System Tests in Small Aircraft F3064/F3064M-18a Standard Specification for Aircraft Powerplant Control, Operation and Indication F3066/F3066M-15 Standard Specification for Aircraft Powerplant Installation Hazard Mitigation F3117-15 Standard Specification for Crew Interface in Aircraft	With reference to ASTM F3264-17 paragraph 9.1, updated ASTM F3235-17a is included as a means of complying with CS 23.2500. AMC 20-42 – Airworthiness Information Security Risk Assessment may be considered as a means of complying with CS 23.2500(b).'

Rationale

EASA, in coordination with the FAA, performed a comprehensive rewrite of CS-23, and in particular of Subpart F — Systems and Equipment.

The ARAC ASISP Working Group reviewed the new paragraph CS 23.2500 about systems and equipment function and considered that the objective of the paragraph embraced ASISP.

It is not, however, proposed to create a new paragraph, but to clarify in the GM that 'improper functioning' also includes 'intentional unauthorised electronic interaction (IUEI)'.

AMC1 to CS-23 Subpart F is also amended to make reference to AMC 20-42.

3.1.2. Draft decision amending CS-25

The following CS 25.1319 is inserted:

'**CS 25.1319 Equipment, systems and network information security protection**

a. Aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions that may result in adverse effects on the safety of the aeroplane. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.

b. When required by paragraph a, the applicant must make procedures and instructions for continued airworthiness (ICA) available that ensure that the security protections of the aeroplane equipment, systems and networks are maintained.'

The following GM 25.1319 is inserted:

'**GM 25.1319 Equipment, systems and network information security protection**
In showing compliance with CS 25.1319, the applicant may consider AMC 20-42, which provides acceptable means, guidance and methods to perform security risk assessments and mitigation for aircraft information systems.'

The following Appendix H25.6 is inserted:

'**Appendix H25.6 Information system security instructions for continued airworthiness**

The applicant must prepare instructions for continued airworthiness (ICA) that are applicable to aircraft information system security protection as required by CS 25.1319 (see also AMC 20-42 Section 9).

Rationale

The term 'intentional unauthorised electronic interaction (IUEI)' was developed jointly by RTCA and EUROCAE (see the definition and scope of IUEI in Eurocae ED-203A, Section 2.1).

The term 'adverse effects on the safety of the aeroplane' limits the scope of this provision to security breaches that impact on the safety and airworthiness of the aeroplane and its operation, rather than security breaches that may impact on the systems that have no safety effect on the aeroplane. For example, while the manufacturer and the operator may have real concerns about protecting a device that is used to process passenger credit cards and securing passenger information, EASA does not regard this as being subject to review and approval as part of the certification of the system, but instead as

something that the operator or manufacturer would address as part of its business practices and responsibilities to the customer.

The term 'mitigated as necessary' clarifies that the applicant has the discretion to establish appropriate mitigations against security risks.

The term 'procedures and instructions for continued airworthiness' clarifies that, while the ICA may be one mechanism for providing the necessary instructions to maintain airworthiness, the security protections may go beyond traditional ICA material, and also include other procedures provided to the operator. This aligns with the existing practices among those applicants that have been issued SCs to address aircraft information system security protection.

3.1.3. Draft decision amending CS-29

The following CS 29.1319 is inserted:

'**CS 29.1319 Equipment, systems and network information security protection**

a. Rotorcraft equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions that may result in catastrophic or hazardous/severe major effects on the safety of the rotorcraft. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.

b. When required by paragraph a, the applicant must make procedures and instructions for continued airworthiness (ICA) available that ensure that the security protections of the rotorcraft equipment, systems and networks are maintained.'

The following GM 29.1319 is inserted:

'**GM 29.1319 Equipment, systems and network information security protection**

In showing compliance with CS 29.1319, the applicant may consider AMC 20-42, which provides acceptable means, guidance and methods to perform security risk assessments and mitigation for aircraft information systems.'

The following Appendix A.29.5 is inserted:

'**Appendix A.29.5 Information security instructions for continued airworthiness**

The applicant must prepare instructions for continued airworthiness (ICA) that are applicable to aircraft information system security protection as required by CS 29.1319 (see also AMC 20-42 Section 9).'

3.1.4. Draft decision amending CS-27

The following CS 27.1319 is inserted:

'**CS 27.1319 Equipment, systems and network information security protection**

a. Rotorcraft equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions that may result in catastrophic or hazardous/severe major effects on the safety of the rotorcraft. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.
b. When required by paragraph a, the applicant must make procedures and instructions for continued

airworthiness (ICA) available that ensure that the security protections of the rotorcraft equipment, systems and networks are maintained.'

The following GM 27.1319 is inserted:

'**GM 27.1319 Equipment, systems and network information security protection**

In showing compliance with CS 27.1319, the applicant may consider AMC 20-42, which provides acceptable means, guidance and methods to perform security risk assessments and mitigation for aircraft information systems.'

The following Appendix A.27.5 is inserted:

'**Appendix A.27.5 Information security instructions for continued airworthiness**

The applicant must prepare instructions for continued airworthiness (ICA) that are applicable to aircraft information system security protection as required by CS 27.1319 (see also AMC 20-42 Section 9).'

Rationale

CS-27 rotorcraft have operating capabilities (such as multiple engines, Cat A and IFR capability) that are similar to those of CS-29 rotorcraft, and they may need to demonstrate security compliance if critical systems are installed to provide similar operating capabilities. EASA therefore proposes that the specifications for normal category rotorcraft (CS-27) should be similarly bounded to only require the consideration of catastrophic and hazardous/severe major effects on safety that are caused by intentional unauthorised electronic interactions.

3.1.5. Draft decision amending CS-E

CS-E 25 is amended as follows:

'**CS-E 25 Instructions for Continued Airworthiness**

(c) The following information must be considered, as appropriate, for inclusion into the manual(s) required by CS-E 25(a).

(1)
[…]
(13) Instructions applicable to information system security protection as required by CS-E 50(l).'

CS-E 50 is amended as follows:

'**CS-E 50 Engine control system**

[…]

(l) Information system security protection. Engine control systems, including networks, software and data, must be designed and installed so that they are protected from intentional unauthorised electronic interactions that may result in adverse effects on the safety of the aircraft. The security risks and vulnerabilities must be identified, assessed and mitigated as necessary. The applicant must make procedures and instructions for continued airworthiness (ICA) available that ensure that the security protections of the engine controls are maintained.'

The following GM E 50(l) is inserted:

'**GM E 50(l) Engine information security protection**

For engine control systems, AMC 20-42 provides acceptable means, guidance and methods to address CS-E 50(l), with special consideration given to the interfaces between the aircraft and the engine, if applicable. In particular, specific cases of intentional unauthorised electronic interactions that could potentially have similar effects on all the engine control systems of an aircraft should be taken into account in the security risk assessment, rather than any interactions that could only have an adverse effect on a single engine.'

3.1.6. Draft decision amending CS-P

CS-P 40 is amended as follows:

'**CS-P 40 Instructions for Continued Airworthiness**

(c) The following information must be considered, as appropriate, for inclusion into the manual(s) required by CS-P 40(a).

(1)
[…]

(13) Instructions applicable to information system security protection as required by CS-P 230(g).'

CS-P 230 is amended as follows:

'**CS-P 230 Propeller Control System**

[…]

(g) Information system security protection. Propeller control systems, including their networks, software and data, must be designed and installed so that they are protected from intentional unauthorised electronic interactions that may result in adverse effects on the safety of the aircraft. The security risks and vulnerabilities must be identified, assessed and mitigated as necessary. The applicant must make procedures and maintenance instructions available that ensure that the security protections of the propeller control systems are maintained.'

AMC P 230 is amended as follows:

'**AMC P 230 Propeller Control System**

[…]
(5) Information system security protection

For electronic propeller control systems, AMC 20-42 provides acceptable means, guidance and methods to address CS-P 230(g), with special consideration given to the interfaces between the aircraft and the engine, if applicable. In particular, specific cases of intentional unauthorised electronic interactions that could potentially have similar effects on all the propeller control systems of an aircraft in a relatively short period of time, and the resulting adverse effect on the safety of the aircraft, should be taken into account for the security risk assessment, rather than any interaction that results in an adverse effect on a single propeller.'

Rationale

For avionics systems that contain digital processing, EASA proposes to also apply, with appropriate tailoring, the provisions of CS-25 to the similar systems that are associated with engines and propellers, in accordance with the guidance provided in DO-326A/ED-202A, DO-355/ED-204 and DO-356A/ED-203A.

A separate type certificate may be issued for engines and propellers. However, as they are connected to the aircraft systems, some tailored protection measures are necessary for engines and for propeller systems.

3.1.7. Draft decision amending CS-ETSO

In Subpart A, Section 2 is amended as follows:

'2. STANDARDS TO MEET TECHNICAL CONDITIONS

[…]

2.7 Information security protection

An ETSO article may be designed with a security assurance level (SAL), according to the procedure provided in AMC 20-42.'

3.1.8. Draft decision amending AMC-20

Rationale

The following text proposes an AMC for the certification of products, parts and appliances whose information systems are subject to potential information security threats that may have an impact on aviation safety. It is extracted and adapted from the interpretative material (IM) of the generic special condition (SC) and certification review item (CRI) used for large transport aeroplanes, the certification action item (CAI) used for large rotorcraft, and the CAI used for general aviation class IV aeroplanes during the initial type certification, modification and supplemental type certification of already type-certified products. Since the applicability of this guidance will continue beyond the certification of the aircraft, the main changes compared with the original IM are the use of the terms 'product' and 'part' instead of 'aircraft', and the removal of some specific CSs to allow the common use of this AMC with a wider range of products, parts and appliances that are certified by EASA.

The following AMC 20-42 is inserted:

'**AMC 20-42: Airworthiness information security risk assessment**

1. Purpose

(a) This AMC describes an acceptable means, but not the only means, to show compliance with the applicable regulations for the certification of products and parts. Compliance with this AMC is not mandatory, and therefore an applicant may elect to use an alternative means of compliance. However, any alternative means of compliance must meet the relevant requirements and be accepted by EASA.

(b) This AMC recognises the following European Organisation for Civil Aviation Equipment (EUROCAE) and Radio Technical Commission for Aeronautics (RTCA) documents:

— EUROCAE ED-202A/RTCA DO-326A, Airworthiness Security Process Specification, dated June 2014;

— EUROCAE ED-203A/RTCA DO-356A, Airworthiness Security Methods and Considerations, dated June 2018;

— EUROCAE ED-204/RTCA DO-355, Information Security Guidance for Continuing Airworthiness, dated June 2014.

(c) This AMC establishes guidance to use ED-202A, 203A and 204 in the different context of the initial and continued airworthiness of products and parts, and the certification of aviation-related services (e.g. traffic management, data links, etc.).

Note: EUROCAE ED is hereinafter referred to as 'ED'; RTCA DO is hereinafter referred to as 'DO'. Where the notation 'ED-XXX/DO-XXX' appears in this document, the referenced documents are recognised as being equivalent.

2. Applicability

This AMC applies to products and part manufacturers, equipment and service providers, and design approval holders (DAHs) who apply for:

— the type certification of a new product (i.e. an aircraft, engine or propeller);

— a supplemental type certificate (STC) to an existing type-certified product;

— a change to a product;

— the approval of a new item of equipment or a change to equipment to be used in an ETSO article. In such a case, credit can be taken from its security assurance level (SAL) during the installation of the ETSO article by the design organisation approval holder (DOAH), depending on the information system security risk assessment of the product;

— the certification of other systems or equipment that provide air service information whose certification is required by a national regulation;

— the approval of products and parts of information systems that are subject to potential information security threats and that could result in unacceptable safety risks.

3. Replacement

Reserved.

4. General principles

(a) The information systems identified in Section 2 should be assessed against potential security threats that could result in unacceptable safety risks. This risk assessment is referred to as a 'product information security risk assessment (PISRA)' and is further described in Section 5 of this AMC.

It is an assessment of the information security of the systems that are specific to a product or part.

(b) The result of this assessment, after any necessary mitigation measures have been identified, should be that either the systems of the product or part have no identifiable vulnerabilities, or those vulnerabilities cannot be exploited by any known security threat to create a hazard or generate a failure condition that would have an effect that is deemed to be unacceptable against the certification specification of the product or part considered.

(c) When a risk needs to be mitigated, the applicant should demonstrate, as described in Section 5, that the mitigations provide sufficient grounds for evaluating that the residual risk is acceptable.

(d) Once the overall risk has been deemed to be acceptable, the applicant should develop instructions, as described in Section 9, to maintain the information security risk of the systems of the product or part at an acceptable level after the entry into service of the product or part.

5. Product information security risk assessment

(a) The general product information security risk assessment (PISRA) should cover the following aspects:

(i) determination of the operational environment for the information security of the product;

(ii) identification of the assets;

(iii) identification of the attack paths;

(iv) assessment of the safety consequences of the threat to the affected items;

(v) evaluation of the potentiality of a successful exploit, or of the difficulty of performing a successful attack that would have an impact on safety;

(vi) determination of whether the risks, which are the result of comparing the severities with the potentiality to attack (or, inversely, the difficulty of attacking), are acceptable:

If yes, preparation of the justification for certification, including the means to maintain the risk at an acceptable level (see Section 8);

If no,

(A) implementation of mitigation means,

(B) evaluation of the effectiveness of the mitigation means with respect to the severity of the threat;

(vii) iteration from point (vi) until all the residual risks are acceptable.

(b) The process identified in ED-202A Section 2.1.1 is acceptable as guidance for performing the PISRA for products and parts under Part 21.

7. Reporting

The operator of a product or part should report any information security occurrences to the designer of this product or part, in a manner that would allow a further impact analysis and corrective actions, if appropriate. If this impact analysis identifies a reasonably high potential for an unsafe condition, the designer of that product or part should report it to the competent authority in a timely manner. For example, for organisations to which Regulation (EU) No 748/2012 applies, the reporting should be done in accordance with point 21.A.3A of Annex I (Part 21) to that Regulation.

8. Validation and verification of the security protection

(a) If information security risks that are identified during the product information security risk assessment (PISRA) need to be mitigated, security verification should be used to evaluate the efficiency of the mitigation means.

(i) This verification may be performed by a combination of analysis, security-oriented robustness testing, inspections, and reviews; and

(ii) When necessary, by security testing that addresses information security from the perspective of a potential adversary.

9. Instructions for continued product and part information security protection

The applicant should identify the information security assets and protection mechanisms to be addressed by the ICA of the product or part (for example, physical and operational security, auditing

and monitoring of the security efficiency, key management procedures that are used as assumptions in the security assurance process), and develop the appropriate procedures to maintain the security efficiency after the product or part enters into service.

When an in-service occurrence is reported, the applicant should consider the possibility that it originated from a violation of the system and information security rules, and should take any required corrective action accordingly. If a violation of the system and information security rules has generated an unsafe condition, then information about the occurrence, the investigation results and the recovery actions should be reported to EASA in accordance with point 21A.3A of Part 21.

According to Article 2(7) of Regulation (EU) No 376/2014, an occurrence is defined as any safety-related event which endangers, or which, if not corrected or addressed, could endanger an aircraft, its occupants or any other person, and includes, in particular, any accident or serious incident. Article 4 of Regulation (EU) No 376/2014 requires the applicant to report to EASA any occurrence that represents a significant risk to aviation safety.

The applicant should also assess the impact of new threats that were not foreseen during previous product information security risk assessments (PISRAs) of the systems and parts of the product. If the assessment identifies an unacceptable threat condition, the applicant should notify the operators of the need and the means to mitigate the new risk.

Guidance on continued airworthiness can be found in EUROCAE ED-203A/RTCA DO-356A and ED-204/RTCA DO-355.

Acceptable/Unacceptable Risk: whether a risk is unacceptable depends on the context and the criteria that are considered for the certification specifications of the product or the affected part. The risk may be acceptable in some cases and unacceptable in others. For example, a threat condition that has a potential major safety effect, as defined in CS 25.1309, will not be acceptable if the probability that the associated threat scenario is successfully exploited is too high. The same safety risk may be acceptable for products that are certified under CS-29.

10. Definitions

The terminology used in this AMC is consistent with the glossary provided in document EUROCAE ER 013 AERONAUTICAL INFORMATION SYSTEM SECURITY GLOSSARY.'

3.1.9. Draft decision amending Appendix A to GM 21.A.91 'Classification of changes to type certificate'

Rationale

The current GM on the classification of changes to a type certificate requires a change to be classified as either major or minor. Wherever there is doubt as to the classification of a change, EASA should be consulted for clarification, and Appendix A 'Examples of Major Changes per discipline' to GM 21.A.91 provides technical examples that are intended to help to reach early understanding and agreement on the classification of a change.

Appendix A 'Examples of Major Changes per discipline' to GM 21.A.91 is amended as follows:

'4. Systems

[…]

For other codes, the principles noted above may be used. However, due consideration should be given to specific certification specifications/interpretations.

For systems that fall under CS 25.1319, CS 27.1319, CS 29.1319, CS-E 50(i), CS-P 230(g), in the context of a product information security risk assessment, a change may be considered to be major if the security environment is impacted and the initial analysis shows that before the implementation of mitigation

means, there is a potential for an unsafe condition. The following examples do not provide a complete list of conditions to classify a modification as major, but rather they present the general interactions between security domains. Examples of modifications that may be classified as major are when any of the following changes occur:

— A new digital communication means, logical or physical, is established between a more closed, controlled information security domain, and a more open, less controlled security domain.

- For example, in the context of large aircraft, a communication means is established between the aircraft control domain (ACD) and the airline information services domain (AISD), or between the AISD and the passenger information and entertainment services domain (PISD) (see ARINC 811).

  Exception: a simplex digital communication means (e.g. ARINC 429) is established from a controlled domain to a more open domain, unless it can be shown that the simplex control can be reversed.

— A new service is introduced between a system of a more closed, controlled information security domain and a system of a more open, less controlled security domain, which allows the exploitation of a vulnerability of the service that has been introduced, creating a new threat path.

  For example:

- opening and listening on a UDP port in an end system of an already certified topology;
- activating a protocol in a point-to-point communication channel.

— The modification of a service between a system of a more closed, controlled security domain and a system of a more open, less controlled security domain.

5. Propellers

[…]’

4. Impact assessment (IA)

4.1. What is the issue

4.1.1. Safety risk assessment

Aircraft systems are increasingly connected, and those 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 interactions that can be triggered by human action, either intentionally or unintentionally. Such threats have the potential to affect the airworthiness of a product or equipment 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 interference.

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 avionic systems.

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

This SC requires large aircraft systems and networks to be assessed against potential failures caused by information security threats in order to evaluate their vulnerabilities to these threats.

Since for all categories of aircraft, systems are increasingly connected, and are thus potentially vulnerable to security threats, EASA needs to reflect the state-of-the-art means of protection against these threats. This could be achieved by amending the CSs for the various aviation products and equipment that EASA certifies.

4.1.2. Who is affected

— Applicants for TCs/STCs for aircraft, engines or propellers, as well as equipment designers and manufacturers.

4.1.3. How could the issue/problem evolve

The continuing lack of CSs that reflect the state of the art in terms of aircraft cybersecurity would neither ensure that applicants take the necessary actions to protect their designs, nor that the CSs are consistently applied in all certification projects. Such a situation would not contribute to reducing the vulnerability of aircraft systems, and this ultimately would not contribute to reducing the risk of cybersecurity incidents or accidents.

4.2. What we want to achieve — objective

— The objective of this proposal is to improve safety by mitigating the vulnerability of aircraft systems to cybersecurity threats. EASA observed the development of the ARAC ASISP Working Group report and considers its recommendations to be a solid basis to achieve this objective.

4.3. How it could be achieved — options

Table 1: Selected policy options

Option No	*Short title*	**Description**
0	No change	No policy change (no change to the rules; risks remain as outlined in the analysis of the issue)
1	Amend CSs + all related AMC/GM	Amendment of the CSs and all their respective AMC/GM, based on the existing SC and the recommendations of the ARAC ASISP Working Group
2	Amend CSs + create one AMC-20	Amendment of the CSs, based on the existing SC and the recommendations of the ARAC ASISP Working Group; and Creation of one AMC-20 item containing all the AMC material related to cybersecurity for products and parts

4.4. What are the impacts

4.4.1. Option 0

Overall, the impacts of Option 0 are negative: for the certification of large aeroplanes, EASA would continue to apply the SC mentioned above. Therefore, the safety risk for this category of aircraft would be addressed as it is currently done. For other products, the increasing risk would also need to be managed by issuing new SCs and/or interpretative material when required by the nature of the certification project.

In the absence of adequate CSs and AMC/GM, an applicant may not necessarily be aware of EASA's expectations in the domain of cybersecurity, and may start to develop designs that are not sufficiently protected against the associated threats. Such a situation could have a significant negative economic impact for the applicant.

Furthermore, the use of SCs may lead to some inconsistencies in the way in which they are applied to different certification projects, with negative impacts on resources for both the applicants and EASA.

4.4.2. Options 1 & 2

4.4.2.1 Safety impact

The availability of CSs that reflect the state of the art in terms of aircraft cybersecurity will ensure that applicants take the necessary actions to protect their designs against cybersecurity threats. It will also enable applicants to consistently apply those CSs to all certification projects. It is expected that this will reduce the vulnerability of aircraft systems to cybersecurity threats, and will ultimately reduce the risk of cybersecurity incidents or accidents.

4.4.2.2 Environmental impact

— Not applicable

4.4.2.3 Social impact

— Not applicable

4.4.2.4 Economic impact

— CSs that reflect the state of the art and current best practices will aid the design and certification processes, and thereby reduce costs.

— With the implementation of Option 1 or Option 2, applicants will benefit from having prior awareness of EASA's expectations (for the certification basis). This may prevent the development of unacceptable designs in the early stages of projects, while having no impact on the price of the final products.
A positive-to-neutral economic impact is therefore expected.

4.4.2.5 General aviation and proportionality issues

— The ARAC ASISP Working Group recommendations propose means of compliance that are proportionate to the products and to the associated risks.

4.5. Conclusion

4.5.1. Comparison of options

— The overall impact of Option 0 is negative, while Options 1 and 2 are expected to bring safety and economic benefits.

— The difference between Option 1 and Option 2 concerns whether to include an AMC in Book 2 of each CS, or to group it into a single AMC-20. The grouping of Option 2 presents additional advantages compared with Option 1:

— easier access for the applicants (all in one place);

— easier 'maintenance': the safety objective in the CSs would remain stable, while the AMC could evolve and all be updated together.

— Option 2 is therefore proposed as the way forward.

4.6. Monitoring and evaluation

EASA will monitor the effects created by the proposed amendments to CS-23, CS-25, CS-27, CS-29, CS-E, CS-ETSO, CS-P, and, as applicable to their related AMC/GM; as regards AMC-20, EASA will collect and evaluate feedback from future products and equipment certification projects.

That feedback will depend on the applications that are received after the amendment of the related CSs. A review will be made at the earliest 5 years after the amendment of the CSs in order to include feedback from the certification of new type designs, as well as the certification of existing designs and STCs.

In addition, the amendments to the CSs might be subject to interim/ongoing/ex post evaluations that will show the outcome obtained after the application of the new provisions, taking into account the earlier predictions made in the impact assessment. The evaluation would provide evidence-based judgement of the extent to which the proposal has been relevant (given the needs and its objectives), effective and efficient, coherent, and has achieved EU added value. The decision as to whether an evaluation will be necessary should also be taken based on the results of the monitoring.

5. References

5.1. Affected/Related regulations

— Not applicable

5.2. Affected 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 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. 2003/16/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

5.3. 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

6. Appendix

Not applicable