EASA
European Union Aviation Safety Agency

PART 21 WORKSHOP CERTIFICATION CONFERENCE

Side Meeting – Cybersecurity: raising awareness about applicability

Aviation Cybersecurity Expert – Borja García-Blanco Castro

Aviation Cybersecurity Expert – Johannes Goebel

PART 21 WORKSHOP

November 26th 2024

Your safety is our mission.

An Agency of the European Union

Agenda

OVERVIEW ON CYBERSECURITY REQUIREMENTS AND AMC

- EASA ED Decision 2020/006/R
- CS 25.1319
- AMC 20-42

EVALUATING CHANGES FROM CYBERSECURITY STANDPOINT

- EUROCAE standards (ED-20X)
- Minor vs major change
- Major change examples

DEFINING LEVEL OF INVOLVEMENT FOR CYBERSECURITY

- CM-21.A/21.B-001 - Issue 03

EASA
European Union Aviation Safety Agency

CYBERSECURITY

Overview on requirements and AMC

An Agency of the European Union

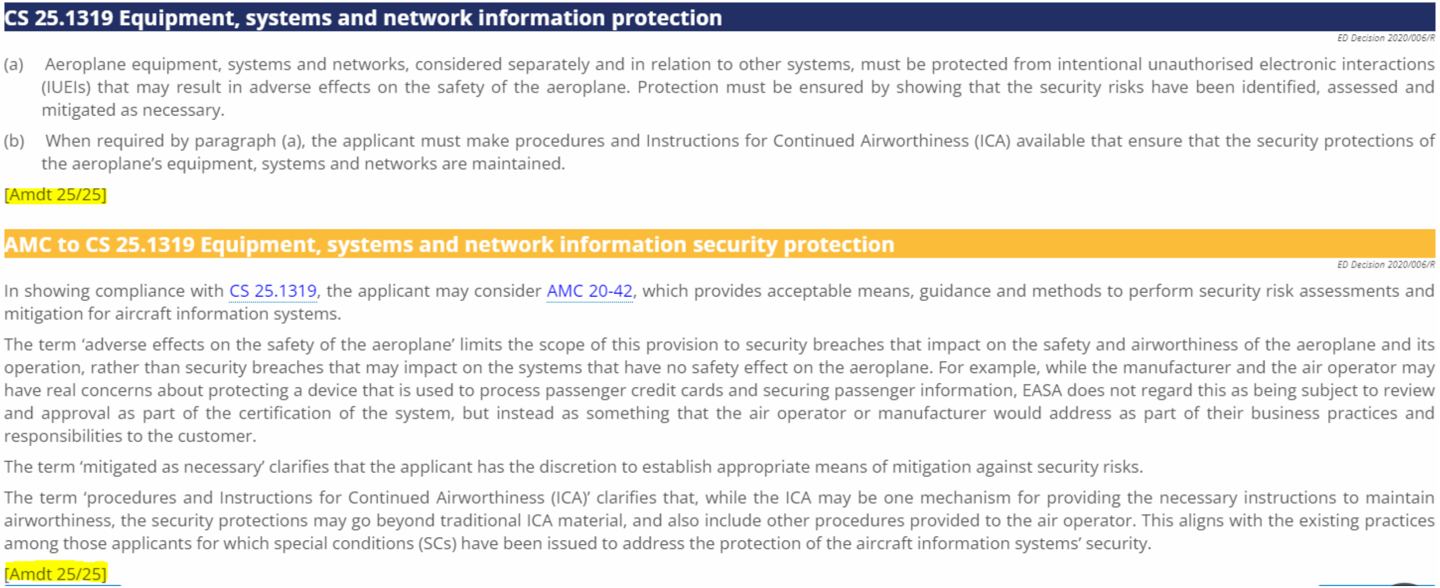
Cybersecurity requirements and AMC

Following up the updated mandate in the Basic Regulation of July 2018, EASA has implemented amendments to the certification provisions in order to address information security aspects in the certification process of aeronautical products. More precisely, the **EASA ED Decision 2020/006/R of July 2020** issued **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 the creation of **AMC 20-42, AMC/GM to CS-23 and AMC/GM to Part 21**.

Cybersecurity requirements in CS 25

Cybersecurity requirements incorporated into Certification Specifications and Acceptable Means of Compliance (Decision 2020/006/R of 01 July 2020)

Applicability Date: **01/JAN/2021**



CS 25.1319 Equipment, systems and network information protection

ED Decision 2020/006/R

(a) Aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions (IUEIs) 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's equipment, systems and networks are maintained.

[Amdt 25/25]

AMC to CS 25.1319 Equipment, systems and network information security protection

ED Decision 2020/006/R

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 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 air 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 air operator or manufacturer would address as part of their business practices and responsibilities to the customer.

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

The term 'procedures and Instructions for Continued Airworthiness (ICA)' 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 air operator. This aligns with the existing practices among those applicants for which special conditions (SCs) have been issued to address the protection of the aircraft information systems' security.

[Amdt 25/25]

Cybersecurity requirements and AMC

European Union Aviation Safety Agency

EASA European Union Aviation Safety Agency — *Annex VII to ED Decision 2020/006/R*

A

European Union Aviation Safety Agency

Cert

EASA European Union Aviation Safety Agency — *Annex VIII to ED Decision 2020/006/R*

A

European Union Aviation Safety Agency

Cert

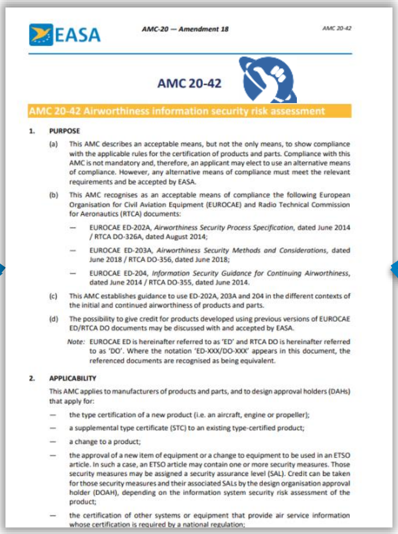
EASA European Union Aviation Safety Agency — *Annex II to ED Decision 2020/006/R*

Ac

Certification Specifications for Normal-Category Aeroplanes
(CS-23)
and
Acceptable Means of Compliance and Guidance Material to the Certification Specifications for Normal-Category Aeroplanes
(AMC & GM to CS-23)

CS-23 Amendment 5 / AMC & GM to CS-23 Issue 3

24 June 2020[1]



EASA — *AMC-20 — Amendment 18* — *AMC 20-42*

AMC 20-42

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 rules 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 as an acceptable means of compliance the following European Organisation for Civil Aviation Equipment (EUROCAE) and Radio Technical Commission for Aeronautics (RTCA) documents:

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

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

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

(c) This AMC establishes guidance to use ED-202A, 203A and 204 in the different contexts of the initial and continued airworthiness of products and parts.

(d) The possibility to give credit for products developed using previous versions of EUROCAE ED/RTCA DO documents may be discussed with and accepted by EASA.

Note: EUROCAE ED is hereinafter referred to as 'ED' and 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 manufacturers of products and parts, and to design approval holders (DAHs) that apply for:

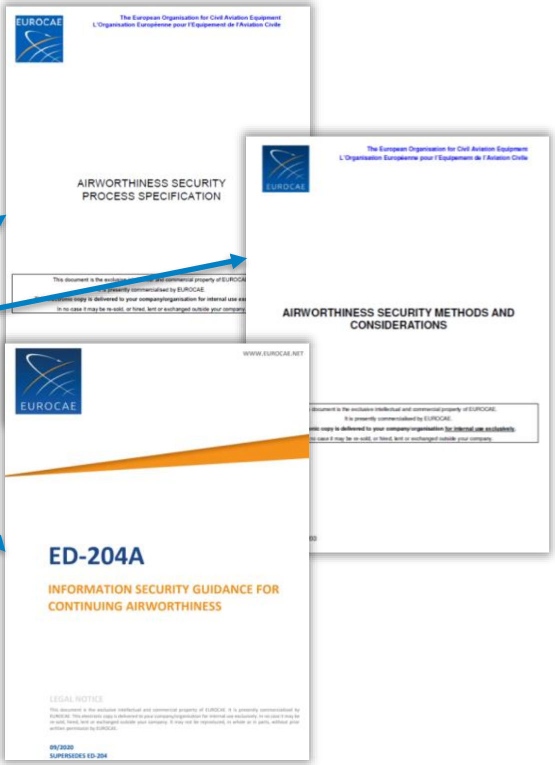
— the type certification of a new product (i.e. an aircraft, engine or propeller);

— 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, an ETSO article may contain one or more security measures. Those security measures may be assigned a security assurance level (SAL). Credit can be taken for those security measures and their associated SALs 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;



EUROCAE — The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Equipement de l'Aviation Civile

AIRWORTHINESS SECURITY
PROCESS SPECIFICATION

This document is the exclusive ... and commercial property of EUROCAE.
... is presently commercialised by EUROCAE.
... electronic copy is delivered to your company/organisation for internal use ex...
In no case it may be re-sold, or hired, lent or exchanged outside your company.

EUROCAE — The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Equipement de l'Aviation Civile

AIRWORTHINESS SECURITY METHODS AND CONSIDERATIONS

... document is the exclusive intellectual and commercial property of EUROCAE.
It is presently commercialised by EUROCAE.
...nic copy is delivered to your company/organisation for internal use exclusively.
...o case it may be re-sold, or hired, lent or exchanged outside your company.

EUROCAE — WWW.EUROCAE.NET

ED-204A

INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS

LEGAL NOTICE

This document is the exclusive intellectual and commercial property of EUROCAE. It is presently commercialised by EUROCAE. This electronic copy is delivered to your company/organisation for internal use exclusively. In no case it may be re-sold, hired, lent or exchanged outside your company. It may not be reproduced, in whole or in parts, without prior written permission by EUROCAE.

09/2020
SUPERSEDES ED-204

AMC 20-42 extracts

→ 2. Applicability

[...] STC to an existing type-certified product; change to a product [...].

→ 4. General Principles

(a) [...] information systems of the products [...] identified in section 2 should be assessed against intentional unauthorised electronic interaction (IUEI) security threat and vulnerability that could result in an unsafe condition. This risk assessment is referred to as “product information security risk assessment (PISRA) [...].

AMC 20-42 extracts

→ 4. General Principles

(b) The result of this assessment, after any necessary means of mitigation have been identified should be [...] systems of the product or part have no identifiable vulnerabilities, or those vulnerabilities cannot be exploited to create a hazard or generate a failure that would have an effect that is deemed to be unacceptable against the CS and AMC [...] including industry standards [...].

(c) When a risk needs to be mitigated, the applicant should demonstrate [...] that means of mitigation provide sufficient grounds for evaluating that residual risk is acceptable [...].

(d) [...] the applicant should [...] develop instructions [...] to maintain the information security risk [...] at an acceptable level, after the entry into service of the product or part.

AMC 20-42 extracts

→ 5. Product information security risk assessment (PISRA) [...]

i. determination of the security environment [...].

ii. identification of the assets;

iii. identification of the attack paths;

iv. assessment of the safety consequences of the threat to the affected assets;

v. evaluation, by considering the existing security protection means, of the level of threat that would have an impact on safety;

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

AMC 20-42 extracts

→ 5. Product information security risk assessment (PISRA)

[...] If they are not acceptable,

A. analysis of the proposed means of mitigation to ensure an acceptable level of safety,

B. implementation of means of mitigation,

C. evaluation of the effectiveness of the means of mitigation [...] with respect to the level of risk (combination of the level of threat and severity of the threat condition)

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

AMC 20-42 extracts

- 7. Reporting

  The operator of a product or part should report any information security occurrences to the designer of this product or part or the aircraft TC/STC holder, in a manner that would allow a further impact analysis and corrective actions [...]. If this impact analysis identifies the potential for an unsafe condition, the designer of that product or part should report it to the competent authority in a timely manner. [...].

- 9. Instructions for continued protection of product and part information security

  The applicant should identify the information security assets and protection mechanisms to be addressed by the Instructions for Continued Airworthiness (ICA) of the product or part [...] and develop the appropriate procedures to maintain the security effectiveness after the product or part enters into service.

EASA
European Union Aviation Safety Agency

CYBERSECURITY

Evaluating changes to aircraft

An Agency of the European Union

Aircraft modifications

→ EUROCAE standards provide guidance

acceptable means of compliance for PISRA for products and parts under Part 21

The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Equipement de l'Aviation Civile

AIRWORTHINESS SECURITY
PROCESS SPECIFICATION

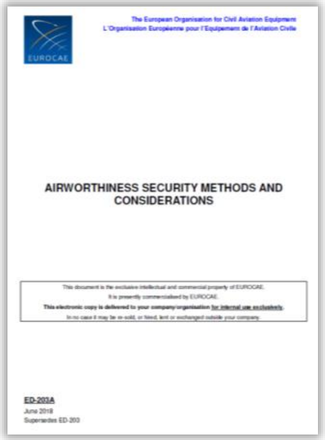
This document is the exclusive intellectual and commercial property of EUROCAE.
It is presently commercialised by EUROCAE.
This electronic copy is delivered to your company/organisation for internal use exclusively.
In no case it may be re-sold, or hired, lent or exchanged outside your company.

ED-202A
June 2014
Supersedes ED-202

ED-202B

Process for Security Risk assessment

- → Chapter 4
  Aircraft modifications
  Change impact analysis
- → Appendix B
  Change impact analysis questionnaire



The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Equipement de l'Aviation Civile

AIRWORTHINESS SECURITY METHODS AND CONSIDERATIONS

This document is the exclusive intellectual and commercial property of EUROCAE.
It is presently commercialised by EUROCAE.
This electronic copy is delivered to your company/organisation for internal use exclusively.
In no case it may be re-sold, or hired, lent or exchanged outside your company.

ED-203A
June 2018
Supersedes ED-203

ED-203A

Guidance material for PISRA (methods and considerations)

- → Section 2.3
  Type design changes and STC considerations

Major/Minor change (GM Part 21.A.91)

A change that may introduce the potential for unauthorised electronic access to product systems ‘major’ if there is a need to mitigate the risks for an identified unsafe condition.

1. 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.

2. 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 attack path.

3. 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.

4. The **modification of a security control** between a system of a more closed, controlled information security domain and a system of a more open, less controlled security domain.

Link to the rule

Major change: some examples

- → SATCOM installation which connects both to cabin and cockpit (criteria 1)
- → Wi-Fi/3G/4G access point to upload aircraft systems SW (criteria 1)
- → Addition of A429 link <u>sending</u> data from cabin systems to aircraft systems (criteria 1)
- → Wireless connection from sensors to aircraft systems offering scalable services (criteria 1 and criteria 2)
- → Update of the dataload interface with new HMI introducing change of security control (e.g. removal of PWD request at start up) – (Criteria 4)

EASA
European Union Aviation Safety Agency

CYBERSECURITY

Defining Level of Involvement

An Agency of the European Union

Defining Level of Involvement for Cybersecurity

Certification Memo

CM-21.A/21.B-001 - Issue 03

- → Attachment 6b
  defining cybersecurity LOI
- → CRD and CM published
  in Jun 2024

- → Definition of **novelty** and **complexity** criteria
- → **Criticality**: clarification that safety includes MAJOR for CS25 and CS23 level 4
- → **DOA performance**:
  applying Avionics rating may not be adequate
- → Clarification on the scope of the activities, data/documents to be assessed, etc..
- → Adjustment of LOI Risk Class to reflect the depth of the assessment by the cybersecurity expert

EASA
European Union Aviation Safety Agency

PART 21 WORKSHOP
CERTIFICATION CONFERENCE

Thank you for your attention.

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union