European Union Aviation Safety Agency

Comment-Response Document 2019-01

RELATED NPA: 2019-01 — RMT.0648 — 24.6.2020

Table of contents

1. Summary of the outcome of the consultation

287 comments were made by 32 stakeholders, including individuals, national aviation authorities (NAAs) or organisations as well as industry companies and associations.

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

Further to the comments received, the text proposed in the NPA has been modified in some parts, for improvement or clarification purposes.

The individual comments and the responses to them are provided in Chapter 2 of this CRD.

2. Individual comments and responses

In responding to the comments, the following terminology has been applied to attest EASA's position:

(a) **Accepted** — EASA agrees with the comment and any proposed amendment is wholly transferred to the revised text.

(b) **Partially accepted** — EASA either agrees partially with the comment, or agrees with it but the proposed amendment is only partially transferred to the revised text.

(c) **Noted** — EASA acknowledges the comment, but no change to the existing text is considered to be necessary.

(d) **Not accepted** — The comment or proposed amendment is not shared by EASA.

(General Comments)	-

comment	*6* comment by: *DGAC France* Please note that DGAC France has no specific comments on this NPA.
response	**Noted**

comment	*7* comment by: *European Powered Flying Union* European Powered Flying Union (EPFU) thanks EASA for preparing this NPA. We studied it, with air operations as starting point, as we think these aspects are as important as the aspects that will be put forward by aircraft and equipment manufacturers. Two questions at the beginning of our commenting the NPA: 1) Why did the Agency not create a Rulemaking Group for its preparation? 2) Should not all relevant RPAS products have been included, as well as CS-LSA, this to get a complete picture of all involved?
response	**Noted** Please find below EASA's responses to the two questions: 1) EASA, in the NPA, has considered the recommendations of the ARAC ASISP WG, in which EASA was represented. EASA considers that this WG was composed of members with the appropriate level of expertise to work on the issue, and that there was no need to duplicate such a group to draft the NPA. 2) RPAS products are not considered in the current task, but will be handled in a future NPA. CS-LSA products are also not considered at this stage (low risk).

comment	*39* comment by: *FAA* Page: General Para AMC 20-42 Referenced Text: AMC 20-42

Comment: The proposed AMC 20-42 provides one of the certification authority's recognition mean of cybersecurity compliance requirements for all products, equipment, and parts. AMC 20-42 provides detailed cybersecurity guidance for all platforms: products, equipment and parts, however, having generic guidance may result in either inadequate or excessive cybersecurity compliance requirements, since each product, equipment and part has its own uniqueness, complexity of design, maintenance, operation, and install level. Therefore, recommend that the proposed AMC 20-42 be tailored to the specific requirement of each platform: product, equipment, part with respect to design implementation, installation and maintenance.
Proposed Resolution: Consistent with discussion within the ARAC working group, FAA continues to study potential sources of guidance for Parts other than 25. Specifically, we hope to be able to base our guidance on industry standards put forth by RTCA and ASTM, and depending on the product type, potentially a combination of both. Ultimately, our decisions regarding guidance will be risk-based and consistent with the safety continuum, and it will be tailored to applicable category.

response **Noted**

comment *44* comment by: *Europe Air Sports*

Europe Air Sports welcomes EASA's attention to cybersecurity threats.
However, we caution that Cybersecurity is not only a technical issue; there may well be politcal elements involved in cybersecurity attacks.

Please see our specific comments.

response **Noted**

comment *48* comment by: *FOCA Switzerland*

a) General support for the objective of the NPA:

FOCA fully supports EASAs efforts to add cybersecurity requirements to aircraft, at least for future designs. We generally support the objective of the NPA and believe in the benefit of it.
However, we do not share the view that "No drawback or adverse economic impacts are expected". Mostly because the inclusion of modified airworthiness certificate in any class of products (CS 23/25/27/29, Engine…) as well as any type of possible authorization (not only Type Certification but any relevant design changes eg. STC, ETSO) in the scope will have impact at organization level. Be it with regard to training or the definition of new processes such as performing an additional risk assessment dedicated to cyber security. Furthermore, it might be difficult to receive data from the original manufacturer for this additional task and it is a requirement which might not have been taken into account in the original business plan of the company (e.g. when dealing with avionics STC, there might not have been the need to address systems connected by safety networks with the TC holder).

Therefore, in order to reduce the expected economic drawback, we propose the following:
1. Gradual implementation of the NPA:

- First step: CS 25, CS 29, CS-E [initial Type certification only, Design Change, STC (new or change to it)]; E-TSO [initial authorization]
- Second step: CS 27 and CS 23 [initial type certification only]

- Third step: CS-23, SC-27[design change, STC (new or change to it), ETSO major change]

2. For design change and STC:

We suggest a requirement to analyse whether proposed changes cause new threats or not. Only if this is the case, the new requirements should be applicable. In other words, an applicant of STC or design change could be negatively affected by an original situation which was designed when no such requirements were in place resulting in unlevel playing field which could consequently prevent changes that might be beneficial in safety. Due to the high interconnectivity of systems and networks, the principle that activities are limited to the area which are affected by the change, is not applicable - the cyber security assessment and the protection must be expanded and modified to already installed systems.

b) Overlap with RMT 0.720:

This NPA on aircraft cybersecurity (RMT 0.648) as currently drafted has overlaps with RMT 0.720 on Part-AISS. The second NPA has however not yet been published, which means that States/organisations not involved in the rule-making progress for 0.720 have not been able to look at both pieces of the coin.

The following comments are based on FOCA's participation in RMT 0.720 and are based on the draft available at the time of writing of these comments:

i. The rules on aircraft cybersecurity should match the horizontal rules in Part 0.720. Care should be taken not to create duplication or gaps. In our view, combined reading of both is necessary once comments to both NPAs have been received.

ii. Care should be taken regarding cybersecurity requirements stemming from aircraft design, that would need to be implemented throughout the lifecycle by other actors in the system (e.g. maintenance, operators etc.) The regulations should create the legal basis for this. There is also a question whether PART-21 should also need to be amended, as some points relevant to cybersecurity are at an organizational level.

iii. Within the discussions on RMT 0.720, it was agreed to take a horizontal and functional approach. This implies that it is not necessarily the size of the airport or operator that should determine whether the rules apply or not, but rather the types of functions (information systems) used and the criticality thereof.

iv. In this sense, for the topic of cybersecurity, a distinction between aircraft size or type may be misleading. In some cases, and depending on the type of operations, some operations with smaller aircraft or rotorcraft may require very precise information and may have smaller margins of error regarding incorrect of unavailable information or systems following a cyberattack

The question of which level of implementation is proportionate for which aircraft type should be discussed and the proportionality may depend rather on functionality and
operations than on aircraft size/type. This should be discussed with experts to find a common understanding on proportionality of the rule.

v. There is currently no legal link between RMT 0.648 and RMT 0.720. Will there be one? Will implementation be coordinated?
vi. We are missing the implementation timelines for RMT 0.648. We would support a gradual implementation. This would lessen the burden on industry, certification and oversight. Gradual implementation would allow for learning opportunities along the way.
vii. We also support introducing the new rules especially for new designs.

Any point on "retrofitting" would also need to be discussed with experts to find a common and proportional point of view.

response

a) Accepted
This will be better reflected in the Explanatory Note of the final deliverable (i.e. ED Decision).

b) Noted
EASA does not consider that there is an overlap between the two tasks. While NPA 2019-01 focuses on certain products, NPA 2019-07 'Management of information security risks' (RMT.0720)[1] proposes provisions that are applicable to competent authorities and organisations in all aviation domains.

comment *69* comment by: *FAA*

Note:
Per the FAA Strategic Plan for 2019:
Safety Continuum:
The key to safety lies in effectively managing risk. The successful approach to risk management is not one-size-fits-all. Too little rigor and oversight can leave the system exposed. Too much rigor and oversight can tax resources and stifle safety-enhancing innovations. The optimum real-world level of safety is achieved by applying the right level of rigor at the right time and place for any given situation—a tailored approach. The safety continuum is a data-driven model that informs this balance.

This NPA proposes Rotorcraft leap from a few Certification Action Items (CAI's) and FAA Issue Papers to the imposition of massive cost prohibitive Transport-level regulations and guidance on the Rotorcraft industry.

Comment:
The recommendations for regulations and guidance that came out of the ARAC in 2016 contained elements that are being ignored by EASA in this most-recent 'one size fits all' rule-making push (NPA). Here are a few of relevant items quoted from the ARAC:

[1] https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-07

Recommendation from
"The ASISP working group notes that DO-356 and ED-202, 203, and 204 are not aligned with respect to their applicability to Rotorcraft and recommends these documents be updated and tailored to better address Rotorcraft."

"The Rotorcraft industry believes that experience must be developed with both the GA and RTCA standards before they can be used for compliance with the regulations."

"ASISP working group sees a need to tailor the compliance method for transport category airplanes to be more suitable to proportional security needs in Rotorcraft. This can be done by tailoring the existing RTCA standards or by tailoring the GA recommended practices and guidance for ASISP."

Now some may say the Rotorcraft industry didn't participate and thus never even attempted to tailor the above. This may be true; however, it does not circumvent the need, and is not justification for the imposition of the massive and cost prohibitive Transport-level regulations and guidance on the Rotorcraft industry.

Recommendation:
• Continue working with Issue Papers using CFR 27/29.1309 as the rule basis until we gain a consistent understanding of the subject between all parties as it pertains to aircraft security in the Rotorcraft Industry.

o Recognize this effort and further enhance our experiences through the use of EASA's Certification Review Items (CRI's) and Certification Action Items (CAI's).

o This needs to continue and mature before considering the development of Special Conditions and new Regulations.

• Work with EASA and the Rotorcraft Industry to establish tailored guidance from Part 25 Transport documents RTCA DO-326, DO-355, and DO-356 for Part 29 Rotorcraft

o Finish the ASTM effort to develop Best Practices for GA and Part 27 and incorporate applicable elements as warranted for Part 29 Rotorcraft.

Note: The intent is to cherry-pick and stream-line from all applicable sources. The outcome can result in updated ACs or Industry Standards.

• Apply the Safety Continuum approach to establish guidance for security and other needs of the Rotorcraft Industry based on an understanding of the different classes of Rotorcraft and installed equipment. For example, what we have been seeing in Rotorcraft is the use of EFB connectivity in the cockpit to load software, databases, etc. Many of these external access points can be assessed and mitigated without having the need for new regulations.

response **Noted**

comment *74* comment by: *FAA*

Comment: Cyber security is a broad term like information security, whereas network security is one aspect of cyber security

Suggestion: replace "network security" with "cyber security"

response **Partially accepted**
The terminology will be reviewed to ensure consistency throughout the document.

comment *75* comment by: *FAA*

Comment: Configuration control (test bench configuration including hardware and software part number, connections, switch positions, and other documentation necessary to be able to reproduce the test conditions; type of tools; mode or condition the aircraft or system during testing, etc..)
Suggestion: add to either section 8 or appropriate section: "All security testing used to demonstration regulatory compliance must be performed on conformed equipment. "

response **Noted**
This is part of a usual certification demonstration and configuration control for airworthiness. Information security adds only some difficulties to the exercise as there is not always 'conformed equipment' for security test. The topic of 'conformed equipment' is more appropriate to be addressed at the level of industry standards, for instance in ED 203A (Table 4-2).

comment *104* comment by: *Rolls-Royce plc*

Commentary Summary 1:

What are the units for assessing whether we meet the acceptable/unacceptable risk threshold, and what number is the threshold? For other safety things we generally use hazardous events per engine flying hour. Is the intent we somehow translate cybersecurity risks into this unit of currency (would this even work well?) and keep the E-9 threshold still?

Commentary Summary 2:

There have been security scares in the media around aircrafts being allegedly hacked, which has affected public perception on safety of aircraft. To date, no safety impact has been found due to these alleged hacks, this NPA does not address these kinds of scenarios. Is it within EASA's remit to assist (via standards, etc.) in the assurance of public views on safety? Understand view of EASA on perceived risk by public.

response **Noted**
Commentary Summary 1: the expected guidance can be found in ED-203A (Table 2-2).

	Commentary Summary 2: EASA is committed to raising public awareness about safety with dedicated communication.

comment	*128* comment by: *UK CAA* **Page No:** General Comment **Paragraph No:** **Comment:** There does not appear to be any suggested standardised forms of compliance demonstration. **Justification:** By omitting these, this could result in a lack of consistency of applications dependent on the reviewer. **Proposed Text:** We recommend that the forms are included
response	**Not accepted** ED-202A, ED-203A and ED-204 are considered sufficiently detailed standards. This, however, does not prevent the development of job aids, checklists, trainings, etc.

comment	*129* comment by: *UK CAA* **Page No:** General Comment **Paragraph No:** **Comment:** No competency standards have been identified for personnel undertaking compliance verification with this discipline. We do not expect the cyber review and airworthiness certification to be undertaken by the same individual. **Justification:** By omitting these, this could result in a lack of consistency of competency dependent on the reviewer. **Proposed Text:** We recommend that competency standards are included
response	**Noted** This will be addressed in Part-AISS.AR, point AISS.AR.100 ‘Personnel requirements’.

comment	*165* comment by: *EUROCONTROL* EUROCONTROL reviewed the NPA and does not have any comments.
response	**Noted**

comment	*182* comment by: *John Connolly (Atkins)* 1. It is noted that no changes CSXX – 1309 Equipment, Systems and installations is proposed. The “improper functioning would reduce safety” should be amended to include “unauthorised electronic interactions” to make it coherent with CSXX – 1319.

response	**Noted** Reference to CSXX-1319 in 1309 may be proposed in a future amendment to CS-25.

comment	*183* comment by: *John Connolly (Atkins)* The changes offered tend to be "Information Technology" centric, however "Operating Technology" maybe vulnerable to cyber threats by poor design, manufacture, test, installation, operation and maintenance and management by design of these vulnerabilities this should be addressed at the avionics level.
response	**Noted**

comment	*184* comment by: *John Connolly (Atkins)* Little or no guidance or reference to cyber security standards is made, including where these standards are not appropriate to air systems.
response	**Not accepted** The relevant aeronautical information security standards are addressed in the proposed AMC 20-42.

comment	*185* comment by: *John Connolly (Atkins)* Change the term from Cyber Security to Cyber Resilient. Air Systems (aircraft and mission critical ground systems) should be resilient to cyber-attack. They need to be able to maintain their airworthiness during operation both on the ground and in the air whether the attack is on the ground systems on directly on the aircraft.
response	**Not accepted** This is part of the risk assessment. As a result, some systems may need to be fail-safe or resilient, depending on the impact and likelihood.

comment	*187* comment by: *John Connolly (Atkins)* The amendment and supporting references point to IUEI as the only source of threat, yet it fails to recognise the role unintended interventions may have. There is a 2x2 matrix of 'intended' to 'unintended' vs 'malicious' to 'non-malicious' threats to help focus the types of mitigations that may be needed to be employed. This should be added as guidance.
response	**Noted** The definition for 'IUEI' can be found in ED-202A.

comment	*189* comment by: *John Connolly (Atkins)* The amendment focuses on impacts to Safety and fails to discuss cyber effects that impact Safety and Functionality. A cyber-attack may deceive, deny, destroy, degrade and/or disrupt the air system in such a way as to adversely impact safety and desired functionality.
response	**Noted**

While NPA 2019-01 focuses on certain products, NPA 2019-07 'Management of information security risks' (RMT.0720)[2] proposes provisions that are applicable to competent authorities and organisations in all aviation domains to avoid disruption of the air system.

comment *190* comment by: *John Connolly (Atkins)*

The amendment does not recognise the potential safety and security vulnerabilities that may be inherent in the designs of legacy systems that are inherited from previous systems and airframes.

response **Noted**
Changes to legacy systems are outside the scope of this task; nevertheless, cybersecurity-relevant issues in legacy products may be addressed by special conditions (SCs).

comment *191* comment by: *John Connolly (Atkins)*

AMC 20-42 recognised EUROCAE ED 202A, ED-203A and ED-204 should be updated to better address:
· supply chain and third party risks;
· monitoring and the effect this may have on CSXX – 1309 "information concerning unsafe operating conditions" and "minimising aircrew errors";
· Media connectivity;
· Privileges;
· Operational resilience priorities;
· Segregation including the effects this may have with respect to system solutions such as Integrated Modular Avionics; and
· Change assurance.

response **Noted**
Some of the above will be also addressed in Part-AISS (refer to NPA 2019-07 'Management of information security risks' (RMT.0720)[3]) or they are part of the security risk assessment of the product.

comment *236* comment by: *Aerospace and Defence (ASD)*

From a general point of view, ASD has a positive position regarding NPA 2019-01, which introduces aircraft cybersecurity new considerations in the certification specification, in place of the currently existing Special Conditions.

ASD supports also the creation of the AMC 20-42 that recognise the industrial standards for cybersecurity jointly released by EUROCAE WG-72 and RTCA SC-216.

response **Noted**

comment *237* comment by: *Aerospace and Defence (ASD)*

[2] https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-07
[3] https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-07

Commented text
Based on the fact ED-203A guidelines were developed in the context of 14 CFR Part 25 and EASA CS-25, the need to tailor these guidelines has been recognised by customising the text of CS27.1319 and CS29.1319 compared to CS 25.1319. This need for tailoring may also be required for defining the acceptability of the risk and the security assurance measures.

Furthermore, the proposed CS27.1319 and CS29.1319 requirements are indicating that protection must be ensured "as necessary". Guidance material is necessary to clarify what is meant by "as necessary". Indeed, the ARAC ASISP Working Group report specified that "The term "mitigated as necessary" clarifies that the applicant has discretion, as the applicant has for all risks, to establish appropriate mitigations against security risks.

In order to provide legal certainty in the interpretation of the CS requirement and to recognise the specific tailoring need for CS-27 and CS-29 product we propose to introduce a new sentence to GM 27.1319 and GM 29.1319

Proposed modification
Add new sentence to GM 27.1329 and GM 29.1329.

The term "As necessary" indicates that the identification, assessment and mitigation of the security risks should consider specific architectural and operational capabilities of the rotorcraft. In doing so, the applicant may propose criteria suitable for his product, for example by tailoring the standards referred to in AMC 20-42.

response **Partially accepted**

comment *287* comment by: *GE Aviation*

GE Aviation would like to thank EASA for the work in coordinating efforts with other regulatory authorities to establish consistent and harmonised rules, with industry for establishing suitable standards for use as Acceptable Means of Compliance and for the opportunity to provide comments on this NPA.

GE Aviation has performed a review by all relevant areas within the company and submitted all comments through industry organisations AIA, ASD and GAMA to reduce duplication of comments and to try to ensure industry consensus in comments on the NPA and requests for updates.

response **Noted**

comment *295* comment by: *Bombardier*

Bombardier concurs with the comments submitted by GAMA.

response	**Noted**

comment	*296* comment by: *THALES AVS FRANCE* From a general point of view, THALES Avionics has a positive position regarding this NPA which introduces aircraft cybersecurity new considerations in the certification specification, in place of the currently existing Special Conditions. THALES Avionics also supports the creation of the AMC 20-42 that recognizes the industrial standards for cybersecurity jointly released by EUROCAE WG-72 and RTCA SC-216. THALES Avionics has contributed to the consolidation of comments within ASD and concur then with all ASD comments. Therefore no additional comment is provided here.
response	**Noted**

EXECUTIVE SUMMARY p. 1-2

comment	*186* comment by: *John Connolly (Atkins)* Terminology is inconsistent throughout the document. With the mixture of terms such as Information Security, Security, Cybersecurity. Some terms such as Cybersecurity Threat are not recognised terms in the cyber industry and hence require specific meanings. The term 'Cyber-threat' is sufficient and more precise.
response	**Partially accepted** The terminology will be reviewed to ensure consistency throughout the document.

comment	*188* comment by: *John Connolly (Atkins)* There is no reference to a cyber-vulnerability assessment including penetration testing at the system of systems, system and product levels. This is a vital component of the testing process and should be performed alongside that of functional and safety testing.
response	**Not accepted** Information security testing is addressed in AMC 20-42.

comment	*207* comment by: *L. Riegle AIA* 2.4 - What are the expected benefits and drawbacks of the proposals "No drawbacks or adverse economic impacts are expected." Proposed modification Cost of development is expected to increase. These costs are expected to be less than the positive impact on safety and security for the population. Either delete statement or amend to reflect realistically that changes are not cost neutral.

	Justification As a new (or at least changed) process is being introduced to Design Organizations and their supply chain, it cannot be expected to state that there will be no adverse economic impacts. As a minimum, cybersecurity studies will need to be performed which will raise costs.
response	**Accepted** This will be better reflected in the Explanatory Note of the final deliverable (i.e. ED Decision).

2. In summary - why and what | 2.1. Why we need to change the rules — issue/rationale p. 4

comment	*1* comment by: *Bryn Jones* While cybersecurity is an unauthorised human attack upon aircraft and aviation systems, it's manifestation and impact may not appear to be any different to environmental (cosmic rays, solar protons, neutrons) and electromagnetic (solar radio bursts, geomagnetic activity) causes. Single Event Effects (SEE's) and Multiple Bit Upsets (MBU's) can occur within any avionics components. Differentiating between cyber and environmental interactions may therefore, not be straightforward nor identifiable. Awareness of the space weather environment must also be considered within the scenario of investigating cybersecurity so that correct, focused actions and mitigation is carried out.
response	**Noted**

comment	*9* comment by: *European Powered Flying Union* 2.1. Why we need to change the rules - issue/rationale page 4/20 block 8 The Agency writes "since aircraft systems are increasingly connected..." This is an obvious fact. We therefore think that provisions must be prepared to cover autonomous flights operated with aircraft not covered with the CS's included in this NPA. In order not to be too late we propose to incorporate RPAS/autonomous flight ops in this rulemaking activity. After reading your statement in 4.1.1. Safety risk assessment, 5th text block, page 16/20, "since for all categories of aircraft, systems are increasingly connected and thus potentially vulnerable...", we promote a study on operational aspect, the rationale: "all" these aircraft operate in a common airspace, therefore all CS's should be looked at, and all relevant RPAS should be integrated without delay. In addition, political aspects should not be disregarded: unauthorised access, (mis-)use, disclosure, denial, disruption, (unauthorised) modification, distruction are terms the Agency uses repeatedly in the NPA. Therefore: Purely technical AMC and GM are not sufficient to protect us from criminal activities, more should be done, at political levels.

response **Noted**
RPAS products are not considered in the current task, but will be handled in a future NPA.
While NPA 2019-01 focuses on certain products, NPA 2019-07 'Management of information security risks' (RMT.0720)[4] proposes provisions that are applicable to competent authorities and organisations in all aviation domains.

comment *17* comment by: *Universal Alloy Corporation Design*

The need for Cybersecurity is totally understood and unreservedly supported. The global rise in the numbers and capabilities of individuals and state sponsored organisations who are willing to "hack" into any company or institution is a fact. There is no reason to believe that such cyber terrorists would baulk at hacking into an aircraft system and EASA should be guided by the threat capability and not the threat intent.

This DOA totally supports the NPA in its intent but this DOA is not technically competent to comment on many details of the specifics of regulation and International Standards.

response **Noted**

comment *49* comment by: *European Cockpit Association*

State-of-the-art must consider (due to the long lifetime of such systems and long update cycles) the latest state-of-the-art. E.g., if choosing an encryption or hashing function, a future proof or latest version should be used. Often there are several newer and older solutions (e.g., algorithms) currently accepted but some are older and some newer. If the newer versions are more secure (and thus more future proof) they should be used. It must be ensured that the state-of-the-art is kept (i.e., if a used technology becomes unsecure it must be ensured that an update to a new technology is provided is a timely manner).

response **Noted**

comment *70* comment by: *FAA*

Page 4
Para 2.1 par 6
Referenced Text: EASA participated in the ASISP Working Group whose assigned subtasks included considering the EASA requirements and guidance material for regulatory harmonization purposes.
Comment: The ARAC report suggests that small airplanes use the ASTM ASISP standard that is in works and being matured. For the purpose of harmonization, EASA's NPA is not 100% aligned with the ARAC recommendations and could be construed to reflect a one size fits all for the entire aviation industry.
Proposed Resolution/Change: the ASISP approach in the NPA and accept ARAC report recommendation to accept the ATSM ASISP standard once it is matured.

[4] https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-07

response **Accepted**
ASTM F-44 future standards on cybersecurity may be referenced in AMC to CS-23, once they are available.

comment *71* comment by: *FAA*

Page 4
Para 2.1 par 8
Ref Text: EASA has therefore decided to transpose the above-mentioned SC ito certain CSs and/or AMC/GM, while also considering the recommendations of the ASISP Working Group report.

Comment: The NPA out come is not aligned with the new Part 23 rewrite or the safety continuum by both agencies. We believe this NPA will be too burdensome on the smaller part 23 manufactures that do not have same level of ASISP connectivity as the commercial PART 25 aircraft do. DO-326A, 356A and 355 are more aligned with Part 25 certification.

Proposed Resolution: Change the ASISP approach in the NPA and accept ARAC report recommendation to accept the ASTM ASISP standard once it is matured. This will support harmonization between the two certification authorities and align with the safety continuum for smaller Part 23 airplanes.

response **Accepted**
ASTM F-44 future standards on cybersecurity may be referenced in AMC to CS-23, once they are available.

comment *81* comment by: *General Aviation Manufacturers Association / Hennig*

GAMA applauds the European Aviation Safety Agency (EASA) for issuing a Notice of Proposed Amendment (NPA) that addresses aircraft cybersecurity. Significant work has been undertaken by EASA, other regulators, and industry to develop processes for managing cybersecurity risks. As acknowledged by EASA, "cybersecurity is addressed as part of certification activities of new large aeroplane type designs and STCs. ...in accordance with" the process for Special Conditions, which have been applied to dozens of CS-25 aeroplanes.

GAMA welcomes EASA basing NPA 2019-01 on the 2015-2016 Aviation Rulemaking Advisory Committee (ARAC) Aircraft System Information Security / Protection (ASISP) working group recommendations. EASA basing an agency NPA on an FAA-chartered working group exemplifies the type of international harmonisation and cooperation activities that the worldwide aviation industry desires.

GAMA's comments are filed in context of the ASISP recommendations, but -- where different from the ASISP recommendations -- are based on the continued evolution that has taken place in the cybersecurity discussions underway between regulators and industry stakeholders as this field of aviation safety continues to mature.

GAMA comments are focused on the following key policy areas:

- Section 3.1.1: The importance of a proportional set of requirements for CS-23 aeroplanes. As noted by the agency earlier, historically, Special Conditions have only been applied to CS-25 aeroplanes and consideration of risk as well as threat vectors for smaller aeroplanes are recognized to be significantly different.

- Section 3.1.2: The agency proposes a new CS 25.1319 to address cybersecurity systems. GAMA recommends that the agency ensure that the proposed threshold ("adverse effect on safety") is appropriate.

- Sections 3.1.3 and 3.1.4: The agency making it clear, as part of this NPA process, what the justification are for its proposed structure of the cybersecurity regulation for rotorcraft in CS-27 and CS-29 in context of both the proposal for small / large aeroplanes and the agency's experience with issuing Special Conditions for these aircraft.

- Section 3.1.8: The importance of the agency providing clarity about what cybersecurity considerations should be made by an applicant for installation of Communications, Navigation, and Surveillance (CNS) equipment that relies on an ETSO or interoperability standard.

- Section 3.1.9: The importance of providing clarity around how design changes should be classified as "major" in context of cybersecurity considerations.

And, the agency ensuring that the full impact of cybersecurity is considered to help inform how to structure the proposed CS and associated regulatory updates for OEMs, CAMO, and Operators when implementing cybersecurity best practices as part of design, continued airworthiness, and operations.

response **Noted**

comment *180* comment by: *John Connolly (Atkins)*

Para 8 reads "…to security threats…" terminology is inconsistent and out of alignment with the industry. Change to "…to cyber-threats…".

response **Partially accepted**
The terminology has been reviewed to ensure consistency throughout the document.

comment *193* comment by: *Lufthansa*

Comment on last paragraph:

State-of-the-art must consider (due to the long lifetime of such systems and long update cycles) the latest state-of-the-art. E.g., if choosing an encryption or hashing function, a future proof or latest version should be used. Often there are several newer and older solutions (e.g., algorithms) currently accepted but some are older and some newer. If the newer versions are more secure (and thus more future proof) they should be used.
It must be ensured that the state-of-the-art is kept (i.e., if a used technology

	becomes unsecure it must be ensured that an update to a new technology is provided is a timely manner).
response	**Noted**

comment	*272* comment by: *IATA* IATA Comment: "....EASA needs to consider the state-of-the-art means...." State-of-the-art must consider (due to the long lifetime of such systems and long update cycles) the latest state-of-the-art. E.g., if choosing an encryption or hashing function, a future proof or latest version should be used. Often there are several newer and older solutions (e.g., algorithms) currently accepted but some are older and some newer. If the newer versions are more secure (and thus more future proof) they should be used. It must be ensured that the state-of-the-art is kept (i.e., if a used technology becomes unsecure it must be ensured that an update to a new technology is provided is a timely manner). The question of state-of-the-art and threat landscape needs to be mapped back to impact, particularly with respect to safety of flight. If it's acknowledged a flight safety component might be affected by future threats, the effectiveness of the control may need to be questioned.
response	**Noted**

2. In summary - why and what | 2.3. How we want to achieve it — overview of the proposals p. 5

comment	*45* comment by: *Europe Air Sports* EAS Comment to 2.3 Overview of the proposals We notice that no requirements for CS-LSA and CS-VLA are included in the NPA. We find that very good and reasonable, but note that the reasons are not stated in the NPA. For example, is the risk regarded as low because of the limited number of people aboard, or due to the fact that small aircraft generally have few flight-critical electronic systems, or because their value as a cybercrime "attack target" is low, or due to the fact that they are operated in VFR where even a total electric failure can be less catastrophic compared to an aircraft operated in IFR? Could therefore also some CS-23 aircraft types, for example CS-23 aircraft operated in VFR, or otherwise "very low-risk" in terms of cybersecurity, be excluded from the scope of this NPA, similarly to LSA and VLA aircraft? EAS proposes this to be considered in the next phases of this Rulemaking Task.
response	**Noted** Cybersecurity considerations will not be mandatory for certification level 1, level 2 and level 3 CS-23 aircraft, as well as for LSA and VLA.

comment	*82* comment by: *General Aviation Manufacturers Association / Hennig*

The NPA is limited to amendments for CS-23, CS-25, CS-27, CS-29, CS-E, CS-ETSO, and CS-P as well as associated guidance material as supported by the ASISP WG recommendations. As a result, the NPA applies requirements to Type Certificate Holders (TCHs) and applicants for different aircraft systems.

However, the ASISP recommendations were provided in parallel to the U.S. Federal Aviation Administration (FAA) having published guidance for operators and maintenance organisations in Advisory Circular 119-1, Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP). AC 119-1 provides guidance about the operation of an aircraft that has a special condition related to security of onboard computer networks. As noted by EASA in NPA 2019-1, the objective of amending the different Certification Specifications is to "transpose the above-mentioned [Special Condition] into certain CSs and/or AMC/GM, while also considering the recommendations of the ASISP Working Group report."

The amendments to CS-25, -27, and -29 identify "procedures and instructions for continued airworthiness" in subpart b. of the proposed Certification Specification (i.e., "When required by paragraph a, the applicant must make procedures and instructions for continued airworthiness (ICA) available that ensure that the security protections... are maintained.") This establishes a requirement on the applicant to produce procedures and ICA to support cybersecurity, but the complementary requirement for the operator and maintainer to adhere to the "procedures" is less clear. (There is an existing requirement to adhere to the ICA, but the ICA does not necessarily provide the complete security protections.)

- A continuing airworthiness management organisation (CAMO) / MRO is expected to adhere to security procedures established as part of the certification process and communicated by the TCH through Instructions for Continued Airworthiness (ICA) and associated procedures. Is the CAMO community aware of these new responsibilities?

- An operator of an aircraft that today has a Special Condition (and in the future may have a cybersecurity feature approved as a result of this amendment) is expected to adhere to the security processes of the design. Is the operator aware of these new responsibilities? Is the operator of a CS-25 aeroplane aware? Is an operator of a CS-23 aeroplane aware?

The proposed AMC 20-42, Section 7, includes a requirement on an operator to provide "Reporting" of "...any information security occurrences to the designer of [the] product or part", but does not include a requirement on the operator to adhere to the processes or procedures issued by the manufacturer about how to maintain the security of the system.

GAMA recommends that EASA determine if guidance and / or regulatory updates also are warranted for aircraft operators or maintainers to complement this NPA in the manner that FAA's AC 119-1 complements the Special Conditions for operators and maintainers. As an example, should amendments be made to Regulation (EU) No 1321/2014 to address Part 145 and the responsibilities for aircraft maintainers. Should amendments be made to Regulation (EU) 965/2012 to address Parts ARO/ORO and operator responsibilities to comply with security procedures and / or ICA that contain security?

	GAMA also notes that ICA and security operating procedures may contain information that is subject to certain constraints and security controls. The NPA is silent about how EASA envisages the manufacturer, maintainer, and operator control or have a responsibility to protect the security procedures and ICA from public dissemination (i.e., similar to processes for Sensitive Security Information)?
response	**Noted**

comment	*93* comment by: *ENAC* General comment I fully agree with "What we want and how we want to achieve".
response	**Noted**

comment	*97* comment by: *ENAC* General Comment: the NPA doesn't refer to the "non installed equipment" introduced by EU 2018/1139 (refer to Art. 3 definitions item (29))
response	**Noted** RMT.0727 defines the scope, conditions and process for the certification of 'non-installed equipment' (NIE). https://www.easa.europa.eu/document-library/terms-of-reference-and-group-compositions/tor-rmt0727

comment	*117* comment by: *FOCA Switzerland* **Comment FOCA:** As mentioned in the general comments, FOCA sees the need to link this RMT with RMT 0.720. Furthermore, we see the need for face-to-face discussion between experts regarding the proportionality of the rule, especially concerning different types of aircraft and potentially retrofitting. **Proposal FOCA:** Add reference to a step of face-to-face consultation with experts and a step to double-check for legal consistency with RMT 0.720.
response	**Not accepted** EASA considers at this stage that the two topics do not contradict each other, and do not require a joint workshop.

comment	*130* comment by: *UK CAA* **Page No:** 5 **Paragraph No:** Section 2.3 **Comment:** CS-APU Appears to have been omitted from the list of applicable documents. It is not understood why this has been omitted.

Justification:
CS-APU is still in use and it is unclear why it has been excluded from the list of affected documents.

Proposed Text: Add CS-APU to the list of affected documents.

response **Accepted**

2. In summary - why and what | 2.4. What are the expected benefits and drawbacks of the proposals p. 5

comment *34* comment by: *FAA*

Page 5
Para 2.4, para -3
Comment: While some large manufacturers of products have already been incorporating cybersecurity measures into their products by using SC's, and will not have such a large economic impact, smaller manufacturers may find it difficult to comply, especially manufacturers of those who mostly work with CS 23, 27, & 29.
Proposed Resolution: No drawbacks or adverse economic impacts are expected. (Recommend adding robust language stating economic impact to manufacturers and operators here or in 4.4.2.4.)

response **Accepted**
This will be better reflected in the Explanatory Note of the final deliverable (i.e. ED Decision).

comment *72* comment by: *FAA*

Page 5
Para 2.4 par 1
Ref Text: What are the expected benefits and drawbacks of the proposals.
Comment:The level of burden placed on smaller Part 23 airplanes which adhere to this NPA will have an economic impact to the small aircraft manufacturers which are already struggling to survive.
Proposed Resolution: Using the ASTM, ASISP aligns with the safety continuum and will have minimum possible impact while addressing ASISP safety.

response **Accepted**
ASTM F-44 future standards on cybersecurity may be referenced in AMC to CS-23, once they are available.

comment *94* comment by: *ENAC*

I do not agree with "No drawback or adverse economic impacts are expected".
The new basic regulation requires a great attention to this aspects (refer to EU 2018/1139 art.89)
Stakeholders will have an impact at organization level in term of human resources, training and new processes definition (i.e. perform risk assessment specifically dedicated to cyber security).

response **Accepted**
This will be better reflected in the Explanatory Note of the final deliverable (i.e. ED Decision).

comment *95* comment by: *ENAC*

In order to reduce the economic impact among the different CS, it could be useful to implement cybersecurity measures gradually, taking into account the performance and risk of operation applicable to the kind of aircraft. For example (first step) start with initial type certification of CS 25, CS 29 aircraft, CS E, CS ETSO and new STC then (second step) aircraft falling within CS 27 and CS 23 initial type certification.

response **Noted**
Cybersecurity considerations will not be mandatory for certification level 1, level 2 and level 3 CS-23 aircraft, as well as for LSA and VLA.

comment *118* comment by: *FOCA Switzerland*

Comment FOCA: We disagree with the statement that "no drawbacks or adverse economic impacts are expected" for the following reasons:
First, there is a possible overlap between security and safety assessments iteration, refer to later comments under AMC. If not implemented correctly, there could be negative safety impacts. Secondly, there will definitely be economic impacts in the short term as industry, operators and authorities learn about this topic and train or hire new experts. We see this as an investment in the long term, so not necessarily an "adverse" economic impact.

Proposal FOCA: The significant investment in time and resources needed to train and or hire new experts should feature prominently.

response **Accepted**
This will be better reflected in the Explanatory Note of the final deliverable (i.e. ED Decision).

comment *181* comment by: *John Connolly (Atkins)*

1. This section is unclear and confusing. It leads the reader to make assumptions and is not explicit enough. The last statement "cybersecurity incidents and accidents' should read 'cyber security incidents'. Again this para should discuss malicious and non-malicious incidents.

response **Noted**
This will be considered for the Explanatory Note of the final deliverable (i.e. ED Decision).

comment *229* comment by: *The Boeing Company*

Page: *5*
Paragraph: *2.4*

THE PROPOSED TEXT STATES:

"-No drawbacks or adverse economic impacts are expected."

REQUESTED CHANGE:
Delete sentence

JUSTIFICATION:
Currently, ETSO/TSO does not have security requirements on the level of DO-326A/356A, thus there will be an adverse economic impact. Our experience of Special Conditions (SCs) has proved that security certification does have a significant cost. As we have experienced in discussions at the RTCA Special Committee (SC) 216 there are experts in industry that believe if there is a significant cost, it will preclude from performing the necessary security activities or making the airframe manufacturer shoulder the entire cost burden, rather than a supplier with an ETSO/TSO.

response **Partially accepted**
This will be better reflected in the Explanatory Note of the final deliverable (i.e. ED Decision).

comment *238* comment by: *Aerospace and Defence (ASD)*

Commented text
"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 "

Proposed modification
To modify the sentence in order to limit the extent of those "necessary actions" during the design of the product. Such a sentence may be interpreted extensively to any environmental tools, benches, means for providing information between stakeholders during the product development, etc…
· "… will ensure that applicants assess and mitigate the cybersecurity risks on products or parts, and that the CSs..."

Justification
The purpose of the comment is not to exclude design environment of the products from the protection against cybersecurity threats, but to avoid any "actions" to be demonstrated to authorities beyond the scope of a relevant security perimeter.

response **Partially accepted**
This will be better reflected in the Explanatory Note of the final deliverable (i.e. ED Decision).

comment *239* comment by: *Aerospace and Defence (ASD)*

Commented text
"No drawbacks or adverse economic impacts are expected."

Proposed modification
Cost of development is expected to increase slightly. These costs are less than the positive impact on safety and security for the population.

Justification
As a new (or at least changed) process is being introduced to Design Organisations and their supply chain, it cannot be expected to state that there will be no adverse economic impacts. As a minimum, cybersecurity studies will need to be performed which will raise costs.

response **Partially accepted**
This will be better reflected in the Explanatory Note of the final deliverable (i.e. ED Decision).

3. Proposed amendments and rationale in detail | 3.1. Draft certification specifications (Draft EASA decision) | 3.1.1. Draft decision amending the AMC and GM to CS-23 p. 6-7

comment *2* comment by: *Luftfahrt-Bundesamt*

"Improper funcioning...could lead to a failure condition more sever than major,..."
Recommend to directly address catastrophic or hazardous/severe major effects, like the expression used in CS XX.1319a. : "may result in catastrophic or hazardous/severe major effects"

response **Partially accepted**
'Catastrophic or hazardous/severe major' is a wording that exists only in the specifications for rotorcraft, and is coming from AC 29.2c.
The text will be updated as follows: '(…) systems whose improper functioning could lead to catastrophic or hazardous failure conditions'

comment *10* comment by: *European Powered Flying Union*

3.1.1. Draft decision amending AMC and GM to CS-23
page 6/20
GM 23.2500(b)

We support your draft.

response **Noted**

comment *35* comment by: *FAA*

Page 6
Para 3.1.1, para 1
Referenced Text: "Improper functioning of equipment and systems"

Comment: "Improper functioning" - is difficult to distinguish cybersecurity threat without the knowledge of the equipment intended function.

	Proposed Resolution: 1) ~~Improper functioning~~ Abnormal behavior with respect to its intended function of equipment and systems may be caused by intentional unauthorized electronic interaction (IUEI). (2) replace "improper functioning" with "abnormal behavior"
response	**Not accepted** 'Improper functioning' is the text used in CS 23.2500. The GM explains that this 'improper functioning' may be caused by IUEI.

comment	*50* comment by: *European Cockpit Association* Proposal: 3.1.1 "*The applicant may then also consider..*". Replace "*may*" with "*should*" Rationale: Such important considerations should be more than just an option.
response	**Accepted**

comment	*86* comment by: *Panasonic Avionics* Should read "more severe than Minor" to be in accordance with DO-356A/ED-203A 2.2.3 and 2.7.3. Or "Major impacts or higher".
response	**Noted** Due to several other comments on the need to maintain the safety continuum principle, the text has been changed into 'unacceptable threat condition' and acceptability is developed in a dedicated section and to enforce the safety continuum.

comment	*96* comment by: *ENAC* The difference between the requirement drafted for CS 23 and CS 27 as reflected in the current proposal might be difficult to justify. In the NPA different operations are recalled e.g. CAT-A, IFR. But IFR apply as well to CS 23.
response	**Accepted** The wording 'hazardous/severe major' comes from the FAA AC 27-1b Change 4. This wording has been changed in the proposed text and will be consistent with the scope of RMT.0712 on the 'enhancement of the safety assessment processes for rotorcraft designs'.

comment	*119* comment by: *FOCA Switzerland* **Comment FOCA**: In our opinion, with the current draft, there is a possible confusion between safety analysis and cybersecurity assessment. Therefore, as far as the applicability to CS 23 is concerned, please refer to our proposal under the general comments a) 1.

The difference between the requirement drafted for CS 23 and CS 27 as reflected in the current NPA is not justified. In the NPA different operations are recalled e.g. CATA, IFR but IFR apply as well to CS 23.
Moreover, the text proposed for GM 23.2500(b) merges the safety assessment with the cyber security assessment creating a misleading interpretation on the two following area:

- Equipment/systems leading to failure condition more severe than MAJOR upon a safety analysis only, are not implicitly the same of equipment leading to failure condition more severe than MAJOR when IUEI are possible source of malfunction (as required by the GM 23.2500(b)).
- Guiding the applicant to consider IUEI as source of malefaction goes into the direction of requiring a "modified" safety assessment, which is misleading with respect to the cyber security assessment guided by ED 20X;

For the above, the actual GM results to unclear both in the equipment scope of the analysis, both in the kind of analysis outcome of this GM and hence, the current GM 23.2500(b) is considered misleading, not supporting certification liaison and prone to be source of conflicts and not harmonized position.

Proposal FOCA: The cybersecurity assessment should be a clearly identified separate step. Especially considering that cybersecurity assessments have to be carried out again after a while to ensure that they are still current. They are not static processes.

As mentioned under in the general comments a) 1. (gradual implementation of this NPA) and a) 2. (For design change and STC) above mitigate the concerns expressed to 3.1.1.

Furthermore, the differences between CS 27 and CS 23 look not justifiable: GM 23.2500(b) should be then equivalent to CS 27 1319, in order to keep the requirement clear and clean.
The NPA calls for OPS aspect in order to justify the differences but multiple engine and IFR ops are in common to both CS23 and 27. As a matter of fact, CS 27 CAT A might drive the difference (because of the third party protection) so the following proposal is additionally made: refrain to insert GM 23.2500(b) and include the cyse requirement in CS 27 Appendix C (CATA), so that only CATA helicopter should comply to it, focusing on larger aircraft and more prone operation

response **Noted**
This point has been discussed during the ARAC ASISP Working Group. See ARAC ASISP Recommendation 10 and associated rationale.

comment *131* comment by: *UK CAA*

Page No: 6

Paragraph No: 3.1.1

Comment: The reference to "intentional unauthorised electronic interaction (IUEI)" excludes cyber attacks that may be authorised (insider, account compromise etc) and excludes accidental/unintentional cyber threats. It is not

understood if this is the intent. Both of those vectors would be considered as standard for cyber security purposes. In the case of non-targeted cyber attacks where vulnerable systems are compromised when these are "released in the wild" the intentional aspect would be possibly questionable.

Justification: This is limiting the scope of threat vectors and types of cyber-attacks typically considered as part of cyber security.

Proposed Text: Improper functioning of equipment systems may be caused by intentional/unintentional authorised/unauthorised electronic interaction.

OR

The definition of IUEI assumes that any malicious interaction is unauthorised (irrespective of the method of cyber-attack) and intentional (to include both passive and active attack types).

response

Not accepted
This point has been discussed during the ARAC ASISP Working Group. The results can be found in the ARAC report in Section 2.2.4.1.

comment *132* comment by: *UK CAA*

Page No: 6

Paragraph No: 3.1.1, GM 2500(b)

Comment: By applying to failure conditions more severe than major only, a lower standard is proposed for CS-23 than for CS-25. The NPA provides no justification for the application of a lower standard. In the absence of adequate justification, the standard applied to CS-23 should be the same as for CS-25.

Justification: It is not required that CS-23 be a lower standard than CS-25; a lower standard should only be applied where appropriate, e.g. due to disproportionate cost/weight.

Proposed Text: Suggest that the 3rd sentence of GM 23.2500(b) is modified to read "In showing compliance with CS 23.2500(b) for equipment and systems whose improper functioning could adversely affect the safety of the aeroplane, the applicant may consider AMC 20-42.".

response

Noted
Due to several other comments on the need to maintain the safety continuum principle, the text has been changed into 'unacceptable threat condition' and acceptability is developed in a dedicated section and to enforce the safety continuum.

comment	*133* comment by: *UK CAA* **Page No:** 6 **Paragraph No:** 3.1.1 **Comment:** "AMC20-42 – Airworthiness Information Security Risk Assessment". The terms cyber security, information security and security are used interchangeably throughout the document. It is not understood why there is a lack of consistency in the usage of these terms. **Justification:** For consistency we suggest one defined term is used. **Proposed Text:** "Airworthiness Security Risk Assessment" OR "Airworthiness Cyber Security Risk Assessment"
response	**Partially accepted** The terminology will be reviewed to ensure consistency throughout the document.

comment	*168* comment by: *Embraer S.A.* EASA seeks alignment with FAA ARAC ASISP recommendations but this text is stricter than the proposed text of PS-AIR-21.16-02 Rev. 2 "Establishment of Special Conditions for Aircraft Systems Information Security Protection" regarding Part 23 aircraft. The proposed text covers all part 23 aircraft while FAA PS targets only 14 CFR part 23 Class 4, Commuter Category Airplanes. *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.* To: *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 used in Class 4 Commuter Category Airplanes 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.*
response	**Noted** Due to several other comments on the need to maintain the safety continuum

principle, the text has been changed into ‘unacceptable threat condition’ and acceptability is developed in a dedicated section and to enforce the safety continuum.

comment *179* comment by: *General Aviation Manufacturers Association / Hennig*

EASA introduces new Guidance Material (GM) in section 3.1.1 to address intentional unauthorised electronic interaction (IUEI). GAMA welcomes EASA leveraging the "new" CS-23 regulatory structure to address cybaersecurity risks for normal, utility, aerobatic, and commuter aeroplanes.

Amendment 5 to CS-23 established an internationally harmonised approach to general aviation aeroplane certification. Section 23.2500 (proposed as 23.1315, but updated prior to publication) is intended to address both unintentional and intentional interference with a system.

As the agency knows, work is underway at ASTM to finalise the associated guidance material for both unintentional and intentional interference. It is important that the agency leverage the updated ASTM standard for CS-23 aeroplanes when finalised by the ASTM working group.

GAMA also recommends a review of the proposed GM 23.2500 (b) and the use of the term "may" in the second sentence. The agency proposes that "The applicant may then also consider cybersecurity threats as a possible source of 'improper functioning' of equipment and systems."

The sentence may confuse the applicant and lead to the conclusion that the applicant may not have to consider cybersecurity, because of the use of the word "may" in the sentence.

GAMA proposes that the sentence be updated to read:

"The applicant <u>should</u> consider cybersecurity threats [IUEI] as a possible source of 'improper functioning' of equipment and systems."

response **Noted**
Due to several other comments on the need to maintain the safety continuum principle, the text has been changed into ‘unacceptable threat condition’ and acceptability is developed in a dedicated section and to enforce the safety continuum.

comment *211* comment by: *L. Riegle AIA*

3.1.1
Commented text
"[…] failure condition […]"

Proposed modification
Change to threat condition
Is the use of "failure condition" language intentional and to tie security and safety process together?

If yes, add a separate paragraph that explains that the two processes should interact (see also ED202A) rather than using terms that can be ambiguous and this intent is lost.

Justification
The use of terminology of failure condition is related to safety effects - unintentional defects such as random failures or wear out. For intentional effects, also described as IUEI, the use of threat condition should be used.

Commented text
"improper functioning"

Proposed Modification
Modify to "abnormal behavior"

Justification
Improper functioning is not standard language and may be ambiguous. Standard terminology for the intended purpose is abnormal behavior.

Commented text
"GM"

Proposed Modification
"AMC"

Rationale
Industry has invested significant resources to establish ED203A. The document was specifically designed to provide both guidance material and acceptable means of compliance for the anticipated rules - as stated in Chapter 1.3 of ED203A identifying sections to be used as GM, AMC or only considerations for industry. By only using ED203A as GM (via AMC 20-42 and GMs in the individual parts), ED203A is not classified as an AMC to the new rules. As there is only Guidance Material, Special Conditions will still need to be applied to all programmes. This is counter to industry's endeavour to harmonise approaches rather than individually negotiated responses to CRIs. This is critical to ensure a level playing field, similar levels of safety and security and to reduce costs in the supply chain by allowing simple reuse of systems and components.

response

Point 1: **Accepted**

Point 2: **Not accepted**

Quoting from ARAP/ASISP Section 2.4.2: ‘This working group, as a result, concluded that the proposed 23.1315 is an appropriate regulatory vehicle by which airplane systems and equipment standards for Aircraft System Information Security /Protection to address airworthiness can be addressed. The easiest mechanism for the FAA, in coordination with other regulators, to address system security concerns is by establishing guidance that “abnormal operation” in the proposed 23.1315 also includes the applicant addressing Intentional Unauthorized Electronic Interaction (IUEI).’

The status of CS-23 Amendment 5 was still ‘draft’ at that time and, by the time of

publication, evolved from 1315 to 2510 in the FAA and 2500 in the EASA rule, and the text 'abnormal operation' became 'improper functioning' in the EASA rule and remained 'abnormal operation' in the FAA rule.

comment *217* comment by: *General Aviation Manufacturers Association / Hennig*

GAMA appreciates EASA adhering to the recommendations of the ASISP working group including with regards to the applicability of the cybersecurity requirements to different types of aircraft, specifically CS-23, -27, and -29 based on a consideration of safety risk and proportional applicability of requirements. GAMA appreciates that EASA has differentiated the requirements for non-CS-25 aeroplanes.

In reviewing the proposal from the agency, however, we note that the different structure proposed for CS-23 versus CS-27 and -29 may cause confusion about the intended objective, even though the intended objective is likely the same.

The proposed GM for CS 23.2500(b) states:

"...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."

The proposed CS 29.1319 and 27.1319 state:

"Rotorcraft equipment, systems and networks, considered separately and in relation to other systems must be protected from [IUEI] that may result in catastrophic or hazardous/severe major effects on the safety of the rotorcraft."

Is the intent to address cybersecurity for the same safety effect (*i.e.*, "more severe than major" equates to "catastrophic or hazardous / severe major" safety effects)?

GAMA recommends that EASA review the safety (security) objective intended to be addressed by the CS-23, -27, and -29 regulations and determine whether aligning the safety objective and the effects of the Failure Condition with regard to how it is identified in the proposed GM for 23 and related CS for 29 and 27.

response **Noted**
Due to several other comments on the need to maintain the safety continuum principle, the text has been changed into 'unacceptable threat condition' and acceptability is developed in a dedicated section and to enforce the safety continuum.

comment *227* comment by: *Bombardier*

Issue: inconsistent definitions

Details: Draft text for GM 23.2500(b) says that "Improper functioning of equipment and systems may be caused by intentional unauthorised electronic interaction (IUEI)."

This conflicts with the draft text for 4.1.1 Safety Risk Assessment that says "[T]hreats are caused by unauthorised electronic interactions that can be triggered by human action, either intentionally or unintentionally [emphasis added]."

Recommend: changing 3.1.1 to "Improper functioning of equipment and systems may be caused by intentional or unintentional unauthorised electronic interaction (IUEI)."

response **Not accepted**
The definition of 'IUEI', as stated in the rationale, can be found in ED 202A and it is defined as '...human initiated actions with the potential to affect the a/c due to unauthorised access, use, disclosure, denial, disruption, modification or destruction of electronic information or electronic aircraft system interfaces. This definition includes the effect of malware on infected devices...'

comment *240* comment by: *Aerospace and Defence (ASD)*

Commented text
"[…] could lead to a failure condition more severe than major".

AMC20-42, §9: "[…] 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".

Proposed modification
Create §6, which is missing, and remove text from §9:

§6 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 depending on the level of threat of the associated threat scenario. The same safety risk may be acceptable for products that are certified under CS-29.

Justification
Consistency between CS.xx rules, AMC20-42 and recognised ED-203A.

Comment
Will EASA clarify in an AMC the accepted level at an individual CS level, or will it be taken from ED203A?

response **Accepted**
The intent is to recognise 'acceptability' as in ED-203A.

comment	*241* comment by: *Aerospace and Defence (ASD)* **Commented text** "[…] failure condition […]" See also page 12, Point 4(b). **Proposed modification** Change to threat condition **Justification** The use of terminology of failure condition is related to safety effects - unintentional defects such as random failures or wear out. For intentional effects, also described as IUEI, the use of threat condition should be used.
response	**Accepted**

comment	*273* comment by: *IATA* GM23.2500(b) Replace "may" with "should" in the second sentence.
response	**Not accepted** The applicant may propose an alternative to AMC 20.42 as a means of compliance. In particular, if and when a dedicated standard is available for CS-23 aircraft (ASTM), it may be also proposed in the AMC1 reference to this standard.

3. Proposed amendments and rationale in detail | 3.1. Draft certification specifications (Draft EASA decision) | 3.1.2. Draft decision amending CS-25 p. 7-8

comment	*51* comment by: *European Cockpit Association* Proposal: pg 7 « intentional electronic interaction (IUEI) » should be defined clearly in this NPA. If strict ED203A definition is to be used, exclusions such as jamming should be clearly stated and evaluated. Rationale: The NPA 2019-01 makes extensive use of the term « intentional electronic interaction (IUEI) » without clearly defining it. In a note p.7 it is said that it comes from RTCA/EUROCAE ED203A section 2.1. However, during ED203A draft work there have been a lot of discussions on the scope, perimeter and exclusions of "IUEI". For example, "jamming" has been specifically excluded from ED203A IUEI definition whereas it could still be a major threat for "products" or "parts" taken separately.
response	**Not accepted** This is the consensus of the ARAC/ASISP WG and of joint discussions within EUROCAE and RTCA.

comment	*73* comment by: *FAA*

Page: 7
Rationale Par 1
Ref Text: It is not, however, proposed to create a new paragraph, but to clarify in the GM that 'improper
Comment: This rational is harmonized with FAA's approach to add guidance material to AC-23.1309E to clarity that 'abnormal operation' includes 'intentional unauthorized electronic interaction (IUEI)'. In Addition material will be added to reference the ASTM ASISP stand as a means to address IUEI.
Proposed Rationale: work together to mature the ASTM ASISP for common acceptance.

response **Noted**

comment *76* comment by: *FAA*

Page: 7
Para: section 3.1.2 CS 25.1319
Comment: To demonstrate the security functions have been implemented and perform properly.
Proposed Resolution: Suggest to add: c. Compliance with the requirements of paragraph (a) of this section must be shown by analysis, and where necessary, by appropriate ground, flight or simulation tests to demonstration that the security requirements related to intended functions are met.

response **Not accepted**
This text is the result of the ARAC ASISP WG. It is proposed without a change for regulatory harmonisation reasons. Compliance with the requirement by analysis and testing is defined in AMC 20-42 Section 8.

comment *84* comment by: *General Aviation Manufacturers Association / Hennig*

EASA proposal to amend CS-25 by establishing a new CS 25.1319, Equipment, systems and network information security protection is supported by industry. The proposed regulatory text aligns with the recommendations of the ASISP WG which is appreciated.

CS-25, however, is not necessarily a homogenous group of aeroplanes. CS-25 products include aeroplanes with 9-12 passengers used in business and commercial charter operations with mostly known passengers, up to and including aeroplanes with 300-500 seats used in scheduled passenger operations with mostly unknown passengers. It is clear that the cybersecurity threat and risk of these operations is not homogenous.

EASA proposes that CS-25 aeroplanes equipment, systems and networks... must be protected from intentional unauthorised electronic interactions that may result in adverse effects on the safety of the aeroplane. GAMA is concerned that the agency proposes a threshold of "adverse effect on safety" for CS-25 while the regulatory language for CS-23, 27, and 29 seem more appropriate and bounded to address the safety impact.

As proposed by EASA at the level of an "adverse effect on safety" in the NPA, this would require that a completely isolated system with an overall hazard of only minor be "protected" even though the effects are minor and other random failures of the system can be probable. An exemplifying system often used in these discussions is a cabin management system with no direct (or indirect) connection to an essential system.

GAMA recommends that EASA review the CS-25 proposed regulatory language with two objectives. First, EASA should determine whether the threat on all aeroplanes type certificated to CS-25 is the same and, if not, enable a different means of compliance for aeroplanes under a certain threshold (*e.g.*, 19 seats). Second, EASA should determine whether the level of an "adverse effect on safety" is too stringent for CS-25 and, if yes, consider aligning the CS-25 threshold with other certification parts as proposed.

response **Noted**

comment *87* comment by: *Panasonic Avionics*

3.1.2, first para, end of last sentence
To be consistent with DO-356A/ED203A 2.2.3 and 2.7.3 and to avoid misinterpretation, clarify statement to read "that may result in safety effects with Major impact or higher to the aeroplane." Or see acceptable phrase on p.8.

response **Not accepted**
This text is the result of the ARAC ASISP WG. It is proposed without a change for regulatory harmonisation reasons.

comment *122* comment by: *FOCA Switzerland*

Comment FOCA: The procedures and instructions for continued airworthiness (ICA) are just one part of the possible measures necessary to ensure cyber resilience throughout the lifecycle.

Proposal FOCA: See under general comments, consider legal links to ensure correct implementation throughout lifecycle also by operators, pilots etc.

response **Noted**

comment *134* comment by: *UK CAA*

Page No: 7 and throughout

Paragraph No: 3.1. 2 and throughout

Comment: "…systems and network information security…." The terms cyber security, information security and security are used interchangeably throughout the document. It is not understood why there is a lack of consistency in the usage of these terms.
"security risks" and "security protections" are also used

Justification:. For consistency we suggest one defined term should be used. The EASA basic regulation uses “cyber security”.

Proposed Text: “security” OR “cyber security”

“CS 25.1319 Equipment, systems, network and information related cyber security protection”
OR

“CS 25.1319 Equipment, systems, network and information related security protection”

response **Noted**
The terminology will be reviewed to ensure consistency throughout the document.

comment *167* comment by: *Embraer S.A.*

This section does not provide the reference level for risk acceptability as provided for parts 23, 27 and 29.

Embraer believes that the reference is required to perform the risk assessment and keep the alignment with PS-AIR-21.16-02 Rev. 2.

To change the text from:

‘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.

To:

‘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 major, hazardous or catastrophic 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.

response **Not accepted**
This text is the result of the ARAC ASISP Working Group. It is proposed without a change for regulatory harmonisation reasons. Compliance with the requirement is limited to major and higher safety effect in ED-203A, which is recognised as AMC.

comment *214* comment by: *L. Riegle AIA*

3.1.2

Commented text
"GM"

Proposed Modification
"AMC"

Rationale
Industry has invested significant resources to establish ED203A. The document was specifically designed to provide both guidance material and acceptable means of compliance for the anticipated rules - as stated in Chapter 1.3 of ED203A identifying sections to be used as GM, AMC or only considerations for industry. By only using ED203A as GM (via AMC 20-42 and GMs in the individual parts), ED203A is not classified as an AMC to the new rules. As there is only Guidance Material, Special Conditions will still need to be applied to all programmes. This is counter to industry's endeavour to harmonise approaches rather than individually negotiated responses to CRIs. This is critical to ensure a level playing field, similar levels of safety and security and to reduce costs in the supply chain by allowing simple reuse of systems and components.

Commented text
"aircraft information systems"

Proposed modification
aircraft systems or aircraft digital systems

Justification
Flight control systems can be loaded using field loadable methods. All aircraft systems that are connected to other systems should be included. Information systems has a specific and almost universal meaning in Cybersecurity. Aircraft information systems may be confused with Aircraft Information Systems Domain and thus applicants may incorrectly narrow the scope of their activities and neglect critical areas such as Aircraft Control Domain.

response

Point 1: **Accepted**
Point 2: **Not accepted**

comment

242 comment by: *Aerospace and Defence (ASD)*

Commented text
“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.”

Proposed modification
The above text is to be removed from Rationale and inserted as GM 25.1319 (resp GM E 50(I), GM P 230).

Justification
The terms ‘adverse effects on the safety of the aeroplane’ and ‘mitigated as necessary’ need clarification.

response **Accepted**

comment *243* comment by: *Aerospace and Defence (ASD)*

Commented text
“GM”

Proposed modification
“AMC”

Justification
The Certification Specifications currently only have AMCs rather than GMs. Industry spent large efforts in establishing a Standard that was intended to be used as an AMC. By use of GM, special conditions will still be required and consistency across industry will not occur.

Why is CS 23 and CS P the only ones that have this information as an AMC?

This comment is applicable for:

3.1.2 – Draft decision amending CS-25
3.1.3 – Draft decision amending CS-29
3.1.4 – Draft decision amending CS-27
3.1.5 – Draft decision amending CS-E

response **Accepted**
The proposed text will be defined as AMC, instead of GM.

comment	*288* comment by: *IATA* CS25.1319 (b) There needs to be some context of the risk, ie. why these procedures and instructions are in place rather than simply following a list for compliance.
response	**Noted**

comment	*289* comment by: *IATA* Page 8 - top section ending in "responsibilities to the customer". In this scenario, should a manufacturer highlight an unmitigated risk exists within a service, however it is non-safety related and the responsibility of an operator to use in a secure manner.
response	**Noted**

comment	*294* comment by: *Bombardier* **Issue**: Security provisions for information system security ICA **Comment**: The draft CS 25.1309(b) requires the applicant to make security-related ICA available to operators. We fully support the requirement for ICAs related to information system security, and believe that appropriate ICA are essential, both in the need for OEMs to develop them, and in the need for operators to follow them correctly. We have concerns over the widespread distribution of security-related information, as it can also be used to exploit a known vulnerability by a hostile party, prior to actions being taken by the operator. While not the topic of this rulemaking, this applies equally to the case of mandatory corrective actions - some security-sensitive information should have restricted access. **Recommend**: Add provisions for restricted access to security information.
response	**Not accepted** The decision to include confidentiality as a security control should be based on the result of the risk assessment, but cannot be mandated in advance by the regulator.

3. Proposed amendments and rationale in detail | 3.1. Draft certification specifications (Draft EASA decision) | 3.1.3. Draft decision amending CS-29 p. 8

comment	*88* comment by: *Panasonic Avionics* "that may result in catastrophic or hazardous/severe or major effects on the safety…" is acceptable alternative phrasing for p.7 comment.
response	**Noted** However, the comment does not indicate which paragraph is proposed to be changed.

comment	*135* comment by: *UK CAA* **Page No:** 8 **Paragraph No:** 3.1.3, CS 29.1319 **Comment:** By applying to failure conditions more severe than severe major only, a lower standard is proposed for CS-29 than for CS-23 or CS-25. The NPA provides no justification for the application of a lower standard. In the absence of adequate justification, the standard applied to CS-29 should be the same as for CS-25. **Justification:** CS-29 helicopters typically carry 19 passengers + two crew which is as many as some CS-25 aeroplanes and more than most (all?) CS 23 aeroplanes It is not required that rotorcraft standards be lower than fixed wing standards; a lower standard should only be applied where appropriate, e.g. due to disproportionate cost/weight. **Proposed Text:** UK CAA suggest that the 1st sentence of CS 29.1319.a is modified to read "Rotorcraft equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions that could adversely affect the safety of the rotorcraft.".
response	**Partially accepted** This text has been changed to consider also other comments and is now consistent with the proposal made in this comment from the UK CAA.

comment	*169* comment by: *Embraer S.A.* Embraer believes that the text of this paragraph is "unusual". The text used is this section is different from the other sections and FAA PS-AIR. To change the text from: '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. […]* To: *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 major, hazardous or catastrophic effects on the safety of the rotorcraft. […]*
response	**Partially accepted** This text has been changed to consider this comment, as well as other comments received.

comment	*215* comment by: *L. Riegle AIA* 3.1.3 **Commented text** "GM" **Proposed Modification** "AMC" **Rationale** Industry has invested significant resources to establish ED203A. The document was specifically designed to provide both guidance material and acceptable means of compliance for the anticipated rules - as stated in Chapter 1.3 of ED203A identifying sections to be used as GM, AMC or only considerations for industry. By only using ED203A as GM (via AMC 20-42 and GMs in the individual parts), ED203A is not classified as an AMC to the new rules. As there is only Guidance Material, Special Conditions will still need to be applied to all programmes. This is counter to industry's endeavour to harmonise approaches rather than individually negotiated responses to CRIs. This is critical to ensure a level playing field, similar levels of safety and security and to reduce costs in the supply chain by allowing simple reuse of systems and components.
response	**Accepted** The proposed text will be defined as AMC, instead of GM.

3. Proposed amendments and rationale in detail | 3.1. Draft certification specifications (Draft EASA decision) | 3.1.4. Draft decision amending CS-27 p. 8-9

comment	*11* comment by: *European Powered Flying Union* 3.1.4. Draft decision amending CS-27 page 8/20 CS 27.1319 We support your draft.
response	**Noted**

comment	*136* comment by: *UK CAA* **Page No:** 8 **Paragraph No:** 3.1.4, CS 27.1319 **Comment:** By applying to failure conditions more severe than severe major only, a lower standard is proposed for CS-27 than for CS-23 or CS-25. The NPA provides no justification for the application of a lower standard. In the absence of adequate justification, the standard applied to CS-27 should be the same as for CS-25.

Justification: CS-27 helicopters carry as many passengers as CS 23 aeroplanes It is not required that rotorcraft standards be lower than fixed wing standards; a lower standard should only be applied where appropriate, e.g. due to disproportionate cost/weight.
Proposed Text: UK CAA Suggest that the 1st sentence of CS 27.1319.a is modified to read "Rotorcraft equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions that could adversely affect the safety of the rotorcraft.".

response **Not accepted**
This point has been discussed in the ARAC ASISP Working Group, and the text proposed in the NPA reflects the consensus reached by the Working Group.

comment *137* comment by: *UK CAA*

Page No: 8 & 9

Paragraph No: Sections 3.1.3 and 3.1.4

Comment:

It is unclear why the requirement for the Part 29 and Part 27 analyses are limited to catastrophic and hazardous failure effects. It is accepted that a standard cascade analysis would identify cascading failures/events that could result in catastrophic and/ or hazardous effects, however, it may be unwise to assume that an analysis would identify the potential for multiple major or minor effects that would cumulatively result in a hazardous or catastrophic event, unless there is a specific direction to do this.

Justification:

Failure to include major and minor events in the analyses could lead to viable and significant attack paths being missed.

Proposed Text:

We recommend that the requirements are extended to include major and minor effects or use similar wording to that used for CS-25.

response **Noted**

comment *138* comment by: *UK CAA*

Page No: 8 - 9

Paragraph No: 3.1.3, 3.1.4, 3.1.5

Comment: Where procedures must be provided it is unclear whether these will consider the intended operational use/options as part of the risk assessment, and how frequently these will be updated

Justification: Cyber security risk is contextual to the use of the system and may vary markedly, this risk also changes quite regularly and would need to be kept up to date to ensure the instructions remain appropriate. As an example, if the risk assessed on the basis that the equipment is not vulnerable to known threats and is not interconnected then the guidance should be refreshed periodically to ensure that if that equipment in future becomes vulnerable appropriate additional mitigations are incorporated. Similarly, if the risk assessment relies on the equipment not being interconnected this should be clearly stated so in future if a need to interconnect arises the risk assessment and guidance would be recompleted.

Proposed Text:

"the applicant must make procedures and instructions for continued airworthiness (ICA) available that ensure that the cyber security protections…… are maintained. These procedures and instructions must be kept relevant and should include guidance on contextual use."

response **Noted**
Consideration for ICA is provided in more detail in AMC 20-42 (3.1.8-9).

comment *139* comment by: *UK CAA*

Page No: 8 - 9

Paragraph No: 3.1.3. and 3.1.4

Comment: It is unclear if the intended scope is to include: equipment, systems, networks and information.

Justification: There seems to be a lack of consistency in terminology used to identify scope. We are identifying this as a challenge as part of other areas of cyber security oversight (including Network and Information Systems regulation implementation). We are working to clarify the definition of "system" and identification of critical system scope with our industry and other interested parties. Is there a need to introduce some reference to criticality to help refine scope linked to adversity of the event?

Proposed Text:

"CS 25.1319 Cyber security protection related to equipment, systems, network and information"
"GM 29.1319 Cyber security protection related to equipment, systems, network and information"
"Appendix A.29.5 Cyber security instructions for continued airworthiness"
"CS 27.1319 Cyber security protection related to equipment, systems, network and information"

OR

"CS 25.1319 Cyber security protection related to critical aircraft systems."

*Critical systems can be identified as equipment, network, software and/or information systems where improper functioning could lead to a failure condition……"

response

Not accepted
The text needs to be consistent with the final report of the ARAC ASISP Working Group for regulatory harmonisation reasons.

comment

170 comment by: *Embraer S.A.*

Embraer believes that the text may mislead the reader as it is.

The text used is this section is different from the other sections and FAA PS-AIR.

To change the text from:

'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. […]

To:

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 major, hazardous or catastrophic effects on the safety of the rotorcraft.[…]

response

Partially accepted
The wording 'hazardous/severe major' comes from FAA AC 27-1b Change 4. This wording is now changed to 'hazardous' and is consistent with the scope of RMT.0712 on the 'enhancement of the safety assessment processes for rotorcraft designs'.

comment

216 comment by: *L. Riegle AIA*

3.1.4

Commented text
"GM"

Proposed Modification
"AMC"

Rationale
Industry has invested significant resources to establish ED203A. The document was specifically designed to provide both guidance material and acceptable means of compliance for the anticipated rules - as stated in Chapter 1.3 of ED203A identifying sections to be used as GM, AMC or only considerations for industry. By only using

	ED203A as GM (via AMC 20-42 and GMs in the individual parts), ED203A is not classified as an AMC to the new rules. As there is only Guidance Material, Special Conditions will still need to be applied to all programmes. This is counter to industry's endeavour to harmonise approaches rather than individually negotiated responses to CRIs. This is critical to ensure a level playing field, similar levels of safety and security and to reduce costs in the supply chain by allowing simple reuse of systems and components.
response	**Accepted**

comment	*226* comment by: *General Aviation Manufacturers Association / Hennig* EASA proposes a new CS 27.1319 that is modeled after the regulation applied to larger rotorcraft. The ASISP WG supported EASA (and FAA) issuing a regulation for normal category rotorcraft focused on catastrophic and hazardous/severe major safety effects. The ASISP WG provided its recommendations in 2016. Since then, GAMA is not aware of EASA or FAA having issued CRI for CS-27 rotorcraft to address cybersecurity. If there has not been sufficient reason for the agency to write a CRI for a small rotorcraft, GAMA questions whether a there is a basis to publish a new CS to address a perceived cybersecurity problem. GAMA requests that EASA determine whether amending CS 27 with a new section can be justified not based on the agency's experience with specific projects. If the answer is no, EASA may want to consider a lighter touch to CS-27 such as the standards envisioned for CS-23.
response	**Noted**

3. Proposed amendments and rationale in detail | 3.1. Draft certification specifications (Draft EASA decision) | 3.1.5. Draft decision amending CS-E p. 9-10

comment	*89* comment by: *Panasonic Avionics* 3.1.5 last sentence, replace "rather than" with "in addition to". I think we still want the security risk assessment to consider adverse effects on a single engine, in addition to any that may affect all engines.
response	**Partially accepted**

comment	*105* comment by: *Rolls-Royce plc* Comment Summary 1 : The CS-E 50 proposed wording introduces (for the first time in CS-E) the phrase "that may result in adverse effects on the safety of the aircraft" Since this is an engine-level requirement shouldn't the requirement be stated in engine level terms? Suggested Resolution 1:

How about:
"that could result in hazardous engine effects"
If accepted then CS-P would need to be similarly changed to be consistent

Comment Summary 2:
No amendment is proposed to CS-E 20 in relation to this NPA, yet agreement with the airframer on the security requirements ought to form part of the manuals relating to the installation of the the engine into the aircraft.

Suggested Resolution 2:
Add "security interface requirements" to the text in CS-E 20 (d).

response

Suggested Resolution 1: **Not accepted.**

For cybersecurity, because of the notion of intentional threat condition, a threat on an engine is a threat to all engines, so ultimately, it is the aircraft that is impacted.

Suggested Resolution 2: **Partially accepted.**

comment *140* comment by: *UK CAA*

Page No: 9

Paragraph No: 3.1.5

Comment: There seems to be a lack of consistency in terminology “Engine information security protection”

Justification: Lack of consistency

Proposed Text:

“Engine cyber security protection”

response

Partially accepted
The terminology will be reviewed to ensure consistency throughout the document.

comment *141* comment by: *UK CAA*

Page No: 9

Paragraph No: Section 3.1.5

Comment:

The second sentence of the proposed GM for E50 “…in particular, specific cases of ...” could be read to imply that events that would only affect a single engine do not need to be considered. In the context of maintaining overall safety (e.g. addressing events that occur after an engine loss has already occurred), it might be unwise to imply that events affecting a single engine do not have to be considered at all.

Additionally, the reference to “all the engine control systems“ and “a single engine“ could make it difficult to interpret the intent of this text. This is because it is not specifically clear whether the requirement relates to all the engine control system elements on a single engine, (e.g. channel 1 and channel 2 controls) or all the engine control systems on an aircraft and, by inference, all the engines on an aircraft

Justification:

Failure to consider events that affect single engines could result in the potential loss of more than one engine should a potential attack be realised after one or more engines has already been lost as a result of other issues.

Proposed Text:

We recommend that the requirements are extended to apply to single engine effects.

response **Accepted**

comment *212* comment by: *L. Riegle AIA*

3.1.5
Commented text
"[…] with special consideration given to the interfaces between the aircraft and the engine, if applicable. In particular, specific cases of intentional unauthorized 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."

Proposed Modification
Modify to "[...] with special consideration given to any external interfaces of the engine and to the interfaces between [...]"

Justification
Engines and propellers are separate Type Certificates from the rest of the aircraft. Sharing of risk and responsibilities is necessary to simply certification processes for all involved - the aircraft TC applicant needs to be able to rely on engines/propellers not introducing risks via common interfaces and vice versa as neither will have insight into design of other TC applicant. Current Special Conditions required aircraft TC holders to make statements on security of entire aircraft including powerplants without the easy insight and oversight of any external connections that the powerplants may have. By adding appropriate text, this can be simplified in the future - the aircraft TC applicant no longer needs to make statements on behalf of the powerplants and only needs to check that the aircraft systems do not create a risk to the powerplant. Similarly, the powerplant TC applicants need to ensure that any external interfaces are secured and that no risks are being introduced to that aircraft via the interface.

Commented text
"GM"

Proposed Modification
"AMC"

Rationale
Industry has invested significant resources to establish ED203A. The document was specifically designed to provide both guidance material and acceptable means of compliance for the anticipated rules - as stated in Chapter 1.3 of ED203A identifying sections to be used as GM, AMC or only considerations for industry. By only using ED203A as GM (via AMC 20-42 and GMs in the individual parts), ED203A is not classified as an AMC to the new rules. As there is only Guidance Material, Special Conditions will still need to be applied to all programmes. This is counter to industry's endeavour to harmonise approaches rather than individually negotiated responses to CRIs. This is critical to ensure a level playing field, similar levels of safety and security and to reduce costs in the supply chain by allowing simple reuse of systems and components.

Commented text
"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 unauthorized 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"

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

response

Proposed Modification 1: Accepted.

Proposed Modification 2: Accepted.

Proposed Modification 3: Partially accepted. The text has been modified to consider also other comments.

comment *234* comment by: *Bombardier*

Issue: Draft text for GM E 50(l) "Engine information security protection" should still include single engine assessment

Recommend: Change "rather than" in text to "as well as":

[S]pecific 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, as well as any interactions that could only have an adverse effect on a single engine.

response **Partially accepted**

comment *244* comment by: *Aerospace and Defence (ASD)*

Commented text
"[…] 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."

Proposed modification
Modify to "[...] with special consideration given to any external interfaces of the engine and to the interfaces between [...]"

Justification
Engines and propellers are separate Type Certificates from the rest of the aircraft. Sharing of risk and responsibilities is necessary to simply certification processes for all involved - the aircraft TC applicant needs to be able to rely on engines/propellers not introducing risks via common interfaces and vice versa as neither will have insight into design of other TC applicant. Current Special Conditions required aircraft TC holders to make statements on security of entire aircraft including powerplants without the easy insight and oversight of any external connections that the powerplants may have. By adding appropriate text, this can be simplified in the future - the aircraft TC applicant no longer needs to make statements on behalf of the powerplants and only needs to check that the aircraft systems do not create a risk to the powerplant. Similarly, the powerplant TC applicants need to ensure that any external interfaces are secured and that no risks are being introduced to that aircraft via the interface.

response **Accepted**

3. Proposed amendments and rationale in detail | 3.1. Draft certification specifications (Draft EASA decision) | 3.1.6. Draft decision amending CS-P p. 10-11

comment *3* comment by: *Luftfahrt-Bundesamt*

chapter 3.1.6, AMC P230:
"In particular,...could potentially have similar effects on all the propeller control systems..., rather than any interaction that results in an adverse effect on a single propeller."
Does "rather than" means that the potential adverse effect on a single propeller do not need to be analyzed at all?

response **Noted**

	The text has been modified to consider also other comments.
comment	*12* comment by: *European Powered Flying Union* 3.1.6. Draft decision amending CS-P page 10/20 CS-P 40 and CS-P 230 AMC P-230 We support the idea. However, the first sentence of your rationale does not make us happy. Rationale: In several cases of the past provisions for large aeroplane haven been broken down to light aeroplanes level, with limited success, to say the least. Careful examination is required before putting into force provisions that do not necessarily fit.
response	**Noted**
comment	*142* comment by: *UK CAA* **Page No:** 10 **Paragraph No:** Section 3.1.6 **Comment:** The second sentence of the proposed AMC “in particular, specific cases of ...” could be read to imply that events that would only affect a single propeller do not need to be considered. In the context of maintaining overall safety (e.g. addressing events that occur after a propeller system loss has already occurred), it might be unwise to imply that events affecting a single propeller not have to be considered at all. Additionally, the reference to “all the propeller control systems“ and “a single propeller “ could make it difficult to interpret the intent of this text. This is because it is not specifically clear whether the requirement relates to all the propeller control system elements on a single engine, (e.g. channel 1 and channel 2 controls) or all the propeller control systems on an aircraft and, by inference, all the propeller systems on an aircraft **Justification:** Failure to consider events that affect single propellers could result in the potential loss of more than one propeller system should a potential attack be realised after one or more propeller systems has already been lost as a result of other issues. **Proposed Text:** We recommend that the requirements are extended to apply to single propeller effects
response	**Accepted**

comment	*213* comment by: *L. Riegle AIA* 3.1.6 **Commented text** "[…] with special consideration given to the interfaces between the aircraft and the engine, if applicable. In particular, specific cases of intentional unauthorized 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." **Proposed Modification** Modify to "[...] with special consideration given to any external interfaces of the engine and to the interfaces between [...]" **Justification** Engines and propellers are separate Type Certificates from the rest of the aircraft. Sharing of risk and responsibilities is necessary to simply certification processes for all involved - the aircraft TC applicant needs to be able to rely on engines/propellers not introducing risks via common interfaces and vice versa as neither will have insight into design of other TC applicant. Current Special Conditions required aircraft TC holders to make statements on security of entire aircraft including powerplants without the easy insight and oversight of any external connections that the powerplants may have. By adding appropriate text, this can be simplified in the future - the aircraft TC applicant no longer needs to make statements on behalf of the powerplants and only needs to check that the aircraft systems do not create a risk to the powerplant. Similarly, the powerplant TC applicants need to ensure that any external interfaces are secured and that no risks are being introduced to that aircraft via the interface. **Commented text** "engine" **Proposed Modification** Modify word to "propeller control system" or sentence to "interfaces between the propeller and engine" **Justification** CS-P does not use Engine to refer to the propeller/propeller systems. The intent of the statement should be ensuring that due consideration is made on how the propeller control system interacts with other systems, particularly those by other Type Certificate Holders and covered by other parts of the Certification Specifications. **Commented text** "AMC" **Proposed Modification** Clarify inconsistency in approaches across Certification Specifications - CS-P is the only CS that has an AMC
response	Proposed Modification 1: **Accepted.**

	Proposed Modification 2: **Accepted.** Proposed Modification 3: **Noted.** The text has been modified to consider also other comments.

comment	*235* comment by: *Bombardier* **Issue**: Draft text for AMC P 230 should still include single propeller assessment **Recommend**: Change "rather than" in text to "as well as": "[S]pecific 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, as well as any interaction that results in an adverse effect on a single propeller."
response	**Partially accepted**

comment	*245* comment by: *Aerospace and Defence (ASD)* **Commented text** “engine” **Proposed modification** Modify word to “propeller control system” or sentence to “interfaces between the propeller and engine” **Justification** CS-P does not use Engine to refer to the propeller/propeller systems. The intent of the statement should be ensuring that due consideration is made on how the propeller control system interacts with other systems, particularly those by other Type Certificate Holders and covered by other parts of the Certification Specifications.
response	**Partially accepted**

3. Proposed amendments and rationale in detail | 3.1. Draft certification specifications (Draft EASA decision) | 3.1.7. Draft decision amending CS-ETSO p. 11

comment	*14* comment by: *Pratt@Whitney Rzeszow APUs* Draft decision amending CS-APU CS-APU 30 is amended as follows: **‘CS- APU 30 Instructions for Continued Airworthiness** (c) The following information must be considered, as appropriate, for inclusion into the manual(s) required by CS- APU 30 (a).

(1)
[…]
(13) Instructions applicable to information system security protection as required by CS-APU 90(d).'

CS-APU 90 is amended as follows:

'**CS-APU 90 APU control system**

[…]
(d) Information system security protection. APU 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 APU controls are maintained.'

The following AMC CS-APU 90 is amended as follows:

'**AMC CS-APU 90 APU Control System**
The following sentence is inserted after current text:
[…]
The AMC 20-42 in the CS-20 document provides acceptable means, guidance and methods to address
CS-APU 90(d), with special consideration given to the interfaces between the aircraft and the APU, if
applicable.'

response **Accepted**

comment *16* comment by: *Pratt@Whitney Rzeszow APUs*

Proposed is to amend the CS-APU text similar to requirements as for type certificated products, because according to ANNEX I (PART-21) to Regulation (EU) No 748/2012, para 21.A.604, authorization of new APU and approval of design changes is processed under the same procedures as certificated products, using CS-APU. Therefore, amendment to Subpart A, Section 2 of CS-ETSO will not cover APUs because CS-ETSO codes do not include requirements applicable to APU.

response **Accepted**

comment *143* comment by: *UK CAA*

Page No: 11

Paragraph No: 3.1.7

Comment: "security assurance level" needs to be further clarified as the meaning is unclear. We would welcome a definition.
Justification: This could be read to mean that a security assurance level would have different tiers or different levels. If that is the intent would that be based on the cyber risks identified or the impacts of an adverse effect? For example, if the adverse impact could result in X then a security assurance level of 5 is required.

response **Noted**
The definition can be found in ED-203A *Airworthiness Security Methods and Considerations*.

comment *210* comment by: *L. Riegle AIA*

3.1.7
Commented text
"An ETSO article may be designed with a security assurance level (SAL), according to the procedure provided in AMC 20-42."

Proposed modification
Modify to "An ETSO article may be designed with consideration for a specified threat condition or threat condition severity, according to the procedure provided in AMC 20-42." or if SAL is preferred, "An ETSO article may be designed with a security assurance level (SAL) for specified security measures, according to the procedure provided in AMC 20-42."

Justification
Common practice for ETSOs has been to specify the failure condition for safety to ensure they can remain commodity items (intent to allow changing of units without affecting TC) but allowing the freedom of developers to implement an appropriate design with flexibility in architecture and thus DAL. This principle should be carried forward for security and not specifying the SAL but instead the severity of the threat conditions to be expected. It may be advisable for some articles to specify common security measures where ETSO articles have connectivity to untrusted systems or are otherwise highly exposed.
A SAL in absence of security measures does not provide value as SAL is an assurance of security measures.
SAL is described in DO-356A/ED-203A section 4.4. SAL can be assigned to security measures and assets. Only SAL 0 is assigned to assets that are not security measures. Therefore, it is more correct to refer to SAL of security measures for the purpose of this paragraph.

response **Partially accepted**

comment *246* comment by: *Aerospace and Defence (ASD)*

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

Proposed modification
Modify to “An ETSO article may be designed with consideration for a specified threat condition or threat condition severity, according to the procedure provided in AMC 20-42.”

Justification
Common practice for ETSOs has been to specify the failure condition for safety to ensure they can remain commodity items (intent to allow changing of units without affecting TC) but allowing the freedom of developers to implement an appropriate design with flexibility in architecture and thus DAL. This principle should be carried forward for security and not specifying the SAL but instead the severity of the threat conditions to be expected. It may be advisable for some articles to specify common security measures where ETSO articles have connectivity to untrusted systems or are otherwise highly exposed.

response **Not accepted**
It is difficult to know the threat condition on an ETSO article before its installation. The only thing that an ETSO supplier can provide the installer with is some assurance that the information security has been taken into account to a certain level.

3. Proposed amendments and rationale in detail | 3.1. Draft certification specifications (Draft EASA decision) | 3.1.8. Draft decision amending AMC-20 p. 11-14

comment *13* comment by: *European Powered Flying Union*

3.1.8. Draft decision amending AMC-20
page 11-14/20
AMC 20-42 Airworthiness information security risk assessment

We support your proposals. We particularly like the last text block of chapter 9 on page 14/20 where you make clear statement on acceptable and/or unacceptable risks. Our comment no 12 (CS-P) was made on this base.

Rationale:
Considering the wide range of aircraft falling under the term "cyber security" or "cyber threats" a high degree of flexibility is very important.

response **Noted**

comment *18* comment by: *Universal Alloy Corporation Design*

The proposed AMC20-42 states, “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. "

This implies that the applicant DOA is required to have an ongoing 'anti-virus' function, potentially with a team of 'white-hat' hackers searching for vulnerabilities. We suppose a more passive monitoring approach is possible, where the risk assessment is revisited only when new threats are known. However, how does a DOA come to know about them? There appears to be no provision for a published list of threats, a position that is at odds with other aircraft safety arrangements, where ADs SIBs etc. are deliberately publically available. There are obviously security concerns with publishing known security threats before they have been countered. There are obvious analogies with the wider software world. If an IT Security Company for instance finds a vulnerability in Windows, the 'done thing' is to give Microsoft notice of this privately and only publish once a patch is available. This obviously only works for a single system and if the vulnerability is more widespread and not every affected developer is informed, then on publication, those who did not get the chance to develop a patch are immediately vulnerable.

The NPA appears to be aimed at original manufactures of equipment, who hold the keys to the code and have full knowledge of the system. However, it does not address the DOA function of third party modification. If a DOA installs a piece of COTS avionics equipment under cover of an STC, it has no knowledge of how it works from a software security perspective. Up until now, all the DOA is required to do is a limited investigation of the equipment qualification and Design Assurance (DA) levels together with a system assessment in accordance with CS XX.1309. However, the DOA is responsible for the ICA for the installed equipment. Beyond instructing operators to install the latest updates from the equipment OEM, how can a DOA hope to comply with the provision of the NPA? Even OEM updates may or, may not, include changes to code that address vulnerabilities, but the DOA does not know, because they are not published. Furthermore, the update may actually introduce a new vulnerability. If a DOA is responsible for the ongoing security of the equipment, is EASA expecting each DOA to make a comprehensive security risk assessment of each OEM software update to equipment installed under our STC, completely blind of the detailed changes made by the equipment OEM?

The two issues discussed above show an expectation by the NPA that DOAs have a software expertise that is far in excess of reality and that DOAs can make assessments and decisions concerning cybersecurity equivalent to those of the equipment software developers. Unfortunately, this is not the case. DOAs often have little to no software expertise.

response **Noted**
STC applicants need either to perform their own risk assessment and/or enter into an agreement with the OEM. Guidance can be found in ED 203A Section 4 'Aircraft Modification'.

comment *20* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION THE COMMENT IS RELATED TO:
Page 12, AMC 20-42, section 3.1.8.4 (a)

2. PROPOSED TEXT / COMMENT:
The text "[The PISRA] is an assessment of the information security of the systems that are specific to a product or part." should be replaced with "[The PISRA] is an assessment of the information security of the systems of a product or part that are identified in the section 2 of the AMC

3. RATIONALE / REASON for comment:
The meaning of the term "specific" is not clear.

response **Accepted**

comment *21* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION YTHE COMMENT IS RELATED TO:
Page 12, AMC 20-42, section 3.1.8.4 (d)

2. PROPOSED TEXT / COMMENT:
The text "Once the overall risk has been deemed to be acceptable, the applicant should develop instructions, as described in Section 9 […] » should be replaced by « Once the overall risk has been deemed to be acceptable, the applicant should develop instructions if necessary, to ensure that mitigations are effective as described in Section 9 (…] ».

3. RATIONALE / REASON for comment:
The necessity to have instructions will depend on the design solution and cannot be determined a priori.

response **Accepted**

comment *22* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION THE COMMENT IS RELATED TO:
Page 13, AMC 20-42, section 3.1.8.5 (a) (iv)

2. PROPOSED TEXT / COMMENT :
Consider replacing "affected items" by "affected assets"

3. RATIONALE / REASON / JUSTIFICATION for the Comment:
Use of "item" is misleading because the threat may also be related to a function or system. "Asset" is already used in the preceding statements and defined in ED-203A

response **Accepted**

comment *23* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION THE COMMENT IS RELATED TO:
Page 13, AMC 20-42, section 3.1.8.5 (a) (v)

2. PROPOSED TEXT / COMMENT:
"by considering the existing security protection means" should be added in the sentence (see next comment)

3. RATIONALE / REASON for comment:
Procedural and technical security protection means are often already included in initial concept and design. These protections should be taken into account when determining the initial security risk, without requiring a second iteration of a PISRA.

response **Accepted**
Reference: ED 202A Section 3.2.2.

comment *24* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION THE COMMENT IS RELATED TO:
Page 13, AMC 20-42, section 3.1.8.5 (a) (v)

2. PROPOSED TEXT / COMMENT:
The text “evaluation of the potentiality of a successful exploit, or of the difficulty of performing a successful attack that would have an impact on safety » should be replaced by “evaluation, by considering the existing security protection means, of the level of threat that would have an impact on safety”

3. RATIONALE / REASON for comment:
“Potentiality of exploitation” and “difficulty of attack” are two redundant descriptions of the same kind of analysis that focuses on the attacker perspective. The level of threat is that which is defined in ED 203 table 2.2.

response **Accepted**
Reference: ED 202A Section 3.2.2.

comment *25* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION THE COMMENT IS RELATED TO:
Page 13, AMC 20-42, section 3.1.8.5 (a) (vi)

2. PROPOSED TEXT / COMMENT:
The text "determination of whether the risks, which are the result of comparing the severities with the potentiality to attack […]" should be replaced by "determination of whether the risks, which are the result of combination of the severities and the potentiality to attack […]".

3. RATIONALE / REASON for comment:
Severity and potentiality to attack are two different matters and thus cannot be compared.

response **Accepted**

comment *26* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION THE COMMENT IS RELATED TO:
Page 13, AMC 20-42, section 3.1.8.5. (b)

2. PROPOSED TEXT / COMMENT:

It is Airbus understanding that only paragraph 2.1.1 of ED-202A is applicable as read in section 3.1.8. 5. (b) even though other references of ED-202A are found in 3.1.8 1. (b) and (c).
Could it be confirmed ?

response **Noted**

Section 3.1.8.5.(b) refers to ED 202A Section 2.1.1 as guidance.

It does not limit the applicability of ED 202A to that section. Therefore, there can be more references, when necessary.

comment *27* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION THE COMMENT IS RELATED TO:
Page 13, AMC 20-42, section 3.1.8

2. PROPOSED TEXT / COMMENT:
Section 3.1.8 6 is missing.

3. RATIONALE / REASON for comment:
It should be added for document structure consistency.

response **Noted**
The text has been modified to consider also other comments.

comment *30* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION THE COMMENT IS RELATED TO:
Page 13, AMC 20-42, section 3.1.8.9

2. PROPOSED TEXT / COMMENT:
The text "for example, physical and operational security" should be replaced by "for example, physical and operational procedures".

3. RATIONALE / REASON for comment:
“operational security” is not what is expected here.“operational security procedures” would be more appropriate as the paragraph is dealing with instructions.

response **Accepted**

comment *31* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION THE COMMENT IS RELATED TO:
Page 14, AMC 20-42, section 3.1.8.9

2. PROPOSED TEXT / COMMENT:
The text “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 » should be replaced with “For example, a threat condition that has a potential major safety effect, as defined in CS

25.1309, will not be acceptable depending on the level of threat of the associated threat scenario."

3. RATIONALE / REASON for comment:
Probability is related to safety assessment that addresses a list of events from which act of sabotage is explicitly excluded.

response **Accepted**

comment *32* comment by: *FAA*

Para 3.1.8(b) AC 20-42 proposes a method of compliance to aircraft systems information security protection for CS-23, CS-25, CS-27, CS-29, CS-E, CS-ETSO, CS-P rulemaking which would require compliance to ED-202A/RTCA DO-326A, ED-203/RTCA DO-356A, ED-204/RTCA DO-355

Comment: The European Documents (ED) / RTCA documents listed in the referenced text were developed as a means of compliance for Transport Category Airplanes.

Proposed Resolution: Require the ED / RTCA documents for CS-25 only. Allow other standards such as American Society for Testing and Materials (ASTM) F-44 ASISP be used as a means of compliance for CS-23, CS-27, CS-29, CS-E and CS-P. The security threats and vulnerabilities are different across aircraft types.

response **Not accepted**

Its content is generic enough to be used for other kinds of products. Applicability is not mandated at standard level but in the AMC.

EASA will consider the applicability of the ASTM F-44 standard for general aviation (GA), once it is published.

comment *36* comment by: *FAA*

Page 13 and 14
Para 8 and 9
Comment: The mitigation can be fast or slow, expensive or cheap, what matters is the effectiveness. The focus should be on "Effectiveness".
Proposed Resolution: 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~~ effectiveness of the mitigation means.

response **Accepted**

comment *37* comment by: *FAA*

Page 11
Para AMC 20-42
Referenced Text: RTCA documents
Comment: need to include ASTM for part 23, general aviation
Proposed Resolution: add ASTM F44 standard reference to this list.

response | **Not accepted**
The applicability of ASTM F-44 will be considered by EASA, once it is published.

comment | *38* comment by: *FAA*

Page 12
Para 4
Referenced Text: general principles
Comment: for consistency: cybersecurity is specific to information data network, and not physical security
Proposed The information systems identified in Section 2 should be assessed against any potential IUEI security threats and vulnerabilities that result in an unsafe condition.

response | **Accepted**

comment | *41* comment by: *EUROCAE - Anna Guegan*

3.1.8 Draft decision amending AMC-20

COMMENT 1: Page 11 – 1. Purpose

EUROCAE welcomes the referencing of its EUROCAE Documents in this Notice of Proposed Amendment (NPA). In addition to ED-202A/ DO-326A, ED-203A/ DO-356A and ED-204/DO-355 currently mentioned, please note that we have recently published ED-205 - Process Standard for Security Certification and Declaration of ATM ANS Ground Systems, published in March 2019.

Furthermore, revisions of ED-204/ DO-355 and ED-201 - Aeronautical Information System Security (AISS) Framework Guidance are currently being prepared. A new document, ED-xxx /DO-xyz - Guidance on Security Event Management is also under development.
If you have any question on EUROCAE document, please don't hesitate to contact us.

COMMENT 2: Page 13 5. Product information security risk assessment (=PISRA)

(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.
For the sake of clarity, the sentence could be amended as follows:
(b) The process for Security Risk Assessment identified in ED-202A Section 2.1.1 is acceptable as guidance for performing the PISRA for products and parts under Part 21.
Rationale:
The fact that the RMT refers to PISRA while the ED refers only to PASRA and PSSRA can be misleading. Specifying for Security Risk Assessment provides clarification.

response | Comment 1: **Noted**
Comment 2: **Accepted**

comment | *42* comment by: *General Aviation Manufacturers Association / Hennig*

EASA proposes in AMC 20-42: Airworthiness information security risk assessment, section 1. Purpose (c) that AMC 20-42 "establishes guidance to use ED-202A... and the certification of aviation-related services (e.g. traffic management, data links, etc.)".

GAMA notes that separate efforts are underway to review the standards used for air traffic management-related services including communications (data link), navigation (GPS), and surveillance (ADS-B) with the objective of including cybersecurity requirements as part of the industry standard or related E/TSO where appropriate. As an example, some of these efforts may result in amendments to the standard (*e.g.*, reference to RTCA SC-159 Terms of Reference, SPECIFIC GUIDANCE, 5. "New MOPS will address, to the extent practicable, the threats of intentional interference and spoofing.)." Related to this review, some CNS-cybersecurity risk analysis is being undertaken by dedicated groups (*e.g.*, EASA RMT.524, Task 5).

Industry must adhere to and meet the requirements identified by EASA in the ETSO and is not permitted to make changes that adversely impact the interoperability of a system.

This issue was discussed in the FAA ARAC ASISP WG recommendations (reference to Recommendation
27; https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/ARACasisp-T1-20150203R.pdf). In response to this recommendation, certain regulators have conducted a table top review of the standards, and where suitable, initiated work to update the standards per above.

The inclusion of the example in the proposed section 1 (c) likely would cause confusion as to what an applicant needs to do, especially for air traffic management and CNS equipment that relies on mature links and functionality.

GAMA recommends that EASA does not include the example by rewriting (c) to state:

"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." [DELETE: ~~and the certification of aviation-related services (e.g. traffic management, data link, etc.~~]

response **Accepted**

comment *43* comment by: *Virgin Atlantic Airways Ltd*

EASA wish to take a risk-balanced approach to Aircraft Cyber Security, which VAA fully endorses. However, this NPA seems to concentrate on OEMs/ TCHs/ STCHs / Service providers etc. performing the risk assessments and implementing mitigations. That's great except when you get to the elements which are implemented by operators, such as the IT systems that support the eOps function. These are certainly not devoid of risk and how they are implemented can have a significant impact on the level of risk posed to the aircraft and aircraft systems. Thus it would make sense for the operators to also take a risk managed approach to implementing things such as the Ground Support Information Systems (GSIS) the EFBs and other IT-related systems that interact directly and indirectly with the aircraft.

However, it is difficult for operators to achieve this without the full facts about the vulnerabilities in the first place. If you follow the logical pathway:

Vulnerability = the weakness
Threat = the actor or method which can leverage a vulnerability
Likelihood = the probability of the threat being able to have an effect (could also be called frequency)
Risk = the resulting score of the three items above.
Operators could make an informed assessment and suggest mitigations. Yet currently it is the OEMs/ TCHs/ STCHs/ Service providers etc. who know the risks and who communicate instructions and recommendations to mitigate these risks. This information is passed on without informing the Operators of the detail, just a recommendation on measures to implement. This seems non-sensical to me. In the course of our work on e-enabled aircraft VAA has discovered multiple software vulnerabilities some of which appear to have mitigation recommendations, and worryingly, some that don't. How can an Operator ensure Assurance of the Aircraft Systems if we do not know the full risk picture? Seeing as operators have a fair amount of freedom to implement their own solutions in whatever way they seem fit, how can an operator know for sure whether their configuration will increase or decrease the risk? How can an operator implement risk management over issues to which they are not aware but are fully exposed to? The manufacturer may have a very different appetite for risk to the Operator, so how is that dealt with at the corporate level?

VAA understands that aircraft IT vulnerabilities would be an extremely sensitive subject and sharing them would not be without concern, but there are ways of ensuring confidentiality between the operator and the manufacturer that would permit such information to go back and forth. There is already in place such channels for other Security Sensitive information. Without which Operators will continue to implement IT systems of which they are devoid of the full facts behind the risk they pose to both their internal networks and the Aircraft they support.

response **Noted**

comment *52* comment by: *European Cockpit Association*

Proposal: pg.12: Add "*continuously*" in Section 2 *should continuously be assessed against.*

Rationale: Cyber threats, vulnerabilities and risks are ever changing. Thus, a continuous / regular assessment / reassessment is required.

response **Not accepted**
This is part of the instructions for continued product and part information security protection (Section 3.1.8.9). It can be continuously, periodically or vulnerability driven (vulnerability management).

comment *53* comment by: *European Cockpit Association*

Proposal: Pg. 12: Change & Add: It is an assessment of the information security of the systems of a product or part. It should be extended to systems connected to the product or part in question if new information security risks may be introduced.

Rationale: assessments cannot be focused on just a specific system but must be considered in relation to "system of systems". A change in one system may introduce new risks to other systems it is connected with. Thus, the interfaces and connected systems must be considered in an assessment as well.

response **Not accepted**
Although agreed in principle, the methodology requires to define the security environment first, which includes connected systems, but for which the OEM has no control (e.g. signal in space).

comment *54* comment by: *European Cockpit Association*

Proposal: pg. 12: replace *known*by *potential*

Rationale: threats that are not known / available today may become relevant in future. Thus, also potential risks should be considered as the threat landscape may change or new exploits for vulnerabilities may become available.

response **Noted**
The text has been changed based on other comments.

comment *55* comment by: *European Cockpit Association*

Proposal: Pg. 12: Add *Identified vulnerabilities that are not mitigated should be communicated to the operator.*

Rationale: Operators are ultimately responsible for the safety. Operators have the view on the whole system and can assess the overall risk. Furthermore, they need to be able to decide whether they accept the risks introduced by the vulnerabilities.

response **Not accepted**
Vulnerability is not mitigated when the assessment shows that the risk is acceptable. Operators may require this information from the OEM but it is outside the scope of type certification.

comment *56* comment by: *European Cockpit Association*

Proposal: Pg. 12: Add *The mitigation should be provided to the operators in a timely manner*.

Rationale: To reduce risks, a mitigation should be provided to the operators in a timely manner.

response **Partially accepted**
This section is about the development of the product. The communication to the operator of mitigation means during operation of the product is part of the continuing airworthiness phase (Sections 7 and 9).

	The proposal to update Section 3.1.8.9 is **accepted**.
comment	*57* comment by: *European Cockpit Association* Proposal: Pg. 13, pg...: for consistency purpose the same" IUEI" terminology should be used for AMC 20-42 and subsequent paragraphs as well. Rationale: In CS23, CS29, CS-E, CS-P, and AMC P230 the term « intentional electronic interaction (IUEI) » is consistently used. However, in AMC 20-42 (p.12) "information security threats" is used in the same context. As other examples, "violation of the system and information rules" (p.9) or "information security occurrences" (p.14) are used with quite the same meaning.
response	**Partially accepted**
comment	*58* comment by: *European Cockpit Association* Proposal: pg. 13: replace "*reasonably high potential for an unsafe condition*" by "*identifies potential for an unsafe condition".* Rationale: It is stated that "*operators should report to authority in a timely manner if their impact analysis identifies 'reasonably high potential 'or an unsafe condition*". Here, operators can judge and to assess their own products. In this respect, guideline for reporting must be clear and more conservative. In this respect, "reasonably high potential" is too vague and can be misinterpreted. [p. 13 5, a, v)] In calculation of the probability of an attack, it should not be assumed, that the attacker is onboard the aircraft and risks his own life with a crash, because he could also hack in via the satcom or via a 'trojanized' laptop connected to the IFE using the onboard internet connection.
response	**Accepted**
comment	*59* comment by: *European Cockpit Association* Proposal[p.13 5, a, vi) A] Add: ...mitigation means *as in section 8*... Rationale: Ensure that security testing and a penetration test is conducted as part of the evaluation.
response	**Not accepted** Section 8 is about security testing.
comment	*60* comment by: *European Cockpit Association* Proposal[p.13 5, b]: Add (c) *Operators should be allowed to read the PSIRA documentation.* Rationale: The operators are responsible for the safety of their passengers and crews. Thus, they should have transparency over the scope of the risk assessment, the identified risks, the basis for the risk severity rating and the mitigation means. This would enable operators to evaluate whether potential risks are within their risk

	appetite or if they may want to be more cautious and introduce further mitigation measures.
response	**Not accepted** Operators should enter into an agreement with the manufacturer, if they want to have access to the PISRA.

comment	*61* comment by: *European Cockpit Association* Proposal[p.13, 7] Add: *the competent authority and the operators of this product or part.* Rationale: The operator should be put in the position to evaluate the risk for their operations independently. This would allow the operator to decide about mitigating measures or even a grounding of an aircraft even if the competent authority did not order it as a mandatory measure yet.
response	**Not accepted** See Article 4 of 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 (OJ L 122, 24.4.2014, p. 18)[5]. It refers only to the competent authority.

comment	*62* comment by: *European Cockpit Association* Proposal[p. 13 8, a, i): replace *may* by *should* Rationale: This is important and *should*be done.
response	**Accepted**

comment	*63* comment by: *European Cockpit Association* Proposal[p.13 8, *add*(**b) (c) (d):** *(b) Security testing that addresses information security from the perspective of a potential adversary must be conducted by an independent body during the design and continuously during the lifecycle of a part or product. The scope of such tests must not be limited to the initial attack surface available to an attacker but should test systems behind the perimeter as well to ensure that the defence in depth is appropriate.* *(c) Reports of security testing including the scope of the testing and identified open vulnerabilities must be made available to the competent authority and the operators of the product.* *(d) The applicant must grant the operator a right to audit the security measures and the conducted security testing. This will include the provision of software and firmware versions and configurations used (e.g., Firewall rules) as well as information on security architecture, processes and policies (e.g., secure development methodologies).*

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1579096167575&uri=CELEX:32014R0376

Rationale: Penetration testing should always be conducted to verify the security protection. Furthermore, such tests should be done continuously to adapt for new threats and attack measures. Penetration testing is an important measure to detect otherwise undetected flaws, vulnerabilities and weaknesses in systems.
The operators are responsible for the security of their passengers and crews. Thus, they must be empowered to verify the security measures taken. This includes sharing of security measures, test results, configurations. This will allow operators to do their risk assessments and decide if additional measures are required and how they react on possible unclosed vulnerabilities. Proprietary source codes do not have to be shared with operators.

response **Not accepted**

comment *64* comment by: *European Cockpit Association*

Proposal: [p.14] the applicant "*should notify the operators and the competent authority of the need and the practical means to mitigate the new risk (or the absence of them), in a timely manner*" [+ reference to EU 748/2012 point 21 A 3 A Annex I Part 21 ----] see Paragraph 7 Reporting p.13.
Rationale:[p.14] it is stated that the applicant should also assess the impact of new threats that were not foreseen during previous risk assessments and should, in turn, inform operators of the need and means to mitigate the risk.
It can be stressed that they should report not only to their customers/operators but also to their competent authority.
Moreover, in most of the cases new attacks or threats use multi-vendors or nonspecific vectors (i.e. against widely used hardware, features, protocols etc.) consequently, in most cases, an applicant alone will not be able to find immediate practical mitigations and must state it clearly to authority and operators. In turn other applicants using the same technology should be
Finally, this report to the competent authority should be done in the same timeframe ("*timely manner")*as underlined in the previous paragraph 7 (reporting).

response **Accepted**

comment *65* comment by: *European Cockpit Association*

Proposal[p.14]: **add**"*The applicant should provide information of the part's or product's security measures and security architecture to the operator to enable the operator conducting security testing that addresses information security from the perspective of a potential adversary. The applicant should provide the operator with procedures to ensure that the part or product can be reset in a state that is in accordance with its specifications after security testing".*

Rationale: Operators are ultimately responsible for the safety. Operators have the view on the whole system and can assess the overall risk. Furthermore, they need to be able to decide whether they accept the risks introduced by the vulnerabilities.

response **Not accepted**
It is not in within the scope of the regulation. This kind of agreement should be concluded between the operator and the OEM.

comment	*67* comment by: *Certification Expert* §2 Applicability The following sentence of §3.1.8 « A change to a product » is proposed to be clarified as follows : "A major change to a product in the context of a product information security risk assessment". Otherwise, it may be understood that the cybersecurity evaluation has to be performed for any product change and the proposal is consistent with explanation provided in §3.1.9.
response	**Not accepted** A change to a product may be considered as 'minor change' from a safety perspective. It does not prevent the OEM performing a change impact assessment on information security. A minor change does not mean the applicant must do nothing — it means that the applicant can approve the change under its privileges when applicable.

comment	*77* comment by: *FAA* Page: 11 Section 3.1.8 AMC 20-42 Comment: corrected dates DO-326A, dated August 06, 2014; DO-356A, dated June 21, 2018; DO-355, dated June 17, 2014 Page: 13 Section 5(a) Comment: Provide sufficient airplane security information Proposed Resolution: suggest to add: "summarizes the airplane network security architecture design"; "summarizes the security requirements and controls implemented by individual systems".
response	Page 11: **Accepted.** Page 13: **Not accepted.** EASA considers that it is more appropriate to include such details in the standards.

comment	*78* comment by: *FAA* Page: 13 Section 5(a) Comment: Provide methodology Proposed Resolution: suggest to change item (iv) assessment of the safety consequences of the threat to the affected items including a summary of the methods and security control technologies used throughout the airplane.
response	**Not accepted** At step 3.1.8.5(a)(iv), there may be no security controls yet. As a result of step 3.1.8.5(a)(vi), it will be determined whether or not there is a need for security controls.

comment	*79* comment by: *FAA*

	Page: 13 Section 8 Comment: Security Test consist two fundamental types: Tests of security requirements and tests of security robustness. Penetration testing is performed on the airplane. Proposed Resolution: suggest to change item (a)(i) to "The security testing may be performed by a combination of analysis, security-oriented robustness testing, inspection and where necessary, by appropriate ground, flight or simulation tests; and"
response	**Not accepted** Analysis is not testing but, like testing, it is a form of verification.

comment	*83* comment by: *General Aviation Manufacturers Association / Hennig* AMC 20-42, Section 7. Reporting, states that "The operator of a product or part should report any information security occurrence to the designer of this product or part..." GAMA interprets this statement to mean that the operator is responsible to report directly to the holder of the TSO/PMA, which may bypass the TC/STC holder. GAMA recommends rewording this statement as follows to allow flexibility in the reporting mechanism: "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 to allow further impact analysis and corrective actions, if appropriate."
response	**Accepted**

comment	*90* comment by: *Panasonic Avionics* 4.(a), insert "(per ED-203A 2.7.3)" after "unacceptable" to make clear what basis is used to determine risk acceptability.
response	**Not accepted** Depending on the product, other acceptability matrices may be recognised.

comment	*91* comment by: *Panasonic Avionics* 3.1.8 in Acceptable/Unacceptable Risk section, insert after "…the probability that the associated threat scenario is successfully exploited is too high" this reference, "(refer to Risk Acceptability Matrix in ED-203A Table 2-2)" because risk acceptability is a matrix decision based on likelihood and impact severity.
response	**Not accepted** Depending on the product, other acceptability matrices may be recognised.

comment	*98* comment by: *AIRBUS*

1. PAGE / PARAGRAPH / SECTION THE COMMENT IS RELATED TO:
Page 13, AMC 20-42, section 3.1.8.8 (a)

2. PROPOSED TEXT / COMMENT:
Consider replacing "efficiency of the mitigation means" by "effectiveness of the mitigation means"

3. RATIONALE / REASON for comment:
Terminology of ED-203A should be used. Efficiency (commonly defined as the relationship between obtained results and resourced engaged) is not relevant to determine whether the protection sufficiently mitigates the risk. But effectiveness (commonly defined as the relationship between obtained results and objectives) is.

response **Accepted**

comment *99* comment by: *ENAC*

AMC 20-42 paragraph 2. Applicability includes service providers (traffic management). We are concerned that AMC 20-X can deal with such entities without a dedicated CS. Guidelines applicable to service and service provider should be better included in a different set of requirements. - Alternatively reference to ED-205 (Process Std for ATM/ANS ground system security aspects for certification/declaration) should be included in the AMC 20-42 par. 1.(b) where applicable ED are listed.

response **Not accepted**

comment *100* comment by: *ENAC*

Paragraph 7
Reporting
The meaning "operator" is not immediately clear to me. Does it mean the aircraft operator? The word operator may have variuos meaning in civil aviation. It should be considered to specify better the intention.

response **Noted**
Any part or product operator has the responsibility to notify the designer/ manufacturer of that part or product; it is not only aimed at air operators.

comment *101* comment by: *ENAC*

AMC 20-42
Editorial
par. 6 is missing

response **Noted.**
The text has been modified to consider also other comments.

comment *102* comment by: *ENAC*

NPA clearly states that effects of cybersecurity threads (under the scope of the NPA) are those having effects on safety and the ones having effects limited to confidentiality with no impact on safety are out of the scope. ED20X include "Confidentiality" as part of their guided assessment and Loss of confidentiality is not dealt anyhow differently than loss of integrity or availability.
In the AMC20-42 consideration should be given for including a statement that parts of ED 20X relevant to loss of confidentiality might be considered not applicable when their effect on the aircraft safety is negligible.

response **Not accepted**
The AMC clarifies that it is safety driven. As such, confidentiality, integrity and availability are to be considered in the scenario having a safety impact only.

comment *107* comment by: *Dassault-Aviation*

Text:
P12 Section 3.1.8, 1. Purpose (c)

Proposed text:
To state clearly that the scope of applicability of AMC 20-42 is broader than the scope of the NPA as it includes certification of aviation-related services that is not addressed in the regulations addressed in the NPA.

Rationale:
Certification of aviation-related services (e.g. traffic management, data links, etc.) has been added in AMC while the scope of NPA is limited to CS-23, CS-25, CS-27, CS-29, CS-E, CS-ETSO, CS-P. It is confusing when reading the AMC in this context.

response **Accepted**

comment *108* comment by: *Dassault-Aviation*

Text:
P12 Section 3.1.8, 4. General Principles (b)

Proposed text:
“those vulnerabilities cannot be exploited by any security threat considered in the risk assessment”.

Rationale:
“those vulnerabilities cannot be exploited by any known security threat” is hardly achievable.

response **Noted**
The text has been modified.

comment *109* comment by: *Dassault-Aviation*

Text:
P13 Section 3.1.8, 5. Product information security risk assessment , (a) (i)

Proposed text: To replace “operational environment” by “security environment” as in ED-202A.

Rationale: Security environment is more accurate and may include when relevant the operational environment.

response **Accepted**

comment *110* comment by: *Dassault-Aviation*

Text:
P13 Section 3.1.8, 5. Product information security risk assessment , (a) (vi) (B)

Proposed text:
“evaluation of the effectiveness of the mitigation means with respect to the level of risk (combination of level of threat and severity of Threat Condition)”

Rationale: Severity is not applicable to threat, but to Threat Condition.

response **Accepted**

comment *111* comment by: *Dassault-Aviation*

Text:
P 13 Section 3.1.8, 7. Reporting:

Proposed text: If you maintain sub-section 7 on “operator”, then the operator should be informed about this obligation in appropriate regulations.

response **Noted**

comment *112* comment by: *Dassault-Aviation*

Text:
P14 Section 3.1.8, 9. Instructions for continued product and part information security protection - Last paragraph on Acceptable/Un acceptable risk:

Proposed text:
Consider moving this last paragraph in a new section §3.1.8, 6. **Risk acceptability**

Rationale:
This paragraph seems general and not linked with continued airworthiness.

response **Accepted**

comment *113* comment by: *Dassault-Aviation*

Text:
P14 Section 3.1.8, 9. Instructions for continued product and part information security protection - Last paragraph on Acceptable/Un acceptable risk:

Proposed text:
clarification requested

Rationale:
There is no Risk Acceptability Matrix referenced as GM in this sub-section. It is understood that last paragraph of this sub-section provides the rationale for it.
Shall we understand that the DAH has the ability to suggest and negotiate with EASA for approval of its own Table, or risk by risk?

response **Noted**
Guidance on the acceptability matrix for large aircraft can be found in ED-203A.

comment *114* comment by: *Dassault-Aviation*

Text:
P14 Section 3.1.8, 9. Instructions for continued product and part information security protection:

Proposed text:
replace “probability” by “level of threat” or “potentiality”.

Rationale:
The word “probability” is inappropriate in the context of cyber security.

response **Accepted**
The possibility of the level of threat and the likelihood of an asset to be a target is now included.

comment *120* comment by: *FOCA Switzerland*

Comment FOCA on AMC 20-42 vs ED-20X LOSS OF CONFIDENTIALITY:
The NPA general text clearly states that effects of cyse threads under the scope of the NPA are those having effects on safety and the ones having effects limited to confidentiality with no impact on safety, are out of the scope. This is not consistent with the reference to ED20X, as ED20X includes Confidentiality as part of their guided assessment and Loss of confidentiality is not dealt anyhow differently than loss of integrity or availability.

Proposal FOCA on AMC 20-42 vs ED-20X LOSS OF CONFIDENTIALITY: AMC20-42 should include a statement that parts of ED 20X relevant to loss of confidentiality might be considered not applicable when their effect on the aircraft safety is null. It will not be easy to simply divide it, but the message should be passed anyhow by the AMC when recalling ED-20X material without any discrimination in the content.

Comment FOCA on AMC 20-42 Services and Service Provider:
AMC 20-42 has aviation related service (traffic management) in the Applicability’s scope (AMC 20-42 §2), we are concerned that AMC 20-X can deal with it while having no CS dedicated to it. Guidelines applicable to service and service provider should be better included in a different set of requirements.

Proposal FOCA on AMC 20-42 Services and Service Provider:

AMC20-42 should keep services and service provider out of the Applicability. Alternatively, ED-205 (Process Std for ATM_ANS ground system security aspects for certification_declaration) should be included in the set of ED-20X here recalled by the AMC 20-42.

Comment FOCA on AMC 20-42 General principle – Instructions and Implementation of mitigation means:
AMC 20-42 §4.d) requires to provide substantiation that mitigation are effective for the scope of managing the risk acceptability and para §5 a) vi) requires to implement mitigation means "until" the risk is not acceptable.
Those mitigation might be preventive measure at organization level outside DOA. eg. Screening of personal background for maintenance personnel. The actual frame does not pose any possibility for DOA to mandate licensing requirements for maintenance or other organization measures. Does it mean that those mitigation cannot be considered to provide sufficient ground?

Proposal FOCA on AMC 20-42 General principle – Instructions and Implementation of mitigation means:

- Clarify whether any measures falling outside the possibility of what is mandated to different organization can be considered effective once identified (e.g. included in the ICA) or not.
- Introduce a specific paragraph in the AMC 20-42 dealing with organizational measure coming from PISRA .

Comment FOCA on AMC 20-42 – §7- REPORTING:
It looks incorrect to have reporting in the AMC 20-42. This content should be moved to AMC/GM to Part 21A 3. Additionally, as expressed now it applies to operators and as such it is not possible to have it mandated by initial airworthiness regulatory material.

Proposal FOCA on AMC 20-42 – §7- REPORTING:

- Delete part relevant to occurrence reporting and ref to to AMC/GM to Part 21A3
- Delete part relevant to acceptability of risk. Alternatively move it to §5 and specify which are the mean to propose acceptability criteria different from those considered by ED 20X

Comment FOCA on Point 2 of the AMC (Applicability):
In general, FOCA supports the reference to the existing EUROCAE documents and procedures.

Comment FOCA on Point 2 of the AMC (Applicability):
Why is there a reference to "service providers"? Which service providers are meant by this? Should this not rather be covered under RMT 0.720?

Comment FOCA on Point 5 (Product information security risk assessment):
(a) (vi) -> Before the point on implementation of mitigation measures, should there not be a safety analysis to ensure that the proposed mitigation measures do not have a negative safety impact?

Proposal FOCA on Point 5 (Product information security risk assessment):

Should we not add point a) analysis of the proposed mitigation measures to ensure they do not negatively affect safety? And then add existing points (A) and (B) as new points (B) and (C)?
This may need to also be discussed face-to-face with experts.

Comment FOCA on Point 7 (Reporting):This should be included/covered by RMT 0.720 and not RMT 0.648.

Proposal FOCA on Point 7 (Reporting): Delete point 7 from this AMC.

response

Comment/proposal on AMC 20-42 v ED-20x Loss Of Confidentiality: Not accepted

The AMC clarifies that it is safety driven. As such, confidentiality, integrity and availability are to be considered in the scenario having a safety impact only. There is no distinction made between the CIA attributes in AMC 20-42. Only the impact on safety is the dimensioning factor.

Comment/proposal on AMC 20-42 Services and Service Provider: Noted

The issue has been addressed through other comments and the reference to service providers has been removed.

Comment on AMC 20-42 General Principle — Instructions and Implementation of mitigation means:

Proposal 1: Noted

The mitigation provided by preventive measures at organisation or process level can be used as assumptions during the aircraft information security risk assessment.

Proposal 2: Accepted

Comment on AMC 20-42-7. Reporting:

Proposal 1: Not accepted

It is not unusual to have a section dealing with reporting in AMC-20 material.

Proposal 2: Partially accepted

The text has been modified to consider also other comments.

Comment on Point 2 of the AMC (Applicability): Noted

Comment on Point 2 of the AMC (Applicability): Noted

The text has been modified due to other comments.

Comment/proposal on Point 5 (Product Information Security Risk Assessment: Partially accepted

The text has been modified to consider also other comments.

Comment/Proposal on point 7 (Reporting): Not accepted

It is a different kind of reporting.

comment *123* comment by: *Garmin International*

3.1.8 Draft decision amending AMC 20, AMC 20-42 section 4. General principles item (b):

This item refers to a “failure condition”. The ED-202A/DO-326A process generally assesses threat conditions.

Update “generate a failure condition” to read “generate a threat condition”.

response **Partially accepted**

comment *124* comment by: *Garmin International*

3.1.8 Draft decision amending AMC-20, AMC 20-42 section 5. Product information security risk assessment item (a)(v):

This item uses the phrases “successful exploit” and “difficulty of performing a successful attack”, which is not terminology used in the DO-326A/ED-202A family. It seems that this item’s wording is attempting to capture both the “Effectiveness” and “Likelihood” methods discussed in DO-356A/ED-203A section 3.6.1. Additionally, this terminology is inconsistent with that used in section 5 item (a)(vi).

Rephrase this item to, “evaluation of the possibility of a successful attack, considering either the likelihood of success against a measure or the effectiveness of a measure, that would have an impact on safety;”

response **Not accepted**
The proposed change does not add clarity to the text.

comment *125* comment by: *Garmin International*

3.1.8 Draft decision amending AMC-20, AMC 20-42 section 5. Product information security risk assessment item (a)(vi):

This item uses the phrases “potentially to attack” and “difficulty of attacking” which are not terminology used in the DO-326A/ED-202A family. It seems that this item’s wording is attempting to capture both the “Effectiveness” and “Likelihood” methods discussed in DO-356A/ED-203A section 3.6.1. Additionally, this terminology is inconsistent with that used in section 5 item (a)(v).

Change “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” to “determination of whether the risks, which are the result of comparing the resulting threat conditions with the likelihood of an attack’s success against a measure or the effectiveness of a measure against an attack, are acceptable”

response **Not accepted**
The proposed change does not add clarity to the text.

comment *126* comment by: *Garmin International*

3.1.8 Draft decision amending AMC-20, AMC 20-42 section 5. Product information security risk assessment item (a)(vii):

The location of (a)(vii) is inconsistent with the risk assessment flow in ED-202A/DO-326A Figure 2-1. If risks are acceptable there is no need to iterate from this decision point.

Suggest changing as follows:
" ~~(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.
(c) iteration from point (a)(vi) until all the residual risks are acceptable."

response **Not accepted**

comment *127* comment by: *Garmin International*

3.1.8 Draft decision amending AMC-20, AMC 20-42 section 8. Validation and verification of the security protection item (a):

The text uses the phrase "evaluate the efficiency". The goal of security verification, as described in DO-356A/ED-203A section 5.9.3, is to confirm that the product works as expected. Efficiency of a given measures is generally not a security consideration.

Change "evaluate the efficiency of the mitigation means" to "ensure the mitigation means operates as intended" or "evaluate the efficacy of the mitigation means".

response **Partially accepted**

comment *144* comment by: *UK CAA*

Page No: 11-15

Paragraph No: Section 3.1.8 General

Comment:
As the AMC proposes a separate security risk assessment, more guidance should be provided on how the interface with the safety assessment requirements specified in paragraph xx.1309 and its supporting AMC should be addressed. It would also be helpful to have more information on the interfaces with paragraphs 1301 and 1302.

Justification:
The PISRA will be one part of an overall set of safety arguments and appropriate guidance regarding the interface between the PISRA and the safety assessments is important to ensure that the results of the PISRA are accurately accounted for in the safety assessments.

Proposed Text:
None provided as the development of this guidance is likely to be the subject of additional, harmonised, requirements/guidance.

response **Noted**

comment *145* comment by: *UK CAA*

Page No: 11-15

Paragraph No: Section 3.1.8

Comment:
Given the complexity of some aircraft systems and products, it is likely that problems will occur during the development of these systems and/or products that could affect security. Within the safety domain, there are requirements related to classification of problem reports and management of outstanding problem reports. Additional guidance on how these requirements would link to the PISRA would be helpful.

Additionally, within the safety domain, ARP 4754 or ARP 4754A (whichever is appropriate) have been included in the Type Certification requirements for many recent products. ARP 4754/4754A places specific obligations on organisations designing and developing aircraft products related to the assessment of the overall set of outstanding problem reports that are extant at the point of certification. It would be helpful to have further guidance on how the PISRA related processes will interact with the overall problem reporting assessment processes required by ARP 4754/ARP 4754A.

Justification:
Failure to properly consider all aspects of problem reports that are outstanding at certification can result in potentially significant safety issues being missed.

Proposed Text:
None provided as the development of this guidance is likely to be the subject of additional, harmonised, requirements/guidance.

response **Noted**

comment *146* comment by: *UK CAA*

Page No: 12

Paragraph No: 2. Applicability

Comment: “the certification of other systems or equipment that provide air service information” feels very broad in scope. However, “the approval of products and parts of information systems that are subject to potential security threats and that could result in unacceptable safety risks” is quite open to interpretation of both potential security threats and what would be considered an “unacceptable” safety risk.

Justification: It may be quite difficult to interpret when this should be applied, if that is the case then this may be omitted in some cases where it should not have been and included in other cases where it isn’t required. For consistency we suggest splitting this into a “who”, “what”, “when” and “to consider”. For example:

Applicability

Who – this AMC applies to products and part manufacturers, equipment providers, service providers and design approval holders

What – Products (i.e. an aircraft, engine or propeller, existing certified products, systems or equipment that provide air service information that require certification)

When – new certification, supplemental type certificate application, change, approval of a new item to be used in an ETSO article ***(in the context of at what stages would this apply)***

Consider – at all stages any product or part where improper functioning as a result of IUEI could result in an unacceptable safety risk.

In this way you ensure that the scope can be applied more broadly where required and more specifically where unacceptable safety risk has been identified (which is the key impact).

Proposed Text: as above but in a different format.

response **Not accepted**
For the purpose of consistency with AMC-20.

comment *147* comment by: *UK CAA*

Page No: 12

Paragraph No: 4 (a) General Principles

Comment: The term 'Product Information Security Risk Assessment' introduces inconsistencies

Justification: There is also the potential that if an "item" isn't considered a product, as the "what" isn't always defined as a product in the regulation, then it may be thought that it doesn't apply.

Proposed Text: Cyber Security Risk Assessment

OR

Aircraft Cyber Security Risk Assessment (if this can't be used more broadly)

response **Not accepted**
The term 'product' allows to address also engines, ETSOs, APUs, etc.

comment *148* comment by: *UK CAA*

Page No: 12

Paragraph No: 4 (d) General Principles
Comment: It is unclear whether the NPA is trying to maintain the cyber security risk at a consistent level or maintain the security controls that have been identified as required to address cyber security risks, identified as part of the risk assessment.

Justification: A risk can be maintained at an "acceptable level" with varying controls or maintain the same controls but the risk "level" may vary due to increases/decreases in various factors (like threat, likelihood etc).

Proposed Text: Clarification on this point would be welcomed

response

Noted
The aim is to maintain the cybersecurity risk at a consistent level.

comment *149* comment by: *UK CAA*

Page No: 13

Paragraph No: 5 Product Information Security Risk Assessment

Comment: The risk assessment doesn't seem to consider supply chain or an interconnected operational environment. Should this be based on an "untrusted unsecure" operational environment in (a)(i).

Justification: By basing an assessment on the worst case, an open untrusted uncontrolled environment can ensure cyber security controls at a product level. The risk assessment seems focused on an individual product or item, if through the assessment it's determined that mitigating controls (i.e. segmentation in a secure controlled environment) are required then these can be implemented. By determining a single operational environment as part of the assessment, this means that future use in other contexts or changes to the operational environment either also need to be considered frequently (which isn't clear from the text) or set to a static determination.

response

Noted
Supply chain will be addressed in Part-AISS.

comment *150* comment by: *UK CAA*

Page No: 13

Paragraph No: AMC Text Section 5, Paragraph (a)(v) and (a)(vi)

Comment:

These are essential elements of the proposed analysis, but they will require an interface with the safety analyses performed at the system and aircraft level. The safety assessments are ongoing tasks that evolve during the process of certification/approval. We suggest that additional guidance on how to manage the interface with the various safety assessment would be helpful.

Justification:
It is important for the results of the PISRA to be properly accounted for in safety assessments related to the same product/part.

Proposed Text:
None provided as the development of this guidance is likely to be the subject of additional, harmonised, requirements/guidance.

response **Noted**
The guidance mentioned is already contained in ED-203A.

comment *151* comment by: *UK CAA*

Page No: 13

Paragraph No: 3.1.8, AMC 20-42 Section 7

Comment: The term "reasonably high potential" needs to be defined.

Justification: The lack of a proper definition could lead to under reporting.

Proposed Text: The term "reasonably high potential" should be replaced with "CS xx.1309 unacceptable risk".

response **Partially accepted**

comment *152* comment by: *UK CAA*

Page No: 13

Paragraph No: 7. Reporting

Comment: It is unclear why 'reporting of IUEI' is not a "must"?

Justification: If there is a high potential for an unsafe condition we believe that this would be a "must" report to both designer and to competent authority. It would be helpful if the "timely manner" could also be further defined, unless all organisations would be encompassed in the reg identified.

Proposed Text: "must report it to the competent authority within X days or X hours of identification".

response **Not accepted**
This document is an AMC.

comment *153* comment by: *UK CAA*

Page No: 13

Paragraph No: 8. Validation and verification of the security protection

Comment: It is unclear whether full penetration testing of a product is expected and assurance that there is no dissonance between products. Is it intended that each product be tested? Is it envisaged that security testing includes all mitigations at both operating environment as well as at product level? Means and mechanisms for testing will vary depending on the controls and mitigations, we suggest that this should be broader to account for this and future changes and advancements in cyber security testing. We also believe that the word "efficiency" should probably be "effective".

Justification:
Consistency in terminology. In addition, it would be helpful if, further detail could be provided to clarify what "security testing" may be required particularly where that is from the perspective of a potential adversary.

Proposed Text:
a) If cyber security risks that are identified during the product cyber security risk assessment (PCSRA) need to be mitigated, cyber security verification should be mused to evaluate the effectiveness of the mitigation means.
i) This cyber security verification may be performed by a combination of methods (for example, analysis, testing, inspections, reviews) dependent on the mitigation means and should consider the perspective of a potential adversary.

response **Not accepted and i) Not accepted**
Analysis, robustness testing and inspections do not need to be addressed from the perspective of a potential adversary. They can be done against coding rules, etc.

comment *154* comment by: *UK CAA*

Page No: 14

Paragraph No: AMC text section 9 final paragraph

Comment:

The contrasting example using CS 25 and CS 29 may be contentious as it infers that a lower level of security would be acceptable for CS 29 aircraft. It might be helpful to use a different and less potentially contentious example.

Justification:

The use of a contentious example is likely to detract from the point that is being made.

Proposed Text:
We suggest that an example based on functional context is used rather than type context.

response **Noted**

comment *155* comment by: *UK CAA*

Page No: 14

Paragraph No: 3.1.8, AMC 20-42 Section 9

Comment: It is not clear how an applicant could assess the probability of a threat given that it is intentional and unauthorised. In CS 25.1309, there is a maximum acceptable frequency for major safety effects.

Justification: The lack of guidance could lead to inconsistency in application and/or unsafe outcomes.

Proposed Text: We recommend that some guidance is provided/referenced on how threat probability should be estimated.

response **Noted**
Guidance can be found in the referenced standards.

comment *156* comment by: *UK CAA*

Page No: 14

Paragraph No: 9, 4th paragraph "the applicant should also assess the impact of new threats"

Comment: It is not clear how this will this be done actively. It is not understood why this does not require a new detailed PISRA. It is unclear whether operators are to be given the detail of the PSIRA or told when it was completed so they can identify frequency of update.

Justification: There may be concerns in sharing the full PISRA with the operators, but the operator should have a means to understand how frequently these have been assessed and what types of threats and new vulnerabilities have been considered as part of the assessment. Otherwise operators may assume this is happening and there isn't anything new, so they haven't been told, similarly applicants may decide to do this at unacceptable intervals i.e. once every 5 years or 10 years.

Proposed Text: "the applicant should also assess the impact of new threats or vulnerabilities and notify the operators that this assessment has occurred. If the assessment identifies an unacceptable threat condition, the applicant must notify the operators of the need and means to mitigate the new risk within X timeframe".

response **Partially accepted**

comment *157* comment by: *UK CAA*

Page No: 14

Paragraph No: 9, 2nd paragraph "from a violation of the system and information security rules"

Comment: It is not clear whether these are rules or instructions or guidance.

Justification: It is unclear whether these can be substituted by perceived comparable mitigations or amended by the operator.

Proposed Text: "from a violation of the instructions to maintain the necessary cyber security controls required for safe operation"

response **Not accepted**
It is not only about a violation of the instructions to maintain the necessary cybersecurity controls, but from any IUEI.

comment *158* comment by: *UK CAA*

Page No: 14

Paragraph No: 3.1.8 Section 10

Comment: A more comprehensive set of definitions would be helpful. In addition, this section introduces terms that are themselves unclear, e.g. "UDP port" and "certified topology".

Justification: Clear and comprehensive definitions are required in order to ensure consistency.

Proposed Text: Improve/expand definitions section.

response **Noted**

comment *171* comment by: *Embraer S.A.*

Embraer suggests clarifying the meaning of information systems read in section 4(a) and clarify that the proposed AMC applies for approval of products and parts of information systems that are subject to potential information security threats and that could result in unacceptable safety risks. Furthermore, to change the last bullet to indicate that systems with internal or external interfaces that provides connectivity that creates an entry point or attack path to other systems.

This change to section 2 (applicability) is being proposed in order to clarify the text of section 4(a) (general principles). In section 4(a), it is read that:

*"The **information systems** identified in Section 2 should be assessed against potential security threats that could result in unacceptable safety risks."*

However, if one reads section 2, one may have some trouble on identifying the aforementioned "information systems", since such section is read as:

"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."*

"Information systems" are only mentioned in the last bullet of section 2. However said bullet seems to apply to all previous bullets, since the proposed AMC, for instance, does not apply to any change to a product, but to those changes in which information systems are subject to potential information security threats that could result in unacceptable safety risks.

Furthermore, we consider that is necessary to clarify the about the applicability listed in the last bullet. The risk acceptance is only defined after the application of the security risk assessment process. Even in case of a modification, the risk acceptability can change as a result of the modification or the security environment as pointed by ED-203A. Thus, we propose to change the text of the proposed last bullet to indicate that systems with internal or external interfaces that provides connectivity that creates an entry point or attack path to other systems.

Therefore, it is proposed to rewrite section 2 to reflect the aforementioned points.

To change the text from:

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.

To:

This AMC applies to the approval of products, parts, equipment and service related to information systems which interfaces (external or internal) that are subject to potential information security threats, creating an entry point or attack path to other

systems. Those approved products' and part's 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.~~

response

Not accepted
Analysis is the prerequisite, and this cannot be considered as a given at this stage.

comment

172 comment by: *Embraer S.A.*

Embraer suggests to provide an example of other systems or equipment that provide air service information.

To make the text clearly by providing an example of other systems or equipment that provide air service information.

To change the text from:

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

To:

[...]
— the certification of other systems or equipment that provide air service information whose certification is required by a national regulation (e.g.: XM weather);
[...]

response

Not accepted

comment

173 comment by: *Embraer S.A.*

Embraer believes that this section doesn't provide guidance how to deal with products certified using previous versions of ED/DO documents.

Previous products may be certified using DO-326/ED-202, DO-356 and ED-203 with different activities and criteria from those present in DO-326A/ED-202A and DO-356A/ED-203A.

To include a new item:

1. Purpose

[…]

(d) Credit for products developed using previous versions of ED/DO documents shall be negotiated and accepted by EASA.

[…]

response **Partially accepted**

comment *174* comment by: *Embraer S.A.*

The present text will produce an extensive list of assets that should be excluded from security risk assessment demanding a long time to list and analyze.

During the development of ED-203A/DO-356A section 3.1.1, the committee agreed that to list all assets would be exhaustive and unnecessary since some of them could not be exposed to threats, only assets exposed by products interfaces along the attack path should be listed and assessed.

To change the text from:

(a) The general product information security risk assessment (PISRA) should cover the following aspects:
[...]
(ii) identification of the assets;
[...]

To:

(a) The general product information security risk assessment (PISRA) should cover the following aspects:
[...]
(ii) Identification of the exposed assets;
[...]

response **Not accepted**
The purpose is to identify what is of value.

comment *175* comment by: *Embraer S.A.*

The term “item” may have different interpretations and this can be misleading.

The term “item” is defined by ER-13 as “A hardware or software element having bounded and well-defined interfaces.” This can be understood as the lowest level of the product’s architecture while the consequence can exist in higher level so Embraer understand that the objective is to assess the consequence to the affected asset.

To change the text from:

[...]

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

[...]

To:

[...]

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

[...]

response **Accepted**

comment *176* comment by: *Embraer S.A.*

In section 7. Reporting, the current text will overload the DAH with reports that are not safety related.

As the concern is about security events with safety impact, the operator should follow the instructions present in the product manuals about the security events that should be reported.

Furthermore, we consider that the terminology used in the text differs from DO/ED documents.

ED-204 and ER-13 define “security event” instead of “information security occurrences“ and this text allows two possible interpretations for an aircraft operator in case of an occurrence:
1) it shall contact the aircraft supplier or
2) it shall contact the system supplier.

To change the text from:

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.

To:

The operator of a product or part should report ~~any information security occurrences to the designer~~ security event to the DAH, following the instructions provided in manual 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~~ DAH 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.

response **Not accepted**
It is about occurrence reporting according to Regulation (EU) No 376/2014[6].

comment *177* comment by: *Embraer S.A.*

Embraer suggest to reference EUROCAE documents to help applicants to understand the definitions.

The use of EUROCAE and RTCA terminology should be prioritized and co-related to other regulations as necessary to guide the applicant.

To change the text from:

[…]

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. […]

To:

[…]

~~According to Article 2(7) of Regulation (EU) No 376/2014, an occurrence is defined~~ ED-204 and ER-13 define security incident similarly to Article 2(7) of Regulation (EU) No 376/2014 defines an occurrence 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. […]

response **Not accepted**
It is about occurrence reporting according to Regulation (EU) No 376/2014[7].

6 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1579096167575&uri=CELEX:32014R0376
7 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1579096167575&uri=CELEX:32014R0376

comment	*178* comment by: *Embraer S.A.* If the intent is to promote a periodic assessment during the product or part life cycle, it is necessary to provide some guidance about the acceptable interval. Currently the frequency of re-assessment is negotiated case-by-case and this document could provide guidance about this. To change the text from: *[…]* *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. […]* To: *[…]* *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 in a period of time agreed by EASA. […]*
response	**Not accepted** EASA does not wish to agree on a fixed period of time for the regular evaluation of risks. This can be driven by vulnerability management.

comment	*194* comment by: *Lufthansa* **4. General principles (a)** Change & Add last paragraph: It is an assessment of the information security of the systems of a product or part. It must be extended to systems connected to the product or part in question if new information security risks may be introduced. Rationale: Assessments cannot be focused on just a specific system but must be considered in realtion to "system of systems". A change in one system may introduce new risks to other systems it is connected with. Thus, the interfaces and connected systems must be considered in an assessment as well.
response	**Not accepted** Although agreed in principle, the methodology requires to define first the security environment, which includes connected systems, but for which the OEM has no control (e.g. signal in space).

comment	*195* comment by: *Lufthansa* **4. General principles (c)** Add: The mitigation must be provided to the operators in a timely manner.

	Rationale: To reduce risks, a mitigation must be provided to the operators in a timely manner.
response	**Partially accepted**

comment	*196* comment by: *Lufthansa*
	4. General principles (b) Replace: "any known" with "any potential" Rationale: Threats that are not known / available today may become relevant in future. Thus, also potential risks should be considered as the threat landscape may change or new exploits for vulnerabilities may become available.
response	**Partially accepted**

comment	*197* comment by: *Lufthansa*
	4. General principles (b) Add: Identified vulnerabilities that are not mitigated must be communicated to the operator. Rationale: Operators are ultimatively responsible for the safety. Operators have the view on the whole system and can assess the overall risk. Furthermore, they need to be able to decide whether they accept the risks introduced by the vulnerabilities.
response	**Not accepted** Vulnerability is not mitigated when the assessment shows the risk is acceptable. Operators may require this information from the OEM but it is outside the scope of type certification.

comment	*198* comment by: *Lufthansa*
	5. Product information security risk assessment (a)(v) Comment: In calculation of the probability of an attack, it should not be assumed, that the attacker has to be onboard the aircraft and risks his own live with a crash, because he could also hack in via the satcom or via a trojanized laptop connected to the IFE using the onboard internet connection.
response	**Noted**

comment	*199* comment by: *Lufthansa*
	5. Product information security risk assessment (a)(vi)(B) Add: ...mitigation means as in section 8 with respect to the severity of the threat. Rationale: Ensure that seurity testing and a penentration test is conducted as part of the evaluation
response	**Accepted**

comment	*200* comment by: *Lufthansa* **5. Product information security risk assessment New (c)** Add: (c) Operators should be allowed to read the PSIRA documentation. Rationale: The operators are responsible for the safety of their passengers and crews. Thus, they should have transparency over the scope of the risk assessment, the identified risks, the basis for the risk severity rating and the mitigation means. This would enable operators to evaluate whether potential risks are within their risk appetite or if they may want to be more caucious and introduce further mitigation measures.
response	**Not accepted** Operators should enter into an agreement with the manufacturer, if they want to have access to the PISRA.

comment	*201* comment by: *Lufthansa* Comment: 6. is missing between 5. Product information security risk assessment and 7. Reporting
response	**Noted** Changes have been made, based on other comments.

comment	*202* comment by: *Lufthansa* **7. Reporting** Add: "report it to the competent authority and the operators of this product or part in a timely manner" Rationale: The operator should be put in the position to evaluate the risk for their operations independantly. This would allow the operator to decide about mitigating measures or even a grounding of an aircraft even if the competent authority did not order it as a mandatory measure yet.
response	**Not accepted** See Article 4 of Regulation (EU) No 376/2014[8]. It refers only to the competent authority.

comment	*203* comment by: *Lufthansa* **8. Validation and verification of the security protection (a)** Add: Regardless of the PSIRA result, security verification must be conducted for products or parts which can cause a catastrophic failure condition. Rationale: The typical lifecycle of an aircraft from design to its end of life is about 40 years. It's practically impossible to evaluate attack paths and the difficulty of performing a successful attack this far in the future (remember, 40 years ago the was no Internet, buffer overflows, WiFi, CERT, side channel attacks, …). To get sufficient

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1579096167575&uri=CELEX:32014R0376

defense in depth, the most safety critical systems should always be tested to vulnerabilities.

response **Not accepted**
It is not possible to foresee 40 years of potential security threats. This will be part of the continued airworthiness activities.

comment *204* comment by: *Lufthansa*

8. Validation and verification of the security protection New (b); New (c); New (d)

Add: (b) Security testing that addresses information security from the perspective of a potential adversary must be conducted by an independant body during the design and continously during the lifecycle of a part or product. The scope of such tests must not be limited to the initial attack surface available to an attacker but should test systems behind the perimeter as well to ensure that the defense in depth is approbriate.

(c) Reports of security testing including the scope of the testing and identified open vulnerabilities must be made available to the competent authority and the operators of the product.

(d) The applicant must grant the operator a right to audit the security measures and the conuducted security testing. This will include the provision of software and firmware versions and configurations used (e.g., Firewall rules) as well as information on security architecture, processes and policies (e.g., secure development methodologies).

Rationale: Penetration testing should always be conducted to verify the security protection. Furthermore, such tests should be done continously to adapt for new threats and attack measures. Penetration testing is an important measure to detect otherwise undetected flaws, vulnerabilities and weaknesses in systems.
The operators are resposible for the security of their passengers and crews. Thus, they must be empowered to verify the security measures taken. This includes sharing of security measures, test results, configurations. This will allow operators to do their risk assessments and decide if additional measures are required and how they react on possible unclosed vulnerabilities. Propietary source codes do not have to be shared with operators.

response **(d) Not accepted**
Operators should enter into an agreement with the manufacturer, if they want to have access to this information.

comment *205* comment by: *Lufthansa*

9. Instructions for continued product and part information security protection

Add: The applicant should provide information of the part's or product's security measures and security architecture to the operator to enable the operator conducting security testing that addresses information security from the

perspective of a potential adversary. The applicant should provide the operator with procedures to ensure that the part or product can be reset in a state that is in acordance with its specifications after security testing.

Rationale: Operators are ultimatively responsible for the safety. Operators have the view on the whole system and can assess the overall risk. Furthermore, they need to be able to decide whether they accept the risks introduced by the vulnerabilities.

response **Not accepted**
It is not within the scope of the regulation. This kind of agreement should be concluded between the operator and the OEM.

comment *206* comment by: *Lufthansa*

Attachment #1

We provided several comments (comments #194 to #205) regarding information on security architecture, sharing of risk information, procedures and requirements for penetration testing. The attached file provides further reasoning for our prior comments.

response **Noted**

comment *209* comment by: *L. Riegle AIA*

3.1.8

Commented text
"[…] will not be acceptable if the probability that the associated threat scenario is successfully exploited is too high."

Proposed modification
Change probability to likelihood or level of threat

Justification
While probabilities are used in safety to great effect, the use of probabilities for security have been discussed at length in industry forums to generate the standards proposed as AMC to the new rules. For security, there is no objective means, e.g. handbook or testing, that can be agreed upon to calculate a probability of attack and/or success of an attack. For safety, this would be reliability handbooks, stress calculations and various types of testing. For safety, the failure rate and failure means is a function of design and manufacture and remains static throughout lifetime while design and manufacture are unchanged. For security, the probability of attacks and success will change during lifetime of a design as intention to attack will be influenced by geopolitical and criminal considerations and the means to attack will change as technologies and know-how improve. Thus the goal of the standards was to define a process that is not impacted by an uncertain probability of attack and instead focuses on putting appropriate security measures for threat consequences in place and to monitor the effectiveness of security measures as part of continuing airworthiness - updating security measures when needed if attack means are found

to overcome the security measures or vulnerabilities are found posing a risk to the aircraft.

Commented text
"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."

Proposed Modification
Provide EASA's criteria for acceptability of risk for each Part, e.g. . why Part 23 only applies security to Catastrophic or Hazardous Threat Conditions but not lower severity TCs and why Part 25 applies to all TCs. This would be the same rationale as for safety in e.g. AMC 25.1309 where EASA describes setting numerical target levels in regulation based on consumer acceptability of historic accident rates.
Provided there is a rationale for different levels of acceptance for different classes of aircraft, provide matrix in AMC 20-42 that maps out the acceptability criteria for each design Part as it overrules Table 2-2 of ED-203A that is called by AMC 20-42.

Justification
Section 3.1.1 states in GM 23.2500(b) proposed text that only conditions more severe than major (i.e. Catastrophic or Hazardous) are to be considered - major or minor are excluded. The provided rationale does explain why.
Section 3.1.2 states that all adverse effects need to be considered which would be the whole range of Minor to Catastrophic. This could be considered to be going beyond Table 2-2 of ED-203A which considers minor threats to be acceptable for all levels of threat.
Section 3.1.3 states that only catastrophic or hazardous/severe major threats need to be considered, implying that major or minor are excluded. There is no provided rationale
Section 3.1.4 states that only catastrophic or hazardous/severe major threats need to be considered, implying that major or minor are excluded.
Section 3.1.5 states that all adverse effects need to be considered which would be the whole range of Minor to Catastrophic. This could be considered to be going beyond Table 2-2 of ED-203A which considers minor threats to be acceptable for all levels of threat.
Section 3.1.6 states that all adverse effects need to be considered which would be the whole range of Minor to Catastrophic. This could be considered to be going beyond Table 2-2 of ED-203A which considers minor threats to be acceptable for all levels of threat.

Commented text
"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."

Proposed Modification
Narrow the scope to "[...] have no identifiable vulnerabilities based on accepted

methods, or those vulnerabilities cannot be expected to be exploited due to lack of accessibility or protection inside design [...]" or indicate that this is adequately addressed by the standard in the AMC (ED203A) by modifying the final part of the sentence to "[...] certification specification and the acceptable means of compliance including industry standards [...]"

Justification
The statement here appears very broad and compliance can be hard to show. It is the industry position that the standard offered for use as an Acceptable Means of Compliance (ED203A) will provide the means to show the reasonable and appropriate means for identifying vulnerabilities (and accepting those that could not/have not been identified) as well as demonstrating exploitability of identified vulnerabilities to the satisfaction that risks are acceptable.

Commented text
"[…] failure condition […]"

Proposed modification
Change to threat condition
Is the use of "failure condition" language intentional and to tie security and safety process together?
If yes, add a separate paragraph that explains that the two processes should interact (see also ED202A) rather than using terms that can be ambiguous and this intent is lost.

Justification
The use of terminology of failure condition is related to safety effects - unintentional defects such as random failures or wear out. For intentional effects, also described as IUEI, the use of threat condition should be used.

Commented text
"potentiality"

Proposed Modification
"likelihood" or "possibility"

Justification
Use of term potentiality is unusual and not used anywhere else in industry

Commented text
"assessed against potential security threats"

Proposed Modification
Modify to "assessment against IEUI" or "assessment against information security threats"

Justification
Security threats can be ambiguous and be misunderstood to be all types of security threats including hijacking and other (physical) unlawful interference. The intent of the AMC is dealing with cybersecurity or information security threats as encapsulated within the definition of IEUI.

Commented text
"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."

Proposed Modification
"Acceptable/Unacceptable Risk: whether a risk is unacceptable depends on the certification specifications of the product or the affected part. The risk may be acceptable in some cases and unacceptable in others."

Rationale
The text can be ambiguous and misinterpreted by organisations. The aim of developing ED203A was to establish common approach and framework for security to replace the inconsistent approaches due to individual negotation of CRIs by applicants. This first statement may lead organizations to believe they are able to use their own risk acceptability matrix contrary (and less strict) than the ones agreed in ED203A.

Commented text
"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."

Proposed Modification
Suggestion is to rewrite the paragraph as:
"The result of this assessment, after any necessary mitigation measures have been identified, should be that the systems of the product or part have no identifiable vulnerabilities that can 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."

Rationale
Once systems are connected there will always be a level of vulnerability in the system.

Commented text
"determination of the operational environment for the information security of the product"

Proposed Modification
Suggest changing it to:
determination of the operational environment of the product;

Rational
The product when being developed will have a DAL and a SAL assigned which will be

based on assessment of safety consequences. Further the term "information security" could be considered as a limited in scope.

response

Comment 1: Partially accepted

Comment 2: Noted. This point is considered with other similar comments received.

Comment 3: Accepted

Comment 4: Accepted

Comment 5: Partially accepted

Comment 6: Partially accepted

Comment 7: Not accepted. The purpose of the text is to ensure safety continuum.

Comment 8: Not accepted. The initial text is already limited to only identifiable vulnerabilities that can be exploited.

Comment 9: Partially accepted

comment *219* comment by: *General Aviation Manufacturers Association / Hennig*

The proposed AMC 20-42 is applied as a means of compliance for all aircraft types (*i.e.*, 23, 25, 27, 29). The proposed AMC recognizes the joint EUROCAE/RTCA documents developed by aviation stakeholders over the past decade, including ED-202A/DO-326A, ED-203A/DO-356A, and ED-204/DO-355. These industry standards are suitable for certain applications, such as new type designs, and certain organisation, such as CS-25 aeroplane manufacturers, but less suitable for legacy aircraft and non-CS-25 aeroplanes.

It is also important to recognize that manufacturers have used a number of different processes and standards to address cybersecurity risks over the last couple of decades. Some of those standards are more mature and industry has greater experience with them than with the EUROCAE/RTCA documents (*e.g.*, ISO, NIST/FIPS). Other standards are being developed to complement the EUROCAE/RTCA work products, but are tailored to certain segments of aviation (*e.g.*, ASTM).

GAMA requests that EASA enable applicants through AMC 20-42 to use standards other than the EUROCAE/RTCA documents. EASA should recognize the availability of more mature cybersecurity standards for use on CS-25 aeroplane projects. EASA also should recognize the need for a lighter approach for aeroplanes such as CS-23 aeroplanes, VFR-only aircraft, etc., to address cybersecurity risks in a proportional manner.

response

Noted
EASA does not prohibit the use of a particular standard, as long as it is found acceptable. Standards will be evaluated upon availability.

comment *224* comment by: *L. Riegle AIA*

Commented text
Product Information Security Risk Assessment

Proposed modification
Confirm that "PISRA" is term to use instead of PASRA/PSSRA/SSRA/ASRA and if yes, suggest new nomenclature for "Plan for Security Aspects of Certification Summary" to "Security Accomplishment Summary"

Justification
ED203A uses the terms (Preliminary) Aircraft Security Risk Assessment and (Preliminary) System Security Risk Assessment. Is it intentional by EASA to deviate from this nomenclature? If the intention by EASA is to modify ED203A nomenclature for preferred terms, it is suggested to find a new term for Plan for Security Aspects of Certification Summary as it is quite lengthy and does not harmonize well with equivalent titles from System/Software/Hardware development.

response **Noted**
Yes, it is intentional, because it is not only about aircraft systems.

comment *225* comment by: *General Aviation Manufacturers Association / Hennig*

The proposed AMC states that any mitigation requires validation and verification. However, an architecture put together intelligently will have many mitigations built into it.

When an applicant conducts a safety analysis of the aircraft architecture and determines that no hazardous or catastrophic hazards due to electronic security exist, the guidance could still be interpreted to still drive the applicant into testing of all mitigations to prove that they are no critical hazards when this is not the intent of the rule.

GAMA recommends that EASA provide a clarification whether validation and verification is required for aircraft architectures that have no hazardous or catastrophic hazards due to electronic connectivity.

response **Noted**
It is already addressed by 3.1.8 5(vi).

comment *228* comment by: *Bombardier*

Issue: Applicability for changed products is not well defined

Comment: Draft text of AMC 20-42, Applicability says that the AMC applies to "a change to a product". This should be specified to apply only to product changes where a Changed Product Rule determintation of Significant has been made, requiring the use of the current certification basis.

Recommend: Change text to "a change to a product resulting in the adoption of the latest certification basis, in accordance with GM 21.A.91 "Classification of changes to type certificate".

response **Not accepted**
This point is addressed in point 21.A.91. The AMC does not supersede Part 21.

comment *230* comment by: *The Boeing Company*

Page: *12*
Paragraph: *3.1.8, 2. Applicability*

THE PROPOSED TEXT STATES:
"…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;"

REQUESTED CHANGE:
*"…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). C**redit can be taken **for those** ~~from its~~ security **measures and their associated** ~~assurance level (SAL) during the installation of the ETSO article~~ **SALs in the context of an aircraft certification project** by the design organisation approval holder (DOAH), depending on the information system security risk assessment of the product;"*

JUSTIFICATION:
SAL is described in DO-356A/ED-203A section 4.4. SAL can be assigned to security measures and assets. Only SAL 0 is assigned to assets that are not security measures. Therefore, it is more correct to refer to SAL of security measures for the purpose of this paragraph.

response **Accepted**

comment *231* comment by: *Bombardier*

Issue: imprecise CS 25.1309 terminology

Comment: Draft Text for AMC 20-42, 9. states "[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." this is inconsistent with CS 25.1309 terminology

Recommend: Change text to "[A] threat condition that could result in a major failure condition, as defined in CS 25.1309...."

response **Partially accepted**

comment *233* comment by: *Bombardier*

Issue: PISRA use for in-service aircraft not well defined

Comment: PISRA process defined in Draft AMC 20-42 Section 5 is focused on new product certification

Recommend: Add guidance and/or examples on applicability of process to in-service aircraft

response **Noted**

comment *247* comment by: *Aerospace and Defence (ASD)*

Commented text
The necessity to have instructions will depend on the design solution and cannot be determined a priori.

Proposed modification
The text "Once the overall risk has been deemed to be acceptable, the applicant should develop instructions, as described in Section 9[…]" should be replaced by "Once the overall risk has been deemed to be acceptable, the applicant should develop instructions if necessary, to ensure that mitigations are effective as described in Section 9 […]".

response **Accepted**

comment *248* comment by: *Aerospace and Defence (ASD)*

Commented text
"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."

Proposed modification
Narrow the scope to "[...] certification specification and the acceptable means of compliance including industry standards [...]"

Justification
The statement here appears very broad and compliance can be hard to show. It is the industry position that the standard offered for use as an Acceptable Means of Compliance (ED203A) will provide the means to show the reasonable and appropriate means for identifying vulnerabilities (and accepting those that could not/have not been identified) as well as demonstrating exploitability of identified vulnerabilities to the satisfaction that risks are acceptable.

response **Accepted**

comment *249* comment by: *Aerospace and Defence (ASD)*

Commented text
N/A

Proposed modification
A new step (viii) must be added to take into account the updating of the PISRA as new security vulnerabilities are discovered or new threats emerge.

The applicant should also assess the impact of new threats and new discovered vulnerabilities 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.

Justification
Align aviation stakeholders means of compliance.

response **Not accepted**
It is covered by 3.1.8.9.

comment *250* comment by: *Aerospace and Defence (ASD)*

Commented text
Use of "item" is misleading because the threat may also be related to a function or system. "Asset" is already used in the preceding statements.

Proposed modification
Consider replacing "affected items" by "affected assets". "Asset" is defined ED 203.

Justification
Clarity.

response **Accepted**

comment *251* comment by: *Aerospace and Defence (ASD)*

Commented text
AMC 20-42, Section 3.1.8.5 (a) (v) - Procedural and technical security protection means are often already included in initial concept and design. These protections should be taken into account when determining the initial security risk, without requiring a second iteration of a PISRA.**Proposed modification**
"by considering the existing security protection means" should be added in the sentence (see next comment).

response **Accepted**

comment *252* comment by: *Aerospace and Defence (ASD)*

Commented text
"Potentiality of exploitation" and "difficulty of attack" are two redundant descriptions of the same kind of analysis that focuses on the attacker perspective.

But the protection perspective that evaluates existing protection means is missing and should be added.

Proposed modification
The text “evaluation of the potentiality of a successful exploit, or of the difficulty of performing a successful attack that would have an impact on safety” should be replaced by “evaluation, by considering the existing security protection means, of the level of threat that would have an impact on safety”.

Justification
The level of threat is that which is defined in ED 203 table 2.2.

response **Accepted**

comment *253* comment by: *Aerospace and Defence (ASD)*

Commented text
AMC 20-42, Section 3.1.8.5 (a) (vi) - Severity and potentiality to attack are two different matters and thus cannot be compared.If the risk table of 203A is used then you are comparing

Proposed modification
The text “determination of whether the risks, which are the result of comparing the severities with the potentiality to attack […]” should be replaced by “determination of whether the risks, which are the result of combination of the severities and the potentiality to attack […]”.

response **Accepted**

comment *254* comment by: *Aerospace and Defence (ASD)*

Commented text
AMC 20-42, Section 3.1.8.5 (b) - Is only paragraph 2.1.1 of ED-202A applicable, as read in section 3.1.8. 5. (b), even though other references of ED-202A are found in 3.1.8 1. (b) and (c)?

response **Noted**
Section 3.1.8.5.(b) refers to ED 202A Section 2.1.1 as guidance. It does not limit the applicability of ED 202A to that section. Therefore, there are more references, when necessary.

comment *255* comment by: *Aerospace and Defence (ASD)*

Commented text
Section 3.1.8 6 is missing.

response **Noted**
The text has been modified to consider other comments.

comment *256* comment by: *Aerospace and Defence (ASD)*

Commented text
AMC 20-42, Section 3.1.8.8 (a) - Efficiency (commonly defined as the relationship between obtained results and resourced engaged) is not relevant to determine whether the protection sufficiently mitigates the risk. But effectiveness (commonly defined as the relationship between obtained results and objectives) is.
Proposed modification
Consider replacing "efficiency of the mitigation means" by "effectiveness of the mitigation means".

Justification
ED 203 is defining "effectiveness".

response **Accepted**

comment *257* comment by: *Aerospace and Defence (ASD)*

Commented text
AMC 20-42, Section 3.1.8.9 - "operational security" is not what is expected here. "operational procedure" or "operational security procedures" would be more appropriate as the paragraph is dealing with instructions. Operational security is a term that's used in ED204 but tends to be used as "operational security measures".
Proposed modification
The text "for example, physical and operational security" should be replaced by "for example, physical and operational procedures".

response **Accepted**

comment *258* comment by: *Aerospace and Defence (ASD)*

Commented text
The PISRA is a continuous process, BUT this implies a single process, Security perimeter and boundary.

Proposed modification
This needs to be clarified.

response **Noted**

comment *259* comment by: *Aerospace and Defence (ASD)*

Commented text
Product Information Security Risk Assessment

Proposed modification
Confirm that "PISRA" is term to use instead of PASRA/PSSRA/SSRA/ASRA.

Justification
ED203A uses the terms (Preliminary) Aircraft Security Risk Assessment and (Preliminary) System Security Risk Assessment. Is it intentional by EASA to deviate from this nomenclature?

Applicable in multiple sections.

response **Noted**
Yes, it is intentional, because it is not only about aircraft systems.

comment *260* comment by: *Aerospace and Defence (ASD)*

Commented text
AMC 20-42 Section 3.1..8.7. - The term **reasonably** is unclear.

Proposed modification
Does EASA plan to quantify what this term means?

response **Noted**
The text has been changed.

comment *261* comment by: *Aerospace and Defence (ASD)*

Commented text
AMC 20-42, Section 3.1.8.5(a)(v) - "potentiality"

Proposed modification
"likelihood" or "possibility"

Justification
Use of term potentiality is unusual and not used anywhere else in industry.

response **Noted**
The text has been changed.

comment *262* comment by: *Aerospace and Defence (ASD)*

Commented text
Section 3.1.8, 5. Product information security risk assessment, (a) (vi) (B) - N/a

Proposed modification
"evaluation of the effectiveness of the mitigation means with respect to the level of risk (combination of level of threat and severity of Threat Condition)"

Justification

	Severity is not applicable to threat, but to Threat Condition.
response	**Accepted**

comment	*263* comment by: *Aerospace and Defence (ASD)* **Commented text** 13 Section 3.1.8, 7. Reporting - If you maintain sub-section 7 on "operator", then the operator should be informed about this obligation in appropriate regulations.
response	**Noted**

comment	*264* comment by: *Aerospace and Defence (ASD)* **Commented text** AMC 20-42, Section 3.1.8.9 - Probability is related to safety assessment that addresses a list of events from which act of sabotage is explicitly excluded. **Proposed modification** The text "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" should be replaced with "For example, a threat condition that has a potential major safety effect, as defined in CS 25.1309, will not be acceptable depending on the level of threat of the associated threat scenario."
response	**Accepted**

comment	*265* comment by: *Aerospace and Defence (ASD)* **Commented text** AMC 20-42, Section 3.1.8.9 - Probability is related to safety assessment that addresses a list of events from which act of sabotage is explicitly excluded. **Proposed modification** The text "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" should be replaced with "For example, a threat condition that has a potential major safety effect, as defined in CS 25.1309, will not be acceptable depending on the level of threat of the associated threat scenario."
response	**Accepted**

comment	*266* comment by: *Aerospace and Defence (ASD)* **Commented text** AMC20-42 10 Definitions – should refer to the current version of ER-13 or be able to use the latest version of ER-13 as it evolves. **Proposed modification** EASA must confirm whether a latest revision of ER-13 can be used for AMC as EASA is a part of EUROCAE, so it could be acceptable to use an evolving document.

	Otherwise a clearly indicated specific revision of ER-13 should be used or the relevant definitions from ER-13 should be copied into the AMC.
response	**Noted**

comment	*274* comment by: *IATA* "The information systems identified in Section 2 should be assessed against..." IATA Comment: Change: "in Section 2 **should continously be assessed against"** Reason: Cyber threats, vulnerabilities and risks are always changing. Thus, a continous / regular assessment / reassessment is required.
response	**Not accepted** This is part of the instructions for continued product and part information security protection (Section 3.1.8.9). It can be continuously, periodically or vulnerability driven (vulnerability management).

comment	*275* comment by: *IATA* (a) ..... "It is an assessment of the information security....." IATA Comment: Change & Add: It is an assessment of the information security of the systems of a product or part. It should be extended to systems connected to the product or part in question if new information security risks may be introduced. Reason: Assessments cannot be focused on just a specific system but must be considered in realtion to "system of systems". A change in one system may introduce new risks to other systems it is connected with. Thus, the interfaces and connected systems must be considered in an assessment as well.
response	**Not accepted** Although agreed in principle, the methodology requires to define the security environment first, which includes connected systems, but for which the OEM has no control (e.g. signal in space).

comment	*276* comment by: *IATA* "....cannot be exploited by any known security threat...." Replace: known with potential Reason: Threats that are not known / available today may become relevant in future. Thus, also potential risks should be considered as the threat landscape may change or new exploits for vulnerabilities may become available.
response	**Not accepted**

	The result of the assessment can be only about known threats. It would be impossible to cover all potential threats.
comment	*277* comment by: *IATA* At the end of 4 - para (b) "……of the product or part considered". Add: "Identified vulnerabilities that are not mitigated should be communicated to the operator." Rationale: Operators are ultimatively responsible for the safety. Operators have the view on the whole system and can assess the overall risk. Furthermore, they need to be able to decide whether they accept the risks introduced by the vulnerabilities. Operators may also be able to add mitigations/countermeasures not considered, or deemed practicable by the manufacturer. Additionally, the risk scenario's considered by the assessor should be passed on to downstream consumers, eg. manufacturer to operator.
response	**Not accepted** Vulnerability is not mitigated when the assessment shows the risk is acceptable. Operators may require this information from the OEM but it is outside the scope of type certification.
comment	*278* comment by: *IATA* 4. para (c) - at the end of the paragraph. Add: "The mitigation should be provided to the operators in a timely manner." Reason: To reduce risks, a mitigation should be provided to the operators in a timely manner. Given the everchanging threat landscape, aircraft systems and their software components should be designed and built to enable timely implementation of mitigations.
response	**Accepted**
comment	*279* comment by: *IATA* 5. (a) (v) Comment: In calculation of the probability of an attack, it should not be assumed, that the attacker has to be onboard the aircraft and risks his own live with a crash, because he could also hack in via the satcom or via a trojanized laptop connected to the IFE using the onboard internet connection.
response	**Noted**
comment	*280* comment by: *IATA* 5. (a) (vi) (B)

	Add: ...mitigation means as in section 8 ... Reason: Ensure that seurity testing and a penentration test is conducted as part of the evaluation
response	**Accepted**

comment	*281* comment by: *IATA* 5. Add at the end of the section Add: (c) Operators should be allowed to read the PSIRA documentation. Rationale: The operators are responsible for the safety of their passengers and crews. Thus, they should have transparency over the scope of the risk assessment, the identified risks, the basis for the risk severity rating and the mitigation means. This would enable operators to evaluate whether potential risks are within their risk appetite or if they may want to be more caucious and introduce further mitigation measures.
response	**Not accepted** Operators should enter into an agreement with the manufacturer, if they want to have access to the PISRA.

comment	*282* comment by: *IATA* 7. "...should report it to the competent authority...." Add: "the competent authority and the operators of this product or part" Reason: The operator should be put in the position to evaluate the risk for their operations independantly. This would allow the operator to decide about mitigating measures or even a grounding of an aircraft even if the competent authority did not order it as a mandatory measure yet.
response	**Not accepted** According to Regulation (EU) No 376/2014[9], mandatory reporting is only for the competent authority.

comment	*283* comment by: *IATA* 8. (a) Add: Regardless of the PSIRA result, security verification must be conducted for products or parts which can cause a catastrophic failure condition.

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1579096167575&uri=CELEX:32014R0376

	Rationale: The typical lifecycle of an aircraft from design to its end of life is about 40 years. It's practically impossible to evaluate attack paths and the difficulty of performing a successful attack this far in the future (remember, 40 years ago the was no Internet, buffer overflows, Wifi, CERT, side channel attacks, …). To get sufficient defense in depth, the most safety critical systems should always be tested to vulnerabilities.
response	**Not accepted**

comment	*284* comment by: *IATA* 8 (a) (i) Replace: "should" instead of "may"
response	**Accepted**

comment	*285* comment by: *IATA* Section 8 After (a) Add: (b) Security testing that addresses information security from the perspective of a potential adversary must be conducted by an independant body during the design and continously during the lifecycle of a part or product. The scope of such tests must not be limited to the initial attack surface available to an attacker but should test systems behind the perimeter as well to ensure that the defense in depth is approbriate. (c) Reports of security testing including the scope of the testing and identified open vulnerabilities must be made available to the competent authority and the operators of the product. (d) The applicant must grant the operator a right to audit the security measures and the conuducted security testing. This will include the provision of software and firmware versions and configurations used (e.g., Firewall rules) as well as information on security architecture, processes and policies (e.g., secure development methodologies). Reason: Penetration testing should always be conducted to verify the security protection. Furthermore, such tests should be done continously to adapt for new threats and attack measures. Penetration testing is an important measure to detect otherwise undetected flaws, vulnerabilities and weaknesses in systems. The operators are resposible for the security of their passengers and crews. Thus, they must be empowered to verify the security measures taken. This includes sharing of security measures, test results, configurations. This will allow operators to do their risk assessments and decide if additional measures are required and how they react on possible unclosed vulnerabilities.Propietary source codes do not have to be shared with operators.

response **Not accepted**
The exchange of such information needs to be part of an agreement to be concluded between the operator and the OEM.

comment *286* comment by: *IATA*

Section 9. Instructions....

Page 14 before sentence - Guidance on continued.....

Add: The applicant should provide information of the part's or product's security measures and security architecture to the operator to enable the operator conducting security testing that addresses information security from the perspective of a potential adversary. The applicant should provide the operator with procedures to ensure that the part or product can be reset in a state that is in acordance with its specifications after security testing.

Reason: Rationale: Operators are ultimatively responsible for the safety. Operators have the view on the whole system and can assess the overall risk. Furthermore, they need to be able to decide whether they accept the risks introduced by the vulnerabilities.

response **Not accepted**
This kind of agreement is to be concluded between the operator and the OEM.

comment *290* comment by: *IATA*

1.(b)

Should references to specific and dated documents be made, or preferably to a document and its revisions. Especially since these documents are in review. Propose automatic grandfathering. eg. applies 2yrs after revision date

response **Noted**
The practice is to reference the latest applicable standard.

comment *291* comment by: *IATA*

4.
...
(d)

as noted earlier, context for the instructions should be documented and supplied.

response **Noted**

comment *292* comment by: *IATA*

5. (a)
...
(vi) - Assumptions made about the operational environment need to be made clear

response	**Noted**

comment	*293* comment by: *IATA* 7. Reporting Perhaps more definition is required here. "Any information security occurrences" is ambiguous and could lead to under or over reporting of events and incidents.
response	**Noted**

3. Proposed amendments and rationale in detail | 3.1. Draft certification specifications (Draft EASA decision) | 3.1.9. Draft decision amending Appendix A to GM 21.A.91 'Classification of changes to type certificate' p. 14-15

comment	*4* comment by: *Luftfahrt-Bundesamt* "Examples of modifications that may be classified as major...:" The introduction or modification of authentication and/or encryption methods could be added in this list of examples.
response	**Accepted** The proposal is also extended to security controls.

comment	*15* comment by: *Pratt@Whitney Rzeszow APUs* Instead of: CS 25.1319, CS 27.1319, CS 29.1319, CS-E 50(i), CS-P 230(g) Should be: CS 25.1319, CS 27.1319, CS 29.1319, CS-E 50(i), CS-P 230(g), CS-APU 90
response	**Partially accepted** The text has been modified.

comment	*66* comment by: *European Cockpit Association* Proposal: [p.15] *"As an exception, new simplex digital communication means (e.g. ARINC 429) from a controlled domain to a more open domain is not considered as major modification if it has been assessed, evaluated and proven that the simplex control cannot be reversed by any known UIEI".* Rationale: [p.15] It is proposed that new simplex links (e.g. ARINC 429) are not considered as major changes unless "it can be shown that the simplex control can be reversed". Recent attacks (see Cherokee Jeep attack, Charlie Miller et Chris Valasek, 2015) targeting logically defined simplex links have shown that it is possible, through firmware modifications for example, to reinstall dual links where simplex one were used and to enable write feature on segregated data bus As a consequence, the proof should be reversed and the possibility to reinstall dual link should be carefully taken

into account, assessed and analyzed. Thus, by default, new simplex links should also be considered as major modifications unless “it can be shown that the simplex control *cannot* be reversed”.

response **Partially accepted**

comment *85* comment by: *General Aviation Manufacturers Association / Hennig*

The NPA provides proposed guidance about how to classify design changes in an amendment to GM 21.A.91. How to handle design changes for existing products is an area that would benefit from continued engagement among EASA, other regulators, and industry stakeholders through cooperative efforts in support of this NPA being finalized.

Prior efforts have identified certain considerations. As an example, FAA policy PS-AIR-21.16-02 (as amended) discusses the need for a special condition when certain design changes involving connectivity occur. ED-203/DO-356, Airworthiness Security Methods and Considerations, contains one chapter about type design changes. ASISP section 2.2.4.2, Type Design Changes, provides a general discussion about STCs.

GAMA recommends that EASA engage with industry to advance the design change area for cybersecurity further, because the guidance and associated policy discussion is not mature as the following examples show:

- EASA states that certain design changes "may" be classified as "major" when certain changes occur. The word "may" could cause confusion and the agency, based on the defined changes listed in 3.1.9, likely intended to use the more affirmative "should" about the criteria (e.g., establishing connectivity between the ACD and the AISD).
- The agency states that a change should be considered "major" if the security environment is impacted. The use of the term "environment" is too broad and could be understood to mean changes to things outside the aircraft. Alternatively, is it intended that if there is no security environment change, then the new regulations would not be applied or would the new rules be applied because a non-security related change tripped the major change criteria? GAMA believes that the agency intended to refer to the aircraft's "security architecture" and not the security environment. A clarification of this criteria is needed.
- Additionally, with regards to the use of the term "security architecture" (sic: environment), it is important that EASA recognize that not all changes to the security architecture are "major" by default, but only changes that could weaken an existing security measure or introduces a new threat condition or attack vector.
- Finally, the "major" change definition does not address safety and generally infers that any security changes are deemed a major change to the system. In GAMA's view, this should not be true for hazards other than catastrophic and hazardous for rotorcraft and CS-23 aeroplanes.

GAMA recommends that EASA specifically work with industry to review and provide improved guidance about the type design change process as it finalizes the NPA for publication as an amendment to the different CSs.

response

Point 1: **Accepted**

Point 2 and point 3: **Partially accepted**

The text has been modified based on other similar comments.

Point 4: **Not accepted**

The appropriate definition appears in the respective CS.

comment *92* comment by: *Panasonic Avionics*

"PISD" should read "PIESD", per ARINC 811.

response **Accepted**

comment *115* comment by: *Dassault-Aviation*

Text:
P15 Section 3.1.9. Draft decision amending Appendix A to GM 21.A.91 'Classification of changes to type certificate':

Proposed text:
proposed text to replace first example:
- "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 (PIESD) (see ARINC 811). Except if a nominally unidirectional digital communication means (e.g. ARINC 429) is established that cannot be reversed."

Rationale:
- Stating an exception ("unless") in an exception is confusing.
- Simplex is not defined thus ambiguous

response **Noted**

comment *116* comment by: *Dassault-Aviation*

Text:
P14-15 Section 3.1.9. Draft decision amending Appendix A to GM 21.A.91 'Classification of changes to type certificate'

Proposed text:
The text "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." is proposed to be replaced by:
"A change that may introduce the potential for unauthorised electronic access to aircraft systems may be considered to be major if there is a need to mitigate the risks for an identified unsafe condition (CAT / HAZ)."

Rationale:

- Reference to CS 2x.1319 and CS-E 50(i), CS-P 230(g) should be removed because classification of a change should not depend on the applicable certification basis but rather on the nature of the change itself.
- The Security environment impact as a trigger condition should be removed because it is already addressed by the identification of the unauthorized electronic accesses. Moreover, the possible further updates of the security environment are considered as out of the scope of the initial airworthiness and already addressed by the Continued Airworthiness.
- The meaning of "initial analysis" and "before the implementation of mitigation means" should be clarified.

response **Partially accepted**

comment *121* comment by: *FOCA Switzerland*

Comment FOCA on Point 9 (Instructions for continued product and part information security protection):
See comment #122 on the need for legal links to ensure implementation of procedures by other actors in the chain to ensure resilience throughout the lifecycle.

Proposal FOCA on Point 9 (Instructions for continued product and part information security protection): :
Ensure legal link regarding implementation of measures throughout lifecycle exists and is broad enough. Reporting of occurrences should be covered by RMT 0.720 (and its links to Reg. 376/2014) and should not be included in this AMC. **Comment FOCA on GM 21.A.91 Classification of change:**
GM to Part 21 is not listed in material affected by this NPA and the part of the GM to Part 21 affected by cyse appear as much larger than the classification of change (e.g. ToA, privileges, disciplines). Moreover, the NPA does not differentiate between MAJOR or MINOR change so no need to discuss it in the frame of the NPA.

Proposal FOCA on GM 21.A.91 Classification of change:
Delete GM 21.A.91 Classification of change.

Comment FOCA on Amendment of Appendix A to GM 21.A.91 Point 4 (Systems):
The third line in the text refers only to "the initial analysis shows that before the implementation of mitigation means, there is potential for an unsafe condition". What about the analysis of potentially unsafe conditions after the implementation of cyber mitigation measures? Should this not be also part of the analysis? See also above comment #120 regarding Product information security risk assessment.

response Point 1: **Noted.** It is covered in Part-AISS.

Point 2: **Not accepted.** Part-AISS will be high level; therefore, it is included here to be more detailed for products. Additionally, it does not contradict Part-AISS.

Point3: **Noted.** It will be referenced on the first page of the publication.

Point 4 : **Not accepted**

Point 5: **Noted**

comment	*159* comment by: *UK CAA* **Page No:** 14 - 15 **Paragraph No:** 3.1.9 Appendix A **Comment:** This is the first reference to security domains. This is a well-recognised term and we suggest it should be added to the glossary and used throughout the document to explain a trust environment. A major change should be based on an assessment of any changes to security mitigations (of which establishing a security domain is a mitigation or control) or within a security domain where changes aren't between domains. This section seems quite detailed comparative to the rest of the text (e.g. listening on a UDP port). We suggest that it would be assumed that any domain which is not the controlled domain described by the applicant would need to be assessed to be at the same level or would automatically be a "less controlled security domain".
response	**Noted**

comment	*160* comment by: *UK CAA* **Page No:** 14 - 15 **Paragraph No:** 3.1.9 Appendix A **Comment:** Determination of a major change should require cyber security competency (to determine vulnerabilities, threat paths and complete the analysis) as well as safety competency to determine the potential for an unsafe condition. **Justification:** To determine if a change is major identification is required to establish f the security environment (or domain) is impacted and also if there is a potential unsafe condition. The competency requirements to make these determinations should be made clear. **Proposed Text:** We recommend that competency requirements are added.
response	**Noted** It is covered in Part-AISS.

comment	*164* comment by: *AIRBUS* **1. PAGE / PARAGRAPH / SECTION YTHE COMMENT IS RELATED TO:** Pages 14-15, section 3.1.9 ("Draft decision amending Appendix A to GM 21.A.91 'Classification of changes to type certificate") **2. PROPOSED TEXT / COMMENT :** The text " 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." is proposed to be replaced by :
"A change that may introduce the potential for unauthorised electronic access to product systems may be considered to be major if there is a need to mitigate the risks for an identified unsafe condition (CAT / HAZ)."

3. RATIONALE / REASON / JUSTIFICATION for the Comment:
Reference to CS 2x.1319 and CS-E 50(i), CS-P 230(g) should be removed because classification criteria minor/major defined in GM.21.A.91 do not refer to Certification Specifications and classification of a change should not depend on the applicable certification basis but rather on the nature of the change itself.
The Security environment impact as a trigger condition should be removed because it is already addressed either by the identification of the unauthorized electronic accesses or by §9 of AMC 20-42.
The meaning of "initial analysis" and "before the implementation of mitigation means" should be clarified.

response **Partially accepted**

comment *192* comment by: *John Connolly (Atkins)*

The incorrect term 'threat path' is used where, correctly, 'attack path' is used previously.

response **Accepted**

comment *208* comment by: *L. Riegle AIA*

3.1.9

Commented text
"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."

Proposed modification
Reword to state: "Exception: a nominally unidirectional directional communication means (e.g. ARINC 429) is established from a controlled domain to a more open domain and demonstration is provided that communication flow cannot be returned from the open domain by reversing the communication direction (e.g. through compromise of digital controller chips).

Justification
Use of simplex needs to be defined as it may be ambiguous to different users. Intention here should be that a unidirectional communication from controlled to uncontrolled domain is acceptable and can be added without need for classification as a major change. Any additional communication means that adds a path from uncontrolled to controlled domain - either intentionally or unintentionally - is a major change. The intentional path may be obvious to most in the industry (e.g. A664, ethernet, etc.) but unintentional consequences such as having a nominally unidirectional databus such as A429 compromised to change the direction of

communication needs to be explained so it is considered by all. Simplex is not defined in A429 or other standards.

Commented text
"[…] a change may be considered to be major if the security environment is impacted […]"

Proposed modification
Change to security architecture

Justification
Changes to security environment are out of control of an applicant and not related to any changes being proposed. Changes to security architecture are the scope of changes being proposed. Any adverse effects to security environment should be handled by continuing airworthiness processes - i.e. if a new attack type is identified, it should be handled over this route to ensure all related aircraft are secured as soon as possible. Otherwise, the current text provides the adverse incentive to not secure aircraft to avoid cost associated with a major change.

Commented text
"[…] a change may be considered to be major if the security environment is impacted […]"

Proposed modification
Amend 21.A.91 to add further guidance on how to interpret the "may" statement on when changes to the security architecture will be classified as major or when it can be reverted to minor. Insert after quoted sentence (assumes other comment on changing security environment to architecture has been accepted):
The changes to security architecture are only major if they have the potential for weakening existing security measures or introduce new threat conditions or attack vectors. When changes to the security architecture occur, the applicant should provide a risk assessment demonstrating that no undue risks are being introduced into the design. The applicant should use approved procedures for assessing security risks due to design changes and classify changes through procedures approved by compliance to 21.A.239 (Design assurance system) or 21.A.611 (Design Changes).
Add another example that a change can introduce a new interface but is not actually major because existing security measures can protect against it. Example could be: An engine has a satellite communication interface for transferring usage data. The applicant chooses to add (or replace with) a WIFI communication module for cheaper transmissions. The bidirectional data will be passed through the same security measures used for the satellite communication ensuring confidentiality, integrity and availability (as appropriate) are not impacted.

Justification
This NPA proposes to use "may" in a classification criteria rather than the usual practice of "should" for criteria in this section. This general approach is appreciated as it is not rigidly forcing all changes to be classified major, e.g. any time a new interface is introduced. However, this section needs to be clarified on the process and procedure of how the "may" is to be determined. It is recommended to include a security risk assessment process as part of the change classification process and approved as part of a company's approved manuals.

Commented text
N/A

Proposed modification
Amend Part 21 sections on continuing airworthiness to include considerations for security and to call AMC 20-42 as means for demonstrating compliance
Suitable sections need to be found for introducing passages for obligations set in ED204 (e.g. incident management, instructions for continued airworthiness). For these passages, AMC 20-42 should be provided as GM or AMC.
Sections to be targeted could be:
21.A.3A (Failures, malfunctions and defects) - include specific needs for security in occurrence reporting, identification of vulnerabilities in design and subsequent rectification
21.A.61 (Instructions for continued airworthiness), 21.A.107 (Instructions for continued airworthiness) and 21.A.120A (Instructions for continued airworthiness) - include Aircraft Security Operator Guidance although this may be sufficiently covered by ED203A in AMC 20-42
Note: As these changes may be quite extensive, do not have available material at this stage and have not been discussed with industry, it may not be possible to introduce at this stage. NPA 2019-03 introduces extensive changes to Part 21 that could be used as vehicle to make more extensive changes. Alternatively with imminent NPA for Part AISS, these issues could be covered via Part AISS updates. However, this may mean a gap in support and coverage of continuing airworthiness of parts and appliances until RMT 0720 is complete.

Justification
AMC 20-42 lists ED204 which provides guidance for continuing airworthiness. Part 21 includes regulations for continuing airworthiness that should drive the activities described in ED204. In current state, only initial airworthiness aspects to design are clear through updates to CS-23, -25, -27, -29, -E, -P and -ETSO. Organizations that need to perform continuing airworthiness activities - in particular MRO and Operators - will not be aware of AMC 20-42 and activities set forward in ED204 without correct references in relevant sections to their operations - mainly Part 21.

Commented text
"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 [...]"

Proposed Modification
Update GM 21.A.101 to clarify that security is an “area” under Step 6 of the workflow (i.e. compliance to 21.A.101(b)(2)) and thus changes to security – and consequently updates to the use of standards for establishing security compliance and compliance to other areas – should be considered independently.

Justification
There is concern that the addition of security into the classification of “minor/major” changes could have unintended, far-reaching and costly consequences. There is the concern that when security drives a classification of “major” – when it otherwise would be minor – that large areas of the changed product would be unnecessarily affected and standards used for compliance required to be updated. Similarly, the

converse is true – if a change that is classified “major” but does not affect information security (security classification “minor” e.g. no external interfaces or data handling affected), the overall major classification would require establishment of new compliance material using AMC 20-42 which would not materially benefit the safety and security of the product. By treating security as an independent “area” under 21.A.101(b)(2), a correct measured response is established where update to compliance finding is done when appropriate. In the classification of information security changes, the scope of the product (i.e. which items, functions, SW modules, etc.) that have a security relevance under the change is established and updates to compliance finding are then performed only for these affected portions.

response

Comment 1: **Noted.** The text has been modified.

Comment 2: **Partially accepted.** The text has been modified.

Comment 3: **Partially accepted**

Comment 4: **Noted.** It will be taken into consideration in the future.

Comment 5: **Noted.** It should be addressed in a future update of Part 21.

comment

221 comment by: *General Aviation Manufacturers Asso ciation / Hennig*

Editorial: The abbreviation "UDP" is not defined. Recommend spelling out UDP in first use.

response

Accepted

comment

222 comment by: *General Aviation Manufacturers Association / Hennig*

The proposed text in Appendix A "Examples of Major Changes per discipline" to GM 21.A.91 includes an amendment for systems.

GAMA notes that the section concludes with:

5. Propellers

[...]

There is, however, no specific guidance about propellers, but the agency does propose an amendment to AMC P 230 Propeller Control System.

GAMA requests clarification whether or not the agency intended to provide guidance about Major Changes for propellers in this section.

response

Noted
There is no modification as regards propellers. It is only to indicate the proper location for the new text between ‘4. Systems’ and ‘5. Propellers’.

comment

223 comment by: *General Aviation Manufacturers Association / Hennig*

EASA proposes an "exception" to classifying modifications as major if a "simplex digital communications means (e.g. ARINC 429) is established from a control domain

to a more open domain, unless it can be shown that the simplex control can be reversed."

GAMA appreciates EASA identifying a design change that can be exempted, but the proposed text may cause confusion.

GAMA recommends that EASA clarify the proposed exemption. The agency may want to consider language from FAA PS-AIR-21.16-02 Rev. 2, Establishment of Special Conditions for Aircraft Systems Information Security Protection, published 22 February 2017 which states:

"...data transfer services without capability of transmitting to aircraft systems, e.g., read only data services connected via receive only ARINC 429 bus, do not require issuance of special conditions."

GAMA's proposed change to the exempted design change language is:

"Exception: A new digital communications mechanism that uses a unidirectional communications means (e.g., ARINC 429) to establish a connection between the controlled domain to a more open domain should not be classified as major, if it can be shown that the communication direction cannot be reversed."

response

Partially accepted
This section has been amended with the same intent, due to other comments. The new text proposed considers this comment from GAMA.

comment

232 comment by: *Bombardier*

Issue: minor text discrepancies

Comment: Draft text for GM 21.A.91 "Classification of changes to type certificate"

- UDP not defined
- Section 5. Propellers has no text

Recommend: Change text:

- define UDP as User Datagram Protocol
- Complete section 5 or delete.

response

Point 1: **Accepted**
Point 2: **Noted**
There are no changes to section '5. Propellers'.

comment

267 comment by: *Aerospace and Defence (ASD)*

Commented text
The text " 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."

Proposed modification
"A change that may introduce the potential for unauthorised electronic access to product systems may be considered to be major if there is a need to mitigate the risks for an identified unsafe condition (CAT / HAZ)."

Justification
Reference to CS 2x.1319 and CS-E 50(i), CS-P 230(g) should be removed because classification of a change should not depend on the applicable certification basis but rather on the nature of the change itself.
The Security environment impact as a trigger condition should be removed because it is already addressed by the identification of the unauthorised electronic accesses. Moreover, the possible further updates of the security environment are considered as out of the scope of the initial airworthiness and already addressed by the Continuing Airworthiness.
The meaning of "initial analysis" and "before the implementation of mitigation means" should be clarified.

response

Point 1: **Partially accepted**
Point 2: **Noted**
This part of the proposal has been changed, based on other comments, from 'security environment' to 'security perimeter'.

comment

268 comment by: *Aerospace and Defence (ASD)*

Commented text
"[…] a change may be considered to be major if the security environment is impacted […]"

Proposed modification
Amend 21.A.91 to add further guidance on how to interpret the "may" statement on when changes to the security architecture will be classified as major or when it can be reverted to minor. Insert after quoted sentence (assumes other comment on changing security environment to architecture has been accepted):

The changes to security architecture are only major if they have the potential for weakening existing security measures or introduce new threat conditions or attack vectors. When changes to the security architecture occur, the applicant should perform and record a risk assessment demonstrating that no undue risks are being introduced into the design. The applicant should use approved procedures for assessing security risks due to design changes and classify changes through procedures approved by compliance to 21.A.239 (Design assurance system) or 21.A.611 (Design Changes).

Add another example that a change can introduce a new interface but is not actually major because existing security measures can protect against it.

EASA to provide examples, stating whether major or minor.

Justification
This NPA proposes to use “may” in a classification criteria rather than the usual practice of “should” for criteria in this section. This general approach is appreciated as it is not rigidly forcing all changes to be classified major, e.g. any time a new interface is introduced. However, this section needs to be clarified on the process and procedure of how the “may” is to be determined. It is recommended to include a security risk assessment process as part of the change classification process and approved as part of a company’s approved manuals.

response **Noted**
This part has been changed, based on previous comments, from ‘may’ to ‘should’.

comment *269* comment by: *Aerospace and Defence (ASD)*

Commented text
N/A

Proposed modification
Propose to have a dedicated rulemaking task for addressing continuing airworthiness aspects across all users, design approval holders.

Justification
AMC 20-42 lists ED204 which provides guidance for continuing airworthiness. Part 21 includes regulations for continuing airworthiness that should drive the activities described in ED204**.** In current state, only initial airworthiness aspects to design are clear through updates to CS-23, -25, -27, -29, -E, -P and -ETSO. Organisations that need to perform continuing airworthiness activities - in particular MRO and Operators - will not be aware of AMC 20-42 and activities set forward in ED204 without correct references in relevant sections to their operations - mainly Part 21

response **Noted**

comment *270* comment by: *Aerospace and Defence (ASD)*

Commented text
"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 [...]"

Proposed Modification

Update GM 21.A.101 to clarify that security is an "area" under Step 6 of the workflow (i.e. compliance to 21.A.101(b)(2)) and thus changes to security – and consequently updates to the use of standards for establishing security compliance and compliance to other areas – should be considered independently.

Justification
There is concern that the addition of security into the classification of "minor/major" changes could have unintended, far-reaching and costly consequences. There is the concern that when security drives a classification of "major" – when it otherwise would be minor – that large areas of the changed product would be unnecessarily affected and standards used for compliance required to be updated. Similarly, the converse is true – if a change that is classified "major" but does not affect information security (security classification "minor" e.g. no external interfaces or data handling affected), the overall major classification would require establishment of new compliance material using AMC 20-42 which would not materially benefit the safety and security of the product. By treating security as an independent "area" under 21.A.101(b)(2), a correct measured response is established where update to compliance finding is done when appropriate. In the classification of information security changes, the scope of the product (i.e. which items, functions, SW modules, etc.) that have a security relevance under the change is established and updates to compliance finding are then performed only for these affected portions.

response **Noted**

comment *271* comment by: *Aerospace and Defence (ASD)*

Commented text
"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."

Proposed modification
Reword to state: "Exception: a nominally unidirectional directional communication means (e.g. ARINC 429) is established from a controlled domain to a more open domain and demonstration is provided that communication flow cannot be returned from the open domain by reversing the communication direction (e.g. through compromise of digital controller chips).

Justification
Use of simplex needs to be defined as it may be ambiguous to different users. Intention here should be that a unidirectional communication from controlled to uncontrolled domain is acceptable and can be added without need for classification as a major change. Any additional communication means that adds a path from uncontrolled to controlled domain - either intentionally or unintentionally - is a major change. The intentional path may be obvious to most in the industry (e.g. A664, ethernet, etc.) but unintentional consequences such as having a nominally unidirectional databus such as A429 compromised to change the direction of communication needs to be explained so it is considered by all. Simplex is not defined in A429 or other standards.

response **Noted**

4. Impact assessment (IA) | 4.1. What is the issue | 4.1.1. Safety risk assessment p. 16

comment *68* comment by: *Certification Expert*

In §4.1.1, the safety risk assessment "do not include physical attacks", do we have to understand that a volunteer connection to a system by a unauthorized person is excluded or is it only related to physical damages in the goal to destroy the system/components ?
If well understood, it is proposed to clarify the objective as follows: "do not include physical unauthorized connection to the electronic aircraft system interfaces as well as physical damages of electronic aircraft systems"

response **Partially accepted**
The text has been modified to provide for clarity.

comment *161* comment by: *UK CAA*

Page No: 16

Paragraph No: 4.1.1

Comment: We do not believe it is possible to protect against unknown/undefined threats other than by isolating the systems.

Justification: The protection of flight critical systems must be guaranteed, and this can only be achieved by isolating those systems.

Proposed Text: The text should be modified to state that all flight critical systems must be isolated.

response **Not accepted**

Isolation has first to be defined, and an air gap does not isolate a critical system from the ground. It still can be compromised by software update along the supply chain or the maintenance process.

It is also about risk acceptability. Depending on the severity of the impact and the likelihood of a successful attack, the risk has to be assessed. If the risk is not acceptable, mitigation means have to be provided and this may lead to the decision to increase the difficulty of attack by regrouping critical functions in a dedicated logical domain like it is done today in the Aircraft Control Domain and to limit down link, one-way connection to less controlled domain. Acceptable means of 'isolation' are one-way Arinc 429, logical diodes, etc.

4. Impact assessment (IA) | 4.1. What is the issue | 4.1.2. Who is affected p. 16

comment *19* comment by: *Universal Alloy Corporation Design*

This DOA is concerned that the NPA does not fully comprehend the implementation difficulties that would be faced by DOAs. The need for training is mentioned, almost as an afterthought. The equipment software developers do understand the potential threats in depth but the same cannot be said of the typical DOA personnel.

Looking back in time over similar step changes in the way in which assessments and certification are performed:

a. Electrical Wiring Interconnect Systems (EWIS). Following a succession of accidents, the EWIS measures were introduced under a range of AMCs but the operational tasks were supported by mandated training, by flowcharts, checklists and by copious documentation explaining the problems and rationales for improvement.

b. Software and Airborne Electrical Hardware (SW and AEH). SW and AEH was introduced by CMs and by reference to International Standards. To date the only training we have managed to find is an EASA training Course but the required input standard is "experts". We have acquired an internal EASA Work Instruction (WI) that has been very helpful. Nevertheless, unless we are missing an important set of documents, there appears no standardised training approach to this extremely challenging subject.

c. Cybersecurity. Cybersecurity is now being proposed without a clear training strategy. Open questions are: who will be eligible to conduct the assessment? What training will they need? How will the various product systems be assessed and, most importantly, how will the gap between the NPA referenced International Standards and the aircraft installation be bridged?

At present it appears that, although the topics are getting more and more complex, the prescribed level of support available for the DOAs is getting less and less. This DOA believes that it is essential that an agreed training strategy and implementation plan for cybersecurity be authorised before the regulation changes proposed in the NPA are enacted.

response **Noted**
While NPA 2019-01 focuses on certain products, NPA 2019-07 'Management of information security risks' (RMT.0720)[10] proposes provisions that are applicable to competent authorities and organisations in all aviation domains.

4. Impact assessment (IA) | 4.2. What we want to achieve — objective p. 16

comment *46* comment by: *Europe Air Sports*

EAS Comment to 4.4.2.5 General aviation and proportionality issues

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

[10] https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-07

Comment:
The provision refers to the FAA document "Report from the Aviation Rulemaking Advisory Committee (ARAC) Aircraft System Information Security / Protection (ASISP) working group to the Federal Aviation Administration." used by EASA in this NPA.

This document has a section "2.4 Rulemaking Recommendations: Small Airplanes".

EAS generally approves of the contents of Section 2.4.

However, we caution that the risk handling procedures introduced by the NPA may in certain cases add significant burden for the manufacturer. Therefore the proportionality of the requirements need to be carefully considered.

We note that this 2016 report points to a separate "set of best practices" in Appendix G comprising 47 pages. However, it appears the Appendix G is to a large extent on a fairly high level and offers a limited amount of really "hands-on" guidance. This makes it somewhat difficult to assess if the requirement level is reasonable. We appreciate more clarity on this topic.

response **Noted**
The aim of EASA is to propose proportionate rules.
This comment will be considered in the preparation of the final deliverables.

4. Impact assessment (IA) | 4.4. What are the impacts | 4.4.2. Options 1 & 2 p. 17-18

comment *80* comment by: *General Aviation Manufacturers Association / Hennig*

GAMA appreciates the EASA statement that manufacturers are expected to adhere to state of the art and current best practices as they relate to cybersecurity as discussed in section 4.

GAMA however disagrees with the statement in 2.4 that "No adverse economic impacts are expected." This statement seems to imply that there will not be any costs from cybersecurity certification or design considerations. There will be costs on stakeholders to comply with the cybersecurity standards.

GAMA expects some of the following costs to be incurred:

- OEMs: Employ staff, expand expertise, conduct additional safety and risk analyses, and possible redesigns.
- CAMO: Train staff to understand security requirements and establish processes for controlling certain information and computer systems as identified by the OEM in Instructions for Continued Airworthiness (ICA) and related operating procedures.
- Operators: Train staff about cybersecurity and how to comply with the ICAs and operating procedures.

GAMA recommends that the agency acknowledge these costs as part of finalizing this regulatory proposal and amendment to the Certification Specifications. The final regulation should consider a thorough analysis of the costs as related to each

	modified CS and AMC to ensure the proposed rules provide adequate benefit irrespective of the current use of CRIs and CAIs. Additionally, the impact assessment seems to be focused on CS-25 aeroplanes which have been subject to Special Conditions. It is essential that the agency recognizes that CRIs and CAIs have typically not been applied to certain types of aircraft (e.g., CS-23. -27, or -29). The agency proposes a proportional approach to cybersecurity for these aircraft which is welcomed. The agency, however, can help justify the proportional approach to cybersecurity by conducting a complete cost--benefit analysis for all aircraft types.
response	**Noted** The aim of EASA is to propose proportionate rules. This comment will be considered in the preparation of the final deliverables.

comment	*103* comment by: *ENAC* ref 4.4.2.3 Social impact The statement "Not applicable" appears to simple. New basic regulation EU 2018/1139 (recital 68 and art. 115) requires a great attention to social aspects
response	**Noted** This comment will be considered in the Explanatory Note of the final deliverable (i.e. ED Decision).

comment	*162* comment by: *UK CAA* **Page No:** 18 **Paragraph No:** 4.4.2.5 **Comment:** This statement does not appear to have any supporting justification. **Justification:** Any relaxation/alleviation for any particular aviation sector should be properly justified. **Proposed Text:** The conclusions of the ARAC ASISP Working Group should be included in the NPA (e.g. in an appendix), and the full documentation should be referenced.
response	**Not accepted** Link to the ARAC report is included in the NPA.

4. Impact assessment (IA) | 4.5. Conclusion | 4.5.1. Comparison of options p. 18

comment	*8* comment by: *European Powered Flying Union* 4.5.1. Comparison if options page 18/20

For our community "Option 2" is the optimum as well.

Rationale:

To present all relevant provisions in one single AMC-20 is user-friendly, updating is simpler, we think manufacturer will easily find what is important, thus time and money is saved.

response **Noted**

comment *47* comment by: *Europe Air Sports*

EAS Comment:
We agree with the choice of Option 2.

response **Noted**

4. Impact assessment (IA) | 4.6. Monitoring and evaluation p. 18

comment *163* comment by: *UK CAA*

Page No: 18

Paragraph No: 4.6

Comment: It is not clear how the effectiveness of cybersecurity protection can be monitored/ evaluated. We believe that it would not be known whether an attack has been attempted unless it is successful.

Justification: It is important to know whether the measures deployed to protect against cybersecurity threats are effective. The lack of successful attacks is insufficient - this may only indicate a lack of attempts. Pro-active assessment of vulnerability and effectiveness of the cyber security protection required should form part of the evaluation. Due to the nature of cybersecurity and changes in both threat and vulnerability this should happen at regular intervals to understand how change and increased/decreased risk profiles have been assimilated.

Proposed Text: If available/possible, means of logging the number of cybersecurity attacks should be required. Monitoring and evaluation should also include the results of pro-active testing to determine the effectiveness of cybersecurity protection.

response **Noted**

EASA will monitor and evaluate the effectiveness of the proposed amendments to the CSs once they enter into force. Due to the evolving nature of cybersecurity threats and vulnerabilities, monitoring indicators could not be specified exhaustively. However, access to the number of security attacks would be required, as well as review of the results of regular proactive testing of the effectiveness of the cybersecurity protections. It should be noted that EASA could access through ECCAIRS cybersecurity occurrences related to design and production issues and report on them.

3. Appendix A — Attachments

Pentesting_LH_Group_Position_v1.02.pdf

Attachment #1 to comment #206