AMC 20-42

AMC 20-42 Airworthiness information security risk assessment

ED Decision 2020/006/R

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;

— 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 of the products, parts or equipment identified in Section 2 should be assessed against any potential intentional unauthorised electronic interaction (IUEI) security threat and vulnerability that could result in an unsafe condition. This risk assessment is referred to as a 'product information security risk assessment' (PISRA) and is further described in Section 5 of this AMC.

(b) The result of this assessment, after any necessary means of mitigation have been identified, should be that either the 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 certification specification and the acceptable means of compliance including industry standards for the product or part considered.

(c) When a risk needs to be mitigated, the applicant should demonstrate, as described in Section 5, that the means of mitigation provide sufficient grounds for evaluating that the residual risk is acceptable. The means of mitigation should be provided to the operators in a timely manner.

(d) Once the overall risk has been deemed to be acceptable, the applicant should, if necessary, 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 security environment for the information security of the product[1];

(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:

If they are acceptable, preparation of the justification for certification, including the means to maintain the risk at an acceptable level (see Section 9);

[1] To address the assumptions about external factors like organisations, processes, etc., see reference in ED-202A.

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 as in Section 8 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.

(b) The process for the Security Risk Assessment identified in ED-202A Section 2.1.1 is an acceptable means of compliance for performing the PISRA for products and parts under Annex I (Part 21) to Regulation (EU) No 748/2012[1]. Guidance material for the PISRA can be found in ED-203A.

6. RISK ACCEPTABILITY

Acceptable/Unacceptable Risk: whether or not a risk is unacceptable depends on the context and the criteria that are considered for the certification of the affected product or 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 xx.1309, may be not acceptable in the context of CS-25 products depending on the level of threat and the associated threat scenario. The same safety risk may be acceptable for products that are certified under CS-29.

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 appropriate. 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. 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

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 effectiveness of the means of mitigation.

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

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

[1] 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=1574094487050&uri=CELEX:32012R0748).

9. INSTRUCTIONS FOR THE 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 (for example, physical and operational security procedures, auditing and monitoring of the security effectiveness, key management procedures that are used as assumptions in the security assurance process), and develop the appropriate procedures to maintain the security effectiveness 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 an IUEI and should take any required corrective action accordingly. If an IUEI 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 21.A.3A of Annex I (Part 21) to Regulation (EU) No 748/2012.

According to Article 2(7) of Regulation (EU) No 376/2014[1], 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 the same Regulation 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 and the competent authority in a timely manner of the need and the means to mitigate the new risk (or the absence of a risk).

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

10. DEFINITIONS

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

[Amdt 20/18]

[1] Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007 (OJ L 122, 24.4.2014, p. 18) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0376).