EASA
European Union Aviation Safety Agency

ETSO Workshop
Information security protection

21.Sep.2022

Nicolas Durandeau – Avionics systems expert

Your safety is our mission.

An Agency of the European Union

Agenda

- → Context
- → Do I need security measure(s)?
- → How to develop my security measure(s)?
- → Conclusion

EASA
European Union Aviation Safety Agency

CONTEXT

Cybersecurity requirements and AMC

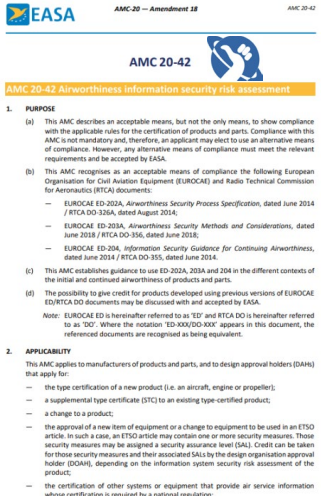
Since 2006 EASA introduced criteria to certify products including information security aspects.

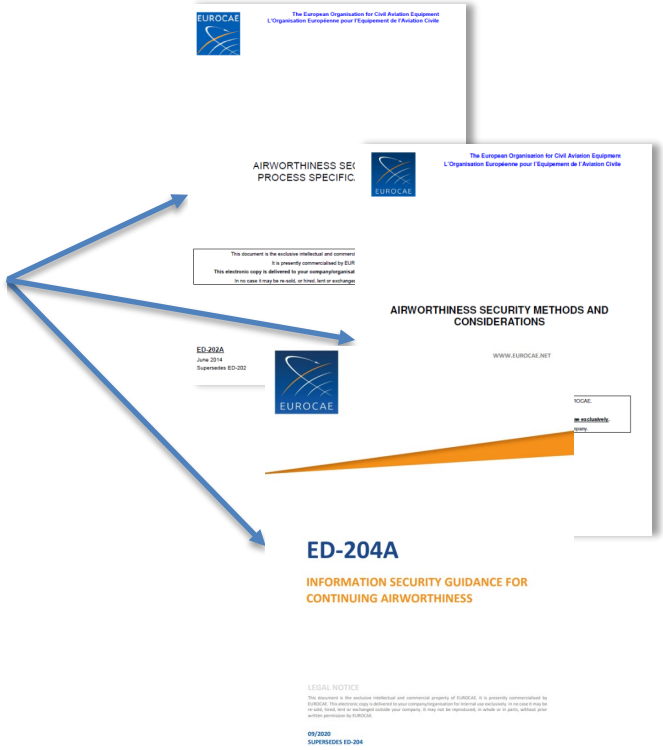
These requirements were amended and incorporated into Certification Specifications and Acceptable Means of Compliance (Decision 2020/006/R of 01 July 2020)




In the near future, it will also certify UAS.

Cybersecurity requirements and AMC





CS ETSO and AMC 20-42

→ CS ETSO subpart A amendment 15 introduces:

SUBPART A — GENERAL

2. STANDARDS TO MEET TECHNICAL CONDITIONS

[…]

2.6 Information security protection

An ETSO article may be designed with a security assurance level (SAL) that is appropriate for specified security measures, according to the procedure provided in AMC 20-42.

→ AMC 20-42:

[…]

— 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;

→ Further clarification of EASA expectations follows…

EASA
European Union Aviation Safety Agency

Do I need security measure?

The risk acceptability matrix

- The need for security measure stems from the risk assessment at aircraft or system level

TABLE 2-2: AIRWORTHINESS RISK ACCEPTABILITY MATRIX

	Severity of the Threat Condition Effect				
Level of Threat	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
Moderate	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
Low	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
Extremely Low	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable*

- **Step1:** Assume the applicable threat conditions AND related threat scenarios
- **Step2:** Assume the expected level of threat

Step1: Assessing the connectivity and interfaces

- The connectivity should be understood to determine the behavior of the connected systems considering safety effects caused by intentional unauthorized electronic interaction (IUEI) occurring in the system under assessment. (ref ED-203A §2.2.2)

- Listing the connectivity features of the equipment:
  - Physical interfaces: USB plugs, SD slot, Ethernet ports…
  - Wireless interfaces 802.11 b/a/c/g/n/ac/ax, Bluetooth/cellular/NFC/RFID/Infrared
  - Logical connections: Network protocols (IP, ARINC664P7…), services (DNS, FTP, Telnet, HTTPS…)
  - Accessibility Requirements: expected location

Step1: Assessing the connectivity and interfaces

→ Listing the expected interfaces of the equipment inside and outside of the aircraft:

- → Write access through internal connections to one or more onboard systems?
- → External untrusted services connectivity (e.g. including airline operations centers, maintenance equipment, or wireless connections)
- → Bidirectional internal connections to other Minor or lower systems?
- → Field loadable software (FLS), Databases transmitted through the aircraft dataloading functions from the external interfaces that support maintenance

Step1: Security environment and trust

- Physical attack is out scope: no consideration of plugs, connectors, cables and any piece of equipment that are *not readily accessible* to unauthorized persons
- Evaluate the trustworthiness of external entities that may be a threat source if untrusted (list given in §2.6 of ED-203A)
- Type of attacks (on path attack, DoS…) along with threat sources (§3.1.3 from ED-203A)
- Security environment and trustworthiness assumptions are to recorded in the integrator guidance document (SSIG)

Step1: Assume the threat condition

- Given:
  - Connectivity analysis
  - Assumptions made on aircraft interfaces and security environment
- Threat conditions and the related threat scenarios with safety impact can be anticipated

TABLE 2-2: AIRWORTHINESS RISK [illegible]CEPTABILITY MATRIX

	Severity of the [illegible]reat Condition Effect				
Level of Threat	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
Moderate	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
Low	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
Extremely Low	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable*

Step2: Assume the Level of threat

- Difficult to evaluate without knowing mitigations put at aircraft level → **conservatism should apply**
- Depends on a given threat scenario and various methods can be used (e.g. Appendix E of ED-203A):
  - Window of opportunity
  - Preparation means
  - Execution means

TABLE 2-2: AIRWORTHINESS RISK ACCEPTABILITY MATRIX

	Severity of the Threat Condition Effect				
Level of Threat	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
Moderate	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
Low	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
Extremely Low	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable*

EASA
European Union Aviation Safety Agency

How to develop my security measure(s)?

Security measures development

- → Develop the adequate Security measure by
  - → Refining the attack path at the lowest level
- → Using state of the art technique
  - → ED-203A §5
  - → Ensuring independence/diversity/isolation

Security assurance

→ Security measures perform as intended and that the final product is acceptably free of known and exploitable vulnerabilities, which may be introduced during development.

TABLE 2-2: AIRWORTHINESS RISK ACCEPTABILITY MATRIX

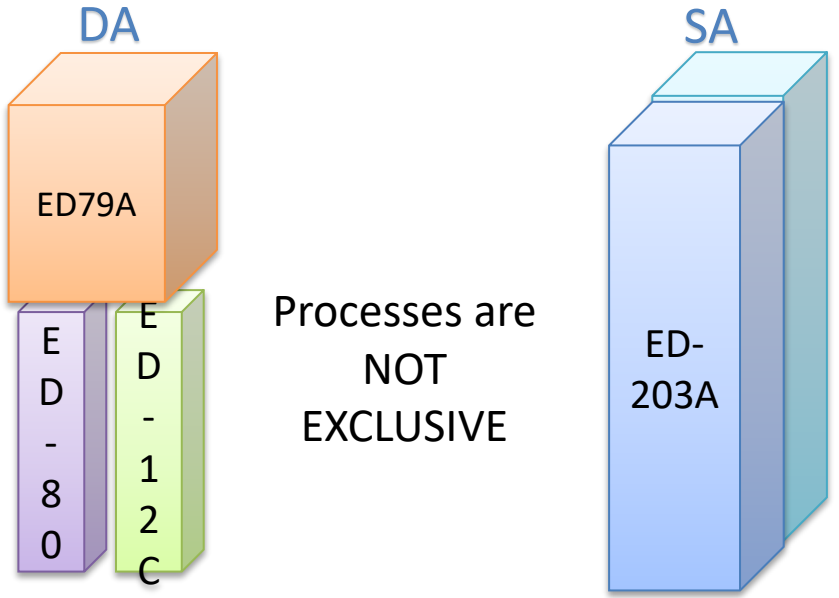
	Severity of the Threat Condition Effect				
Level of Threat	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
Moderate	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
Low	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
Extremely Low	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable*

TABLE 4-4: SECURITY ASSURANCE RELATION TO THREAT CONDITION SEVERITY

Threat Condition Effect Severity	Minimum Security Assurance
Catastrophic	SAL 3 + SAL 2
Hazardous	SAL 3
Major	SAL 2
Minor	SAL 0
No Safety Effect	SAL 0

Security assurance objectives

- Two types of objectives:
  - Security development assurance:



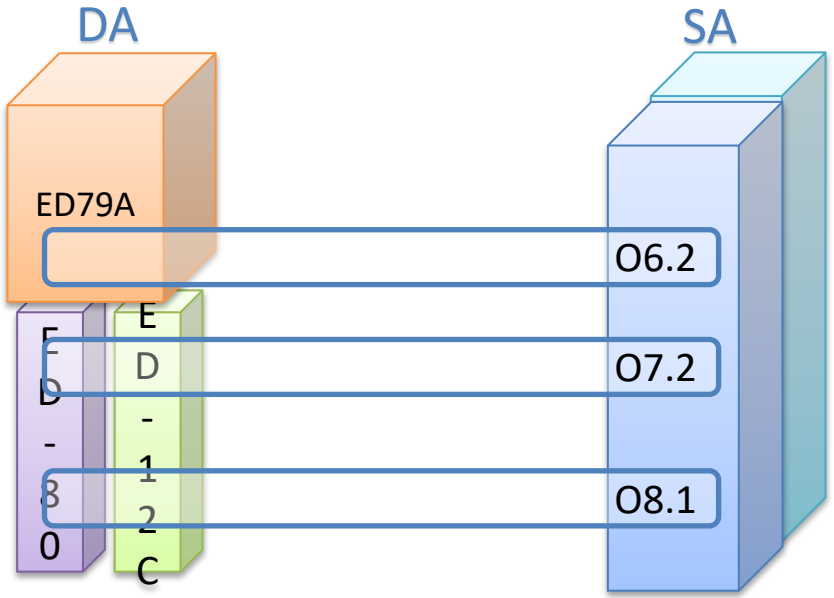
  - Security specific assurance:
    - Security risk assessment
    - Vulnerability/refutation testing

Security development assurance 1/2

A.1.2 Security Development Assurance

TABLE A-2: SECURITY DEVELOPMENT ASSURANCE OBJECTIVES ALLOCATION TABLE

Ref.	Objective	Scope	SAL 3	SAL 2	SAL 1	SAL 0	Security specific	Document sections
Requirements Objectives								
O6.1	Security requirements, security measure interfaces and assumptions are defined.	AC, S, I	R	R	A	N	no	4.2.1, B.2.8
O6.2	Security requirements are validated. Assumptions are negotiated with the Authority or validated.	AC, S, I	R*	R	A	N	no	4.2.1, B.2.8
O6.3	Derived requirements are defined and justified.	S, I	R	N	N	N	no	4.2.1, B.2.8
O6.4	Security requirements comply with higher level requirements.	S, I	R	R	N	N	no	4.2.1, B.2.8
O6.5	Derived requirements are validated against security risk assessments.	S, I	R*	N	N	N	augmented	4.2.1, B.2.8



→ On the condition security process is integrated with DA/ SW DA /HW DA, some **security development assurances** objectives can be directly fulfilled.

Security development assurance 2/2

A.1.2 Security Development Assurance

TABLE A-2: SECURITY DEVELOPMENT ASSURANCE OBJECTIVES ALLOCATION TABLE

Ref.	Objective	Scope	SAL 3	SAL 2	SAL 1	SAL 0	Security specific	Document sections
Requirements Objectives								
O6.1	Security requirements, security measure interfaces and assumptions are defined.	AC, S, I	R	R	A	N	no	4.2.1, B.2.8
O6.2	Security requirements are validated. Assumptions are negotiated with the Authority or validated.	AC, S, I	R*	R	A	N	no	4.2.1, B.2.8
O6.3	Derived requirements are defined and justified.	S, I	R	N	N	N	no	4.2.1, B.2.8
O6.4	Security requirements comply with higher level requirements.	S, I	R	R	N	N	no	4.2.1, B.2.8
O6.5	Derived requirements are validated against security risk assessments.	S, I	R*	N	N	N	augmented	4.2.1, B.2.8

→ Some objectives are augmented because they have additional security considerations

Security specific assurance

Vulnerability Identification Objectives								
O2.1	Vulnerabilities in security measures and assets (including COTS) are identified and evaluated for their potential impact on safety.	AC, S, I	**R**	**R**	**A**	**N**	yes	4.1.2, B.2.2, B.2.3
O2.2	Vulnerabilities are treated according to their evaluation.	AC, S, I	**R**	**R**	**A**	**N**	yes	4.1.2, B.2.2, B.2.3
Security Refutation Objectives								
O3.1	Refutation analyses are performed to identify new vulnerabilities.	AC, S, I	**R***	**R***	**R**	**N**	yes	4.1.3, B.2.4, B.2.5
O3.2	Refutation tests are performed to evaluate the exposure of vulnerabilities in the security environment and to challenge the vulnerability evaluation.	AC, S, I	**R***	**R***	**R**	**N**	yes	4.1.3, B.2.4, B.2.5

- Assurance objectives that are not related to other development assurance standards
- Objectives: Security risk assessment/ Vulnerability identification/ Refutation/ Deployment/ continued effectiveness

EASA
European Union Aviation Safety Agency

Conclusion

Wrap up and take away

- Benefit: Ease the integration of equipment in an information security airworthiness context (and maybe other contractual advantage)
- Importance of the security assumptions (for the installer and operators)
- DAL is not SAL (and vice et versa)
- Importance of vulnerability management for suppliers (security specific assurance objectives)

EASA
European Union Aviation Safety Agency

Thank you for your attention!

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union

EASA
European Union Aviation Safety Agency

Annex

Continuing AW

→ ED-204A and ED-206

Typical security environment assumptions

→ Extract from ARINC ABN 035:

Communication of information	Accessible by an unauthorized user (including remote access)	Inaccessible by an unauthorized user
Communications aircraft-ground via Gatelink (e.g., WIFI, GSM, GPRS)	X	
Communications aircraft ground via radio (e.g., HF, VHF, SATCOM,)	X	
ACARS	X	
Communications between Airframe mfg, MRO, suppliers, airline, ANSP	X	
Navigation aids (e.g., VOR, DME, ILS)		X
Communications between aircraft in flight (e.g., TCAS, ADS-B)		X