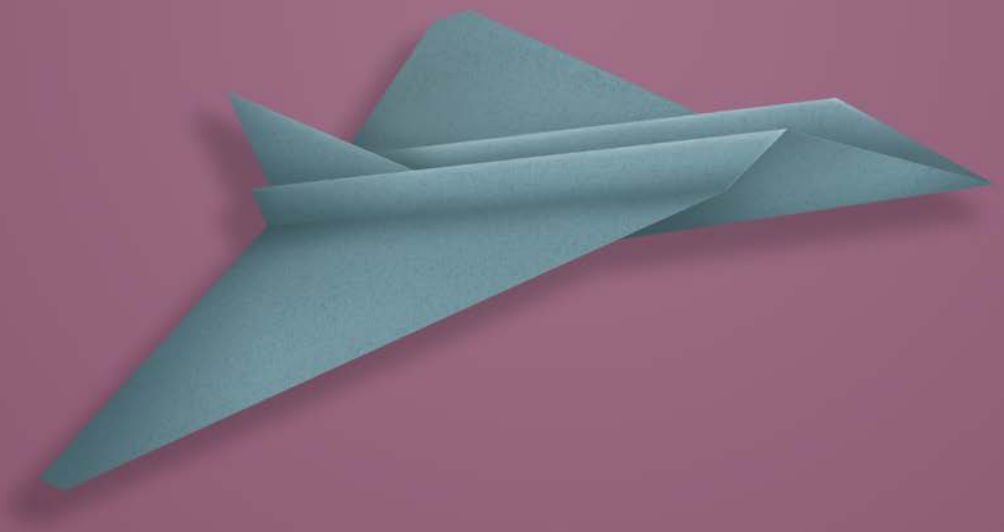
EASA
European Union Aviation Safety Agency

Information Bulletin no. 2019/01

“J-NEWS”



Dear Madam, dear Sir,

Following the success of the ***J-News*** bulletin in 2018, I am pleased to pursue this sharing of information with the Industry, with the first edition of 2019. We are also delighted to address two topics raised by you, the DO community, namely the Cybersecurity and the Good practices on ISM.

This edition tackles six different technical topics, two of them being peculiarly developed.

On the forthcoming pages, you will find useful information on the following topics:

Item 1. Test article conformity determination

Item 2. Combination of DOA and AP-DOA for ETSO holders also holding a DOA

Item 3. Cybersecurity

Item 4. Good Practices on ISM – Implementation of an effective ISM – Part 2

Item 5. ED-248 / SAE ARP-60493 "Guide to Civil Aircraft Electromagnetic Compatibility"

Item 6. Approval of non-conformities/production concessions

I would like to thank particularly Linda BRUSSAARD, Claudio CARUSO, Mariano LANDI, Bülent PEHLIVAN, Cyrille ROSAY, Olivier TRIBOUT and Raphaël AUBERT who proposed and contributed to the articles in this edition, especially as this is an additional task to their normal work.

All *Aircraft & Products* newsletters including the ***J-News*** bulletins are available on our web site.

Yours faithfully,
Markus GÖRNEMANN
Head of the Design Organisations Department
Deputy Certification Director

Note: As usual, should you need more information on any of the topics presented, please get in contact with the DOA Team Leader allocated to your DO.

Part 21 implementation

Item 2019/1/1
Test article conformity determination

Applicants for new Type Certificates[1] (under DOA, ADOA or Certification Programme process) need to produce parts, sub-assemblies and more generally test specimens for the purpose of the demonstration of compliance with the applicable certification basis.

As per 21.A.33(b)(1), the Applicant has to determine the test specimen conformity with applicable design data, in terms of dimensions, materials, manufacturing processes, etc..

The most practical mean to discharge the above obligation is to rely upon a Manufacturer producing under Part 21 Subpart F or G.

In these cases, the Applicant, after having established the required link between design and production (i.a.w. 21.A.122 (b) or 21.A.133 (c), as applicable), can rely upon the EASA Form 1 as a Certificate of Conformity issued by the Manufacturer.

In addition to the above options, Part 21 does not exclude to have the test specimen production and conformity verification processes fully covered by the Applicant itself.

In this case, for verifying the conformity of test specimen, it is expected that the Applicant defines an adequate production inspection system based on the principles of Part 21 Subpart F (i.e. 21.A.126), covering incoming material identification, processes, manufacturing techniques, methods of assembly and inspections.

Subpart F and associated AMC/GM can be used to prepare this set of procedures to be included or referenced to in the DOA Handbook, ADOA Manual or Certification Programme (ELA 1 process). Procedures need to be agreed by Agency before test specimen is produced.

1 The need to produce test specimens may also appear in the course of other projects (e.g. STCs, minor changes, major repairs, etc.).

General DOA information

Item 2019/1/2
Combination of DOA and AP-DOA for ETSO holders also holding a DOA

Background:

EASA drafted in 2017 a proposal to allow applicant for and holder of ETSOA other than APU to demonstrate their capability by holding a DOA (in lieu of APDOA). This policy does not change the current practices for DOA covering APU. At the end of 2017, the Senior management of EASA gave its green light to move forward with the proposal and subsequently different pilot cases have been used in 2018 to fine-tune the policy.

The targeted audience was first the companies holding dual approvals (APDOA and DOA) due to their business models. This new policy allows these companies to "merge" their approvals into one, in order to follow only one set of handbook/procedures, hence simplifying the administrative management of their Design Assurance System.

It is important to note that at this stage, demonstrating its capability as ETSO applicant/holder by holding a DOA is optional.

In addition, if an applicant elects to demonstrate compliance to 21.A.602B(2)(b) through a DOA, then the entire Subpart J becomes applicable and this does not impact the privileges and rights granted through 21.A.263 (at aircraft level) or 21.A.611 (at ETSO level).

Activities to be performed for companies holding dual approvals (APDOA and DOA):

- The DOA and ETSO handbooks can be merged or the ETSO procedures can be cross-referred from the DOA handbook
- As the ADOA will be surrendered, no reference to the APDOA approval should be kept in the handbook and procedures
- The marking procedure should cover both aircraft and ETSO cases (could be achieved by keeping two different procedures)
- The configuration management procedure should cover both aircraft and ETSO (could be achieved by keeping two different procedures)
- The classification procedure would need to cover both aircraft and ETSO cases (could be achieved by keeping two different procedures).
- As per 21.A.239(b) the CVE function is required for ETSO activities. For each ETSO standard, at least one CVE needs to be appointed. The letters of authorization of the ETSO CVE needs to clearly reference the ETSO standard (and the aircraft scope in case a CVE covers both ETSO and aircraft projects).
- As per 21.A.239(a) the ISM function needs to cover the ETSO activities
- As per 21.A.239(c) the subcontractor monitoring should include the subcontractors involved in ETSO activities

- The occurrence procedure should cover both products including STC and Major Repair thereto and ETSO.
- Obligations should cover both products including STC and Major Repair thereto and ETSO.
- The DOA holder needs to train the staff working on ETSO projects on the new handbook, especially the need for CVE signature, the ISM surveillance and the supplier monitoring.

Planning:

This new policy is proposed to be implemented in steps:

- Step 1 – 2018 companies holding dual approval can surrender their APDOA and cover their ETSOAs under their DOA;
- Step 2 – 2019: existing APDOA holders for ETSO can migrate to DOA; existing DOA holders can extend their scope to ETSO.
- Step 3 – 2020: new ETSO applicants can choose to hold an ADOA or a DOA.

Next steps:

Please contact your DOATL should you have any question.

If you currently hold a DOA, you are then advised to apply through a Form-82 to extend the scope of your DOA to include ETSO.

EASA regulatory update

Item 2019/1/3
Cybersecurity

Part 1: the Special Condition

Since the introduction of so called "e-enabled" aircrafts in the early 2000, EASA together with other Civil Aviation Authorities identified the possibility that connected systems may be compromised by unethical persons or organisations with potential effect on safety. The certification specifications do not provide guidance or requirement on how to protect aircraft systems against these new threats, therefore EASA issued a Special Condition. The purpose of this special condition was to close this gap by asking the applicant to perform a specific risk analysis by looking at how information security threat could impact safety. To draw a parallel between the traditional safety assessment process and the cybersecurity where one talks about Failure Conditions, we have there Threat Conditions. This "Thread Condition" is defined as follows: "a condition of the aircraft with an adverse effect on safety which can result from an information security threat. A condition that involves assets, people, or processes having an effect on either the airplane or its occupants, or both, either direct or consequential, in possible conjunction with operating conditions, failure conditions, and environmental conditions." (cf. Eurocae report ED-013).

In short, the Special Condition requires to protect the systems from intentional unauthorised electronic interactions, and to provide procedures and guidance on how to maintain the effectiveness of the protection during operation.

This Special Condition is applicable on **all new aircraft types and on legacy aircraft every time a modification introduces new exposure to cyber threat**. For example, if the modification establishes a direct connectivity between a system in the avionics bay and a more open network, like the Internet, then this Special Condition should be applied, to ensure that the impact of a successful attack on the system is commensurate with the level of threat of this attack. The level of threat is a qualitative evaluation of the possibility that a Threat Condition might occur. The security risk is then a function of the severity of the final event and the level of threat of that event. Similarly to safety where we compare severity of a failure with the probability of this failure to occurs, the information security risk assessment will compare the severity of the impact of a successful attack with the likelihood of this attack to be performed and to be successful. If the risk is not acceptable, means must be provided to mitigate the risk to an acceptable level.

More details on how to address the threats of intentional unauthorised electronic interaction can be found in the industry standard EUROCAE ED-202A/RTCA DO-326A. In June 2018 ED-203A/RTCA DO-356A "Airworthiness Security Methods and Considerations" was published with the objective to provide, in particular, different methods to evaluate the Level of Threat and the security risk. Finally, EUROCAE ED-204/RTCA DO-355 was also developed to provide the necessary guidance material to ensure continuing airworthiness of the aircraft.

Part 2: a comprehensive strategy

However, the security scope does not limit itself to the inside of the aircraft's skin. Aviation is a System of Systems covering all aviation domains where products, services and organisations are increasingly interconnected. Contrary to what we can observe in safety, cybersecurity risks are evolving quickly. A mitigation that was found acceptable to counter a type of threat may not be efficient after some time because of the technological progresses made on the attackers side, or because new hacking tools are made more affordable, easier to use or because new vulnerabilities are discovered in systems. This requires the industry (and authorities) to do the business differently.

To fulfil that objective a comprehensive strategy is being developed at European level, and, as much as possible, at international level.

At European level, a collaborative and executive structure have been established: the European Strategic Coordination Platform (ESCP). This platform includes an executive committee which works at the higher, political level and a technical advisory committee with different work streams to discuss and develop materials on different matters, like the governance, the strategy, regulations, risk sharing, etc.

It is composed of full members and observers.

Members are either European aviation industry associations covering aircraft manufacturers, airlines, air navigation service providers, airports, pilots, maintenance organisations, unions, European institutions, with 4 DGs from the Commission (MOVE, CNECT, GROW and HOME), the European External Action Service, EUROCONTROL, agencies like EASA, EUROPOL, ENISA, EDA, etc.), SESAR-JU and SESAR-DM, and 6 member states plus the ECAC.

On top of this list of members, Observers are ICAO, FAA, TCCA, AIA, NATO.

It is within this structure that the European Cybersecurity Strategy is being developed, regulatory material are being discussed and developed, and that the coherence and consistency of risk management processes is address through all domains and organisations.

The strategy being developed has at the moment the following objectives: Making Aviation an evolutionary cyber-resilient system, which, under attack, can maintain its functionalities and making Aviation self-strengthening by adopting a "built-in security" approach. A significant number of actions have been already identified and organised into 5 enablers: Coordination, Capacity Building, Technical, Regulatory and Standards and methods.

Part 3: the regulatory developments

Having a look at the current European Plan for Aviation Safety, one may notice two rulemaking tasks dedicated to cybersecurity in aviation. The first one, the RMT.0648 is aiming at introducing cybersecurity in the products and parts covered by Part 21. It is under public consultation until May 22, 2019.

The second one, RMT.0720, has the objective to create a regulatory system that efficiently contributes to the protection of the aviation system from cyber-attacks by introducing provisions for the management of cybersecurity risks by organisations in all the aviation domains (design, production, continuing airworthiness management, maintenance, operations, aircrew, ATM/ANS, aerodromes). These provisions would include high-level, performance-based requirements, and would be supported by AMC & GM material and industry standards. The aim is to propose requirements to be met by an organisation to identify, be protected from, detect, respond to and recover from those information security events that could potentially affect aviation safety or could affect the European Aviation Traffic Management Network (composed of the systems listed in Annex I to Regulation (EC) No 552/2004).

The organisations that would be subject to this regulation are foreseen to be POA & DOA required to comply with part 21 Subpart G & J, part-CAMO organisations, part-145 organisations, some air operators subject to (EU) 965-2012 conducting commercial air transport or commercial special operations, some training organisations (ATO and ATCO), ATS, MET, AIS, DAT, CNS, ATFM, ASM Providers and the Network Manager required to comply with (EU) 2017/373.

Part 4: collaboration and information sharing

One other objective, also present in the EPAS 2018-2022, is to promote networking and information sharing among organisations and authorities, promoting the establishment of a cybersecurity culture and trust environment. This should help in understanding the risks and threats landscape and overall situational awareness. To achieve this objective, ECCSA, the European Centre for Cybersecurity in Aviation is ramping up, building a community where any organisation can obtain information, participate in discussions, publish events etc. allowing a widespread safety promotion and knowledge building approach. In its current status, the last moments of the pilot phase, it is composed with a limited number of airlines, airports, manufacturers, MROs, ANSPs, ACSPs and national authorities with the technical support of CERT-EU.

Training and research

With the objective to contribute to enhance the situational awareness on cybersecurity EASA is funding regularly some studies and research projects and provides training on cybersecurity. 2 studies were completed (cryptographic recommendations for algorithms used in aviation, Impact on Aviation of Cybersecurity Threats). One, not started yet, being in the EPAS 2018-2022, will have the objective to study the feasibility of a database of vulnerabilities targeting transport information systems.

Trainings are being developed to increase cybersecurity awareness for EASA, National Authorities, but also the industry. Several modules will cover different levels and fields of expertise from cybersecurity basic education to expertise on systems risk assessment.

Good practice

Item 2019/1/4
Good Practices on ISM – Implementation of an effective ISM– Part 2

Other 'monitoring' means than audit

The main and most popular monitoring means are audits. However there are other activities that could be performed to effectively monitor the Design Assurance System.

In this article an idea on how to conduct this kind of monitoring is provided aiming to give suggestions on how to make use of an existing process management respectively quality management system by adapting it to ISM needs.

Please consider that for some small DOAs, with low number of headcounts, the following proposal may not be appropriate.

First the Part 21 CCL can be split into the applicable DOA core processes as outlined in J-News Information Bulletin 2018/03.

The following steps could be applied afterwards:

Step 1:
Each of the DOA core processes should be mapped in order to identify the deliverables.
Hereafter as process mapping the SIPOC technique is shown as an example.
SIPOC is a Six-Sigma tool which is often used for process modelling, and therefore may be also useful for proper visualization of

- DOA core process = Process
- associated activities = (Sub-)Process
- deliverables = Output (document)
- persons/functions required to receive the deliverable = (Internal)Customer

Example of a SIPOC:
Process: '*Changes*'
Process Owner: *Mrs Example; Head of Airworthiness Office*

(internal) **Supplier**	**Input** (document)	(Sub-) **Process**	**Output** (document)	(internal) **Customer**
Design Engineer	Change Request form xxx	Change classification Process operator: Design Engineer II	Change classification form yyy	Airworthiness Office and Design Engineer I
Design Engineer	Compliance document zzz prepared	Independent Checking Process operator: CVE	Compliance document zzz verified, Compliance summary	Airworthiness Office
...	...	...	...	...

Explanatory Note regarding the SIPOC table by using the first example:

The process operator "Design Engineer II" receives the Input (document) "Change request form xxx" from the (internal) supplier "Design Engineer I" in order to conduct the (Sub-)process "change classification". As a result the process operator fills out the output (document) "Change classification form yyy" and delivers it to the (internal) customers "Airworthiness Office and Design Engineer I".

The (Sub-)Process in the above mentioned table could be illustrated more detailed and dedicated to each Output (document).
The activities in the (Sub-)Process have to be assigned to the dedicated function performing the (Sub-) Process, the so called process operator. The process operator should be clearly identified for each (Sub-)Process by the function it holds in the Design Organisation.
The deliverables (i.e. Output(document)) supplied by the process operator are in the further focus for the following step.

Step 2:

The Process Owner is responsible for proper functioning of the DOA core process and its (Sub-)Processes. Therefore the Process Owner agrees with the HoISM in concurrence with the (internal) Customer on a checklist.
The checklist includes all acceptance criteria respectively parameters related to the Output (document) of associated (Sub-)Process.

Example of a checklist:
Process: '*Changes*'
Process Owner: *Mrs Example; Head of Airworthiness Office*
(Sub-) Process: *Change Classification*
Project: *ABC*

Output (document)	Acceptance Criteria	Actual	Conclusion	
Change classification form yyy Issue zzz	Affected aircraft type is identified in box i	Aircraft Type identified as xyz	☒ Accepted	☐ Not Accepted
	Configuration before the change (i.e. pre-change configuration) is described in box ii	box ii was left blank	☐ Accepted	☒ Not Accepted
	Configuration after the change is described in box iii	box iii was insufficiently described thus configuration after the change is interpretable	☐ Accepted	☒ Not Accepted
	...	...	☐ Accepted	☐ Not Accepted

The checklist should be used by the ISM function for the sample check of accomplished projects, and (if applicable) the ISM function should investigate and consider the results of previous checks on the same (Sub-)process (e.g. KPIs on rejection rate). Feedback about the result of these sample checks (and if applicable of the investigations) needs to be communicated to the Process Owner and to the Head of ISM. The sample checks (and if applicable the investigations) could be even performed by an Engineer, however it has to be ensured that this individual had no direct involvement in related project(s) in order to ensure impartiality.

Conclusions resulting into "Not Accepted" will have to be treated further as explained in next step. If applicable, the results of previous checks on the same (Sub-)process should be considered in the next step as well in case that it can be associated to the applicable Part 21 requirement(s).

Step 3:

The Head of ISM will consider these outputs and record the results for any follow-up actions. These follow-up actions include, but are not limited to, the tracing of the root cause analysis, preventive/corrective measures, the update of the checklist as part of the preventive/corrective action and reporting of the results to the Head of Design Organisation.

Example of checklist conclusion:

Findings summary for project ABC regarding the DOA core process "Changes"				
Finding N°	**Part 21 Requirement(s)**	**Finding Description**	**Finding Level**	**Corrective action owner and due date**
n	21.A.91 GM 21.A.101 3.2.1	Change classification form yyy Issue zzz does not identify the configuration before the change for project ABC.	3	Mrs. Example dd.mm.yyyy
n+1	21.A.91 GM 21.A.101 3.2.2	Change classification form yyy Issue zzz does not sufficiently describe the configuration after the change for project ABC.	2	Mrs. Example dd.mm.yyyy
n+2	…	…	…	…

Additional Notes:

- Close collaboration with the Head of Airworthiness is key for an efficient monitoring and proper findings classification (ref. to GM No 1 to 21.A.245 N° 4.6).
- The described "checklist" will be able to cover the compliance with the documented procedures. However the "checklist" may not be considered as an equivalent replacement for determining adequacy of documented procedures with Part 21 (refer also to Type 1 Questions from previous J-News article on ISM). Another smart way to assess the adequacy of documented procedures with Part 21 would be the involvement of the ISM function into the review of each revision of the DOH, cross-referenced procedure and form in order to assess the adherence to applicable Part 21 requirements. As a result existing checklists might have to be updated as well to capture newly introduced changes.
- As a pre-condition the system of above mentioned monitoring activity has to be described in the ISM related process of the DOA, and it needs to be agreed with the responsible DOATL.

Good practice

Item 2019/1/6
ED-248 / SAE ARP-60493 "Guide to Civil Aircraft Electromagnetic Compatibility"

Last year, Eurocae published a new document containing information, guidance, and methods for demonstrating electromagnetic (EMC) compatibility on civil aircraft. It addresses the compliance for safety and the functional performance of installed electrical and electronic systems. The purpose is to provide technical guidance that can be used to demonstrate that aircraft electrical and electronic systems are electromagnetically compatible with other aircraft systems, that is, inter-system EMC. The guidance can be applied both to new aircraft and modifications to existing aircraft (including small aircraft and rotorcraft).

Prior to the publication of this document, there were no standard methods defined for demonstrating electromagnetic compatibility on civil aircraft, resulting in a wide range of compliance techniques. This document standardizes the EMC demonstration approaches and methods to ensure common application of regulations, consistent evaluation of the results, and confidence in the overall safety of the aircraft.

The document will help the applicant with the demonstration towards the different regulations addressing EMC in a standard way and therefore eases certification and validation activities with authorities. EASA therefore strongly advices to use this document.

This guide does not address aircraft compatibility with the internal electromagnetic environments of portable electronic devices (PED) or with the external electromagnetic environments, such as high-intensity radiated fields (HIRF), lightning, and precipitation static. Other documents are addressing these specific topics. EASA will work on a Certification Memorandum listing what documents are addressing which kind electromagnetic interferences to ease the correct choice for applicants.

Part 21 implementation

Item 2019/1/7
Approval of non-conformities/production concessions

Definitions:

Concession: production non-conformity, also called unintentional deviation to the approved type design happening during the manufacturing process

Design approval holder: holder of an EASA certificate for a design, such as TC, STC, Major change approval, ETSOA, etc.

Purpose and statement:

This article is meant as a reminder of the basic principle allowing a DOA holder or ETSO APDOA holder to approve concessions.

Although not directly visible in the Terms of Approval of each DOA holder or in the Finding of Compliance of each ETSO APDOA, the possibility to approve concessions is limited to parts for which the DOA or APDOA is the design approval holder.

Should a (AP)DOA holder be designer and manufacturer of parts integrated in a TC or a STC, it should request to the design approval holder (TC or STC holder) a delegation in order to approve concessions under the DOA of the design approval holder.

Examples:

- DOA A is the designer and manufacturer of the rear fuselage of a sailplane, where the sailplane TC is hold by DOA B.
  As the 'rear fuselage' does not hold an EASA certificate for design, DOA A is not allowed to approve concessions under its privileges.
  However DOA A can request to DOA B a delegation of DOA B privileges in order to approve concessions under the DOA B (the concessions would then show "approved under the authority of DOA B").
- APDOA C is the designer and manufacturer of an ETSO for which it holds the ETSOA. This ETSO is then installed in an STC held by DOA D.
  APDOA C can approve concessions to its appliance/part under 21.A.611, however APDOA C should liaise with DOA D for the impact of these concessions on the STC. DOA D may be required to raise as well a concession in order to approve the concession at STC level.

Rationale:

The rationale for this principle is based on the following elements:

- From an airworthiness point of view, if the designer/manufacturer of a part, appliance or assembly does not hold an EASA certificate for design (even it holds a design organization approval), it has not been given authority to perform concessions.
- It is the responsibility of the design approval holder (ETSOA, (S)TC holder, others) to control the configuration, including the airworthiness status, of the parts delivered under Form-1 or Form-52, hence concessions can only be performed under its DOA.

European Union Aviation Safety Agency
P.O. Box 10 12 53
D-50452 Cologne, Germany
http://www.easa.europa.eu
Image © Unsplash.com

An Agency of the European Union